INSTALLATION GUIDE

for use with

INTEGRATED CISCO® PRODUCTS

Websense Enterprise®
Websense® Web Security Suite™
-including Corporate Edition

v6.2
## Contents

### Chapter 1  Introduction .................................................................9
  - About this Guide .................................................................9
  - Websense Enterprise Components ............................................10
  - How Websense Works .............................................................12
  - Deployment Tasks ...............................................................14

### Chapter 2  Network Configuration ...............................................15
  - Websense Enterprise Components ............................................15
  - Websense Deployment ...........................................................22
    - Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA) . .23
    - Cisco Content Engine .......................................................25
    - Cisco IOS Routers ............................................................26
    - Switched Environments ......................................................27
    - NAT and Network Agent Deployment ....................................30
    - Directory Services ..........................................................30
  - System Requirements ...........................................................32
    - Supported Cisco Integration Product Versions .........................33
    - User Workstations ..........................................................33
    - External Resources ..........................................................33

### Chapter 3  Upgrading Websense Enterprise .................................35
  - Versions Supported .............................................................36
  - Transferring Configuration Data Without Upgrading ....................36
  - Before You Upgrade ............................................................37
  - Upgrading on Windows ........................................................39
  - Upgrading on Solaris or Linux ..............................................45
  - Upgrading the Remote Filtering Components ..............................50
    - Remote Filtering Server ....................................................51
    - Remote Filtering Client Pack ..............................................51
Contents

Usage Monitor .................................................. 152
RADIUS Agent ................................................. 154
eDirectory Agent ............................................... 156
Logon Agent ....................................................... 157
Remote Filtering Server ................................. 160

Modifying an Installation ................................. 164

Adding Components ......................................... 164
Windows ......................................................... 165
Solaris or Linux .............................................. 173

Removing Components ................................. 176
Windows ......................................................... 176
Solaris or Linux .............................................. 179

Repairing an Installation ................................. 180
Windows ......................................................... 180
Solaris or Linux .............................................. 183

Repairing the Policy Server ............................. 185

Migrating between Integrations After Installation ................................. 186

Stopping or Starting Websense Services ................. 187
Manually Stopping Services .............................. 188
Optional Components ...................................... 188
Principal Components ..................................... 188

Windows ......................................................... 188
Solaris and Linux ............................................. 190

Chapter 5 Initial Setup ........................................ 191

Subscription Key and Master Database Download ................. 192
Identifying the Filtering Service for the Block Page URL .............. 196
Displaying Protocol Block Messages ............................... 197

Creating and Running the Script for Logon Agent ................. 198
Prerequisites for Running the Logon Script ......................... 198
File Location ..................................................... 198
Deployment Tasks ............................................... 199
Preparing the Logon Script .................................. 199
Script Parameters ............................................. 199

Websense User Map and the Persistent Mode ......................... 201
Examples .......................................................... 201
## Contents

- Configuring the Logon Script to Run ........................................... 202
  - Active Directory ............................................................. 202
  - Windows NTLM ............................................................... 204
- Identifying the Proxy Server for the Network Agent .................. 205
- Configuring Network Agent to use Multiple NICs ....................... 207
- Testing Visibility of Internet Traffic to Network Agent ............ 208
  - Running the Websense Traffic Visibility Tool .................... 208
- Firewall Configuration for Remote Filtering .......................... 210
  - Enabling communication between Remote Filtering Server and Remote User Workstations .................... 211
  - Enabling communication between Remote Filtering Server and Filtering Service ............................................ 211

### Chapter 6

**Configuring Your Cisco Integration** ................................. 213

- Cisco PIX Firewall or Adaptive Security Appliance (ASA) .......... 213
  - Console or TELNET Session ............................................... 214
- Cisco Security Appliance Enhanced Caching .......................... 225
- Cisco Secure ACS Authentication ................................. 226
- Cisco Content Engine ....................................................... 227
  - Cisco Web-based Interface .................................................. 227
  - Console or TELNET Session ............................................... 228
- Settings within the Content Engine Environment ..................... 230
  - Configuring Firewalls or Routers ........................................ 230
  - Browser Access to the Internet ......................................... 230
  - Clusters ........................................................................... 231
- Cisco IOS Routers ............................................................... 231
  - Startup Configuration ....................................................... 231
- Configuration Commands ..................................................... 234
- Executable Commands ......................................................... 238

### Appendix A

**Configuring Windows NTLM for User Authentication** ............ 241

- Configuring the Browser for Promptless Authentication ............ 241
- Configuring the Content Engine ........................................... 243
- Configuration and Corresponding Parameters ....................... 244
- Managing the HTTP Proxy Authentication Cache .................... 245
  - Query Individual Users for More Information ................. 246
Contents

Guarantee Re-authentication Next Day ............................................... 246
NTLM User/Group Access Lists ...................................................... 247
Transaction Reporting ................................................................. 249

Appendix B

Stealth Mode .................................................................................... 251
Configuring for Stealth Mode ......................................................... 251
  Windows ....................................................................................... 252
  Solaris or Linux ............................................................................ 253
    Solaris ....................................................................................... 253
    Linux ......................................................................................... 253

Appendix C

Troubleshooting ................................................................................. 255
I made a mistake during installation ................................................. 256
I forgot my Websense Policy Server password ............................... 256
Where can I find download and error messages? ......................... 256
  Windows 2000 and 2003 ............................................................... 256
  Solaris and Linux ........................................................................ 256
The Master Database does not download ...................................... 257
  Subscription Key ........................................................................ 257
  Internet Access .......................................................................... 257
  Restriction Applications ............................................................ 258
Policy Server fails to install ............................................................. 258
I upgraded Websense, and configured users no longer appear under
Directory Objects in Websense Manager ........................................ 259
Network Agent fails to start with stealth mode NIC ..................... 259
  IP address removed from Linux configuration file .................. 259
  Stealth mode NIC selected for Websense communications
    in Solaris and Linux ............................................................... 260
Network Agent is not filtering or logging accurately ..................... 260
Windows 9x workstations are not being filtered as expected ........ 260
Some users are receiving the Websense Global policy ................. 260
  Domain Controller Visibility ...................................................... 261
  NetBIOS .................................................................................. 261
  User Profile Issues ................................................................. 262
Websense Enterprise splash screen is displayed, but installer
does not launch on Windows 2000 .............................................. 262
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Agent cannot communicate with Filtering Service after it has been reinstalled</td>
</tr>
<tr>
<td>I upgraded my Cisco PIX Firewall software to version 7.0, and web filtering stopped working</td>
</tr>
</tbody>
</table>

### Appendix D  
**Technical Support**  
- Websense Technical Services Support Center  
- Premium Support  
- Support Options  
  - Web Portal  
  - Email Questions  
  - Telephone Assistance  
- Customer Care  
- Improving Documentation  

**Index**  

8  
Installation Guide
CHAPTER 1

Introduction

Thank you for choosing Websense Enterprise®, the leading web filtering system that integrates with Cisco® Adaptive Security Appliance (ASA), Cisco PIX® Firewall, Cisco Content Engine, and Cisco Routers. Using Websense in conjunction with an integrated Cisco product 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.

About this Guide

All installation procedures in this guide apply equally to Websense Enterprise and Websense Enterprise – Corporate Edition. The same software is installed for these two products, but the Corporate Edition feature set is enabled only if you enter a Corporate Edition subscription key. For information about Corporate Edition features, refer to the Websense Enterprise Administrator’s Guide.

can download the Quick Start Guide from: http://www.websense.com/global/en/SupportAndKB/ProductDocumentation. If you are installing Web Security Suite integrated with Cisco Adaptive Security Appliance (ASA), Cisco PIX Firewall, Cisco Content Engine, or Cisco Routers, the installation and setup information provided in this installation guide is required to install the Web Security Suite (web filtering) components of your Websense Web Security Suite product. All references to “Websense Enterprise” may be read as “Websense Enterprise and Websense Web Security Suite”.

Websense Enterprise Components

The following is a list of Websense Enterprise components. For detailed information about each of these components, refer to the Websense Enterprise Administrator’s Guide:

- **Filtering Service**: interacts with an integrated Cisco product to provide web filtering.
- **Policy Server**: stores all Websense Enterprise configuration information and communicates this data to other Websense services.
- **Websense Manager**: administrative interface that allows you to configure and manage Websense functionality through the Policy Server. Websense Manager is used to define and customize internet access policies, add or remove clients, configure Policy Server, and much more.
- **User Service**: allows you to apply filtering policies based on users, groups, domains, and organizational units.
- **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, and IM Attachment Manager features, and to log the number of bytes transferred and duration of transfer. Network Agent is also used as the filtering component for a stand-alone (non-integrated) Websense system.
- **Usage Monitor**: tracks users’ internet activity and sends alerts when configured threshold values are crossed.
- **DC Agent**: an optional component that transparently identifies users who authenticate through a Windows® directory service. DC Agent enables Websense to filter internet requests according to particular policies assigned to users or groups.
Chapter 1: Introduction

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

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

- **Logon Agent**: an optional component that works with a Websense client application (LogonApp.exe) to transparently identify users as they log on to a Windows domain via client machines. Logon Agent can be used with a Windows NT-based directory service or with Active Directory, which is LDAP-based. Logon Agent receives its user information from the logon application, LogonApp.exe, which must be run by a logon script in your network.

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

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

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

**NOTE**

The Remote Filtering Client is also available as part of the Client Agent in the Websense Client Policy Manager™ (CPM). For more information, refer to your Websense Client Policy Manager documentation.
Chapter 1: Introduction

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

- **Websense Enterprise Reporter**: 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 Enterprise Reporter documentation for installation and configuration procedures.

- **Websense Enterprise Explorer**: a web-based reporting application available free of charge with Websense Enterprise. Explorer provides a customizable view into the Log Database. It 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.

- **Websense Enterprise Explorer for Unix**: a web-based reporting application available free of charge with Websense Enterprise. Explorer for Unix provides the same functionality as Websense Enterprise Explorer, but for UNIX-based operating systems. 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 a Cisco integration 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 Cisco integration 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. You must install the Network Agent to use protocol management.

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.

If you have purchased the Instant Messaging (IM) Attachment Manager, you can configure Websense Enterprise to restrict file attachment sending and file sharing with IM clients. This feature enhances the default IM controls in Websense Enterprise by allowing you to permit certain IM traffic while blocking the transfer of attachments by those IM clients.
Chapter 1: Introduction

Deployment Tasks

The following sequence is recommended for installing Websense Enterprise and configuring it to filter internet traffic with Cisco Adaptive Security Appliance (ASA), Cisco PIX Firewall, Cisco Content Engine, or Cisco Routers.

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. The information required to make this decision can be found in the Websense Enterprise Deployment Guide. For an overview of basic deployment in a small network (< 500 users), as well as deployment information specific to your integration product, see Chapter 2: Network Configuration.

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: Installing Websense Enterprise for the installation procedures for each operating system.

3. **Configure your integration:** You must direct internet requests through your Cisco integration. This is the last step in the installation and configuration process. See Chapter 6: Configuring Your Cisco Integration for instructions.
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. To determine the appropriate deployment for your network, please refer to the Websense Enterprise Deployment Guide.

The information in this chapter provides an overview of where Websense Enterprise components can be installed to help you determine the relationship of Websense components and your integration product to one another. System requirements for your integration product are included in this chapter. All other system requirements are listed in the Websense Enterprise Deployment Guide.

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 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.
Chapter 2: Network Configuration

- **Websense Manager**: may be installed on the same machine as the Policy Server, and/or on one or more different machines in your network. The Websense Manager machine needs network access to the Policy Server machine, but the two machines do not need to have the same operating system. The Websense 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 Policy Server and is typically installed on the same machine; however, you may install User Service on a different operating system than the Policy Server. If the Policy Server is installed on Linux, for example, you can install User Service separately on a Windows machine. User Service installs on Windows, Solaris, and Linux.

\[\text{IMPORTANT}\]

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**: can be installed on the Filtering Service machine or separately, depending upon your needs and the configuration of your network. Network Agent installs on Windows, Solaris, and Linux. When planning the deployment of 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 27 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 Filtering Service 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.

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

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

Real-Time Analyzer (RTA): can be installed on the same machine as the Filtering Service or on a separate machine. The Real-Time Analyzer installs on Windows only. Real-Time Analyzer (RTA) can be memory and CPU demanding, depending on desired system settings and network load conditions, so it
Chapter 2: Network Configuration

should not be installed on real-time critical machines. See the Websense Enterprise Deployment Guide for more information.

**IMPORTANT**

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

You must have one of the following web servers installed on the machine where you plan to install RTA:

- Apache HTTP Server
- Microsoft IIS

**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 HTTP Server.

For information about supported versions of these web servers, see the Websense Enterprise Deployment Guide.

- **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.
Chapter 2: Network Configuration

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

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

For configuration information, refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide. For detailed deployment information, refer to the white paper titled Transparent Identification of Users in Websense Enterprise on the Websense website at: http://www.websense.com/global/en/SupportAndKB/ProductDocumentation.

- **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. RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services. You can install RADIUS Agent and eDirectory Agent on the same machine or on separate machines in your network. The RADIUS Agent installs on Windows, Solaris, and Linux.

  For configuration information, refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide. For detailed deployment information, refer to the white paper titled Transparent Identification of Users in Websense Enterprise on the Websense website at: http://www.websense.com/global/en/SupportAndKB/ProductDocumentation.

- **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. The eDirectory Agent can be installed in the same network as DC Agent or Logon Agent, but cannot be active at the same time, since Websense Enterprise does not support communication with Windows and Novell directory services simultaneously. The eDirectory Agent installs on Windows, Solaris, and Linux.
Chapter 2: Network Configuration

For configuration information, refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide. For detailed deployment information, refer to the white paper titled Transparent Identification of Users in Websense Enterprise on the Websense website at: http://www.websense.com/global/en/SupportAndKB/ProductDocumentation.

- **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 the accuracy of user authentication in your network. The Logon Agent runs on Windows, Linux, or Solaris, and works together with the User Service and Filtering Service. Logon Agent can be used with a Windows NT-based directory service or with Active Directory, which is LDAP-based. LogonApp.exe, the client application that passes user logon information to Logon Agent, runs only on Windows client machines. You must create a logon script to run LogonApp.exe in your network; refer to Creating and Running the Script for Logon Agent, page 198 for instructions. Logon Agent and eDirectory Agent can be installed in the same network, but cannot be active at the same time, since Websense Enterprise does not support communication with Windows and Novell directory services simultaneously.

For configuration information, refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide. For detailed deployment information, refer to the white paper titled Transparent Identification of Users in Websense Enterprise on the Websense website at: http://www.websense.com/global/en/SupportAndKB/ProductDocumentation.

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

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

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

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

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

- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
- The Remote Filtering Server machine does not have to be joined to a domain.

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

- **Remote Filtering Client**: can be installed on user machines that you want to filter outside the network firewall. To deploy this client application, you can use the provided installer, called the **Remote Filtering Client Pack**, and a third-party deployment tool. A Remote Filtering Client must be able to communicate with a Remote Filtering Server inside the network firewall to enable web filtering on the remote workstation. The Remote Filtering Client Pack and the Remote Filtering Client install only on Windows.

**NOTE**

The Remote Filtering Client is also available as part of the Websense Client Policy Manager™ (CPM). If you are using CPM to manage application filtering on employee desktops, the Remote Filtering Client is provided as part of the CPM Client Agent. For more information, refer to your Websense Client Policy Manager documentation.
Chapter 2: Network Configuration

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

**IMPORTANT**

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

- **Websense Enterprise Reporting 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 and Explorer then use this information to create reports on users’ internet activity. See the Websense Enterprise Reporting documentation for installation and administrative information.

**NOTE**

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

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 some 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, and detailed deployment recommendations, refer to the Websense Enterprise Deployment Guide. System requirements for your integration product can be found in System Requirements, page 32. All other Websense system requirements are listed in the Websense Enterprise Deployment Guide.
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 or Websense Enterprise Reporting components on a machine running a firewall. In addition, Websense, Inc. does not recommend installing Websense Enterprise and Websense Enterprise Reporting components together on the same machine. Filtering and logging functions are CPU intensive and could cause operating system errors. Install Websense Enterprise and Websense Enterprise Reporting components on separate machines inside the network, where they will not have to compete for resources. The exception to this is when Websense Enterprise is being evaluated on a small network or segment of a larger network. For detailed information about how to deploy each of the Websense Enterprise Reporting Tools in your network, see your Websense Enterprise Reporting documentation and the Websense Enterprise Deployment Guide.

Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA)

A simple and common network topology places the Websense Enterprise components on a single machine, communicating with the Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA) through TCP/IP. For the Network Agent to work properly, the Websense Enterprise machine must be installed so that it can directly see internet traffic on your internal network.
Other configurations are possible. Consult your Cisco PIX Firewall or ASA documentation and consider the information in this chapter when deciding on the best configuration for your network.
Cisco Content Engine

In this common configuration, the Websense Enterprise components are installed on a single machine, communicating with the Cisco Content Engine through TCP/IP. For the Network Agent to work properly, the Websense Enterprise machine must be installed so that it can directly see internet traffic on your internal network.

Other configurations are possible. Consult your Content Engine documentation and consider the information in this chapter when deciding on the best network configuration for your environment.
Cisco IOS Routers

In this common configuration, the Websense Enterprise components are installed on a single machine, communicating with the Cisco IOS Router. For the Network Agent to work properly, the Websense Enterprise machine must be installed so that it can directly see 2-way internet traffic on your internal network.

This router has firewall functionality and can be used with or without an accompanying firewall. If you elect to use the Cisco Router with a firewall, ensure that all internet traffic is configured to pass through the router and is not set to bypass the router and go directly to the firewall. Traffic filtered through the firewall in this type of deployment cannot be filtered by Websense.

Other configurations are possible. Consult your Cisco Router documentation and consider the information in this chapter when deciding on the best network configuration for your environment.
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 your Cisco integration product.
Chapter 2: Network Configuration

Remote Office Connection

**Requirement:** The Network Agent must be able to monitor all internal internet traffic from Switch #1, Switch #2, and Switch #3, as well as the internet traffic coming into Router #1 from the remote office.

**Solution:** Install an additional switch (Switch #4) between Router #1 and the firewall. Connect the Network Agent to Switch #4. Configure the port to which the Network Agent is connected to mirror or span the port to which Router #1 is connected.

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**

**Requirement:** To effectively manage internet traffic, Network Agent must see all the traffic from all three network segments.

**Solution:** Install an instance of Network Agent on each network segment. Switch #1, Switch #2, and Switch #3 must be configured to allow the Network Agent to monitor the port connecting the switch to the firewall. Each instance of Network Agent also must be configured to monitor all the traffic on its network segment and to communicate with the same Websense Filtering Service connected to Switch #3.
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. See the Websense Enterprise Deployment Guide for more information.

Directory Services

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

Websense can communicate with the following directory services:

- Windows NTLM-based directories
- Windows Active Directory
- Sun™ Java System Directory Server
- Novell Directory Services/eDirectory

For information about supported versions of these directory services, see the Websense Enterprise Deployment Guide. For information about configuring directory service access, see the 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.
If you are using a Cisco security appliance (PIX Firewall or ASA), we recommend that you use a Websense transparent identification agent such as DC Agent for user authentication. Alternatively, if your users are located in a single domain, you can use Cisco Secure Authentication (also called Cisco Secure ACS) on the security appliance. When you use ACS, the Cisco security appliance sends names of authenticated users to Websense without domain information. ACS therefore only functions properly with Websense when all users are located in a single domain.

**NOTE**
In any environment, Websense 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.

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

- If you are using the Sun Java System Directory Server or Novell Directory Services/eDirectory:
  1. Enable the appropriate directory service 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 if Websense is unable to identify users transparently, it will prompt users to manually authenticate.

  Detailed instructions for each of these tasks can be found in the User Identification chapter in the Websense Enterprise Administrator’s Guide.

- 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 and/or Logon Agent.
  3. Enable manual authentication within Websense so that if Websense is unable to identify users transparently, it will prompt users to manually authenticate.

  Detailed instructions for each of these tasks can be found in the User Identification chapter in the Websense Enterprise Administrator’s Guide.
Chapter 2: Network Configuration

The Websense transparent identification feature allows Websense to filter internet requests from users in a Windows or Novell directory service, without prompting users to manually authenticate. Websense Enterprise can transparently identify users in a Windows domain if the Websense DC Agent and/or Logon Agent is installed. In networks using a Novell directory service, you can transparently identify users by installing the Websense eDirectory Agent.

Once the Websense Filtering Service is configured to communicate with the transparent identification agent (DC Agent, Logon Agent, or 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 your Cisco integration. For information about transparent identification and the Websense DC Agent, Logon Agent, and eDirectory Agent, please see the Websense Enterprise Administrator’s Guide.

System Requirements

Refer to the Websense Enterprise Deployment Guide for a complete list of system requirements for installation of Websense Enterprise components in your network. This section contains system requirements and deployment information specifically related to your integration product.

All Websense Enterprise components, with the exception of the optional remote filtering components, can run on the same Windows machine or can be distributed on separate Windows, Solaris, or Linux machines. Not all Websense Enterprise components are supported on all three operating systems, but components can be installed on machines with the same or different operating systems. For example, Websense Manager is not supported on Linux, but a Websense Manager installed on a Windows or Solaris machine can configure a Policy Server installed on a Windows, Solaris, or Linux machine. See the Websense Enterprise Deployment Guide for a list of supported operating systems for each Websense Enterprise component.

Such factors as network size, network configuration, and internet traffic volume can affect the ability of Websense Enterprise to filter internet requests. Refer to the Websense Enterprise Deployment Guide for hardware
requirements for your network. If you plan to install Websense Enterprise components on a machine that has high CPU demands, make sure that the machine has sufficient resources to accommodate all the software loaded on it.

Supported Cisco Integration Product Versions

Websense Enterprise v6.2 is compatible with the following versions of Cisco PIX Firewalls, Cisco Adaptive Security Appliances (ASA), Cisco Content Engines, and Cisco Routers:

- Cisco PIX Firewall Software v5.3 and higher
- Cisco ASA Software v7.0 and higher
- Cisco Content Engine ACNS v4.1 and higher
- Cisco Routers with Cisco IOS Software Release 12.3 and higher

User Workstations

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

To be filtered by Websense, a user workstation must access the internet through the Cisco integration.

If Websense Enterprise is integrated with a Cisco Content Engine or an IOS Router, workstation browsers must be set for proxy-based connections. If a Cisco PIX Firewall or ASA is being used with Websense Enterprise, workstation browsers must be set to use the PIX Firewall or ASA as the default gateway.

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.
CHAPTER 3

Upgrading Websense Enterprise

This chapter contains procedures for upgrading a previous version of Websense Enterprise to version 6.2. Before upgrading Websense Enterprise, make sure your system meets the system requirements listed in the Websense Enterprise Deployment Guide and in the previous chapter.

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

**NOTE**
If you have the optional Remote Filtering Client application installed on user workstations in your network, see Remote Filtering Client, page 51 for upgrade instructions.

Direct upgrades from version 5.5 or higher are supported. Websense Enterprise “version 5.5 or higher” refers to the following releases:

- 5.5, 5.5.1, 5.5.2
- 6.1, 6.1.1

During upgrade, the installer will configure v6.2 components to use the same network interface cards (NICs) for Websense communications and the same Network Agent used by the earlier version. The installer will also automatically assign the same port numbers to the v6.2 Websense Enterprise components that the existing Websense Enterprise components use.

The Websense Master Database will be removed during upgrade. You can either download the new Master Database during upgrade of the Filtering Service, or download it after the upgrade is complete by using Websense Manager. When scheduling the upgrade, be aware that users will not be filtered by Websense Enterprise until the services are restarted and the new Master Database has been successfully loaded. Depending on how your integration product is configured to respond when Websense Enterprise is unavailable, traffic will either be allowed unfiltered or blocked entirely during the upgrade.
Chapter 3: Upgrading Websense Enterprise

Versions Supported

Direct upgrades from v5.5 or higher are supported. If you are running Websense Enterprise v5.2, 5.1, 5.0.1, or 5.0, an upgrade to v6.2 requires two steps. You must upgrade your earlier version to v5.5 first, and then perform a v6.2 upgrade. The v5.5 installer for your operating system is available from:


If you are running Websense Enterprise v4.4.1 or earlier, an upgrade to v6.2 requires three steps. You must upgrade your 4.x version to v5.2 first, then upgrade to v5.5, and finally upgrade to v6.2. The v5.2 installer for your operating system is available from:

- **Windows**: [http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2.exe](http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2.exe)
- **Solaris**: [http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2_Slr.tar.gz](http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2_Slr.tar.gz)
- **Linux**: [http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2_Lnx.tar.gz](http://www.websense.com/download/v5.2/WebsenseEnterprise_5.2_Lnx.tar.gz)

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 v6.2 system. Configuration files from earlier versions are not compatible with v6.2.

The procedures for converting to v6.2 without upgrading are described in the technical paper titled *Transferring Configuration Settings to a v6.2 System Without Upgrading* located on the Websense documentation site: [http://www.websense.com/global/en/SupportAndKB/ProductDocumentation](http://www.websense.com/global/en/SupportAndKB/ProductDocumentation).

### 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 Policy Server and copy the `config.xml` file, the `websense.ini` file, and the `eimserver.ini` file from the `Websense\bin` folder to a safe location.

- **Non-English language versions**: 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 v6.2 Language Pack, which is released separately. 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
Chapter 3: Upgrading Websense Enterprise

Websense component resides. The installer detects all Websense Enterprise components and upgrades them accordingly.

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

- **Remote Control Utilities**: Upgrade of Websense Enterprise using a remote control utility such as Terminal Services is not supported.
- **Usage Monitor**: When you upgrade a machine that has version 5.5 of the Policy Server installed, the installer will add the Usage Monitor component in addition to upgrading the Policy Server to version 6.2. The Usage Monitor tracks users’ internet activity and sends alerts when configured threshold values are crossed. Beginning with Websense Enterprise 6.1, the Usage Monitor is included as part of a **Typical** installation.
- **Reporting**: To properly generate reports, you must use the same version of Websense Enterprise and the Websense Enterprise Reporting Tools.
- **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.

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

- **Matching locales**: When upgrading a Filtering Service that is installed on a different machine from Websense Manager, you must upgrade the Filtering Service to v6.2 in the same locale environment (language and character set) as the v5.5 or higher Websense Manager.
Chapter 3: Upgrading Websense Enterprise

- When upgrading Filtering Service on Windows, open Control Panel > Regional Options and change the locale to match that of the Websense Manager machine before beginning the upgrade.
- When upgrading on Solaris or Linux, log on to the Filtering Service machine with the locale appropriate to the Websense Manager.

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

**NOTE**

The upgrade process is for use on properly functioning Websense systems.

### Upgrading on Windows

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, be sure you have backed up the following files before proceeding:
- websense.ini
- eimserver.ini
- config.xml

**IMPORTANT**

If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them. To prevent the upgrade process from timing out and failing, stop the services manually and restart them again before beginning the upgrade. For instructions, see *Stopping or Starting Websense Services*, page 187.

To upgrade your Websense Enterprise v5.5 or higher system to v6.2:

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

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

   **IMPORTANT**
   User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense 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.

3. Close all open applications on the installation machine, and stop any antivirus software.

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

4. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from [http://www.my.websense.com/download](http://www.my.websense.com/download) to a folder on the installation machine and double-click to extract the installer files.
     - **Dynamic installer**: This version of `Websense62Setup.exe` is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
     - **Full installer**: This version of `Websense62Setup.exe` is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties with the online installer.
Product CD: The product CD contains all the files needed to install Websense Enterprise components. Run Websense62.exe from the Websense Enterprise v6.2 product CD. (This file will run automatically if autorun is enabled.) Select Install on the start screen to begin.

A screen displays instructions for extracting the setup program.

A screen displays instructions for extracting the setup program.

1. 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.

   ![Installer File Extraction Screen](image)

   Installer File 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.

   **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.

   b. Click Extract to begin decompressing the files. If Websense Enterprise installation files already exist in that location, you may choose to overwrite the existing files.
Chapter 3: Upgrading Websense Enterprise

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.

5. Follow the onscreen instructions and click Next to advance through the welcome screen and the subscription agreement.
The installer detects the Websense components from your earlier version and asks how you want to proceed. You can upgrade the current system or exit the installer.

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

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

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

8. Click Next to begin the upgrade.
If you are using the online installer, the Download Manager progress bars are displayed as Setup downloads the upgrade files from Websense. When the download process is complete, Setup stops the Websense services and begins the upgrade.
An installation progress bar appears while the installer upgrades your system and restarts the Websense services.
   - If you are using the Apache HTTP Server, you must restart it before using the Real-Time Analyzer on your upgraded system. Setup asks if you want to restart Apache now or wait until later. Select Yes or No and 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. Click Next to continue.

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

![Master Database Download Selection Screen]

9. Select a database download option and click Next.

If you have chosen to download the Master Database now, a progress bar appears. Because of its size, the database can take up to 20 minutes to download and decompress.
When the database download is complete, a message appears announcing the status of the download. Click Next to continue.

A message announcing the success of the installation is displayed.

10. Click Next to continue.

- If you have upgraded 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 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.

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

12. If Websense Enterprise is integrated with a Cisco security appliance (PIX Firewall or Adaptive Security Appliance), the following configuration updates are recommended, if they have not already been made. Refer to
Chapter 3: Upgrading Websense Enterprise

* Cisco PIX Firewall or Adaptive Security Appliance (ASA), page 213 for instructions.

- Increase the size of the security appliance’s internal buffer to handle long URL strings.
- Set the URL response block buffer to prevent replies from the web server from being dropped in high traffic situations.

**IMPORTANT**

Make sure you upgrade any other Websense components or products that may have a dependency on the system you just upgraded. This will prevent conflicts caused by incompatible versions.

For example, if you are using Websense Enterprise Reporting Tools, you must upgrade them to the same version as Websense Enterprise to properly generate reports.

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

**Upgrading on Solaris or Linux**

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

- `config.xml`
- `eimserver.ini`
To upgrade Websense Enterprise v5.5 or higher to v6.2:

1. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
2. Log on to the installation machine as the root user.
3. Close all open applications on the installation machine, and stop any antivirus software.
4. Create a setup directory for the installer files.
   For example: /root/Websense_setup
5. Download the installer file for your operating system from http://www.my.websense.com/download, or copy it from the Websense Enterprise CD and save it to the setup directory.
   - Solaris: Websense62Setup_Slr.tar.gz
   - Linux: Websense62Setup_Lnx.tar.gz
   If you download the installer file for your operating system from the website, you can choose between the following two versions:
     - **Dynamic installer**: an **online** installer that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
     - **Full installer**: a complete **offline** installer. It is much larger than the online Dynamic installer, and contains all the files needed to install Websense Enterprise components. Use this installer only if you experience difficulties with the online installer.
6. Enter the following command to unzip the installer file:
   
   ```
   gunzip <download file name>
   ```
   For example:
   
   ```
   gunzip Websense62Setup_Slr.tar.gz
   ```
7. Expand the file into its components with the following command:
   \texttt{tar xvf <unzipped file name>}
   
   For example:
   \texttt{tar xvf Websense62Setup_Lnx.tar}
   
   This places the following files into the setup directory:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.sh</td>
<td>Installation program</td>
</tr>
<tr>
<td>Setup</td>
<td>Archive file containing related installation files and documents.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Release Notes: An HTML file containing release notes and last minute information about Websense. Read this file with any supported browser.</td>
</tr>
</tbody>
</table>

8. Run the installation program from the setup directory with the following command:
   \texttt{./install.sh}
   
   To run the GUI version of the installer, use the following command:
   \texttt{./install.sh -g}
   
   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.

9. Follow the upgrade sequence.
   - **Upgrade option:** The installer detects the earlier version of Websense Enterprise components 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 continue.
   - **Websense services:** A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed.
   - **Samba Client:** Setup advises you that you must install the Samba client (v2.2.8a and higher) to display protocol block messages and onscreen alerts on Windows workstations. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware website at:

   \url{http://www.sunfreeware.com}
Chapter 3: Upgrading Websense Enterprise

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

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

- **Browser location on Solaris**: If the Websense 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, separate warnings are displayed.
  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
  - If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

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

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

   If you are using the online installer, 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 appears while the installer upgrades your system and restarts the Websense services.
Chapter 3: Upgrading Websense Enterprise

- **Language Pack**: 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/global/en](http://www.websense.com/global/en). Press Enter to continue.

- **Master Database Download**: Setup asks if you want to download the Websense Master Database now or at a later time using the Websense Manager. Select a database download option and press Enter.

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

If you have chosen to download the database now, the database is downloaded and decompressed. Because of its size, the database can take up to 20 minutes to download and decompress. When the database download is complete, a message appears advising you of the status of the download. Press Enter to continue.

A message announcing the success of the installation is displayed. Press Enter to continue.

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 launch the Websense Manager. By default, the Manager is selected for launch. Select **Finish** when you are ready to exit the installer.

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

13. If Websense Enterprise is integrated with a PIX Firewall or ASA security appliance, the following configuration updates are recommended, if they have not already been made. Refer to *Cisco PIX Firewall or Adaptive Security Appliance (ASA)*, page 213 for instructions.
Chapter 3: Upgrading Websense Enterprise

- Increase the size of the security appliance’s internal buffer to handle long URL strings.
- Set the URL response block buffer to prevent replies from the web server from being dropped in high traffic situations.

**IMPORTANT**

Make sure you upgrade any other Websense components or products that may have a dependency on the system you just upgraded. This will prevent conflicts caused by incompatible versions.

For example, if you are using Websense Enterprise Reporting Tools, you must upgrade them to the same version as Websense Enterprise to properly generate reports.

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

**Upgrading the Remote Filtering Components**

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

**WARNING**

Be sure to upgrade *all* instances of the Remote Filtering Client when you upgrade Remote Filtering Server. In order for remote filtering to function properly, the version number of the Remote Filtering Clients must match the version number of the Remote Filtering Server.
Remote Filtering Server

The Remote Filtering Server is upgraded in the same manner as the rest of the Websense Enterprise components, by running the v6.2 Websense installer on the machine where the Remote Filtering Server is installed. Refer to the previous sections of this chapter for detailed instructions.

Remote Filtering Client Pack

The Remote Filtering Client Pack can be upgraded in the same manner as the rest of the Websense Enterprise components, by running the v6.2 Websense installer on the machine where the Remote Filtering Client Pack is installed. Refer to the previous sections of this chapter for detailed instructions.

Remote Filtering Client

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

- **Manual upgrade**: Use the v6.2 Remote Filtering Client Pack installer package to manually uninstall the existing version of the Remote Filtering Client on an individual workstation, and then install the new version. See Manual Upgrade of Remote Filtering Client, page 52 for information. This upgrade method does not preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

- **Automatic upgrade with third-party tool**: Use the v6.2 Remote Filtering Client Pack and a third-party deployment tool to automatically uninstall the existing version of Remote Filtering Client on employee workstations, and replace it with the new version. See Upgrading Remote
Installation Guide

Chapter 3: Upgrading Websense Enterprise

Filtering Client with a Third-Party Deployment Tool, page 54 for information.

NOTE
If you are upgrading to a Websense Web Security Suite product that includes the Websense Client Policy Manager™ (Websense Web Security Suite™ – Lockdown Edition™ or Websense Web Security Suite Lockdown – Corporate Edition), or if you are planning to add Client Policy Manager (CPM) to your network when you upgrade, you do not have to upgrade your Remote Filtering Clients as described in this section. Because the Remote Filtering Client is included as part of the CPM Client Agent, you can simply deploy CPM Client Agent with the appropriate remote filtering settings. For more information, refer to the Websense Client Policy Manager documentation.

Manual Upgrade of Remote Filtering Client

To manually upgrade an instance of the Remote Filtering Client on a single Windows workstation to v6.2:

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

1. Run the v6.2 Websense installer on the Remote Filtering Client workstation to upgrade or install the Remote Filtering Client Pack:
   - If a previous version of the Remote Filtering Client Pack is installed on the machine, the Websense installer will detect it. Follow the onscreen instructions to upgrade it to v6.2.
   - If no previous version of the Remote Filtering Client Pack exists on the machine, follow the installation instructions in Remote Filtering Client Pack, page 133.
Chapter 3: Upgrading Websense Enterprise

2. Navigate to the default installation location of
   C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI\CPMClient.msi
   and double-click on the CPMClient.msi file to run the new Remote Filtering Client installer.

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

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

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

6. Restart the machine.

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

8. Click Next to continue.

9. Re-enter the connection information for the primary Remote Filtering Server that this client uses for web filtering. If you are not certain of these values, you can view them in Websense files on the Remote Filtering Server machine:
   a. Navigate to the securewispproxy.ini file, located in the /bin subdirectory in the Websense installation directory on the Remote Filtering Server machine.
   b. Open the securewispproxy.ini file with a text editor to view the values of the following Remote Filtering Server parameters:
      • External IP address or host name: ProxyPublicAddress
      • External communication port: ProxyPort
      • Internal IP address or host name: ProxyIP
      • Internal communication port: HeartBeatPort
   c. If you do not remember the pass phrase you defined when installing the Remote Filtering Server, enter the encrypted key instead. Websense Enterprise generates this key automatically by combining the pass phrase you defined with unpublished Websense keys. If you do not know the encrypted key, you can look it up if you have administrator rights on the Remote Filtering Server machine:
Chapter 3: Upgrading Websense Enterprise

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

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

11. Click Next to continue.

12. Click Install to begin installation.
   
   When the installer is finished, a message appears advising you that the procedure was successful.

13. Click Finish to exit the installer.

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

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

Upgrading Remote Filtering Client with a Third-Party Deployment Tool

This upgrade method allows you to deploy version 6.2 of the Remote Filtering Client to user workstations, while preserving the existing configuration settings.

To obtain the installer for version 6.2 of the Remote Filtering Client, you can:

- Upgrade an existing version of the Remote Filtering Client Pack to version 6.2 (see Remote Filtering Client Pack, page 51 for instructions).
- OR-


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

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

To deploy the new version of the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.
Chapter 3: Upgrading Websense Enterprise

**Upgrade Syntax**

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

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

When the installer upgrades an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration has not changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command. Refer to *Installing Remote Filtering Client with a Third-Party Deployment Tool*, page 140 for a complete list of command line parameters.

**Converting a Stand-Alone System to an Integrated System**

You can convert your Stand-Alone Edition to a system using an integrated Cisco product without losing any configuration settings. The conversion process preserves such settings as port numbers and IP addresses. Upgrades are available for version 5.5 or higher of the Websense Enterprise Stand-Alone Edition.

**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 v5.5 or higher Stand-Alone Edition to the v6.2 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in *Upgrading to the New Stand-Alone Edition*, page 57.

**Task 2:** Restart the machine and run the Websense Enterprise installer again to convert the v6.2 Stand-Alone Edition to an integrated system using a Cisco integration product. Follow the procedures in *Converting to an Integrated System*, page 67.

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

**Task 4:** Configure your Cisco integration to work with Websense Enterprise to filter internet traffic. Refer to Chapter 6: Configuring Your Cisco Integration for instructions.

**Distributed Components**

To convert your Stand-Alone Edition to use a Cisco integration product and distribute some Websense Enterprise components to other machines, perform the following tasks:

**Task 1:** Perform an upgrade of the Websense Enterprise v5.5 or higher Stand-Alone system to the Websense v6.2 Stand-Alone Edition. This will preserve your configuration data and use the settings from your original system. Follow the procedures in Upgrading to the New Stand-Alone Edition, page 57.

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

---

**WARNING**

Removing the Policy Server will delete all existing configuration settings.

**Task 3:** Run the Websense Enterprise installer a third time to convert the v6.2 Stand-Alone system to an integrated system using a Cisco integration product. Follow the procedures in Converting to an Integrated System, page 67.

**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 102 for the following components:

- Websense Manager
- DC Agent
- Network Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent
Chapter 3: Upgrading Websense Enterprise

- Real-Time Analyzer
- Usage Monitor
- Remote Filtering Server
- Remote Filtering Client Pack
- Remote Filtering Client

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

Task 6: Configure your Cisco integration to work with Websense Enterprise to filter internet traffic. Refer to Chapter 6: Configuring Your Cisco Integration for instructions.

Upgrading to the New Stand-Alone Edition

Your first task is to upgrade your v5.5 or higher Stand-Alone Edition to the v6.2 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 187.

Windows

The Websense installer can upgrade version 5.5 or higher of the Websense Enterprise Stand-Alone Edition.

1. Back up the following files before proceeding:
   - websense.ini
   - eimserver.ini
Chapter 3: Upgrading Websense Enterprise

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

3. Log on to the installation machine with **domain** and **local** administrator privileges.
   
   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 in the **Properties** dialog box for Windows services.

4. Close all open applications on the installation machine, and stop any antivirus software.

**WARNING**

Be sure to close the Windows Event Viewer, or the upgrade may fail.
5. 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.
     - **Dynamic installer**: This version of Websense62Setup.exe is an online installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
     - **Full installer**: This version of Websense62Setup.exe is a complete offline installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties with the online installer.
   - **Product CD**: The product CD contains all the files needed to install Websense Enterprise components. Run Websense62.exe from the Websense Enterprise v6.2 product CD. (This file will run automatically if autorun is enabled.) Select **Install** on the start screen to begin.

A screen displays instructions for extracting the setup program.

![Installer File Extraction Screen](image)

**Installer File 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.

**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.

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

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.

6. 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 how you want to proceed. You can upgrade the current system or exit Setup.

7. Select **Upgrade** and click **Next**.

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

8. 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 will continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.
Chapter 3: Upgrading Websense Enterprise

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

9. Click Next to begin the upgrade.

If you are using the online installer, the Download Manager indicates the progress of the file download from Websense. When the appropriate files have been downloaded, Setup stops the Websense services and begins installation.

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

- If you are using the Apache HTTP Server, you must restart it before using the Real-Time Analyzer on your upgraded system, Setup asks if you want to restart Apache now or wait until later. Select Yes or No and 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.websense.com/global/en. Click Next to continue.

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

**IMPORTANT**

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded.
Chapter 3: Upgrading Websense Enterprise

Master Database Download Selection Screen

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

If you have chosen to download the Master Database now, a progress bar appears. Because of its size, the database can take up to 20 minutes to download and decompress.

Master Database Download Progress
When the database download is complete, a message appears advising you that the database has been successfully downloaded. Click **Next** to continue.

A message announcing the success of the installation is displayed.

**11. Click Next to continue.**

- If you have upgraded 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 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.

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

**Solaris or Linux**

The Websense installer can upgrade version 5.5 or higher of the Websense Enterprise Stand-Alone Edition.

1. Back up the following files before proceeding:

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

**NOTE**

Before upgrading to a new version of Websense Enterprise, 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. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
Chapter 3: Upgrading Websense Enterprise

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

4. Close all open applications on the installation machine, and stop any antivirus software.

5. Create a setup directory for the installer files.
   For example: /root/Websense_setup

6. Download the installer file for your operating system from http://www.my.websense.com/download, or copy it from the Websense Enterprise CD and save it to the setup directory.
   - Solaris: Websense62Setup_Slr.tar.gz
   - Linux: Websense62Setup_Lnx.tar.gz
   If you download the installer file for your operating system from the website, you can choose between the following two versions:
     - Dynamic installer: an online installer that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
     - Full installer: a complete offline installer. It is much larger than the online Dynamic installer, and contains all the files needed to install Websense Enterprise components. Use this installer only if you experience difficulties with the online installer.

7. Enter the following command to unzip the installer file:
   
   ```
   gunzip <download file name>
   ```
   For example: gunzip Websense62Setup_Slr.tar.gz

8. Expand the file into its components with the following command:
   
   ```
   tar xvf <unzipped file name>
   ```
   For example: tar xvf Websense62Setup_Lnx.tar

This places the following files into the setup directory:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.sh</td>
<td>Installation program</td>
</tr>
<tr>
<td>Setup</td>
<td>Archive file containing related installation files and documents.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Release Notes: An HTML file containing release notes and last minute information about Websense. Read this file with any supported browser.</td>
</tr>
</tbody>
</table>
Chapter 3: Upgrading Websense Enterprise

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

   ./install.sh

   The installer detects the earlier version of the 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.

10. Select Upgrade and press Enter.

   The upgrade sequence is as follows:

   - **Websense services**: A list of currently running Websense services from the earlier version appears. A message explains that the installer must stop these services before the upgrade can proceed.
   - **Samba Client**: Setup advises you that you must install the Samba client (v2.2.8a and higher) to display protocol block messages and onscreen alerts on Windows workstations. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware website at: http://www.sunfreeware.com

   **NOTE**

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

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

   - **Browser location on Solaris**: If the Websense Manager is being upgraded on Solaris, you must provide the installer with the location of Netscape.
Chapter 3: Upgrading Websense Enterprise

- **System requirements check:** The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
  - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

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

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

If you are using the online installer, 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 appears and the Websense services are restarted.

- **Language Pack:** 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/global/en](http://www.websense.com/global/en). Press **Enter** to continue.

- **Master Database Download:** Setup asks if you want to download the Websense Master Database now or at a later time using the Websense Manager. Select a database download option and press **Enter**.

**IMPORTANT**

During upgrade, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded.
Chapter 3: Upgrading Websense Enterprise

If you have chosen to download the database now, the database is downloaded and decompressed. Because of its size, the database can take up to 20 minutes to download and decompress. When the database download is complete, a message appears advising you of the status of the download. Press Enter to continue.

A message announcing the success of the installation is displayed. Press Enter to continue.

12. 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 launch the Websense Manager. By default, the Manager is selected for launch. Select Finish when you are ready to exit the installer.

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

Converting to an Integrated System

Once you have upgraded your v5.5 or higher Stand-Alone Edition to the v6.2 Stand-Alone Edition, you are ready to convert to a system that integrates with a Cisco integration product.

---

**IMPORTANT**

If you are planning to deploy Websense Enterprise components on separate machines, run the installer now to remove components from the Websense machine before performing the conversion. Remember, however, that removing the Policy Server will delete all of your configuration settings.

---

**Windows**

To convert a Windows Stand-Alone Edition to a system integrated with a Cisco product:

1. Back up the following files before proceeding:
   - websense.ini
   - eimserver.ini
   - config.xml
2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.

3. Log on to the installation machine with domain and local administrator privileges.
   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 in the Properties dialog box for Windows services.

4. Close all open applications on the installation machine, and stop any antivirus software.

5. Run the Websense Enterprise installer (Setup.exe) from your local drive.

6. Follow the onscreen instructions through the welcome screen.
   Websense Setup detects the Stand-Alone Edition and asks how you want to proceed. You can modify the current system (add, remove, or repair components), or convert it to a system that integrates with a Cisco product.
Chapter 3: Upgrading Websense Enterprise

7. Select **Integrate with a firewall, proxy server, or network appliance** and click Next.

A message explains that the installer must stop the Filtering Service before the upgrade can proceed.

8. Click Next to continue.

A dialog box appears listing the supported integration types.

9. Select **Cisco Adaptive Security Appliances, Cisco Content Engine, Cisco PIX Firewall, or Cisco Routers** and click Next.

A message explains that the installer must stop the Filtering Service before the installation can proceed.

10. Click Next to continue.

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

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

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

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

If you are using the online installer, the Download Manager progress bar appears, tracking the progress of the installer download. When the appropriate files have been downloaded, Setup stops the Websense services and begins the upgrade.

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

A message appears advising you that the installation was successful.

12. Click **Next** to continue.

- If you have upgraded 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 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.

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

**Solaris or Linux**

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

1. Back up the following files before proceeding:
   - websense.ini
   - eimserver.ini
   - config.xml
Chapter 3: Upgrading Websense Enterprise

2. Close all Websense Managers anywhere in the network that connect to the Policy Server you are upgrading.
3. Log on to the installation machine as the root user.
4. Close all open applications on the installation machine, and stop any antivirus software.
5. Run the Websense Enterprise installer from the directory where you placed it using the following command:

   ./install.sh

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

   ./install.sh -g

   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.
6. Follow the upgrade sequence:
   - **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 **Cisco Adaptive Security Appliances**, **Cisco Content Engine**, **Cisco PIX Firewall**, or **Cisco Routers** 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, separate warnings are displayed.
     - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
     - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.
   - **Installation summary**: A summary list appears, showing the installation path, file sizes, and the components that will be upgraded.
7. Press Enter to begin the installation.
If you are using the online installer, the Download Manager copies the appropriate installer files from Websense. Conversion begins automatically when the necessary files have been downloaded.

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

8. Press **Enter** to continue.

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

**Migrating Between Integrations After an Upgrade**

If you plan to change the Cisco integration with which Websense Enterprise interacts (from PIX Firewall to an IOS Router, for example), you may do so after you upgrade to Websense Enterprise v6.2 without losing any of your configuration data.

The following procedure assumes that the Policy Server is installed on the same machine as the Filtering Service. If the Policy Server is installed on a separate machine, no changes need to be made to that component, and there is no need to back up the `config.xml` file.

To migrate between Cisco integration products after upgrading to Websense Enterprise v6.2:

1. Install and configure your new Cisco integration product on your network. Make sure it is deployed so that it can communicate with the Websense Enterprise machine (the machine running Filtering Service and Policy Server). Refer to *Websense Deployment* in *Chapter 2: Network Configuration* and your Cisco documentation for instructions.

2. Make backup copies of the following files (found in `Websense\bin`) and copy them to a location outside the `Websense` folder:
   - `config.xml`
   - `eimserver.ini`
   - `websense.ini`

3. Close all open applications on the Filtering Service machine, and stop any antivirus software.

4. Run the Websense Enterprise installer on the Filtering Service machine.
5. Remove the Filtering Service using the procedures in *Removing Components*, page 176.

**WARNING**

Remove the Filtering Service only. *Do not* remove the Policy Server.

6. Restart the machine.
7. Run the Websense Enterprise installer again.
8. Add the Filtering Service using the procedures in *Adding Components*, page 164.
9. When prompted to select an integration, select the new Cisco product (either **Cisco Adaptive Security Appliances**, **Cisco Content Engine**, **Cisco PIX Firewall**, or **Cisco Routers**).
10. Follow the onscreen instructions to complete the installation.

   The installer adds the new integration data to the `config.xml` file, without overwriting any of the previous configuration data.
11. Restart the machine.
12. Check to be sure that the Filtering Service has started.

   Refer to *Stopping or Starting Websense Services*, page 187 for instructions on starting a service.
13. If you stopped your antivirus software, be sure to start it again.

**Changing IP 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

Installing Websense Enterprise

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

Before Installing

Please read the following information before installing Websense Enterprise.

◆ **User authentication**: The Websense Filtering Service must be installed in the same domain (Windows) or the same root context (LDAP) as Cisco Secure ACS for ACS to work properly. If you are using the DC Agent and Manual Authentication, this is not necessary.

◆ **Non-English language versions**: Websense Enterprise v6.2 installs in English only. Language Packs for converting systems to non-English language versions are released separately. Installation instructions are provided with the Language Pack product.

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

◆ **Deployment**: You can install the main Websense Enterprise components together on the same machine or distribute them on separate machines, depending upon the available operating systems and the size of your network. If you plan to distribute your Websense Enterprise components on separate machines in your network, run the installer on each machine and select the **Custom** installation option.

You can install Websense components on separate machines that don’t have the same operating system. For example, you can install Websense Manager on a Windows machine and use it to configure a Policy Server running on a Linux machine. As long as each Websense component is supported on the operating system of the machine where it is installed, the components will work together.
Be sure to read the Websense Enterprise Deployment Guide before beginning installation to determine the appropriate deployment of Websense components in your environment, including the supported operating systems for each component.

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

- **Remote filtering**: To install the optional Remote Filtering components that allow filtering of workstations located outside the network firewall, you must run the Websense Enterprise installer and select a **Custom** installation. Refer to Installing Websense Enterprise Components Separately, page 102 for information.

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

**NOTE**

If you install Network Agent on a machine with multiple NICs, you can configure Network Agent after installation to use more than one NIC. See Configuring Network Agent to use Multiple NICs, page 207 for more information.

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

- **Internet access**: For the Websense Master Database download to occur during installation, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:
  - download.websense.com
  - ddsdom.websense.com
  - ddsint.websense.com
  - portal.websense.com
  - my.websense.com
Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the Filtering Service can access.

- **Remote Control Utilities**: Installation of Websense Enterprise using a remote control utility such as Terminal Services is not supported.

- **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 262*.

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

## Typical Websense Enterprise Installation

This section provides separate instructions for installing Websense Enterprise components on each operating system.

### Windows

Follow the procedures in this section to install Websense Enterprise on a Windows machine. These procedures are for a **Typical** installation, in which the main Websense Enterprise components are installed on the same machine.

If you plan to distribute the main Websense Enterprise components on separate machines in your network, you must install the Policy Server first. Only the Websense Manager can be installed before the Policy Server has been successfully installed. To install components separately, run the Websense Enterprise installer on each machine and select a **Custom** installation. For instructions on installing Websense components separately, refer to *Installing Websense Enterprise Components Separately, page 102*.

If you decide to change the location of a Websense component, add a component, or remove a component, run the Websense Enterprise installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For information about adding or
removing Websense components, refer to *Adding Components*, page 164 and *Removing Components*, page 176.

To install Websense Enterprise on a Windows machine not running your Cisco integration:

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

   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 in the **Properties** dialog box for Windows services.

2. Close all applications and stop any antivirus software.

3. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from [http://www.websense.com/global/en/downloads](http://www.websense.com/global/en/downloads) to a folder on the installation machine and double-click to extract the installer files.
     - **Dynamic installer**: This version of `Websense62Setup.exe` is an **online** installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
     - **Full installer**: This version of `Websense62Setup.exe` is a complete **offline** installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties with the online installer.
   - **Product CD**: The product CD contains all the files needed to install Websense Enterprise components. Run `Websense.exe` from the Websense Enterprise v6.2 product CD. (This file will run automatically if *autorun* is enabled.) Select **Install** on the start screen to begin.
A screen displays instructions for extracting the setup program.

![Installer File Extraction Screen](image)

**Installer File 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.

---

**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.

---

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

4. Click **Next** on the welcome screen and follow the onscreen instructions through the subscription agreement.

You are asked to select a Websense product to install.
5. Select **Websense Enterprise** and click **Next**.

You are offered a choice of two setup types.
Chapter 4: Installing Websense Enterprise

- **Typical**: installs Filtering Service, Policy Server, Websense Manager, User Service, Usage Monitor, and Real-Time Analyzer automatically. The installer asks if you want to install a transparent identification agent or the Network Agent on the same machine.
- **Custom**: allows you to choose individual Websense Enterprise components to install. Use this option to install Websense components on separate machines in your network. For more information, see *Installing Websense Enterprise Components Separately*, page 102.

6. Select **Typical** and click **Next**.

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

![Network Interface Card Selection Screen](image)

7. Select the card to use for Websense Enterprise communication and click **Next**.

The installer asks if you want to run Websense Enterprise in the Stand-Alone filtering mode or integrate it with a firewall, proxy server, or network appliance.
Chapter 4: Installing Websense Enterprise

8. Select Integrated and click Next.

A dialog box appears listing the supported integration types.
9. Select Cisco Adaptive Security Appliances, Cisco Content Engine, Cisco PIX Firewall, or Cisco Routers and click Next.

Setup displays the Websense Subscription Key dialog box.

- **I have a Websense subscription key**: If you have a valid subscription key, select this option and enter your key. You will be given the option to download the Websense Master Database during installation. This will enable Websense Enterprise to begin filtering immediately.

- **I do not wish to use a key at this time**: Select this option to continue the installation without entering a key. You will not be given the option to download the Websense Master Database during installation. You can download the Master Database after installation by entering a valid key in the Websense Manager. Refer to *Subscription Key and Master Database Download*, page 192 for instructions.


10. Click Next to continue.
Chapter 4: Installing Websense Enterprise

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

- If both supported web servers are detected, a dialog box appears asking you to choose one server for the RTA instance.
- If one of the supported servers is detected, the installer continues. No notification appears.
- If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.

![RTA Web Server Dialog Box](image)

If you select the Apache HTTP 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 HTTP Server and run the Websense Enterprise installer again to install Websense.

**NOTE**

Apache HTTP Server documentation is installed in HTML format in the **docs/manual/** directory. It is also available at: [http://httpd.apache.org/docs/2.0/](http://httpd.apache.org/docs/2.0/).
11. Select a web server installation option and click **Next** to continue. If you are installing the Real-Time Analyzer and are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is **Default Web Site**, which is correct in most instances.

![Virtual Directory Selection](image)

12. If you have renamed the default website in the IIS Manager or are using a language version of Windows other than English, select the proper website from the names in the drop-down list, and then click **Next** to continue. The installer asks if you want to install the Network Agent.

**IMPORTANT**

The machine on which the Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.
Chapter 4: Installing Websense Enterprise

Network Agent Installation

You are given the following two options:

- **Install Network Agent**: If the installation machine has the necessary internet traffic visibility, select this option to install the Network Agent.

- **Do not install Network Agent**: Select this option to continue the Websense Enterprise installation without installing the Network Agent. Network Agent can be installed on this machine later, or installed on another machine.

13. Click Next to continue.

If you are installing the Network Agent, 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.

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

**NOTE**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 208.
15. Click **Next** to continue.
   If you are installing Network Agent, a screen appears asking if you want to allow Websense, Inc. to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.

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

16. Select a Network Agent feedback option and click **Next** to continue.
   Setup asks you to select an initial filtering option.
   - **Yes**: configures Websense Enterprise to filter internet traffic immediately after installation, based on a predefined default policy.
   - **No**: configures Websense Enterprise to monitor internet traffic only, while permitting all internet requests. Select this option and install one or more of the Websense Enterprise Reporting Tools if you prefer to evaluate your network traffic before applying internet filtering.
17. Select an initial filtering option and click Next to continue.

Setup displays the **Transparent User Identification** screen, allowing you to select how Websense Enterprise will identify users:

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

- **DC Agent**: Select this option to install DC Agent to authenticate users transparently with a Windows-based directory service.

- **Logon Agent**: Select this option to install the Logon Agent to authenticate users transparently when they log on to the domain. Logon Agent receives its user information from an application called LogonApp.exe that must be run by a logon script in your network. Refer to *Creating and Running the Script for Logon Agent*, page 198 for instructions.

- **DC Agent and Logon Agent**: Select this option to install DC Agent and the Logon Agent to authenticate users transparently. This can increase the accuracy of user identification in some networks.

- **None**: This option does not install a Websense transparent identification agent. Select this option if you plan to configure authentication of users through your Cisco integration product.

**NOTE**

You can also configure manual authentication in Websense Manager after installation and initial setup. Refer to the Websense Enterprise Administrator’s Guide for instructions.
Chapter 4: Installing Websense Enterprise

18. Select a transparent identification method and click **Next** to continue. Setup displays the **RADIUS Agent** screen.

**Transparent User Identification Options**

**RADIUS Agent Installation**
19. If you have remote users who are authenticated by a RADIUS server, you can select Yes to install the optional Websense RADIUS Agent. RADIUS Agent will allow Websense Enterprise to transparently identify these users.

20. Click Next to continue.

21. If you selected DC Agent for installation, Setup 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. Enter the domain and user name, followed by the network password for an account with domain privileges, and click Next to continue.

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

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

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

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

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

23. Click Next to start the installation.

- If you are using the online installer, 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click Next to continue.
Chapter 4: Installing Websense Enterprise

If you provided the installer with 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 Manager.

24. Select a database download option and click Next.
   If you have chosen to download the Master Database now, a progress bar appears. Because of its size, the database can take up to 20 minutes to download and decompress.
When the database download is complete, a message appears advising you that the database has been successfully downloaded. Click **Next** to continue.

A message announcing the success of the installation is displayed.

25. 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.
26. If you stopped your antivirus software, be sure to start it again.

27. See Chapter 5: Initial Setup to perform post installation tasks.

28. Follow the instructions in Chapter 6: Configuring Your Cisco Integration to configure your Cisco security appliance to work with Websense Enterprise.

**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 164.
Chapter 4: Installing Websense Enterprise

Solaris or Linux

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

If you plan to distribute the main Websense Enterprise components on separate machines in your network, you must install the Policy Server first. Only the Websense Manager can be installed before the Policy Server has been successfully installed. To install components separately, run the Websense Enterprise installer on each machine and select a Custom installation. For instructions on installing Websense components separately, refer to Installing Websense Enterprise Components Separately, page 102.

If you decide to change the location of a Websense component, add a component, or remove a component, run the Websense Enterprise installer again on the machine you want to modify and select the appropriate option. The installer detects the presence of Websense components and offers you options for modifying your installation. For information about adding or removing Websense components, refer to Adding Components, page 164 and Removing Components, page 176.

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

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

You can install the Websense 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 102 for instructions on installing individual Websense components.
To install Websense Enterprise on a Solaris or Linux machine:

1. Log on to the installation machine as the root user.
2. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.
   For example: /root/Websense_setup
4. Download the installer file for your operating system from http://www.websense.com/global/en/downloads, or copy it from the Websense Enterprise CD and save it to the setup directory.
   - Solaris: Websense62Setup_Slr.tar.gz
   - Linux: Websense62Setup_Lnx.tar.gz
   If you download the installer file for your operating system from the website, you can choose between the following two versions:
   - Dynamic installer: an online installer that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
   - Full installer: a complete offline installer. It is much larger than the online Dynamic installer, and contains all the files needed to install Websense Enterprise components. Use this installer only if you experience difficulties with the online installer.
5. Enter the following command to unzip the file:
   
gunzip <download file name>
   For example: gunzip Websense62Setup_Slr.tar.gz
6. Expand the file into its components with the following command:
   
tar xvf <unzipped file name>
   For example: tar xvf Websense62Setup_Lnx.tar
This places the following files into the setup directory:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.sh</td>
<td>Installation program.</td>
</tr>
<tr>
<td>Setup</td>
<td>Archive file containing related installation files and documents.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Release Notes: An HTML file containing release notes and last minute information about Websense. Read this file with any supported browser.</td>
</tr>
</tbody>
</table>
Chapter 4: Installing Websense Enterprise

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

    ./install.sh

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

    ./install.sh -g

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

8. Follow the onscreen instructions through the subscription agreement.

9. Provide the installer with the following information.

   - **Installation type**: You are asked to select an installation type:
     - **Typical**: installs Filtering Service, Policy Server, User Service, and Usage Monitor 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 components on separate machines in your network. For more information, see Installing Websense Enterprise Components Separately, page 102

   Select Typical to install the listed Websense components.

   - **Network Interface Card (NIC) selection**: If the installation machine is multihomed, all enabled network interface cards (NICs) appear in a list. Select the card to use for Websense Enterprise communication.

   - **Integration option**: Select Integrated.

   - **Integration product**: Select Cisco Adaptive Security Appliances, Cisco Content Engine, Cisco PIX Firewall, or Cisco Routers.

   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.
Chapter 4: Installing Websense Enterprise

- **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 installing other Websense components.

- **Subscription key**: Setup can download the Websense Master Database during installation if you provide a valid subscription key or evaluation key. This will enable Websense to begin filtering immediately.
  
  - **I have a Websense subscription key**: If you have a valid subscription key, select this option and enter your key when prompted. You will be given the option to download the Websense Master Database during installation.
  
  - **I do not wish to use a key at this time**: Select this option to continue the installation without entering a key. You will not be given the option to download the Websense Master Database during installation. You can download the Master Database after installation by entering your key in the Websense Manager. Refer to **Subscription Key and Master Database Download**, page 192 for instructions.

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

- **Network Agent**: Setup asks if you want to install the Network Agent.

  **IMPORTANT**
  
  The machine on which the Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.
You are given the following two options:

- **Install Network Agent:** If the installation machine has the necessary internet traffic visibility, select this option to install the Network Agent.

- **Do not install Network Agent:** Select this option to continue the Websense Enterprise installation without installing the Network Agent. Network Agent can be installed on this machine later, or installed on another machine.

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

**NOTE**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 208.

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

**NOTE**

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

**Initial filtering options:** Websense Enterprise can be configured to filter internet traffic immediately after installation, based on a predefined default policy, or to monitor internet traffic only. Select **Yes** to filter traffic initially, or **No** if you prefer to evaluate your network traffic before applying any type of filtering. You must install one or more of the Websense Enterprise Reporting Tools to report on network activity.
Chapter 4: Installing Websense Enterprise

- **Transparent user identification**: Select one of the following:
  - **eDirectory Agent**: Select this option to install the eDirectory Agent to authenticate users transparently through Novell eDirectory Server.
  - **Logon Agent**: Select this option to install the Logon Agent to authenticate Windows users transparently when they log on to the domain. Logon Agent receives its user information from an application called LogonApp.exe that must be run by a logon script in your network. Refer to *Creating and Running the Script for Logon Agent*, page 198 for instructions.
  - **None**: This option does not install a Websense transparent identification agent. Select this option if you plan to configure authentication of users through your Cisco integration product.

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

- **RADIUS Agent**: If you have remote users who are authenticated by a RADIUS server, you can choose to install RADIUS Agent to transparently identify them.
- **Samba Client**: Setup advises you that you must install the Samba client (v2.2.8a and higher) to display protocol block messages and onscreen alerts on Windows workstations. You may continue installing Websense and download the Samba client later. To download the Samba client, go to the Sun freeware website at: http://www.sunfreeware.com
**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 Manager separately.

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

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

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

---

**NOTE**

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

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

---

**IMPORTANT**

The full installation path must use ASCII characters only.
Chapter 4: Installing Websense Enterprise

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

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

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

The installer creates the `/opt/Websense` directory, and the `/opt/Websense/Manager` directory if you installed Websense Manager (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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Press **Enter** to continue.

- **Master Database Download**: 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 Manager. Select a database download option and press **Enter**.

    If you have chosen to download the database now, the database is downloaded and decompressed. When the database download is complete, a message appears advising you of the status of the download. Press **Enter** to continue.

A message announcing the success of the installation is displayed.

11. Press **Enter** to continue.

- 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 displays a screen asking if you want to launch the Websense Manager. By default, the Manager is selected for launch. Select **Finish** when you are ready to exit the installer.

**NOTE**

Because of its size, the database can take up to 20 minutes to download and decompress.
12. If you stopped your antivirus software, be sure to start it again.

13. If you did not install the Websense Manager on this machine, you must install it on a separate Windows or Solaris machine in your network. Follow the instructions under \textit{Installing Websense Enterprise Components Separately}, page 102.

14. Follow the instructions in \textit{Chapter 6: Configuring Your Cisco Integration} to configure your Cisco security appliance to work with Websense Enterprise.

\textbf{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 \textit{Modifying an Installation}, page 164.

\section*{Installing Websense Enterprise Components Separately}

All Websense Enterprise components can be installed separately using the \textbf{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:

\textbf{IMPORTANT}

When installing Websense components, always install the Policy Server first. Only the Websense Manager can be installed before the Policy Server has been successfully installed.
Chapter 4: Installing Websense Enterprise

- **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.

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

- **DC Agent**: DC Agent runs on Windows 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.

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

- **Usage Monitor**: Usage Monitor installs on Windows, Solaris, and Linux. You can have only one instance of Usage Monitor for each Policy Server in your network.

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

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

- **Logon Agent**: Logon Agent installs on Windows, Solaris, and Linux. Logon Agent receives user information at logon from a client application called `LogonApp.exe`, which must be run by a logon script. Instructions for creating and running this logon script in your network can be found in *Creating and Running the Script for Logon Agent*, page 198. `LogonApp.exe` runs only on Windows client machines.

**NOTE**

The installation of these Websense components in the presence of other Websense components requires fewer steps. Setup searches for existing Websense initialization files and automatically uses this configuration information to locate the Policy Server and Filtering Service in the network.
Chapter 4: Installing Websense Enterprise

- **Remote Filtering components:**
  The Remote Filtering components—Remote Filtering Server and Remote Filtering Client Pack—are required only if you need to enable web filtering on user workstations located outside your organization’s network firewall. These optional components are only available through a **Custom** installation.

  ![NOTE]
  To enable the Remote Filtering components, you must subscribe to the remote filtering service.

- **Remote Filtering Server:** The Remote Filtering Server installs on Windows, Solaris, and Linux. It must be able to communicate with the Websense Filtering Service and with the Remote Filtering Clients installed on user workstations.

- **Remote Filtering Client Pack:** The Remote Filtering Client Pack is an installer used to deploy the **Remote Filtering Client** to Windows workstations that will be used outside the network firewall. The Remote Filtering Client Pack installs on Windows only.

  To install Websense Enterprise core components individually in a distributed environment, refer to the Websense Enterprise **Deployment Guide** for information that will help you decide how to best deploy the components in your environment.

**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.
2. Close all applications and stop any antivirus software.

3. Run one of the following Websense Enterprise installers:

- **Web download**: Download one of the following packages from [http://www.websense.com/global/en/downloads](http://www.websense.com/global/en/downloads) to a folder on the installation machine and double-click to extract the installer files.
  - **Dynamic installer**: This version of Websense62Setup.exe is an online installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
  - **Full installer**: This version of Websense62Setup.exe is a complete offline installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties with the online installer.

- **Product CD**: The product CD contains all the files needed to install Websense Enterprise components. Run Websense62.exe from the Websense Enterprise v6.2 product CD. (This file will run automatically if autorun is enabled.) Select **Install** on the start screen to begin.

A screen displays instructions for extracting the setup program.

---

**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 DC Agent with such privileges, you may configure administrator privileges for it after installation in the **Properties** dialog box for Windows services.
Chapter 4: Installing Websense Enterprise

**Installer File 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.

  **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.

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

  4. **Click Next** on the welcome screen and follow the onscreen instructions through the subscription agreement.
You are asked to select a Websense product to install.

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

You are offered a choice of two setup types.
6. Select **Custom** and click **Next**.
7. To continue, proceed to the appropriate component section below.

**Websense 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 104.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Websense Manager** and click **Next**.

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

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

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:
   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

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

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

   If you are using the online installer, the Download Manager progress bars are displayed as Setup downloads the appropriate installer files from Websense. Installation begins automatically when the necessary files have been downloaded.
Chapter 4: Installing Websense Enterprise

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

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**.

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

**Network Agent**

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

If this installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. This will result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment will result in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by the Network Agent. For instructions on defining IP address ranges for multiple Network Agents, refer to the Websense Enterprise *Administrator’s Guide*. For detailed information about deploying Network Agent, refer to the Websense Enterprise *Deployment Guide*.

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.
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 164.

**IMPORTANT**

The Websense Filtering Service and the Policy Server must be installed and running prior to installing the Network Agent, or installed at the same time as 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 machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

2. Following the Custom installation path brings you to the component selection screen. Select **Network Agent** 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 the port number if different from the default, and then click **Next**. The installer displays a screen with information about Network Agent. The machine on which the Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly.

**IMPORTANT**

If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.
Chapter 4: Installing Websense Enterprise

You are given the following two options:

- **Continue installation**: If the installation machine has the necessary internet traffic visibility, select this option to install Network Agent.
- **Exit Setup**: If 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.

4. Click **Next** to continue.

   The installer asks you if this machine is running a firewall. Network Agent cannot function properly on a machine running a firewall.

5. Select **Yes** or **No** and click **Next** to continue:
   - Select **Yes** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install the Network Agent 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.

   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.
Chapter 4: Installing Websense Enterprise

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

![Note]
After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See Testing Visibility of Internet Traffic to Network Agent, page 208.

7. 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.

8. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then click Next.
A screen appears asking if you want to allow Websense, Inc. to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.

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

9. Select a Network Agent feedback option and click Next to continue.
Setup asks you to select an installation folder for the Websense Enterprise components.

10. Accept the default path (C:\Program Files\Websense) or click Browse to locate another installation folder, and then click Next to continue.
Chapter 4: Installing Websense Enterprise

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

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

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

11. Click Next to start the installation.

If you are using the online installer, 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.

12. Click Finish to exit the installer.

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

14. Configure Network Agent for use in your network. Refer to the instructions for initial configuration of Network Agent in Chapter 5: Initial Setup, as well as the Network Agent chapter of the Websense Enterprise Administrator’s Guide.

DC Agent

The Websense 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 DC Agent. If you did not install it together with the Filtering Service at that time, and 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 15.

To install DC Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.
2. Following the **Custom** installation path brings you to the component selection screen. Select **DC Agent** and click **Next**.
   
   If the installation machine is multihomed, all enabled network interface cards appear in a list.

3. Select the card you want DC Agent to use to communicate and click **Next**.
   
   Setup asks you to identify the machine on which the Policy Server is installed.

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

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

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

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

If you are using the online installer, the Download Manager progress bars are displayed as 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

When the installer is finished, 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. If you stopped your antivirus software, remember to start it again after Websense components have been installed.

11. Configure User Service to communicate with DC Agent by following the instructions in the User Identification chapter of the Websense Enterprise Administrator’s Guide.
Real-Time Analyzer (RTA)

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

To install RTA on a Windows machine:

1. Download and start the Windows installer using the procedure in Windows Procedures, page 104.

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

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

3. Select the card you want RTA to use to communicate and click Next. Setup asks you to identify the machine on which the Policy Server is installed.

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

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

   - If both supported web servers are detected, a dialog box appears asking you to choose one server for RTA.
   - If one of the supported servers is detected, the installer continues. No notification appears.
   - If neither supported web server is detected, the installer gives you the option to install the Apache HTTP Server or continue the installation without installing RTA.

   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.
Chapter 4: Installing Websense Enterprise

RTA Web Server Dialog Box

If you select the Apache HTTP 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 HTTP Server and run the Websense Enterprise installer again to install Websense.

NOTE

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

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

If you are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is Default Web Site, which is correct in most instances.
Chapter 4: Installing Websense Enterprise

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

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 then click Next to continue.

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

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

A summary list appears, showing the installation path, the installation size, and the components that will be installed.
8. Click **Next** to start the installation.

If you are using the online installer, the Download Manager progress bars are displayed as 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

When the installer is finished, 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. By default, Real-Time Analyzer is selected for launch.
10. Make a selection and click **Finish** to exit the installer.

**NOTE**
Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. See the Websense Enterprise *Administrator’s Guide* for more information.

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

**Usage Monitor**

Usage Monitor tracks users’ internet activity and sends alerts when internet activity for particular URL categories or protocols reaches threshold limits you have configured. You can have only one instance of Usage Monitor for each Policy Server in your network.

To install Usage Monitor on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

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

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

3. Select the card you want Usage Monitor 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.
   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 then click Next to continue.
   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:
   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.
   A summary list appears, showing the installation path, the installation size, and the components that will be installed.

6. Click Next to start the installation.
   If you are using the online installer, the Download Manager progress bars are displayed as 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click Next to continue.
   When the installer is finished, a message appears advising you that the procedure was successful.

7. Click Finish to exit the installer.

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

9. In the Websense Manager, configure the Usage Monitor to send Usage Alerts by selecting Server > Settings > Alerts and Notifications. See the Websense Enterprise Administrator’s Guide for details.
Chapter 4: Installing Websense Enterprise

**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 transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

2. Following the **Custom** installation path brings you to the component selection screen. Select **RADIUS Agent** and click **Next**. Setup asks you to identify the machine on which the Policy Server is installed.

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click **Next**. If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the card you want RADIUS Agent 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 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:

---

**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.
Chapter 4: Installing Websense Enterprise

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

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

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

If you are using the online installer, the Download Manager progress bars are displayed as 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

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

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

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

9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. See the User Identification chapter in the Websense Enterprise *Administrator’s Guide* for instructions.

**eDirectory Agent**

The Websense 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 machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

2. Following the **Custom** installation path brings you to the component selection screen. Select **eDirectory Agent** and click **Next**.
Chapter 4: Installing Websense Enterprise

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

3. Enter the IP address of the Policy Server machine, and the port number if different from the default, and then click Next.
   If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address appear in a list.

4. Select the card you want eDirectory Agent 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 then click Next to continue.
   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:
   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.
   A summary list appears, showing the installation path, the installation size, and the components that will be installed.

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.
7. Click **Next** to start the installation.
   If you are using the online installer, 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.
   When the installer is finished, a message appears advising you that the procedure was successful.

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

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

10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the Websense Enterprise Administrator’s Guide.

**Logon Agent**

The Websense Logon Agent detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from `LogonApp.exe`, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, refer to *Creating and Running the Script for Logon Agent*, page 198.

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 machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.
2. Following the **Custom** installation path brings you to the component selection screen. Select **Logon Agent** and click **Next**.
Chapter 4: Installing Websense Enterprise

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 the port number if different from the default, and then click **Next**.

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

4. Select the card you want Logon Agent 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 then click **Next** to continue.

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

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

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

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

If you are using the online installer, the Download Manager progress bars are displayed as 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click **Next** to continue.

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

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

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

9. Set up the required logon script by following the instructions in *Creating and Running the Script for Logon Agent*, page 198.

10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the Websense Enterprise *Administrator’s Guide*.

**Remote Filtering Server**

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. (For Remote Filtering Client installation instructions, see *Remote Filtering Client*, page 135.)

**NOTE**

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

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and
Chapter 4: Installing Websense Enterprise

tertiary Remote Filtering Server. If the primary server is unavailable, the client will attempt to connect with the secondary, then the tertiary, then the primary again, and so on.

<table>
<thead>
<tr>
<th>IMPORTANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>✷ Install only one primary Remote Filtering Server for each Filtering Service in your network.</td>
</tr>
<tr>
<td>✷ Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.</td>
</tr>
<tr>
<td>✷ Remote Filtering Server is supported on Windows Server 2003 only if Service Pack 1 has been installed.</td>
</tr>
<tr>
<td>✷ Do not enable DHCP on the Remote Filtering Server machine.</td>
</tr>
</tbody>
</table>

To install the Remote Filtering Server on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

2. Following the **Custom** installation path brings you to the component selection screen. Select **Remote Filtering Server** and click **Next**.

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

3. Select the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and click **Next**.

   Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. Setup asks you to provide connection information for this machine.
4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall.

---

**IMPORTANT**

The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 210.
6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall.

   **IMPORTANT**
   Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see *Firewall Configuration for Remote Filtering*, page 210.

7. Click **Next** to continue.

   Setup asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

8. Before selecting a **pass phrase**, consider the following requirements:
   - If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
Chapter 4: Installing Websense Enterprise

- If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.
- If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.
- The pass phrase must include only ASCII characters.
- You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See Remote Filtering Server Connection Information, page 137.)

9. Enter and confirm your pass phrase.

**IMPORTANT**
Be sure to record your pass phrase and keep it in a safe place, as you will not be able to retrieve it from the Websense system later.

10. Click Next to continue.
Remote Filtering Server must be able to communicate with the Websense Filtering Service. Setup asks you to identify the machine on which the Filtering Service is installed.

![Image of Filtering Service Information dialog box]

- **Filter port**: 16086
- **Block Page port**: 16271

Integrated Cisco Products ▶ 131
11. In the first field, enter the actual (internal) IP address of the Filtering Service machine.

12. Is there a firewall or other network device that performs network address translation between the Filtering Service machine and this machine?
   - If yes, enter the translated (external) IP address of the Filtering Service machine.
   - If no, click to deselect the checkbox and grey out the Translated (external) IP address of Filtering Service field.

13. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.

   **IMPORTANT**
   
   The filter port is the default communication port used by the installer to install the Filtering Service. If you installed the Filtering Service using a different communication port, enter that port number.

14. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.

   **IMPORTANT**
   
   If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see Firewall Configuration for Remote Filtering, page 210.

15. Click Next.

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

16. Accept the default path (C:\Program Files\Websense) or click Browse to locate another installation folder, and then click Next to continue.
The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:

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

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

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

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

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

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

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

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

**Remote Filtering Client Pack**

The Remote Filtering Client Pack is an installer package that allows you to install the Remote Filtering Client. Once you have this installer package, you can use it to deploy the Remote Filtering Client on Windows workstations (see *Remote Filtering Client*, page 135). The Remote Filtering Client Pack can be installed on Windows machines only.

**NOTE**

To enable the Remote Filtering components, you must subscribe to the remote filtering service.
To install the Remote Filtering Client Pack on a Windows machine:

1. Download and start the Windows installer using the procedure in *Windows Procedures*, page 104.

2. Following the Custom installation path brings you to the component selection screen. Select Remote Filtering Client Pack and click Next. Setup asks you to select an installation folder for the Remote Filtering Client Pack.

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

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed:
   
   - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
   - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

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

4. Click Next to start the installation.

   If you are using the online installer, the Download Manager progress bars are displayed as 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 on this machine, a message reminds you that features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Click Next to continue.

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

5. Click Finish to exit the installer.

6. If you stopped your antivirus software, remember to start it again after Websense components have been installed.
7. If you accepted the default installation path in Step 3, the Remote Filtering Client Pack can be found in the following location:

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

8. Use the Remote Filtering Client Pack to install the Remote Filtering Client on user workstations that you want to filter when they are outside the network firewall. See Remote Filtering Client, page 135 for details.

**Remote Filtering Client**

The Remote Filtering Client is installed on workstations that will be used outside the network firewall. This component connects with a Remote Filtering Server located inside the network firewall to enable web filtering on the remote workstation. The Remote Filtering Client installs on Windows only.

---

**NOTE**

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

---

The Remote Filtering Client can be installed in the following ways:


- **Automatic deployment with third-party tool**: Use the Remote Filtering Client Pack and a third-party deployment tool to automatically deploy the Remote Filtering Client to user workstations. See Installing Remote Filtering Client with a Third-Party Deployment Tool, page 140 for information.

- **Deployment as part of CPM Client Agent (Websense Client Policy Manager™ users only)**: If you purchased a subscription to the Websense Client Policy Manager™ (CPM), it is not necessary to install the Remote Filtering Client. The Remote Filtering Client application is included as part of the CPM Client Agent, so it will be deployed automatically when you deploy the CPM Client Agent to user workstations. Refer to your Websense Client Policy Manager documentation for more information.


**WARNING**

Do not install the Remote Filtering Client on:

- Machines running Windows 2000, Service Pack 2 or earlier. The installation will fail. See the Websense Enterprise Deployment Guide for information about system requirements.
- Machines where you installed the Remote Filtering Server. A Remote Filtering Client running on the same machine as the Remote Filtering Server will eventually cause remote filtering to fail.

---

**Manual Installation of Remote Filtering Client**

To manually install the Remote Filtering Client on a single Windows workstation:

1. Make sure that the Remote Filtering Server with which this client will connect has been correctly installed on a separate machine. See Remote Filtering Server, page 127 for Windows installation instructions; see Remote Filtering Server, page 160 for Solaris and Linux installation instructions.

2. Install the Remote Filtering Client Pack on the workstation as described in Remote Filtering Client Pack, page 133. Or, if you have already installed the Remote Filtering Client Pack on another machine, you can simply copy the CPMClient.msi file to a folder on the installation workstation. If you selected the default installation path of C:\Program Files\Websense, this file will be located at:

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

3. Double-click the CPMClient.msi file.
   
   The installer for Remote Filtering Client will open.

4. Click Next to continue.

   Remote Filtering Clients must be able to connect with a Remote Filtering Server from outside your organization’s internet gateway or firewall. You are asked to provide connection information for the Remote Filtering Servers that this client will use for web filtering.
Chapter 4: Installing Websense Enterprise

Remote Filtering Server Connection Information

The Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

5. In the Primary Remote Filtering Server section of the screen, enter connection information for the Remote Filtering Server that you want this client to attempt to connect with first:
Chapter 4: Installing Websense Enterprise

- Enter the externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine in the **External IP or Domain Name** field.

**IMPORTANT**

You must use the same external address in the **same address format**—IP address or FQDN—that you entered when you installed this Remote Filtering Server. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address in this field. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

- In the **Port** field to the right of the **External IP or Domain Name** field, enter the port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.

- Enter the internal IP address or machine name of the primary Remote Filtering Server machine in the **Internal IP or Hostname** field.

- In the **Port** field to the right of the **Internal IP or Hostname** field, enter the port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when this Remote Filtering Server was installed.

**NOTE**

If the Remote Filtering Client is on a notebook computer that is used both inside and outside the network firewall, this port allows Websense to determine where the machine is located and filter it appropriately. The machine will be filtered in the same way as an internal client when it is used inside the organization’s network firewall, and by the Remote Filtering Service when it is used remotely.
6. If you have installed the optional secondary and tertiary Remote Filtering Servers to provide failover protection for the primary Remote Filtering Server, enter connection information for these servers in the **Secondary Remote Filtering Server** and **Tertiary Remote Filtering Server** sections of the screen.

7. In the **Encryption and Authentication** section, do one of the following:
   - Select **Passphrase** and enter the same pass phrase that was entered in the **Pass Phrase** field during installation of the primary Remote Filtering Server. (The secondary and tertiary Remote Filtering Servers must have the same pass phrase as their primary Remote Filtering Server.)
   - OR-
   - Select **Encrypted Key** and enter the encrypted key (shared secret) created from the pass phrase and unpublished Remote Filtering Server keys. The encrypted key can be found in the `WSSEK.dat` file on the Remote Filtering Server machine. If you selected the default installation path, this file will be located at:
     
     ```
     C:\Program Files\Websense\bin\WSSEK.dat
     ```
     
     on Windows machines, and
     
     ```
     /opt/Websense/bin/WSSEK.dat
     ```
     
     on Solaris and Linux machines.

8. Click **Next** to continue.

9. Click **Install** to begin installation.

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

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

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

    If no message appears, restarting the machine is not required.
Installing Remote Filtering Client with a Third-Party Deployment Tool

Before deploying the Remote Filtering Client to user workstations, make sure that the Remote Filtering Server with which these clients will connect has been correctly installed on a separate machine. See Remote Filtering Server, page 127 for Windows installation instructions; see Remote Filtering Server, page 160 for Solaris and Linux installation instructions.

To obtain the installer for the Remote Filtering Client, install the Remote Filtering Client Pack on a Windows machine (see Remote Filtering Client Pack, page 133 for instructions). If you selected the default installation path of C:\Program Files\Websense, the installer is placed in the following location:

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

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

Command Line Parameters for Remote Filtering Client Installation

This section provides the command line parameters required to install the Remote Filtering Client using a third-party deployment tool.

Remote Filtering Clients are installed on user workstations or notebook computers that are used outside your organization’s internet gateway or firewall. These machines must be able to connect with a Remote Filtering Server that is located inside the internet gateway or firewall.

Each Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. The Remote Filtering Client will attempt to connect with the primary Remote Filtering Server first, then the secondary, then the tertiary, then the primary again, and so on.

Below are the necessary command line parameters for installing the Remote Filtering Client with a third-party deployment tool:

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>These parameters are not case sensitive.</td>
</tr>
</tbody>
</table>
The following parameters must be configured to allow the Remote Filtering Client to communicate with the primary Remote Filtering Server:

- **PRIMARY_WISP_ADDRESS=<external IP address or FQDN of primary Remote Filtering Server>**
  The externally visible address for the primary Remote Filtering Server machine, as entered in the **External IP Address or Host Name** field when the primary Remote Filtering Server was installed.

- **IMPORTANT**
  This must be the same external address in the **same address format**—IP address or FQDN—that was entered when this Remote Filtering Server was installed. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address here. If you entered a machine name in the form of a fully qualified domain name (FQDN), you must enter the same FQDN here.

- **PRIMARY_WISP_PORT=<external port number of primary Remote Filtering Server>**
  The port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.

- **PRIMARY_INTERNAL_WISP_ADDRESS=<internal IP address or FQDN of primary Remote Filtering Server>**
  The internal address, visible from inside the network firewall, for the machine on which the primary Remote Filtering Server is installed.

- **PRIMARY_INTERNAL_WISP_PORT=<internal port number of primary Remote Filtering Server>**
  The port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when the Remote Filtering Server was installed.
If secondary and tertiary Remote Filtering Servers have been installed, use the following parameters to configure communication with them:

- **SECONDARY_WISP_ADDRESS**=<external IP address or FQDN of secondary Remote Filtering Server>
- **SECONDARY_WISP_PORT**=<external IP address or FQDN of secondary Remote Filtering Server>
- **SECONDARY_INTERNAL_WISP_ADDRESS**=<internal IP address or FQDN of secondary Remote Filtering Server>
- **SECONDARY_INTERNAL_WISP_PORT**=<internal IP address or FQDN of secondary Remote Filtering Server>
- **TERTIARY_WISP_ADDRESS**=<external IP address or FQDN of tertiary Remote Filtering Server>
- **TERTIARY_WISP_PORT**=<external IP address or FQDN of tertiary Remote Filtering Server>
- **TERTIARY_INTERNAL_WISP_ADDRESS**=<internal IP address or FQDN of tertiary Remote Filtering Server>
- **TERTIARY_INTERNAL_WISP_PORT**=<internal IP address or FQDN of tertiary Remote Filtering Server>

These addresses and port numbers must match those entered during installation of the Remote Filtering Servers, as noted above for the primary Remote Filtering Server.

- **PATH**=<installation path>
  Directory where the Remote Filtering Client will be installed on each client workstation. If this parameter is not specified, the default installation path is `C:\PROGRAM FILES\Websense\WDC`, and the WDC directory is hidden by default.

- **PASSPHRASE**=<pass phrase for Remote Filtering Server>
  The Pass Phrase entered when the primary Remote Filtering Server was installed. Note that all Remote Filtering Servers in the same failover group (primary, secondary, and tertiary) must have the same pass phrase.
Chapter 4: Installing Websense Enterprise

- **REBOOT=YES | NO | PROMPT | IF_NEEDED_PROMPT**
  This parameter defines whether the client workstation is automatically restarted after the Remote Filtering Client is installed (or uninstalled). Values for this parameter are:
  - **YES**: Machines are restarted, and employees are not prompted to restart.
  - **NO**: Machines are not restarted, and employees are not prompted to restart.
  - **PROMPT**: Employees are prompted to restart their machines.
  - **IF_NEEDED_PROMPT**: Employees are prompted to restart their machines only if a restart is required. (Default.)

- **IMPORTANT**
  You must restart the workstation after installing the Remote Filtering Client if:
  - The workstation’s operating system is Windows 2000.
  - Check Point® VPN-1® is running on the workstation.

  You must *always* restart the workstation after uninstalling, upgrading, or repairing the Remote Filtering Client.

- **REINSTALL=ALL**
  This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It indicates the components to remove and reinstall. The value should always be set to **ALL**.

- **REINSTALLMODE=veums | voums**
  This parameter is used only when repairing or upgrading an existing installation of Remote Filtering Client. It defines either a repair or an upgrade. The possible values are:
  - **veums**: for repairs only
  - **voums**: for upgrades only

- **/qn**
  Switch for quiet installation mode. When you use this option, Remote Filtering Client will install without displaying information to the employee at the workstation. If you do not use /qn, the installer launches in interactive mode and installation dialog boxes display to the employee during installation. Most organizations choose the quiet mode, as interactive mass deployment has little value.
Chapter 4: Installing Websense Enterprise

Installation Syntax

The following is an example of the syntax to install the Remote Filtering Client on employee workstations using a third-party deployment tool. Replace the variables in angle brackets with appropriate values for your network, and type the command on a single line with no returns.

```
msiexec /i cpmclient.msi PASSPHRASE=<pass phrase for Remote Filtering Server>
PRIMARY_WISP_ADDRESS=<external IP Address or FQDN of primary Remote Filtering Server>
PRIMARY_WISP_PORT=<external port number of primary Remote Filtering Server>
PRIMARY_INTERNAL_WISP_ADDRESS=<internal IP address or host name of primary Remote Filtering Server>
PRIMARY_INTERNAL_WISP_PORT=<internal port number of primary Remote Filtering Server>
REBOOT=<reboot parameter> /qn
```

For example, the installation command might look like this:

```
msiexec /i cpmclient.msi PASSPHRASE=2gbatfM
PRIMARY_WISP_ADDRESS=63.16.200.232
PRIMARY_WISP_PORT=80
PRIMARY_INTERNAL_WISP_ADDRESS=10.218.5.60
PRIMARY_INTERNAL_WISP_PORT=9000
REBOOT=IF_NEEDED_PROMPT /qn
```

If you are using secondary or tertiary Remote Filtering Servers, you must enter parameters for those machines as well.

Repair Syntax

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

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

When the installer repairs an installation of the Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration has not changed, no additional parameters are necessary. However, if you
have changed your configuration, you must include the appropriate parameters and new values in the command.

**NOTE**
For the syntax required to upgrade Remote Filtering Clients to a new version, see *Upgrading Remote Filtering Client with a Third-Party Deployment Tool*, page 54.

**Uninstall Command**

The following is the actual command that can be used to uninstall the Remote Filtering Client with a third-party deployment tool. This command must be typed on a single line with no returns.

```bash
msiexec.exe /x - {14D74337-01C2-4F8F-B44B-67FC613E5B1F} /qn
```

**Solaris and Linux Procedures**

The steps in this section are common to all separate installations of Websense Enterprise 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. Close all applications and stop any antivirus software.
3. Create a setup directory for the installer files.
   For example: `/root/Websense_setup`
   - **Solaris**: `Websense62Setup_Slr.tar.gz`
   - **Linux**: `Websense62Setup_Lnx.tar.gz`

If you download the installer file for your operating system from the website, you can choose between the following two versions:

- **Dynamic installer**: an online installer that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
Chapter 4: Installing Websense Enterprise

- **Full installer**: a complete offline installer. It is much larger than the online Dynamic installer, and contains all the files needed to install Websense Enterprise components. Use this installer only if you experience difficulties with the online installer.

5. Enter the following command to unzip the installer file:
   
   ```
   gunzip <download file name>
   ```
   
   For example: `gunzip Websense62Setup_Slr.tar.gz`

6. Expand the file into its components with the following command:
   
   ```
   tar xvf <unzipped file name>
   ```
   
   For example: `tar xvf Websense62Setup_Lnx.tar`

   This places the following files into the setup directory:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.sh</td>
<td>Installation program</td>
</tr>
<tr>
<td>Setup</td>
<td>Archive file containing related installation files and documents.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Release Notes: An HTML file containing release notes and last minute information about Websense. Read this file with any supported browser.</td>
</tr>
</tbody>
</table>

7. Run the installation program from the setup directory with the following command:
   
   ```
   ./install.sh
   ```

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

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

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

8. Follow the onscreen instructions through the subscription agreement.

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

10. To continue, proceed to the appropriate component section.
Websense 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 145.

2. Following the Custom installation path brings you to a list of components to install. Select Websense Manager and press Enter.

   The installer asks you for the location of your web browser.

3. Provide the full path to the web browser to use when viewing online Help.

   The installer asks you to provide a path to the installation directory in which it can create the /Manager subdirectory and install Websense Manager.

4. Enter the path to the installation directory, or accept the default installation directory (/opt/Websense). If this directory does not already exist, the installer will create it.

   IMPORTANT
   The full installation path must use only ASCII characters.

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

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

A summary list appears, showing the installation path, the installation size, and the component (Websense Manager) you have selected.

5. Press Enter to begin installing the Websense Manager.
If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic. Press Enter to continue.

A message appears advising you that the installation has been successful.

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

**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 installation is part of a multiple deployment of the Network Agent (for load balancing purposes), you must be sure that the IP address ranges for each instance of the Network Agent do not overlap. This will result in double logging. Deploy the Network Agents so that they can filter the entire network. Partial deployment will result in incomplete filtering by protocol and bandwidth, as well as the loss of log data from network segments not watched by the Network Agent. For instructions on defining IP address ranges for multiple Network Agents, refer to the Websense Enterprise Administrator’s Guide. For detailed information about deploying Network Agent, refer to the Websense Enterprise Deployment Guide.

*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.
Chapter 4: Installing Websense Enterprise

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 164.

**IMPORTANT**
The Websense Filtering Service and the Policy Server must be installed and running prior to installing the Network Agent, or installed at the same time as 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 145.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Network Agent** and press **Enter**. The installer 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 the port number if different from the default, and then press **Enter**. Setup displays information about Network Agent. The machine on which the Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly.

**IMPORTANT**
If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.
Chapter 4: Installing Websense Enterprise

You are given the following two options:

- **Continue installation**: If the installation machine has the necessary internet traffic visibility, select this option to install Network Agent.
- **Exit Setup**: If 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.

The installer asks you if this machine is running a firewall.

4. 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 **Yes** if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install the Network Agent 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.

All enabled network interface cards (NICs) on the machine appear in a list.

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

**NOTE**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 208.
Chapter 4: Installing Websense Enterprise

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

6. Enter the IP address of the Filtering Service machine, and the port number if different from the default, and then press Enter.

The installer asks if you want to allow Websense, Inc. to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.

7. Select a Network Agent feedback option, and then press Enter.

The installer asks you for the location of the installation directory.

8. Enter the path to the installation directory, or accept the default Websense installation directory (/opt/Websense). If this directory does not already exist, the installer will create it.

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.

**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.

**NOTE**

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

**IMPORTANT**

The full installation path must use only ASCII characters.
Chapter 4: Installing Websense Enterprise

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

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

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

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

10. Exit the installer when the success message appears.

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

12. Configure Network Agent for use in your network. Refer to the instructions for initial configuration of Network Agent in *Chapter 5: Initial Setup*, as well as the Network Agent chapter of the Websense Enterprise *Administrator’s Guide*.

**Usage Monitor**

Usage Monitor tracks users’ internet activity and sends alerts when internet activity for particular URL categories or protocols reaches threshold limits you have configured. You can have only one instance of Usage Monitor for each Policy Server in your network.

To install Usage Monitor on Solaris or Linux:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 145.

2. Following the **Custom** installation path brings you to a list of components to install. Select **Usage Monitor** and press **Enter**.

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

3. Select the card you want Usage Monitor to use to communicate and press **Enter**.
Chapter 4: Installing Websense Enterprise

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

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

The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (/opt/Websense). If this directory does not already exist, the installer will create it.

IMPORTANT
The full installation path must use only ASCII characters.

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

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

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

6. Press Enter to begin installation.

If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

7. Exit the installer when the success message appears.

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

9. In the Websense Manager, configure the Usage Monitor to send Usage Alerts by selecting **Server > Settings > Alerts and notifications**. See the Websense Enterprise Administrator’s Guide for details.

**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 transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.

To install the RADIUS Agent on Solaris or Linux:

1. Download and start the installer using the procedure in *Solaris and Linux Procedures*, page 145.

2. Following the **Custom** installation path brings you to a list of components to install. Select **RADIUS Agent** and press **Enter**.

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

3. Select the card you want RADIUS Agent 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.
Chapter 4: Installing Websense Enterprise

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

The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

---

**IMPORTANT**

The full installation path must use only ASCII characters.

---

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

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

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

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

If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

7. Exit the installer when the success message appears.

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

9. Configure the RADIUS Agent, and configure your environment for RADIUS Agent. See the User Identification chapter in the Websense Enterprise *Administrator’s Guide* for instructions.
Chapter 4: Installing Websense Enterprise

**eDirectory Agent**

The Websense 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 145.

2. Following the **Custom** installation path brings you to a list of components to install. Select **eDirectory Agent** and press **Enter**.

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

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

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

4. Select the card you want eDirectory Agent to use to communicate and press **Enter**.

   The installer asks for the Novell eDirectory name and password.

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

   The installer asks you for the location of the installation directory.

6. Enter the path to the installation directory, or accept the default Websense installation directory (`/opt/Websense`). If this directory does not already exist, the installer will create it.

   **IMPORTANT**

   The full installation path must use only ASCII characters.
Chapter 4: Installing Websense Enterprise

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

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

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

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

   If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

8. Exit the installer when the success message appears.

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

10. Configure the eDirectory Agent and Novell eDirectory by following the instructions in the User Identification chapter of the Websense Enterprise Administrator’s Guide.

**Logon Agent**

The Websense Logon Agent detects users as they log on to Windows domains in your network via client machines. The Logon Agent receives logon information from `LogonApp.exe`, a separate client application that runs only on Windows client machines, and must be run by a logon script. For information about setting up this script in your network, refer to *Creating and Running the Script for Logon Agent*, page 198.

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.
Chapter 4: Installing Websense Enterprise

To install the Logon Agent on a Solaris or Linux system:

1. Download and start the installer using the procedure in Solaris and Linux Procedures, page 145.

2. Following the Custom installation path brings you to the component selection screen. Select Logon Agent and press Enter.

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

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

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

4. Select the card you want Logon Agent to use to communicate and press Enter.

   The installer asks you for the location of the installation directory.

5. Enter the path to the installation directory, or accept the default Websense installation directory (/opt/Websense). If this directory does not already exist, the installer will create it.

   The full installation path must use only ASCII characters.
Chapter 4: Installing Websense Enterprise

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

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

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

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

   If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

7. Exit the installer when the success message appears.

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

9. Set up the required logon script by following the instructions in *Creating and Running the Script for Logon Agent*, page 198.

10. Configure Logon Agent to communicate with client workstations and the Filtering Service by following the instructions in the User Identification chapter of the Websense Enterprise Administrator’s Guide.
Remote Filtering Server

The Remote Filtering Server provides web filtering for user workstations located outside the network firewall. In order to be filtered through the Remote Filtering Server, a remote workstation must be running the Remote Filtering Client. (For Remote Filtering Client installation instructions, see Remote Filtering Client, page 135.)

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

The Remote Filtering Server should be installed on a separate, dedicated machine. This machine must be able to communicate with the Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine does not have to be joined to a domain.

To provide failover capability for the primary Remote Filtering Server, you can install secondary and tertiary Remote Filtering Servers. Each Remote Filtering Client can be configured to connect with a primary, secondary, and tertiary Remote Filtering Server. If the primary server is unavailable, the client will attempt to connect with the secondary, then the tertiary, then the primary again, and so on.

IMPORTANT
- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- Do not install the Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
- Do not enable DHCP on the Remote Filtering Server machine.

To install the Remote Filtering Server on Solaris or Linux:

1. Download and start the installer using the procedure in Solaris and Linux Procedures, page 145.

2. Following the Custom installation path brings you to a list of components to install. Select Remote Filtering Server and press Enter.
If the installation machine is multihomed, all enabled network interface cards (NICs) with an IP address are displayed.

3. Select the card you want the Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and press Enter.

Remote Filtering Clients must be able to connect to the Remote Filtering Server, both from inside and from outside the internet gateway or network firewall. Setup asks you to provide connection information for this machine.

4. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from outside the firewall.

5. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from outside the network firewall.

<table>
<thead>
<tr>
<th><strong>IMPORTANT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The port entered as the <strong>External Communication Port</strong> must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see <em>Firewall Configuration for Remote Filtering</em>, page 210.</td>
</tr>
</tbody>
</table>

6. In the **Internal Communication Port** field, enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from inside the network firewall.

<table>
<thead>
<tr>
<th><strong>IMPORTANT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Be sure that your network firewall is configured to block connections to the <strong>Internal Communication Port</strong> from workstations located outside the firewall. For more information, see <em>Firewall Configuration for Remote Filtering</em>, page 210.</td>
</tr>
</tbody>
</table>
Chapter 4: Installing Websense Enterprise

Setup asks you to enter a pass phrase of any length for the Remote Filtering Server. This pass phrase will be combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

7. Before selecting a pass phrase, consider the following requirements:
   - If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
   - If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.
   - If you want this installation of the Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.
   - The pass phrase must include only ASCII characters.
   - You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server. (See Remote Filtering Server Connection Information, page 137.)

8. Enter and confirm your pass phrase.

   IMPORTANT
   Be sure to record your pass phrase and keep it in a safe place, as you will not be able to retrieve it from the Websense system later.

Setup asks you to provide information about the machine on which the Websense Filtering Service is installed.

9. Enter the actual (internal) IP address of the Filtering Service machine.
   Setup asks if there is a firewall or other network device that performs network address translation between the Filtering Service machine and this Remote Filtering Server machine.

10. Enter yes or no.
    - If you entered yes, Setup asks for the translated (external) IP address of the Filtering Service machine, visible to this machine. Enter the translated IP address.
11. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.

**IMPORTANT**
The filter port is the default communication port used by the installer to install the Filtering Service. If you installed the Filtering Service using a different communication port, enter that port number.

12. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.

**IMPORTANT**
If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from the Remote Filtering Server, and serve block pages to remote users. For more information, see *Firewall Configuration for Remote Filtering*, page 210.

The installer asks you for the location of the installation directory.

13. Enter the path to the installation directory, or accept the default Websense installation directory (/opt/Websense). If this directory does not already exist, the installer will create it.

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

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.
Chapter 4: Installing Websense Enterprise

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

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

14. Press **Enter** to begin installation.

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

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

15. Exit the installer when the success message appears.

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

Modifying an Installation

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

- Add Websense components.
- Remove Websense components.
- Repair existing Websense components.

Adding Components

After installing Websense Enterprise, you may want to add components to change the configuration of Websense in your network. The following procedures assume that the Filtering Service, Policy Server, User Service, Usage Monitor, and Websense Manager (Solaris and Windows only) are already installed, and that additional components are going to be added. If you are adding remote components, the installer will ask you for the location of the Policy Server.
Chapter 4: Installing Websense Enterprise

Windows

To add Websense Enterprise components in a Windows environment:

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

   **NOTE**
   Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This will allow you to restore your current system with a minimum of downtime, should you decide to do so.

2. Close all applications and stop any antivirus software.

3. Run one of the following Websense Enterprise installers:
   - **Web download**: Download one of the following packages from [http://www.websense.com/global/en/downloads](http://www.websense.com/global/en/downloads) to a folder on the installation machine and double-click to extract the installer files.
   - **Dynamic installer**: This version of Websense62Setup.exe is an online installer package that requires web access during installation. It downloads the necessary product files from the website as needed after product selections have been made.
   - **Full installer**: This version of Websense62Setup.exe is a complete offline installer. It is much larger than the online Dynamic installer package, and contains all the files needed to install Websense Enterprise components. Use this package only if you experience difficulties with the online installer.

   **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.
Chapter 4: Installing Websense Enterprise

- **Product CD**: The product CD contains all the files needed to install Websense Enterprise components. Run Websense62.exe from the Websense Enterprise v6.2 product CD. (This file will run automatically if autorun is enabled.) Select **Install** on the start screen to begin.

A screen displays instructions for extracting the setup program.

![Installer File Extraction Screen](image)

**Installer File 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.

**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.

b. Click **Extract** to begin decompressing the files.
Chapter 4: Installing Websense Enterprise

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.

4. 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.

5. Select Add Websense components and click Next.
   Setup displays a product selection screen.

   ![](Websense Product Selection Screen)

6. Select Websense Enterprise and click Next to continue.
   The installer displays a list of components not currently installed on the installation machine.
Chapter 4: Installing Websense Enterprise

Component Selection Screen

7. Select the components you want to install and click Next.
If you are installing the Real-Time Analyzer and are using IIS as your web server, you are prompted to select the name of the website in the IIS Manager under which the installer should create a virtual directory. The default value is Default Web Site, which is correct in most instances.

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

If you are installing Network Agent, the installer displays a screen describing the features enabled by the Network Agent.

---

**IMPORTANT**

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

---

**Network Agent Installation**

You are given the following two options:

- **Install Network Agent**: If the installation machine has the necessary internet traffic visibility, select this option to install the Network Agent.
- **Do not install Network Agent**: Select this option to continue without installing the Network Agent. Network Agent can be installed on this machine later, or installed on another machine.
9. Click Next to continue.
   If you are installing Network Agent, the installer asks you if this machine is running a firewall. Network Agent cannot function properly on a machine that is being used as a firewall.

10. Select Yes or No and click Next to continue:
   - Select Yes if you are attempting to install Network Agent on a firewall machine, and Setup will exit. Install the Network Agent 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 you are installing the Network Agent, 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.

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

   ![NOTE]
   After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See Testing Visibility of Internet Traffic to Network Agent, page 208.

12. Click Next to continue.
   If you are installing Network Agent, a screen appears asking if you want to allow Websense, Inc. to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering.

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

13. Select a Network Agent feedback option and click Next to continue.
If you 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**

14. Enter the domain and user name, followed by the network password for an account with domain privileges, 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 amount.

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

15. Click **Next** to begin installation.
Chapter 4: Installing Websense Enterprise

If you are using the online installer, 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

A message announcing the success of the installation is displayed.

16. 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.

**NOTE**

Before you can access Real-Time Analyzer and other Websense Reporting Tools, you must first log on to Websense Manager and configure user permissions. See the Websense Enterprise Administrator’s Guide for more information.

- 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.

17. If you stopped your antivirus software, be sure to start it again.
Chapter 4: Installing Websense Enterprise

Solaris or Linux

To add Websense Enterprise components in a Solaris or Linux environment:

1. Log on to the installation machine as the root user.
2. Close all applications and turn off any antivirus software.
3. Run the installation program from the directory where it resides using the following command:
   
   ./install.sh

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

   ./install.sh -g

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

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

4. Select Add Websense 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 are installing Network Agent, the installer displays a screen describing the features enabled by the Network Agent.

**NOTE**

Before adding new components, we recommend that you perform a full system backup as a fallback strategy. This will allow you to restore your current system with a minimum of downtime, should you decide to do so.

**IMPORTANT**

The machine on which the Network Agent is installed must be able to monitor 2-way employee internet traffic to function correctly. If you install Network Agent on a machine that cannot monitor the targeted traffic, Network Agent features such as Dynamic Protocol Management, Bandwidth Optimizer, and IM Attachment Manager will not perform as expected.
You are given the following two options:

- **Install Network Agent**: If the installation machine has the necessary internet traffic visibility, select this option to install the Network Agent.
- **Do not install Network Agent**: Select this option to continue without installing the Network Agent. Network Agent can be installed on this machine later, or installed on another machine.

6. 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. Install the Network Agent on a machine that is not running a firewall.

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

**NOTE**

After installation, you can run the Traffic Visibility Tool to test whether the selected NIC can see the appropriate user internet traffic. See *Testing Visibility of Internet Traffic to Network Agent*, page 208.
• **Network Agent Feedback**: If you are installing Network Agent, the installer asks if you want to allow Websense, Inc. to gather information about the use of Websense-defined protocols. Information will be used in the development of protocol filtering. Select a Network Agent feedback option and continue.

**NOTE**

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

• **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
  - If the installation machine has less than the recommended amount of memory, the installation can continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

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

7. Press **Enter** to accept this installation configuration and to begin installing the displayed Websense Enterprise components.

   If you are using the online installer, the Download Manager copies 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 features such as Protocol Management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to internet traffic.

8. Exit the installer when the success message appears.

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

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

**NOTE**
Before removing components, we recommend that you perform a full system backup as a fallback strategy.

To remove installed Websense Enterprise components in a Windows environment:

1. Log on to the installation machine with local administrator privileges.
2. Close all applications and stop any antivirus software.
3. Go to the Windows Add or Remove Programs dialog box:
   - *Windows 2003*: Select **Start > Control Panel > Add or Remove Programs**.
   - *Windows 2000*: Select **Start > Settings > Control Panel**, and then double-click **Add/Remove Programs**.
4. Select **Websense** from the list of installed applications.
5. Click **Change/Remove** to launch the Websense uninstaller.

There may be a delay of several seconds while the Websense uninstaller starts.

A list of installed components appears.
By default, all components are checked for removal.

6. To keep a component, remove the check mark from the box next to it. When all of the components you want to uninstall are checked, click **Next** to continue.

    **NOTE**
    
    If you are uninstalling Filtering Service, make sure that all associated Network Agents are uninstalled. If you try to uninstall Network Agent *after* its associated Filtering Service has been removed, the installer will be unable to stop Network Agent and will display an error message.

If the Policy Server is not running, a dialog box appears advising you that removing Websense 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.

7. Click **Next** to begin uninstalling the components.

    If you are uninstalling Network Agent on a remote machine after removing the Policy Server, expect the process to take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.

    A completion messages advises you when the procedure is finished.

8. Click **Next** to continue.

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

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

10. If you stopped your antivirus software, be sure to start it again.
Chapter 4: Installing Websense Enterprise

Solaris or Linux

To remove installed components on a Solaris or Linux machine:

1. Log on to the installation machine as the root user.
2. Close all applications and stop any antivirus software.
3. Run the following program from the Websense installation directory (default is /opt/Websense):
   ```
   ./uninstall.sh
   ```
   Run the GUI version of the installer with the following command:
   ```
   ./uninstall.sh -g
   ```
   If you are using a non-English based system, the installer will display an error message advising you that the GUI version is not supported.
   The installer detects the currently installed Websense Enterprise components and displays a list of installed components.
4. Make sure that only the components you want to remove are selected for removal.
5. 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.

   **NOTE**
   Before removing components, we recommend that you perform a full system backup as a fallback strategy.
Chapter 4: Installing Websense Enterprise

**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 message advises you when the procedure is finished.

6. Exit the installer.
7. If you stopped your antivirus software, be sure to start it again.

**Repairing an Installation**

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

**Windows**

Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

To repair your Websense Enterprise installation in a Windows environment:

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

---

**WARNING**

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

**NOTE**

To repair (reinstall) a Policy Server in a distributed environment, see *Repairing the Policy Server*, page 185 for instructions.

---
Chapter 4: Installing Websense Enterprise

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. Close all applications and stop any antivirus software.

**WARNING**
Be sure to close the Windows Event Viewer, or the repair may fail.

4. Run the Websense Enterprise installer.
5. Click **Next** on the welcome screen.
   The installer detects the current Websense Enterprise installation and asks if you want to add, remove, or repair components.
6. Select **Repair existing Websense components** and click **Next**.
   Setup advises you that it will repair the current installation by reinstalling the existing Websense components and asks if you want to continue.
7. Select **Yes** and click **Next**.
   A list of currently running Websense services appears. The message explains that the installer will stop these services before installation.
8. Click **Next** to begin installation.
Chapter 4: Installing Websense Enterprise

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

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

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

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

9. If you are repairing Filtering Service, Setup asks if you want to download the Websense Master Database now or at a later time using the Websense Manager. Select a database download option and click **Next**.

   **IMPORTANT**
   During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded.

If you have chosen to download the Master Database now, a progress bar appears. Because of its size, the database can take up to 20 minutes to download and decompress. When the database download is complete, a message appears announcing the status of the download. Click **Next** to continue.

A message announcing the success of the installation is displayed when the procedure is finished.

10. 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.
Chapter 4: Installing Websense Enterprise

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.

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

**Solaris or Linux**

Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

To repair Websense Enterprise components on a Solaris or Linux system:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any antivirus software.
3. Run the installation program from the directory where it resides by entering the following command:
   
   ```bash
   ./install.sh
   ```

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

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

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

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

4. Select **Repair existing Websense 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 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 Manager on Solaris, Setup prompts you for the location of the browser.
Chapter 4: Installing Websense Enterprise

- **System requirements check**: The installer compares the system requirements for the installation you have selected with the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.
  - If the installation machine has insufficient disk space, the selected components cannot be installed, and the installer will quit.
  - If the installation machine has less than the recommended amount of memory, the installation will continue. To ensure the best performance of the components you are installing, you should upgrade your machine’s memory to the recommended amount.

- **Services restarted**: The Websense services are restarted after the files are reinstalled.

- **Master Database Download**: If you are repairing Filtering Service, Setup asks if you want to download the Websense Master Database now or at a later time using the Websense Manager. Select a database download option and press **Enter** to continue.

  **IMPORTANT**
  During repair of the Filtering Service, the installer removes the existing Master Database. Websense filtering cannot resume until the new Master Database has been successfully downloaded, decompressed, and loaded.

  If you have chosen to download the Master Database now, a progress bar appears. Because of its size, the database can take up to 20 minutes to download and decompress. When the database download is complete, a message appears announcing the status of the download. Press **Enter** to continue.

  A message announcing the success of this installation is displayed when the procedure is finished. Press **Enter** to continue.

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 displays a screen asking if you want to launch the Websense Manager. By default, the Manager is selected for launch. Select **Finish** when you are ready to exit the installer.

6. If you stopped your antivirus software, be sure to start it again.
Chapter 4: Installing Websense Enterprise

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 187 for instructions.
2. Make a backup copy of the config.xml file and put it in a safe location.
3. Restart the Policy Server.
4. Stop the services of the distributed Websense Enterprise components on the individual machines. Refer to Stopping or Starting Websense Services, page 187 for instructions.
5. Close all open applications on the Policy Server machine, and stop any antivirus software.
6. 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.
7. Select Repair existing Websense components when prompted. For specific instructions, refer to Repairing an Installation, page 180.
8. When the installer is finished repairing the system, exit the installer and stop the newly installed Policy Server.

NOTE
Before repairing components, we recommend that you perform a full system backup as a fallback strategy.

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.
9. Replace the config.xml file created by the repair procedure with your backup copy.

10. Restart the Policy Server.

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

12. Restart the services of the remote Websense Enterprise components.

13. Reload the Websense Master Database.

**Migrating between Integrations After Installation**

If you plan to change the Cisco integration with which Websense Enterprise interacts (from PIX Firewall to an IOS Router, for example), you may do so after you install Websense Enterprise v6.2 without losing any of your configuration data.

The following procedure assumes that the Policy Server is installed on the same machine as the Filtering Service. If the Policy Server is installed on a separate machine, no changes need to be made to that component, and there is no need to back up the config.xml file.

To migrate between Cisco integration products after installing Websense Enterprise v6.2:

1. Install and configure your new Cisco integration product on your network. Make sure it is deployed so that it can communicate with the Websense Enterprise machine (the machine running Filtering Service and Policy Server). Refer to *Websense Deployment* in Chapter 2: Network Configuration and your Cisco documentation for instructions.

2. Make backup copies of the following files (found in Websense\bin) and copy them to a location outside the Websense folder:
   - config.xml
   - eimserver.ini
   - websense.ini

3. Close all open applications on the Filtering Service machine, and stop any antivirus software.

4. Run the Websense Enterprise installer on the Filtering Service machine.
Chapter 4: Installing Websense Enterprise

5. Remove the Filtering Service using the procedures in *Removing Components*, page 176.

**WARNING**
Remove the Filtering Service only. *Do not* remove the Policy Server.

6. Restart the machine (Windows only).
7. Run the Websense Enterprise installer again.
8. Add the Filtering Service using the procedures in *Adding Components*, page 164.
9. When prompted to select an integration, select the new Cisco product (either *Cisco Adaptive Security Appliances*, *Cisco Content Engine*, *Cisco PIX Firewall*, or *Cisco Routers*).
10. Follow the onscreen instructions to complete the installation.
    The installer adds the new integration data to the `config.xml` file, without overwriting any of the previous configuration data.
11. Restart the machine (Windows only).
12. Check to be sure that the Filtering Service has started.
    Refer to *Stopping or Starting Websense Services*, page 187 for instructions on starting a service.
13. If you stopped your antivirus software, be sure to start it again.

**Stopping or Starting Websense Services**

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

Occasionally you may need to stop or start a Websense service. For example, you must stop the Filtering Service whenever you edit the `websense.ini` file, and after customizing default block messages.

**NOTE**
When 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
- Logon Agent
- Usage Monitor
- Remote Filtering Server

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 Server

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.
Chapter 4: Installing Websense Enterprise

### Windows 2000 Services List

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Services Session</td>
<td>Enables users to connect...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Themes</td>
<td>Provides user rights...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Uninterruptible Power Supply</td>
<td>Manages an uninterruptible...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Task Scheduler Manager</td>
<td>Manages task scheduling...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Virtual Disk Service</td>
<td>Provides virtual disk...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Diagnostics Service</td>
<td>Provides network diagnostics</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Network List Service</td>
<td>Provides network list...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Client</td>
<td>Enables web browsing...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Application Filtering Service</td>
<td>Filters and logs...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Policy Service</td>
<td>Enables web services...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Real-Time Analyzer</td>
<td>Displays real-time...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Usage Monitor</td>
<td>Tracks internet activity...</td>
<td>Started</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services User Service</td>
<td>Enables communication...</td>
<td>Started</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Wireless Configuration</td>
<td>Enables wireless...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Workstation</td>
<td>Provides network service...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
</tbody>
</table>

### Windows 2003 Services List

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Services Session</td>
<td>Enables users to connect...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Themes</td>
<td>Provides user rights...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Uninterruptible Power Supply</td>
<td>Manages an uninterruptible...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Task Scheduler Manager</td>
<td>Manages task scheduling...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Virtual Disk Service</td>
<td>Provides virtual disk...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Diagnostics Service</td>
<td>Provides network diagnostics</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Network List Service</td>
<td>Provides network list...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Client</td>
<td>Enables web browsing...</td>
<td>Disabled</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Application Filtering Service</td>
<td>Filters and logs...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Policy Service</td>
<td>Enables web services...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Real-Time Analyzer</td>
<td>Displays real-time...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services Usage Monitor</td>
<td>Tracks internet activity...</td>
<td>Started</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Web Services User Service</td>
<td>Enables communication...</td>
<td>Started</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Wireless Configuration</td>
<td>Enables wireless...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Workstation</td>
<td>Provides network service...</td>
<td>Started</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
</tbody>
</table>

Integrated Cisco Products ▶ 189
3. From the Action menu, select Start, Stop, or Restart or click one of the control buttons in the toolbar (Stop ■, Start ▶, or Restart ■ ▶). Restart stops the service, then restarts it again immediately from a single command.

**WARNING**

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

Solaris and Linux

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

1. Go to the /Websense directory.

2. Use the following commands to stop, start, or restart all Websense services in the correct order:
   - ./WebsenseAdmin stop
   - ./WebsenseAdmin start
   - ./WebsenseAdmin restart

3. View the running status of all Websense services with the following command:
   - ./WebsenseAdmin status

**WARNING**

DO NOT use the kill -9 command to stop Websense services. This procedure may corrupt the services.
CHAPTER 5  Initial Setup

This chapter provides initial setup and configuration procedures for preparing Websense Enterprise to communicate with your Cisco integration.

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

◆ If you did not download the Websense Master Database during installation, you must use the Websense Manager and your Websense subscription key to download the database. See Subscription Key and Master Database Download, page 192 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 196 for instructions.

◆ All Windows workstations being filtered must have the Messenger Service enabled to receive protocol block messages. See Displaying Protocol Block Messages, page 197 for instructions.

◆ If the Logon Agent was installed, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. See Creating and Running the Script for Logon Agent, page 198 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 205 for instructions.

◆ If the Network Agent was installed on a machine with multiple network interface cards (NICs), you can configure Network Agent to use more than one NIC. See Configuring Network Agent to use Multiple NICs, page 207.

◆ If the Network Agent was installed, use the Traffic Visibility Tool to test whether Network Agent can see the user internet traffic that you want it to monitor. See Testing Visibility of Internet Traffic to Network Agent, page 208.
Chapter 5: Initial Setup

- If the optional Remote Filtering components were installed, the firewalls in your network must be configured to allow correct filtering of remote users. See *Firewall Configuration for Remote Filtering*, page 210 for instructions.

For additional configuration information, refer to the Websense Enterprise Administrator’s Guide.

Subscription Key and Master Database Download

The Websense Master Database is the basis for filtering and is updated daily by default. It is downloaded from a remote database server so that your version is the most current.

For the database download to occur, the machine running the Websense Filtering Service must have internet access to the download servers at the following URLs:

- download.websense.com
- ddsdom.websense.com
- ddsint.websense.com
- portal.websense.com
- my.websense.com

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

If you did not enter a subscription key to download the Master Database during installation, follow the instructions below to enter your key and download the Master Database now.

**NOTE**

If you have just upgraded Websense Enterprise, your subscription key was retained by the installer and these steps are not necessary.
Chapter 5: Initial Setup

To download the Master Database:

1. Open Websense Manager on any machine where it is installed.
   - **Windows 2000 Server**: Select Start > Programs > Websense > Websense Manager, or double-click the Websense Manager icon on the desktop.
   - **Windows Server 2003**: Select Start > All Programs > Websense > Websense Manager, or double-click the Websense Manager icon on the desktop.
   - **Solaris**: Go to the /Manager directory in the Websense installation directory and enter:
     
     ./start_manager

2. For a first-time installation, if Policy Server was not installed with Websense Manager, the Add Policy Server dialog box appears the first time you open Websense Manager.
   a. Enter the IP address or machine name of the machine on which you installed the Policy Server, and the configuration port established during installation (default is 55806).
   b. Click OK. The Policy Server machine’s IP address or machine name appears beside a server icon in the Manager’s navigation pane.

3. Double-click the icon of the Policy Server in the navigation pane.
   For a first-time installation, the Set Websense Password dialog box appears.

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

   **NOTE**
   Retain this password. It must be entered when you connect to this Policy Server from this or any other Websense Manager, and when you log on to the Reporting Tools web interface.

5. Click OK.
   The Settings dialog box appears.
6. Enter your alphanumeric key in the **Subscription key** field.

**NOTE**
The **Subscribed network users** and **Subscribed remote users** fields show a value of 0 until the database is successfully downloaded.

7. If your network requires authentication to an upstream proxy server or firewall to reach the internet and download the Websense Master Database, perform the following procedure:
   a. Check **Use authentication**.
   b. Be sure to configure the upstream proxy server or firewall to accept clear text or basic authentication (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 Master Database. Establish the proxy settings for the database download as follows:

   a. Check **Use proxy server**.

   b. Identify the upstream proxy server or firewall by entering the machine’s IP address or machine name in the **Server** field.

      Supported machine name formats are as follows:

      - **Windows**: 7-bit ASCII and UTF-8 characters. The DNS server must be able to recognize UTF-8 characters and resolve the name into an IP address. Do NOT use a machine name that has extended ASCII or double-byte characters.

      - **Solaris or Linux**: 7-bit ASCII only.

      **NOTE**

      If Websense 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**.

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

    Websense automatically contacts the Websense database server and begins downloading the Master Database. The status of the download is displayed in the **Database Download** dialog box.

    The first time the subscription key is entered, the following website appears:

    http://www.my.websense.com

    The my.websense.com site provides access to technical assistance customized for your particular version of Websense Enterprise, your operating system, and your integration product. You do not need anything from this site to complete the setup process.
11. Click **Close** in the **Database Download** dialog box when the download is complete.

---

**NOTE**

After downloading the Master Database or updates to the Master Database, and when the Filtering Service is started, CPU usage can be 90% or more while the database is loaded into local memory.

---

To download the Websense Master Database manually at any time, choose **Server > Database Download** in the Websense Manager.

### 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 Filtering Service machine.
  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.

**IMPORTANT**
*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 187).

**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, 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 Logon Agent, you must create a logon script for your users that will identify them transparently as they log on to a Windows domain. Identification is accomplished by the Websense LogonApp.exe application, which provides a user name and IP address to the Logon Agent each time a Windows client machine connects to an Active Directory or a Windows NTLM directory service.

Prerequisites for Running the Logon Script

Make the following network preparations so that the Websense logon script can execute properly on users’ Windows workstations:

- Be sure that all workstations can connect to the shared drive on the domain controller where the logon script and LogonApp.exe will be placed. To determine if a workstation has access to the domain controller, run the following command from a Windows command prompt:
  
  net view /domain:<domain name>

- NetBIOS for TCP/IP must be enabled. In Windows 98, TCP/IP NetBIOS is enabled by default.

- The TCP/IP NetBIOS Helper service must be running on each client machine that will be identified by Logon Agent. This service runs on Windows 2000, Windows XP, Windows 2003, and Windows NT.

File Location

All relevant files are located in the Websense\bin folder on the Logon Agent machine:

- LogonApp.exe: the Websense executable that communicates user information to the Logon Agent.
Deployment Tasks

To deploy LogonApp.exe with a logon script, perform the following tasks:

**Task 1: Prepare the logon script**: Edit the parameters in the sample script file (Logon.bat) to suit your needs. This file contains two sample scripts: a logon script and a logout script. Active Directory can use both types of scripts. If you plan to use both types, you will need two separate .bat files with different names.

**Task 2: Configure the script to run**: You can run your logon script from Active Directory or Windows NTLM directory services using group policies. This requires you to move the Websense executable and logon batch file to a shared drive on the domain controller that is visible to all user workstations. If you use Active Directory, you may create and deploy an optional logout batch file on the shared drive.

Preparing the Logon Script

A batch file, called Logon.bat, is installed with Logon Agent in the Websense\bin folder. This file contains some instructions for using the scripting parameters, and two sample scripts: a logon script that will run LogonApp.exe, and a logout script for Active Directory 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>:<port>

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.
Chapter 5: Initial Setup

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;server&gt;</td>
<td>IP address or name of the machine running the Websense Logon Agent. This must match the machine address or name entered when you configured Logon Agent in Websense Manager.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>The port number used by Logon Agent. Enter 15880 if you accepted the default port number when you configured Logon Agent in Websense Manager.</td>
</tr>
<tr>
<td>/NOPERSIST</td>
<td>Causes LogonApp.exe to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user’s data is automatically cleared at a predefined time interval. The default interval is 24 hours. If the NOPERSIST parameter is not present, LogonApp.exe operates in the persistent mode. In persistent mode, LogonApp.exe resides in memory on the domain server and updates the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes. Refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide for details on configuring the Logon Agent via the Websense Manager.</td>
</tr>
<tr>
<td>/COPY</td>
<td>Copies the LogonApp.exe application to the users’ machines, where it is run by the logon script from local memory. This optional parameter can be helpful if you experience any hangs with your logon script. The application is copied into the %USERPROFILE%\Local Settings\Temp folder. COPY can be used only in the persistent mode.</td>
</tr>
<tr>
<td>/VERBOSE</td>
<td>Debugging parameter that must be used only at the direction of Technical Support.</td>
</tr>
<tr>
<td>/LOGOUT</td>
<td>(Used only in an optional logout script) Removes the user’s logon information from the Websense user map when the user logs off. If you use Active Directory, you can use this parameter to clear the logon information from the user map before the interval defined in Logon Agent has elapsed. Use this optional parameter in a logout script in a different batch file than the one containing the logon script. See the example scripts below.</td>
</tr>
</tbody>
</table>
**Websense User Map and the Persistent Mode**

User identification provided at logon by `LogonApp.exe` is stored in the Websense user map. This information is updated periodically if `LogonApp.exe` is run in persistent mode. The update time interval for the persistent mode and the interval at which the user map is automatically cleared of logon information are configured in the **Logon Agent** tab of the **Settings** dialog box in the Websense Manager. In Active Directory, if you decide to clear the logon information from the Websense user map before the interval defined in the Manager, you can create an accompanying logout script. You cannot configure a logout script with Windows NTLM.

In the non-persistent mode, information in the user map is created at logon and is not updated. The use of the non-persistent mode creates less traffic between Websense and the workstations in your network than does the persistent mode.

For detailed information on configuring Logon Agent in the Websense Manager, refer to the User Identification chapter in the Websense Enterprise Administrator’s Guide.

**Examples**

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

- **Logon Script:** In this example, the edited `Logon.bat` file contains this single command:

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

  The sample script above sends user information to the Logon Agent at logon only. The information is not updated during the user’s session (NOPERSIST). The information is sent to port 15880 on the server machine identified by IP address 10.2.2.95.

  With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This alternative is not available with Windows NTLM.) To accomplish this, you create a companion logout script in a different batch file.
Logout Script: Continuing the example, copy the logon batch file and rename it `Logout.bat`. Then edit the script in `Logout.bat` as shown here:

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

Configuring the Logon Script to Run

You can configure your logon script to run with a group policy on Active Directory or on a Windows NTLM directory service.

**NOTE**

The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense 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 the Microsoft website for assistance.

To configure a logon script (and optional logout script) using Active Directory:

1. Make sure your environment meets the conditions described in *Prerequisites for Running the Logon Script*, page 198.
2. On the Active Directory machine, go to the Windows Control Panel and select **Administrative Tools > Active Directory Users and Computers**.
3. Right-click the domain and select **Properties**. The domain **Properties** dialog box appears.
4. Select the **Group Policy** tab.
5. Click **New** and create a policy called **Websense Logon Script**.
6. Double-click your new policy or click **Edit** to edit the policy. The **Group Policy Object Editor** dialog box appears.
7. In the tree structure displayed, expand **User Configuration**.
8. Expand the **Windows Settings** structure.
9. Select **Scripts (Logon/Logoff)**.
10. In the right pane, double-click **Logon**.
11. In the **Logon Properties** dialog box displayed, click **Show Files** to open the logon script folder for this policy.
   The folder opens in a Windows Explorer window.
12. Copy two files into this folder: your edited logon batch file (Logon.bat) and the application LogonApp.exe.
13. Close the Explorer window and click **Add** in the **Logon Properties** dialog box.
   The **Add a Script** dialog box appears.
14. Enter the file name of the logon batch file (Logon.bat) in the **Script Name** field or browse for the file.
15. Leave the **Script Parameters** field empty.
16. Click **OK** twice to accept the changes.
17. (Optional.) If you have prepared a logout script, repeat Step 7 through Step 16. Choose **Logoff** at Step 10, and use your logout batch file whenever you are prompted to copy or name the batch file.
18. Close the **Group Policy Object Editor** dialog box.
19. Click **OK** in the domain **Properties** dialog box to apply the script.
20. Repeat this procedure on each domain controller in your network as needed.

**NOTE**
You can determine if your script is running as intended by configuring 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 User Identification chapter of the Websense Enterprise Administrator’s Guide.
Chapter 5: Initial Setup

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


**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 198.
2. Copy the Logon.bat and LogonApp.exe files from the Websense\bin folder on the Logon Agent machine to the netlogon share directory on the domain controller machine.
   
   C:\WINNT\system32\Repl\Import\Scripts
   
   Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.
3. In the Control Panel of the domain controller, select Administrative Tools > User Manager for Domains.
4. Select the users for whom the script must be run and double-click to edit the user properties.
   
   The User Properties dialog box appears.
5. Click Profile.
   
   The User Environment Profile dialog box appears.
6. Enter the path to the logon batch file in the User Profile Path field (from Step 2).
7. Enter the name of the logon batch file (Logon.bat) in the Logon Script Name field.
8. Click OK.
9. Repeat this procedure on each domain controller in your network as needed.

**NOTE**
You can determine if your script is running as intended by configuring 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 User Identification chapter in 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 Cisco Content Engines 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 Manager and connect to the Policy Server.
2. Select **Server > Settings**.
   
   The **Settings** dialog box appears.
3. In the **Settings Selections** pane, click the plus sign beside **Network Agent** to expand the tree.
4. Click the plus sign beside **Global Settings**.
5. Select the IP address of the Network Agent you want to configure from the tree structure.
6. In the **Proxy/Cache Machines** section of the right panel, click **Add**.

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

7. Enter an IP address and click **OK** to add the IP address to the list of proxy or cache servers.
Chapter 5: Initial Setup

Proxy/Cache Server List

8. Repeat Step 6 and Step 7 for each proxy server in your network.
9. Click Finish.

For additional information about configuring Network Agent, see the Network Agent chapter in the Websense Enterprise Administrator’s Guide.

Configuring Network Agent to use Multiple NICs

Each Network Agent instance must use at least one designated NIC. However, Network Agent is capable of using multiple NICs. If you installed Network Agent on a machine with multiple NICs, you can configure it to use different NICs for different purposes. For example, you can configure Network Agent to use one NIC for monitoring traffic, and another to send blocking information to Filtering Service.

For instructions on configuring Network Agent to use additional NICs, refer to the Network Agent chapter in the Websense Enterprise Administrator’s Guide.
Testing Visibility of Internet Traffic to Network Agent

If you installed Network Agent and have any doubt about its ability to monitor internet requests from the desired network and to see the replies, you can conduct a traffic visibility test on the Network Agent machine using the Websense Traffic Visibility Tool.

Running the Websense Traffic Visibility Tool

Run the Websense Traffic Visibility Tool on the Network Agent machine to test internet traffic visibility. The NIC that Network Agent is configured to use must be able to monitor 2-way employee internet traffic for Network Agent to function properly.

1. To start the tool:
   - **Windows**: From the **Start** menu, choose **Programs** (or **All Programs**) > **Websense** > **Utilities** > **Traffic Visibility Tool**.
   - **Linux or Solaris**: Run `.TrafficVisibility.sh` from the Websense installation directory (`/opt/Websense`).

   The Websense Traffic Visibility Tool appears.
2. From the **Network Card** drop-down list, select the network interface card (NIC) that the Network Agent is configured to use.

   A default list of networks (netmasks) to test appears. You may use the defaults provided or add your own. These netmasks can reside in different network segments depending upon the IP address ranges to be filtered.

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

   The **Add Network** dialog box appears.

   a. Enter a new netmask value in the **Network ID** field.

      The subnet mask defaults to 255.0.0.0 and changes appropriately as the netmask is defined.

   b. Click **OK** to return to the Websense Traffic Visibility Tool dialog box.

      Your new network appears in the list.

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

5. Click **Start Test** to begin testing all the networks in the list.
Chapter 5: Initial Setup

The counter in the **IP Address Count** column should begin recording internet traffic immediately from the networks listed. The counter increments each time the NIC detects an individual IP address from the target network in a passing packet. The activity bar at the bottom of the dialog box indicates that a test is in progress.

If the count for a network remains at zero or is very low, the selected NIC cannot see the traffic it is supposed to monitor.

6. If the Network Agent NIC is unable to see the desired traffic, perform one or both of the following tasks:
   - If the installation machine has multiple NICs, select a different card to test. If this card can see the desired traffic, configure Network Agent to use this card. Refer to the Network Agent chapter in the Websense Enterprise *Administrator’s Guide* for instructions.
   - Resolve network configuration issues to make sure that the NIC can see the desired traffic. This might involve connecting to a different router or configuring for port spanning in a switched environment. See *Chapter 2: Network Configuration* for deployment information. Make the necessary changes and retest the NIC.

7. Click **Stop Test** when you are finished testing.

8. Click **Close** to exit the Traffic Visibility Tool.

The Network Agent NIC must be able to monitor all targeted internet traffic. If Network Agent cannot see the necessary traffic, you must either reposition the machine in the network, or select another machine on which to install the Network Agent.

**Firewall Configuration for Remote Filtering**

Remote Filtering is an optional Websense service that allows you to filter user workstations located outside your organization’s network firewall. If you installed the Remote Filtering components, some firewall configuration is necessary to enable web filtering on remote workstations. Firewalls must be configured to allow the Remote Filtering Server to communicate with the remote workstations and with the Filtering Service.
Enabling communication between Remote Filtering Server and Remote User Workstations

The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations should be configured as follows:

- Open the Remote Filtering Server’s **External Communication Port** on these firewalls to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.
- Block connections to the Remote Filtering Server’s **Internal Communication Port** from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.

Refer to the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.

Enabling communication between Remote Filtering Server and Filtering Service

If there is a firewall between the Remote Filtering Server machine and the Filtering Service machine, configure it as follows:

- Open the Filtering Service’s **Filter port** (by default, 15868) on this firewall to accept connections from the Remote Filtering Server.
- Open the Filtering Service’s **Block Page port** (by default, 15871) on this firewall to allow Filtering Service to serve block pages to remote users.

Refer to the documentation for your firewall product if you need information about how to accomplish these firewall configuration tasks.
CHAPTER 6

Configuring Your Cisco Integration

When you have successfully installed Websense, you must configure your Cisco integration to work with Websense to filter internet traffic.

This chapter contains instructions for configuring each type of Cisco integration product: Cisco PIX Firewall and Cisco Adaptive Security Appliance (ASA); Cisco Content Engine; and Cisco IOS Routers.

Cisco PIX Firewall or Adaptive Security Appliance (ASA)

This section describes how to configure your Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA) to work with Websense. These devices will be referred to by the general term “security appliances” throughout this section.

Websense works as a filtering engine for the Cisco security appliance (PIX Firewall or ASA), allowing you to enforce your organization’s internet access policies. The Cisco security appliance passes internet requests to Websense, which then analyzes the requests and determines whether to block access to the sites, permit access to the sites, or limit access by using quotas, according to the Websense policies you have defined.

Once Websense is installed on your network, you must configure the Cisco security appliance to send internet requests to Websense. This can be done through a console or TELNET session by following the instructions in this section. Configuration may also be done through one of the Cisco management GUIs: the PIX Firewall Manager, PIX Device Manager, or Adaptive Security Device Manager, depending on the version of software running on your PIX Firewall or ASA security appliance. For information about configuring your security appliance using one of these management GUIs, refer to the Cisco documentation for that GUI, available at www.cisco.com.
Chapter 6: Configuring Your Cisco Integration

Console or TELNET Session

To configure your Cisco security appliance (PIX Firewall or ASA) using a console or TELNET session:

1. Access the security appliance either from the console or by using TELNET to access it from a remote terminal.
2. Enter your login password.
3. Put the security appliance into enabled mode by entering `enable`, followed by your enable password.
4. Activate `configure` mode by entering:
   
   `configure terminal`
   
   The commands you will enter in `configure` mode are described using the following conventions:
   
   - **Boldface** indicates commands and keywords that are entered literally as shown.
   - Angle brackets (`< >`) containing text in *italics* indicate arguments for which you supply values.
   - Square brackets (`[ ]`) indicate optional elements.
   - Braces (`{ }`) indicate a required choice.
   - Vertical bars (`|`) separate alternative, mutually exclusive elements.

   **NOTE**
   
   For help with individual commands, enter `help` followed by the command. For example, `help filter` shows the complete syntax for the `filter` command and explains each of the options.

5. Use the `url-server` command to enable URL filtering by Websense.

   `url-server (<if_name>) host <ip_address> [timeout <seconds>] [protocol {TCP | UDP}] version {1 | 4} [connections <num_conns>]`
The elements of the `url-server` command are defined as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;if_name&gt;</code></td>
<td>Network interface where the Websense Filtering Service resides. In v7.0 of the Cisco security appliance software, a value for this parameter must be entered. In v6.3 and earlier, <code>&lt;if_name&gt;</code> defaults to <code>inside</code> if not specified. Note that you must type in the brackets ( ) when you enter a value for this parameter.</td>
</tr>
<tr>
<td><code>&lt;ip_address&gt;</code></td>
<td>IP address of the machine running the Websense Filtering Service.</td>
</tr>
<tr>
<td><code>timeout &lt;seconds&gt;</code></td>
<td>The amount of time, in seconds, that the security appliance will wait for a response before switching to the next Filtering Service you defined as a <code>url-server</code>, or, if specified, going into <code>allow</code> mode and permitting all requests. If a timeout interval is not specified, this parameter defaults to 30 seconds in v7.0(1), and 5 seconds in earlier versions. v7.0(1): Range: 10 - 120; Default: 30. v6.3: Range: 1 - 30; Default: 5.</td>
</tr>
<tr>
<td>`protocol {TCP</td>
<td>UDP}`</td>
</tr>
<tr>
<td>`version {1</td>
<td>4}`</td>
</tr>
<tr>
<td><code>connections &lt;num_conns&gt;</code></td>
<td>Limits the maximum number of TCP connections permitted between the Cisco security appliance and the Websense Filtering Service. If this parameter is not specified, it defaults to 5, which is the recommended setting. Note that if you select the UDP protocol, this option is not available. Range: 1 - 100. Default: 5.</td>
</tr>
</tbody>
</table>
An example of the `url-server` command might be:

```
url-server (perimeter) host 10.255.40.164
timeout 30 protocol TCP version 4
```

The `url-server` command communicates the location of the Websense Filtering Service to the Cisco security appliance. More than one `url-server` command can be entered. This allows redirection to another Websense Filtering Service after the specified timeout period, if the first server becomes unavailable.

6. Configure the security appliance to filter HTTP requests with the `filter url` command, as shown below. You can view the current URL server rules by entering `show url-server`. To review all the filter rules, enter `show filter`.

To configure HTTP request filtering, use the following command:

```
filter url http <port>[<port>] <local_ip> <local_mask> <foreign_ip> <foreign_mask>
[allow] [cgi-truncate] [longurl-truncate | longurl-deny] [proxy-block]
```

The elements of the `filter url` command are defined as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http &lt;port&gt;[&lt;port&gt;]</code></td>
<td>Defines which port number or range of port numbers the security appliance will watch for HTTP requests. If you do not specify a port number, it defaults to port 80. The option to set a custom web port or port range is only available in v5.2 and later of the Cisco software. NOTE: In v5.2 to 6.3, it is not mandatory to enter <code>http</code> before the port number; you can either enter <code>http</code> (to use port 80), or you can enter a port number. In v7.0, you must always enter <code>http</code>.</td>
</tr>
<tr>
<td><code>&lt;local_ip&gt;</code></td>
<td>IP address requesting access. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This is the source for all connections to be filtered.</td>
</tr>
<tr>
<td><code>&lt;local_mask&gt;</code></td>
<td>Network mask of the local_ip address (the IP address requesting access). You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.</td>
</tr>
</tbody>
</table>
### Parameter Definition

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;foreign_ip&gt;</code></td>
<td>IP address to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.</td>
</tr>
<tr>
<td><code>&lt;foreign_mask&gt;</code></td>
<td>Network mask of the <code>foreign_ip</code> address (the IP address to which access is requested). Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network.</td>
</tr>
<tr>
<td><code>[allow]</code></td>
<td>Enter this parameter to let outbound connections pass through the security appliance without filtering when the Websense Filtering Service is unavailable. If you omit this option, and the Filtering Service goes offline, the security appliance stops all outbound HTTP traffic until the Filtering Service is back online.</td>
</tr>
<tr>
<td><code>[cgi-truncate]</code></td>
<td>Enter this parameter to send CGI scripts to the Websense Filtering Service as regular URLs. Specifically, when a URL has a parameter list starting with a question mark ('?'), such as a CGI script, this will truncate the URL by removing all characters after and including the question mark before sending the URL to the Websense Filtering Service. (Supported in v6.2 and higher.)</td>
</tr>
<tr>
<td>`[longurl-truncate</td>
<td>longurl-deny]`</td>
</tr>
<tr>
<td><code>[proxy-block]</code></td>
<td>Enter this parameter to prevent users from connecting to an HTTP proxy server. (Supported in v6.2 and higher.)</td>
</tr>
</tbody>
</table>
Multiple `filter url` commands may be entered to achieve your filtering needs. The following table provides some examples.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filter url http 0 0 0 0</code></td>
<td>Filters every HTTP request to all destinations. Filtering is applied to traffic on port 80.</td>
</tr>
<tr>
<td><code>filter url http 10.5.0.0 255.255.0.0 0 0</code></td>
<td>Filters the 10.5 Class B network going to any destination. Filtering is applied to traffic on port 80.</td>
</tr>
<tr>
<td><code>filter url http 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255</code></td>
<td>Filters the 10.5.0.69 host going to the 132.239.29.189 destination. Filtering is applied to traffic on port 80.</td>
</tr>
</tbody>
</table>

Using zeroes for the last two entries, `<foreign_ip>` and `<foreign_mask>`, allows access via Websense from the specified local IP address to all websites.

You can enter multiple `filter url` commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. It is recommended that you use a general `filter url` command for all workstations to be filtered, and then use Websense Manager to apply filtering policies to individual clients (users, groups, domains/organizational units, workstations, or networks).

7. Configure the Cisco security appliance to filter HTTPS requests with the `filter https` command, as shown below. You can view the current URL server rules by entering `show url-server`. To review all the filter rules, enter `show filter`.

**NOTE**

The `filter https` command is supported in v6.3 and higher of the Cisco PIX Firewall/ASA software.

To configure HTTPS request filtering, use the following command:

```
filter https <port> <local_ip> <local_mask> <foreign_ip> <foreign_mask> [allow]
```
The elements of the `filter https` command are defined as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Defines which port number the security appliance will watch for HTTPS requests. You can either enter the standard HTTPS port, 443, or a custom port number.</td>
</tr>
<tr>
<td>&lt;local_ip&gt;</td>
<td>IP address requesting access. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This is the source for all connections to be filtered.</td>
</tr>
<tr>
<td>&lt;local_mask&gt;</td>
<td>Network mask of the local_ip address (the IP address requesting access). You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.</td>
</tr>
<tr>
<td>&lt;foreign_ip&gt;</td>
<td>IP address to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.</td>
</tr>
<tr>
<td>&lt;foreign_mask&gt;</td>
<td>Network mask of the foreign_ip address (the IP address to which access is requested). Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network.</td>
</tr>
<tr>
<td>[allow]</td>
<td>Enter this parameter to let outbound connections pass through the security appliance without filtering when the Websense Filtering Service is unavailable. If you omit this option, and if the Filtering Service goes offline, the security appliance stops outbound HTTPS traffic until the Filtering Service is back online.</td>
</tr>
</tbody>
</table>

Multiple `filter https` commands may be entered to achieve your filtering needs. The following table provides some examples.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filter https 443 0 0 0 0</code></td>
<td>Filters every request to all destinations. Filtering is applied to traffic on port 443.</td>
</tr>
<tr>
<td><code>filter https 443 10.5.0.0 255.255.0.0 0 0</code></td>
<td>Filters the 10.5 Class B network going to any destination. Filtering is applied to traffic on port 443.</td>
</tr>
<tr>
<td><code>filter https 443 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255</code></td>
<td>Filters the 10.5.0.69 host going to the 132.239.29.189 destination. Filtering is applied to traffic on port 443.</td>
</tr>
</tbody>
</table>
Using zeroes for the last two entries, <foreign_ip> and <foreign_mask>, allows access via Websense from the specified local IP address to all websites.

You can enter multiple filter https commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. It is recommended that you use a general filter https command for all workstations to be filtered, and then use Websense Manager to apply filtering policies to individual clients (users, groups, domains/organizational units, workstations, or networks).

8. Configure the Cisco security appliance to filter FTP requests with the filter ftp command, as shown below. You can view the current URL server rules by entering show url-server. To review all the filter rules, enter show filter.

```
NOTE
The filter ftp command is supported in v6.3 and higher of the Cisco PIX Firewall/ASA software.
```

To configure FTP request filtering, use the following command:

```
filter ftp <port> <local_ip> <local_mask> <foreign_ip> <foreign_mask> [allow] [interact-block]
```

The elements of the filter ftp command are defined as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Defines which port number the security appliance will watch for FTP requests. You can either enter the standard FTP port number, 21, or a custom port number.</td>
</tr>
<tr>
<td>&lt;local_ip&gt;</td>
<td>IP address requesting access. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This is the source for all connections to be filtered.</td>
</tr>
<tr>
<td>&lt;local_mask&gt;</td>
<td>Network mask of the local_ip address (the IP address requesting access). You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.</td>
</tr>
</tbody>
</table>
### Chapter 6: Configuring Your Cisco Integration

Multiple `filter ftp` commands may be entered to achieve your filtering needs. The following table provides some examples.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;foreign_ip&gt;</code></td>
<td>IP address to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.</td>
</tr>
<tr>
<td><code>&lt;foreign_mask&gt;</code></td>
<td>Network mask of the <code>foreign_ip</code> address (the IP address to which access is requested). Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network.</td>
</tr>
<tr>
<td><code>[allow]</code></td>
<td>Enter this parameter to let outbound connections pass through the security appliance without filtering when the Websense Filtering Service is unavailable. If you omit this option, and the Filtering Service goes offline, the security appliance stops outbound FTP traffic until the Filtering Service is back online.</td>
</tr>
<tr>
<td><code>[interact-block]</code></td>
<td>Enter this parameter to prevent users from connecting to the FTP server through an interactive FTP client. An interactive FTP client allows users to change directories without entering the complete directory path, so the Websense Filtering Service cannot tell if the user is requesting something that should be blocked.</td>
</tr>
</tbody>
</table>

Using zeroes for the last two entries, `<foreign_ip>` and `<foreign_mask>`, allows access via Websense from the specified local IP address to all websites.
You can enter multiple `filter ftp` commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. It is recommended that you use a general `filter ftp` command for all workstations to be filtered, and then use Websense Manager to apply filtering policies to individual clients (users, groups, domains/organizational units, workstations, or networks).

9. After entering commands to define filtering for HTTP, HTTPS, and FTP requests, you can define any required exceptions to these filtering rules by adding the `except` parameter to the `filter` command:

   ```
   filter {url | https | ftp} except <local_ip>
   <local_mask> <foreign_ip> <foreign_mask>
   ```

   This command allows you to bypass Websense Enterprise for traffic coming from or going to a specified IP address or addresses.

   For example, if the following filter command was entered to cause all HTTP requests to be forwarded to the Websense Filtering Service

   ```
   filter url http 0 0 0 0
   ```

   you could enter

   ```
   filter url except 10.1.1.1 255.255.255.255 0 0
   ```

   to allow any outbound HTTP traffic from the IP address 10.1.1.1 to go out unfiltered.

10. If appropriate for your network, you can enable the URL caching feature and set the cache size. When URL caching is enabled, filtering responses from Websense are cached, and cached websites are prevented from being sent to Websense for evaluation or logging. This can improve web filtering response time and may be appropriate in large organizations with a high volume of internet traffic.

    **NOTE**

    To use URL caching, you must set the protocol version to 4 in the `url-server` command.

    You can use the `show url-cache statistics` and the `show perfmon` commands to view current information on the cache size and utilization.
To enable caching and set the cache size, use the command:

```
url-cache dst | src_dst <size>
```

where `<size>` is the size of the cache in KB. Range: 1 to 128.

dst | src_dst specifies either destination caching (dst), or source-destination caching (src_dst). Use the dst option only if Websense is configured to use the same policy for all clients making requests.

Destination caching stores the Websense response for each destination website, regardless of the requesting client’s IP address.

Source-destination caching is where the Cisco security appliance checks its cache for both the client’s IP address and the destination website’s IP address to determine whether the destination website should be permitted or blocked.

For example, you could enter the following command to enable source-destination caching by the Cisco security appliance, with a cache size of 128 KB:

```
url-cache src_dst 128
```

SeeCisco Security Appliance Enhanced Caching, page 225 and your Cisco security appliance documentation for more information about URL caching.

11. Configure the security appliance to handle long URLs using the `url-block url-mempool` and `url-block url-size` commands:

```
url-block url-mempool
```

where `<memory_pool_size>` is the size of the buffer in KB. You can enter a value from 2 to 10240 for a maximum memory allocation of 2 KB to 10.24 MB. The recommended value is 1500.

**NOTE**
The `url-block` commands are supported in v6.2 and higher of the Cisco PIX Firewall/ASA software.
b. Increase the maximum permitted size of a single URL by adding the following line to the configuration:

```
url-block url-size <long_url_size>
```

where `<long_url_size>` is the maximum URL size. You can enter a value from 2 to 4 for a maximum URL size of 2 KB to 4 KB. The recommended value is 4.

12. Configure the URL response block buffer using the `url-block block` command to prevent replies from the web server from being dropped in high traffic situations.

```
url-block block <block_buffer_limit>
```

where `<block_buffer_limit>` is the number of 1550-byte blocks to be buffered. You can enter a value from 1 to 128.

You can use the `show url-block` command to view the current configuration for all three `url-block` commands described in this step and the previous step. To view statistics that show how the current buffer configuration is functioning, including number of pending packets held and number dropped, enter the `show url-block block statistics` command.

13. If you need to discontinue filtering, enter the exact parameters in the original `filter` command, preceded by the word `no`. For example, if

```
filter url http 10.0.0.0 255.0.0.0 0 0
```

was entered to enable filtering, then enter

```
no filter url http 10.0.0.0 255.0.0.0 0 0
```
to disable filtering.
14. Type `exit` to exit `configure` mode.
15. Save the changes by entering:

   `write memory`

Once the Websense Master Database has been downloaded, and Websense Enterprise has been activated within the Cisco security appliance, Websense is ready to filter internet requests. Refer to the Websense Enterprise Administrator's Guide for information on configuring Websense for filtering.

Cisco Security Appliance Enhanced Caching

Cisco security appliances (PIX Firewall and ASA) provide an enhanced caching feature that decreases internet filtering response time. When caching is enabled within the security appliance, Websense sends the security appliance permission to cache an IP address if every site hosted at the address is in a category that is permitted at all times, for every user. Caching works when the Websense Filtering Service adds this “OK to cache” information to responses to certain URL lookup requests sent to the Filtering Service. Depending on Websense configuration settings, this “OK to cache” information may be returned with responses, without the Websense Administrator having to configure anything within Websense related to enhanced caching.

The Cisco security appliance sends the first request for a site to Websense. When Websense responds to the request with permission to cache the IP address of the requested site, the security appliance saves the IP address (not the web page itself), and a time-to-live value. The next time the same site is requested (or any site at that IP address), the security appliance uses the cached information, rather than sending a new request to Websense, thereby decreasing response time.

**NOTE**

Internet requests involving cached IP addresses are not passed to Websense and are not logged. As a result, this activity does not appear in the Real-Time Analyzer or in any reports.

The number of responses the security appliance can cache depends on how customized your filtering policies are. When more clients are filtered with the same policy, more responses can be cached.
Chapter 6: Configuring Your Cisco Integration

If caching is disabled within the security appliance, every HTTP request that the security appliance receives is sent to Websense for filtering. In very large networks or organizations with a high volume of internet access requests, this can increase the time required to return a site to the user, which could decrease overall performance.

To enable caching in a Cisco security appliance, use the `url-cache` command. See Step 10, page 222 for information about command syntax and recommended parameters.

---

**NOTE**

To use enhanced caching on the Cisco security appliance, you must set the protocol version to 4 in the `url-server` command.

---

Cisco Secure ACS Authentication

Do not use Cisco Secure ACS authentication with Websense Enterprise in a multiple domain environment. ACS cannot provide domain information about users to Websense Enterprise, and authentication fails. To identify users in a multiple domain environment, use one of the Websense transparent identification agents, such as DC Agent, or use Websense manual authentication.

For information on installing DC Agent, refer to *DC Agent*, page 113. For information about configuring for manual authentication, or for configuring DC Agent to identify users transparently, refer to the Websense Enterprise Administrator’s Guide.
Cisco Content Engine

Websense Enterprise works as a filtering engine for the Cisco Content Engine, allowing you to enforce your organization’s internet access policies. Once Websense is installed on your network, you must activate it within the Content Engine. This can be done through the Cisco Web-based interface or through a console or TELNET session, by following the instructions in either of the next two sections.

**NOTE**
If load bypass or authentication bypass is enabled in the Content Engine, internet requests that are rerouted are filtered by Websense. See your Content Engine documentation for more information.

Cisco Web-based Interface

To configure Cisco Content Engine using the Web-based interface:

1. Open a web browser and connect to the Cisco Content Engine at:
   - `https://<ip-address>:8003` (for ACNS 5.1 and higher)
   - `http://<ip-address>:8001` (for versions prior to ACNS 5.1)
   where `<ip-address>` is the IP address of the Content Engine machine. The default port is 8003 for ACNS 5.1 and higher.

   The **Enter Network Password** dialog box appears.

2. Enter a valid user name and password that allows access to the initial management page.

3. Select **Caching > URL Filtering**.

4. Select the filtering option appropriate to your ACNS version.
   - For ACNS version 5 and higher, select either **Websense Filtering (Remote)** or **Websense Filtering (Local)**.
   - For ACNS versions prior to version 5, select **Websense Filtering**.
5. Enter the following information in the appropriate fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Websense Filtering Service or Websense Server</td>
<td>Hostname or IP address of the machine running the Websense Filtering Service.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on which Websense will communicate with the Content Engine. This is the Filtering Service port you entered during Webse installed on the Content Engine, use the following command:</td>
</tr>
<tr>
<td>Timeout</td>
<td>Amount of time (between 1 and 120 seconds) that the Content Engine should wait for a response from Websense before permitting a site. The default is 60.</td>
</tr>
</tbody>
</table>

6. If Websense Enterprise is filtering on a cluster of Content Engines, configure the following on each Content Engine in the cluster with the following commands to ensure that all traffic is filtered:

   url-filter http websense server <ip-address>
   port <port-number>
   url-filter http websense allowmode enable

   For Websense installed on the Content Engine, use the following command:
   
   url-filter http websense “local”

### Console or TELNET Session

To configure Cisco Content Engine using a console or TELNET session:

1. Access the Cisco Content Engine, either from a console connection or a TELNET session from a remote terminal.
2. Enter the global configuration mode with the **configure** command. You must be in global configuration mode to enter global configuration commands.

   ```
   Console# configure
   Console(config)#
   ```
3. To enable Websense URL filtering, use the **url-filter** global configuration command.
url-filter http websense server <ip-address>
port <port-number> timeout <seconds>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Host name or IP address of the machine running the Websense Filtering Service.</td>
</tr>
<tr>
<td>&lt;port-number&gt;</td>
<td>Port on which the Websense Filtering Service will communicate with the Content Engine.</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>Amount of time in seconds (between 1 and 120) that the Content Engine will wait for a response from the Websense Filtering Service before permitting a site. The Content Engine only permits sites after the timeout if it has been configured to do so. See Step 4 below for more information.</td>
</tr>
</tbody>
</table>

4. The `url-filter http websense allowmode enable` command configures the Content Engine to permit requests after a Websense Filtering Service timeout.

5. Type the `exit` command to exit the global configuration mode.

6. Save the configuration changes to memory with the `write memory` command.

7. If Websense Enterprise is filtering on a cluster of Content Engines, configure the following on each Content Engine in the cluster with the following commands to ensure that all traffic is filtered:

   url-filter http websense server <ip-address>
   port <port-number>
   url-filter http websense allowmode enable

   For Websense installed on the Content Engine, use the following command:

   url-filter http websense "local"

Once the Websense Master Database has been downloaded, and Websense has been activated within Cisco Content Engine, Websense is ready to filter internet requests. Refer to the Websense Enterprise Administrator’s Guide for information about configuring Websense for filtering.
Settings within the Content Engine Environment

Consider the information in the next three sections if your environment includes Content Engines.

Configuring Firewalls or Routers

To prevent users from circumventing Websense filtering when Websense is integrated with Cisco Content Engine, your firewall or internet router should be configured to allow outbound HTTP, HTTPS, and FTP requests only from the Content Engine.

Those users with Web Cache Communication Protocol (WCCP) on their routers will see internet requests handled transparently by the Content Engine and Websense.

NOTE

If Websense is set to pass through a proxy server or firewall that requires authentication for any HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication in order for Websense to download the Websense Master Database.

Browser Access to the Internet

Cisco Content Engine can regulate internet activity either transparently or nontransparently. In transparent mode, the firewall or internet router is configured to send internet requests to the Cisco Content Engine, which queries Websense. All configuration changes can be performed through the Content Engine and any connected firewalls or routers, with no special configuration required on client workstations. In order to run transparently, you must enable WCCP on both the Content Engine and the firewall or router.

When regulating internet activity non-transparently, web browsers on all client workstations are configured to send internet requests to the Content Engine. Please see your Cisco Content Engine documentation for instructions.

To prevent users from circumventing Websense filtering, your firewall or internet router should be configured to allow outbound HTTP and FTP requests only from the Cisco Content Engine.
Clusters

If you have several Content Engines running in a cluster, you must configure each to use the Websense Filtering Service as an HTTP, HTTPS, and FTP filter. Several Content Engines can utilize the same Websense Filtering Service. See your Content Engine documentation for details on setting up a cluster.

Cisco IOS Routers

Cisco IOS Routers can be configured to send HTTP requests to the Websense Filtering Service. Websense Enterprise analyzes the requests and determines whether to block access to the sites, permit access to the sites, or limit access by using quotas, according to the policies you have defined. The action taken on an HTTP request is cached in the Cisco Router, which can enforce the policy the next time the site is requested without having to communicate with the Filtering Service.

Once Websense Enterprise is installed on your network, you must configure the router to send internet requests to Websense. This can be done through a console or TELNET session. Refer to your Cisco Router documentation for instructions on opening a configuration session.

Startup Configuration

Before Websense can filter internet requests, the Cisco IOS Router must be configured to use Websense as a URL filter.

1. Access the Cisco Routers software, either from a console or from a remote terminal, using TELNET.

2. Enter your login password.

3. Put Cisco Router into enabled mode by entering enable and your enable password.

4. Put Cisco Router into configure mode by entering configure terminal.

5. Identify the Websense Filtering Service that will be filtering HTTP requests by entering the following configuration command:
Chapter 6: Configuring Your Cisco Integration

```
ip urlfilter server vendor websense
    <ip-address> [port <port-number>] [timeout <seconds>] [retransmit <number>]
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address of the Websense Filtering Service.</td>
</tr>
<tr>
<td>&lt;port-number&gt;</td>
<td>Port number on which the Websense Filtering Service listens. The default is 15868.</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>How long Router should wait for a response from the Websense Filtering Service. The default timeout is 5 seconds.</td>
</tr>
<tr>
<td>&lt;number&gt;</td>
<td>How many times Cisco Router should retransmit an HTTP request when there is no response from the Websense Filtering Service. The default is 2.</td>
</tr>
</tbody>
</table>

An example of this command is:

```
ip urlfilter server vendor websense 12.203.9.116 timeout 8 retransmit 6
```

To define an additional Websense Filtering Service as a back up, repeat the command for the IP address of the second server. The configuration settings you create in the following steps will always be applied to the primary server—that is, the first server with which the Cisco Router can establish communications.

6. Enable the logging of system messages to the Websense Filtering Service by entering the following command:

```
   ip urlfilter urlf-server-log
```

This is enabled by default. When logging is enabled, Cisco Router sends a log request immediately after the URL lookup request. If the destination IP address is found in the cache, Cisco Router does not send a URL lookup request but still sends a log request to the Websense Filtering Service.

7. Tell the Cisco Router how to filter URL requests by using the following commands in sequence:

```
ip inspect name <inspection-name> http urlfilter
interface <type> <slot/port>
ip inspect <inspection-name> {in | out}
```
Examples of these commands are:

```plaintext
ip inspect name fw_url http urlfilter
interface FastEthernet 0/0
ip inspect fw_url in
```

For this sequence to function properly, you must create an inspection rule entitled `fw_url` and apply it to the inbound interface of the router. For instructions on creating and applying inspection rules, refer to your Cisco documentation.

8. To save your changes, first leave the `configure` mode by entering `exit` twice, then enter `write memory`.

   Unless you store your configuration settings in the startup configuration of the Cisco Router, the settings will be lost if the router is shut down for any reason or loses power.

9. Use the following commands to view various aspects of your installations:

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip inspect name &lt;name&gt;</code></td>
<td>Displays a specific inspection rule.</td>
</tr>
<tr>
<td><code>show ip inspect all</code></td>
<td>Displays all available inspection information.</td>
</tr>
<tr>
<td><code>show ip urlfilter config</code></td>
<td>Displays all URL filtering information.</td>
</tr>
<tr>
<td><code>&lt;command&gt; ?</code></td>
<td>Displays help on individual commands. For example, <code>ip inspect ?</code> displays the complete syntax for the <code>inspect</code> command and explains each argument.</td>
</tr>
</tbody>
</table>

10. To discontinue filtering for any reason or to change a Websense Filtering Service, enter the following command to remove a server configured in Step 5.

```plaintext
no ip urlfilter server vendor websense <ip-address>
```
Chapter 6: Configuring Your Cisco Integration

Configuration Commands

These commands are used to configure the Cisco IOS Router to filter HTTP requests through Websense. These configuration settings can be saved into the startup configuration. See Step 8 in the preceding procedure for instructions on saving your settings.

Straight brackets ([ ]) indicate an optional value. Curly brackets ({ }) contain the possible values that can be selected. A forward slash (/) separates each value within the curly brackets. Angle brackets (< >) surround variables that must be replaced with actual values in the command syntax.

NOTE
To turn off the feature or service, add the value no before the command.

```
ip inspect name <inspection-name> http urlfilter [java-list <access-list>] [alert {on/off}] [timeout <seconds>] [audit-trail {on/off}]
```

This is a global command to turn on HTTP filtering. The `urlfilter` value associates URL filtering with HTTP inspection rules. You may configure two or more inspections in a router, but the URL filtering feature will only work with those inspections in which the `urlfilter` field is enabled. This setup command is required.

```
ip urlfilter server vendor websense <IP address> [port <num>] [timeout <secs>] [retrans <num>]
```

This is a required setup command that identifies the Websense Filtering Service to the Cisco Router and configures additional values. When using this command, the Cisco Router checks for a primary server—one that is active and being sent URL lookup requests. If a primary server is configured, the system marks the server you are adding as a secondary server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port &lt;num&gt;</code></td>
<td>Specifies the port number on which the Websense Filtering Service listens. The default port number is 15868.</td>
</tr>
<tr>
<td><code>timeout &lt;secs&gt;</code></td>
<td>Specifies how long the Cisco Router should wait for a response from the Websense Filtering Service. The default timeout value is 5 seconds.</td>
</tr>
</tbody>
</table>
Chapter 6: Configuring Your Cisco Integration

ip urlfilter alert

This is an optional setting that controls the system alert. By default, the system alert is enabled. The following messages can be display when alerts are enabled:

- %URLF-3-SERVER_DOWN: Connection to the URL filter server <IP address> is down—level three LOG_ERR type message that appears when a configured Websense Filtering Service goes down. When this occurs, the Cisco Router marks the offline server as a secondary server and attempts to bring up the secondary server you have defined as the primary server. If the router cannot find another Websense Filtering Service, the URLF-3-ALLOW_MODE message is displayed.

- %URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE is off.—message that appears when the Cisco Router cannot find a defined Websense Filtering Service. When the ALLOW MODE is off, all HTTP requests are blocked.

- %URLF-5-SERVER_UP: connection to an URL filter server <IP address> is made, the system is returning from ALLOW MODE—a LOG_NOTICE type message displayed when a Websense Filtering Service is detected as being up and the system returns from ALLOW MODE.

- %URLF-4-URL_TO_LONG: URL too long (more than 3072 bytes), possibly a fake packet—a LOG_WARNING type message displayed when the URL in a GET request is too long.

- %URLF-4-MAX_REQ: The number of pending requests exceeds the maximum limit <num>—a LOG_NOTICE type message displayed when the number of pending requests in the system exceeds the maximum limit defined and subsequent requests are dropped.

ip urlfilter audit-trail

This command controls the logging of messages into the syslog server and is disabled by default. The messages logged are:

- %URLF-6-SITE_ALLOWED: Client <IP address:port number> accessed server <IP address:port number>—a LOG_INFO type message

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retrans &lt;secs&gt;</td>
<td>Specifies how many times the router should retransmit the request when the response doesn't arrive for a request. The default value is 2.</td>
</tr>
</tbody>
</table>
logged for each request whose destination IP address is found in the cache. This message includes source IP address/port number and destination IP address/port number.

- %URLF-6-URL_ALLOWED: Access allowed for URL http://www.websense.com; client <IP address:port number> server <IP address:port number>—message that is logged for each URL requested that is allowed by Websense. This message includes the allowed URL, the source IP address/port number, and the destination IP address/port number. Long URLs (>1000 bytes) are not logged under this category.

- %URLF-6-URL_BLOCKED: Access denied URL http://www.google.com; client <IP address:port number> server <IP address:port number>—message that is logged for each URL requested that is blocked by Websense. This message includes the blocked URL, the source IP address/port number, and the destination IP address/port number. Long URLs (>1000 bytes) are not logged under this category.

**ip urlfilter urlf-server-log**

This command is used to control the logging of system messages to the Websense Filtering Service and is DISABLED by default. To allow logging (and consequently reporting) of internet activity on your system, you must enable this feature.

When logging is enabled, the Cisco Router sends a log request immediately after the URL lookup request. If the destination IP address is found in the cache, the router does not send a URL lookup request but does send a log request to the Websense Filtering Service. The log message contains information such as the URL, host name, source IP address, and destination IP address.

**ip urlfilter exclusive-domain <domain-name>**

This optional command is used to add a domain to or remove a domain from the exclusive domain list. Cisco Router URL filtering provides a way to specify a list of domain names for which the router need not send lookup requests to the Websense Filtering Service.

For example, if www.yahoo.com is added to the exclusive domain list, all the HTTP traffic whose URLs are part of this domain (such as www.yahoo.com/mail/index.html, www.yahoo.com/news, and www.yahoo.com/sports) are permitted without sending a lookup request to the Websense Filtering Service.
You may also specify a partial domain name. For example, you can enter `.cisco.com` instead of the complete domain name. In this case, all the URLs whose domain name ends with this partial name (such as `www.cisco.com/products`, `www.cisco.com/eng`, `people-india.cisco.com/index.html`, and `directory.cisco.com`) are permitted without having to send a lookup request to Websense Filtering Service. When using partial domain names, always start the name with a period, as in `ip urlfilter exclv-domain .sdsu.edu`.

**ip urlfilter cache <number> [timeout <hours>]**

Use this optional command to configure cache parameters. The number field specifies the maximum number of destination IP addresses that can be stored in the cache table. The optional timeout field specifies the time interval in which the cache table is cleared out completely. Cached IP addresses are deleted periodically to keep entries synchronized with the Websense policy database. The default value for the maximum number of cache entries is 5000, and the default value for cache timeout is 12 hours.

**ip urlfilter allowmode {on/off}**

This command controls the default filtering policy if the Websense Filtering Service is down. If the ALLOW MODE is `on`, and the Cisco Router cannot find a Websense Filtering Service, all HTTP requests are permitted. If the ALLOW MODE is `off` when the Websense Filtering Service goes down, all HTTP requests are blocked. The default of the ALLOW MODE is `off`.

**ip urlfilter packet-buffer <number>**

Use this optional command to configure the maximum number of HTTP responses that the Cisco Router can store in its packet buffer. The default value is 200.

**ip urlfilter maxrequest <number>**

Use this optional command to set the maximum number of outstanding requests that can exist at a given time. When this number is exceeded, subsequent requests are dropped. The ALLOW MODE flag is not considered in this case because it is only used when the Websense Filtering Service is down. The default value for `maxrequest` is 1000.
Executable Commands

These Cisco IOS Router commands allow you to view configuration data and filtering information, and to control caching. These settings cannot be saved into the startup configuration.

**clear ip urlfilter cache** \{<IP address>/all\}

This command clears the cache table of destination IP addresses. You can specify whether to flush the entire cache table or only a specific IP address. This is a good command to use when you have made changes to the filtering policy and want to clear the cache to implement the new policy.

**show ip urlfilter cache**

This command displays:

- Maximum number of entries that can be cached
- Number of entries in the cache table
- List of IP addresses that are cached

**show ip urlfilter config**

This command shows configuration information such as number of maximum requests, ALLOW MODE state, and the list of configured Websense Filtering Service. This is the kind of information that technical support typically requests when trying to solve a problem.

**show ip urlfilter statistics**

This command shows statistics of the URL filtering feature. Following is some of the information displayed:

- Number of requests sent to Websense
- Number of responses received from Websense
- Number of requests pending in the system
- Number of requests failed
- Number of URLs blocked
debug ip urlfilter \{function-trace/detailed/events\}

This command enables the display of debugging information from the URL filter subsystem. The possible command values are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>function-trace</td>
<td>Enables the system to print sequence of important functions that get called in this feature.</td>
</tr>
<tr>
<td>detailed</td>
<td>Enables the system to print detailed information about various activities that happen in this feature.</td>
</tr>
<tr>
<td>events</td>
<td>Enables the system to print various events such as queue events, timer events, and socket events.</td>
</tr>
</tbody>
</table>
Configuring Windows NTLM for User Authentication

Proxy authentication through use of a Windows NT Lan Manager (NTLM) proxy server is used to validate client (user) credentials to minimize database queries and improve the performance on the Content Engine and authentication database. The Microsoft Internet Explorer browser can be set to automatically store the user’s credentials for a default time period of 480 minutes (eight hours) or a timeout period to suit your needs, so that subsequent requests can be validated against the domain controller.

Configuring the Browser for Promptless Authentication

Promptless NTLM can be used by customers requiring a single logon or by those looking to transparently log the domain\username in the transaction logs. The NTLM protocol is proprietary and, therefore, only accepted by Microsoft Internet Explorer browsers. If the Content Engine challenges a Netscape browser with NTLM, the Netscape browser will ask for a user name and password.

By default, the Microsoft Internet Explorer browser is not configured to automatically respond to a user’s credentials without prompting for a user name and password. To enable promptless authentication, the browser must be configured to automatically log on with current user name and password.

To configure the Microsoft Internet Explorer browser for promptless authentication:

1. For Windows 2003, go to **Start > Settings > Control Panel > Internet Options**.
   The **Internet Options** dialog box appears (Internet Explorer version 6).
2. Select the **Security** tab.

3. Click **Custom Level** to change the **User Authentication** logon security setting.

4. Scroll to the end of the Options to find and change the security settings for **User Authentication**.

5. Select **Automatic logon with current username and password** to set the automatic logon for promptless user authentication.
Configuring the Content Engine

The Content Engine must be configured with the primary (and secondary if appropriate) domain controller’s host name or IP address and the name of the domain.

NOTE

The Content Engine cannot be configured with more than one domain. If your network has multiple domains, the configured domain must trust all other domains with valid user accounts.

Domains should not include overlapping users and groups, because the Content Engine authenticates the user regardless of the user name and password.

Enter the domain controller’s name or IP address and the name of the domain.

For example:

```
ntlm server host 10.1.1.11 primary
ntlm server domain allcisco
```

IMPORTANT

The Content Engine requires that the domain controller reside in the Domain Name Server (DNS) for both forward and reverse pointer record resolution.

Additionally, the Windows Internet Naming Server (WINS), which determines the IP address associated with a particular network computer, should match the DNS name. The Content Engine checks that the name is supported properly in DNS when the command is entered. If it is not entered properly, an error message is displayed.
Appendix A: Configuring Windows NTLM for User Authentication

Configuration and Corresponding Parameters

The configuration and corresponding parameters are as follows:

```
ntlm server host 10.1.1.11 primary
ntlm server domain allcisco
ntlm server enable
```

```
ce507#sho ntlm
NTLM parameters:
   Primary :           10.1.1.11
   Secondary:          <none>
   State:              Enabled
   Domain name:        allcisco
```

The configured settings for authentication may be verified, using the following ‘show’ commands.

```
ce507# (config) #http authentication ?
   cache    Configure parameters related to Authentication Cache
   header   Specify which type of authentication header CE should use
   realm    Configure realm string for HTTP Basic request authentication
```

```
ce507#show http authentication
HTTP Authentication:
   Header:                Based on URL syntax
   Realm:                 “Cisco Content Engine”
   Cache Timeout:         480 (minutes)
   Cache Maximum entries: 4000
```

ce507#
Managing the HTTP Proxy Authentication Cache

To minimize the impact on the Content Engine and the authentication database, the Content Engine uses an authentication cache. The authentication cache is separately maintained, independent of other caches on the Content Engine. When a new user logs on to the Content Engine, it collects the user information and verifies it against the authentication database. Once the user’s credentials are validated, an entry is created in the authentication cache with the following information and is stored in the authentication cache for a default time period of 480 minutes (an eight-hour work day).

- User name
- Password
- IP address
- Time of last access
- When the user was authenticated.

For example:

```
ce507#show http-authcache

AuthCache
  = = = = = = = = = = = = = = = =
hash 266: uid: ALLCISCO\JIM nBkt: (nil) nLRU: (nil) pLRU: (nil)
  lacc: 5 ipAddr: 10.1.1.7 keyType: IP Address
     Based filterTp: 0 auth
Used: 4
ce507#
```

The next time the user logs on, the Content Engine resets the 480-minute countdown timer. If 480 minutes passes without a request from the user, the Content Engine removes the user from the authentication cache. The next time the user logs on and there is no entry in the authentication cache, the logon request is challenged by the Content Engine.
Appendix A: Configuring Windows NTLM for User Authentication

Query Individual Users for More Information

The administrator may query the individual user for more information. For example:

- Domain\user name
- Client IP address
- Time since the Content Engine last saw a request from the user
- That the Content Engine is using IP Address Based mode (rather than doing a full credential verification)

For example:

```
ce507#show user username ALLCISCO\JIM
Username : ALLCISCO\JIM
Password: *****
IP address: 10.1.1.6
Time since last access: 141 seconds ago
Authenticated in: IP Address Based mode
```

c3507#

Guarantee Re-authentication Next Day

The Content Engine HTTP authentication cache may be cleared with the following command, which is sometimes scripted to run overnight, guaranteeing that all clients are required to re-authenticate the next morning.

```
ce507#clear users request-authenticated
ce507#show http-authcache
The authcache is empty
ce507#
```

**NOTE**

In the event the user’s credentials do not match a user in the Primary Domain Controller (PDC), or if the user resides in a group that is denied access to the internet, the Content Engine posts the following error message:

*Connection: Close WWW authentication failed or is missing*
Appendix A: Configuring Windows NTLM for User Authentication

NTLM User/Group Access Lists

The Content Engine may be configured to allow or disallow web access, based on specific NTLM groups using access lists in the 300 range.

To configure the Content Engine to allow or disallow web access, refer to the following commands:

- access-lists 300 deny|permit groupname (name)
- access-lists enable
- no access-lists enable

In the following example, an access-list configuration was implemented to deny Web-restricted users and permit Web-unrestricted users.

```
ce507#show access-lists 300
Access Control List Configuration
- - - - - - - - - - - - - - - - - - - - -
    Access Control List is enabled

    Groupname-based List (300)
    1. access-lists 300 deny groupname web-restricted
    2. access-lists 300 permit groupname web-unrestricted
    3. access-lists 300 deny groupname any

ce507#
```

The authentication cache was cleared to make sure the user logon is challenged in the authentication process. For example:

```
ce507#clear users request-authenticated

c507#sho http-authcache
The authcache is empty
c507#
```

In the following example, Jim could successfully get to the internet but Brian could not. With the debug application enabled, the Content Engine log fails:
Appendix A: Configuring Windows NTLM for User Authentication

authentication attempts with the statistics of the number of requests permitted or denied.

```
ce507#debug http-authcache ?
   all          Authcache all module debug
   application  Application module debug
   cli          CLI module debug
   daemon       Daemon client module debug

Jul 28 23:31:00 ce507 http_authmod: %CE-
AUTHMOD-3-540047: ***NTLM: query_smb: Invalid
Password; Samba failed to authenticate user
BRIAN domain ALLCISCO

Jul 28 23:42:36 ce507 cache: doHTTPauth: Hit
AUTHENTICATED_NODE - allow

ce507#show statistics access-lists 300
   Access Control Lists Statistics
   - - - - - - - - - - - - - - - - - - - - - -
   Groupname and username-based List (300)
   Number of requests: 16
   Number of deny responses: 11
   Number of permit responses: 5
```

cd507#
Appendix A: Configuring Windows NTLM for User Authentication

Transaction Reporting

The Content Engine appends transaction log entries to the /local1/working.log file in the configured format. The default log format is *squid*.

If the username is to be included in the log, the Content Engine must be configured for extended squid. If the domain name is also to be included, the Content Engine must be configured with *logo-windows-domain*.

The following are some log examples:

```
transaction-logs enable
transaction-logs log-windows-domain
transaction-logs export enable
transaction-logs export interval every-week on Sun at 00:01
transaction-logs export ftp-server 10.1.1.11 anonymous **** /
transaction-logs format extended-squid
```

c507#show transaction-logging
Transaction log configuration:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Logging is enabled.
End user identity is visible.
File markers are disabled.
Archive internal: every-day every 1 hour
Maximum size of archive file: 2000000 KB
Log File format is extended-squid.
Windows domain is logged with the authenticated username if available.

Exporting files to ftp servers is enabled.
File compression is disabled.
Export interval: every-week on Sun at 00:01 local time

```
server   type    username    directory
```

Integrated Cisco Products ◄ 249
10.1.1.11 ftp anonymous /

HTTP Caching Proxy Transaction Log File Info
Working Log file - size: 22427
    age: 1944
Archive Log file -
celog_10.1.1.2_20030723_180000.txt size: 1586
Archive Log file -
celog_10.1.1.2_20030723_190000.txt size: 8763

1059454286.418 60 10.1.1.6 TCP_MISS/200 1542
GET http://www.google.com/ ALLCISCO\JIM
DIRECT/www.google.com -

1059454286.478 20 10.1.1.6 TCP_HIT/200 8788
GET http://www.google.com/images/logo.gif
ALLCISCO\JIM NONE/ - -
APPENDIX B

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.
Appendix B: Stealth Mode

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.


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: Stealth Mode
APPENDIX C

Troubleshooting

You may encounter a situation while installing Websense Enterprise and configuring your Cisco integration 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 D: 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.
- I upgraded Websense, and configured users no longer appear under Directory Objects in Websense Manager.
- Network Agent fails to start on Linux with stealth mode NIC.
- Network Agent is not filtering or logging accurately.
- Windows 9x workstations are not being filtered as expected.
- Some users are receiving the Websense Global policy.
- Websense Enterprise splash screen is displayed, but installer does not launch on Windows 2000.
- Network Agent cannot communicate with Filtering Service after it has been reinstalled.
- I upgraded my Cisco PIX Firewall software to version 7.0, and web filtering stopped working.
Appendix C: Troubleshooting

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 164 for instructions.

I forgot my Websense Policy Server password

Contact Websense Technical Support for assistance. You can find contact information in *Appendix D: Technical Support*.

Where can I find download and error messages?

**Windows 2000 and 2003**

Check the Windows Application Event log or **Websense.log** (located in **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 Websense 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 is accessing the internet through a proxy server by checking the Database Download screen of the Settings dialog box in Websense Manager.
2. If a proxy server is being used, open a web browser (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 Filtering Service to access a DNS server.

If you need assistance, contact Websense Technical Support (see Appendix D: 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 32 for minimum installation requirements.
- Stop all memory-intensive services running on the machine before attempting another Websense Enterprise installation.
I upgraded Websense, and configured users no longer appear under Directory Objects in Websense Manager

If you are using Active Directory as your Directory Service, you may find that user names disappear from the list of directory objects in Websense Manager when you upgrade Websense. This will happen if your user names include characters that are not part of the UTF-8 character set.

To support LDAP 3.0, the Websense installer changes the character set from MBCS to UTF-8 during upgrade, so if your user names include non-UTF-8 characters, those characters will not be properly recognized. To fix this problem, try changing the character set back to MBCS.

1. In Websense Manager, go to Server > Settings > Directory Service.
   
   Active Directory (Native Mode) will be selected in the Directories pane if you are using Active Directory.

2. Click the Advanced Settings button.

3. Click MBCS under Character Set to change the character set from UTF-8 to MBCS.

Network Agent fails to start with stealth mode NIC

IP address removed from Linux configuration file

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 Manager and will be unavailable for use. To reconnect Network Agent to the NIC, restore the IP address in the configuration file.
Stealth mode NIC selected for Websense communications in Solaris and Linux

Network interface cards configured for stealth mode in Solaris and Linux are displayed in the Websense 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 Cisco Content Engine to act as a proxy for internet traffic, you must define the IP address of the proxy server machine in the Websense 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 205 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 if 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.


If your network uses Active Directory, and if you have Windows 98 client machines, refer to the following website for assistance: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp.
Appendix C: Troubleshooting

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 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 onscreen 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.

**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 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 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.**
Appendix C: Troubleshooting

The **Filtering Service Connection** dialog box appears.

7. Select the IP address of the Filtering Service machine from the **Server IP Address** drop-down list.

8. Click **Finish**.

9. Click **OK** in the **Local Settings** dialog box.

10. Click **OK** in the **Settings** dialog box to save the changes.

I upgraded my Cisco PIX Firewall software to version 7.0, and web filtering stopped working

In version 7.0(1) of the Cisco PIX Firewall software, the `url-server` command was changed: the minimum value for the `timeout` parameter was increased to 10 seconds. In previous versions (v6.3 or earlier), the minimum value for this parameter was 1 second, and the default value was 5 seconds. If you had `timeout` set to a value less than 10 seconds when you upgraded your software, the `url-server` command was deleted.

To resolve this issue, simply re-enter the `url-server` command. For more information, see *Cisco PIX Firewall or Adaptive Security Appliance (ASA)*, page 213.
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 products is available 24 hours a day on the internet at:

http://www.websense.com/global/en/SupportAndKB

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

Premium Support

Websense offers two premium fee-based support options: Priority One 24x7 Support and Platinum Support.

Priority One 24x7 Support offers extended service 24 hours a day, 7 days a week, and includes a toll-free number for customers in the U.S.

Platinum Support is our most comprehensive support and education offering. It includes the advantages of Priority One 24x7 Support as well as a dedicated support team, highest priority service, and educational opportunities.

For a complete list of Priority One 24x7 and Platinum Support services, please visit our website at:

http://www.websense.com/global/en/ProductsServices/Services

For additional information, please contact our U.S. Sales Department at 1 800 723 1166 or 1 858 320 8000, or send an email to sales@websense.com.
Appendix D: Technical Support

For information about the availability of premium support programs for customers outside the U.S., please contact your local Websense sales office:

http://www.websense.com/global/en/AboutWebsense/ContactUs

Support Options

Websense Technical Support can be requested 24 hours a day, 7 days a week.

Web Portal

You can submit support tickets through the Web Portal 24 hours a day, 7 days a week. 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/global/en/SupportAndKB/CreateRequest

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
- uksupport@websense.com—London, England

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

Customers in Japan should contact their distributor for the most rapid service.

Telephone Assistance

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

- Websense subscription key.
- Access to the configuration interface for your Websense products.
- Access to the machine running the Filtering Service, the Websense Reporting components, 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 the Websense configuration files.

A list of other applications running on the Filtering Service machine.

For severe problems, additional information may be needed.

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

- U.S. Technical Services in San Diego, California, USA: 1 858 458 2940
- U.K. Technical Services in London, England: +44 (0) 1932 796244

Customer Care

Not sure who to call? Contact Customer Care for assistance with:

- General concerns
- Subscription key questions or issues
- Follow-up on telephone support issues
- General service requests

A Customer Care representative can be reached at:

- Customer Care U.S. in San Diego, California: 1 866 355 0690 (from the U.S. only) or 1 858 320 9777, or customeercare@websense.com
- Customer Care International in Dublin, Ireland: +353 (0) 1 6319360 or intcustcare@websense.com

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

A
ACS (See authentication)
Active Directory, 30
  running logon script from, 202–204
adding components
  Linux, 173–175
  Solaris, 173–175
  Windows, 165–172
Address Resolution Protocol (ARP), 253
Apache HTTP Server
  installing, 84, 116
ASA
  authentication, 226
  commands
    filter except, 222
    filter ftp, 220–222
    filter https, 218–220
    filter url http, 216–218
    show perfmon, 222
    show url-cache statistics, 222
    url-server, 214–216
  configuring
    console or TELNET session, 214–225
    enhanced caching, 225–226
    handling long URLs, 223
    help commands, 214
    HTTP response buffer, 224
    increasing internal buffer, 223
    response block buffer, 224
    Websense Enterprise configuration
      with, 23–24
authentication
  and Cisco Secure ACS, 75
  ASA, 226
  directory services, 30–32
  enabled in Content Engine, 227
  of users, 75
  PIX Firewall, 226
  User Service, 16
Windows NTLM
  browser configuration, 241–242
  configuring the Content Engine, 243–244
  group access lists, 247–248
  managing HTTP proxy cache, 245–246
  querying users on Content Engine, 246
  re-authentication commands, 246
  transaction reporting, 249–250
  with RADIUS Agent, 122, 154

B
Bandwidth Optimizer, 10, 13, 85, 97, 110, 149, 169, 173
block messages
  for protocols, 197–198
block page port, 132, 163
block page URL, 196–197
browser
  and Content Engine Internet access, 230
  configuring for promptless authentication, 241–242
  path to, 147
  proxy-based connections for, 33
  bytes transferred, 10

C
Cisco Routers
  configuration commands
    ip inspect name, 234
    ip urlfilter alert, 235
    ip urlfilter allowmode, 237
Index

ip urlfilter audit-trail, 235
ip urlfilter cache, 237
ip urlfilter exclusive-domain, 236
ip urlfilter maxrequest, 237
ip urlfilter packet-buffer, 237
ip urlfilter server vendor, 234
ip urlfilter urlf-server-log, 236
configuring for Websense Enterprise, 26
config.xml
  incompatibility of with previous versions, 37
  possible problems with during uninstall, 178
  repairing the Policy Server, 186
config.xml file, 37
configuration
  console session
    ASA, 214–225
    Content Engine, 228–229
    PIX Firewall, 214–225
Content Engine with Websense Enterprise, 25
IOS Routers with Websense Enterprise, 26
TELNET session
  ASA, 214–225
  Content Engine, 228–229
  PIX Firewall, 214–225
Websense Enterprise with Cisco ASA, 23–24
Websense Enterprise with PIX Firewall, 23–24
Content Engine
  browser access to Internet, 230
  clusters, 231
  configuring
    Cisco web-based interface, 227
    console or TELNET session, 228–229
    firewalls or routers, 230
    with Websense Enterprise, 25
  Windows NTLM authentication
    browser configuration, 241–242
    configuring, 243–244
    forcing re-authentication, 246
    transaction logging, 249–250
customer support, See technical support

D
database download, See Master Database download
DC Agent
  defined, 10
  deployment of, 18
  installing separately, 113–115
  required privileges for, 78
Default Web Site, 85, 117
deploying Remote Filtering Client
  third party tools for, 54
deployment
  component requirements, 15–22
  directory services, 30–32
  Network Address Translation (NAT), 30
  network requirements, 22–32
  tasks, 14
  Websense in switched environments, 27–29
directory path for installation
  Solaris and Linux, 100
  Windows, 90
directory services
  general requirements, 34
  supported types, 30–32
DirectX requirement, 262
dNS server, 33, 196
domain administrator privileges, 78, 105, 165
domain controller
  testing for visibility from, 261
Index

E
eDirectory Agent
  defined, 11
  deployment of, 19
  installing separately
    Linux, 156–157
    Solaris, 156–157
    Windows, 123–125
eimserver.ini file, 37
  identifying Filtering Service for block page
    URL, 196
enhanced caching with ASA, 225–226
enhanced caching with PIX Firewall, 225–226
error messages
  location of, 256
evaluation key
  website for downloading, 83, 97

F
files
  backups of when upgrading, 37
filter except command, 222
filter ftp command, 220–222
filter https command, 218–220
filter port, 132, 163
filter url http command, 216–218
Filtering Service
  defined, 10
  deployment of, 15
  identifying for block page URL, 196–197
  machine identification, 112, 132, 151, 163
  multiple installations of, 23
  port number, 97

G
Global Websense policy application, 260

H
help commands in ASA, 214
help commands in PIX Firewall, 214
HTTP proxy server
  managing authentication cache, 245–246
HTTP proxy server authentication, 241

I
IIS Web Server
  detecting, 84, 116
IM Attachment Manager, 10, 13, 85, 97, 110, 149, 169, 173
installation
  Apache HTTP Server, 84, 116
  console mode in Windows, 262
  Custom option, 75
  DC Agent, 113–115
  detecting IIS Web Server, 84, 116
eDirectory Agent
  Linux, 156–157
  Solaris, 156–157
  Windows, 123–125
Filtering Service port, 97
Logon Agent, 125–127
  Linux, 157–159
  Solaris, 157–159
Manager
  Linux, 147–148
  Solaris, 147–148
  Windows, 108–109
Network Agent
  Linux, 148–152
  Solaris, 148–152
  Windows, 109–113
Policy Server port, 97
RADIUS Agent
  Linux, 154–155
  Solaris, 154–155
  Windows, 122–123
Real-Time Analyzer, 116–120
Remote Filtering Client, 135–145
Remote Filtering Client Pack, 133–135
Remote Filtering Server, 127–133
  Linux, 160–164
  Solaris, 160–164
  Windows, 127–133
Usage Monitor
  Linux, 152–154
  Solaris, 152–154
  Windows, 120–121
Index

Websense Enterprise
  Linux, 94–102
  separate Windows machine, 77–93
  Solaris, 94–102
Windows installer does not launch, 262
Internet access problems, 257–258
IP addresses
  changing for installed components, 73
  configuring for proxy servers, 205–207
  defining ranges for Network Agent, 17, 109
  disabling for stealth mode, 252
  DNS server resolution, 33
  multiple network interface cards, 81
  overlapping ranges, 28
requirements for Websense
  communication, 96
  stealth mode and, 251
  transparent identification for, 32
  User Service requirements for, 16

L
Language Pack, 75
languages
  Language Pack, 37
  locales, 16
launch.ini file, 262
LDAP directory service, 30
Linux
  adding components on, 173–175
  error messages, 256
  removing components on, 179–180
  repairing components on, 183–184
  starting and stopping Websense
  services, 190
  upgrading Websense Enterprise on, 45–50
  Websense Enterprise installation on, 94–102
load balancing, 23
locales, 16
Logon Agent
  defined, 11
  deployment of, 20
  failure to identify users, 260–262
  installing separately
  Linux, 157–159
  Solaris, 157–159
  Windows, 125–127
logon script
  domain controller visibility issues, 261
  enabling NetBIOS for, 261
  user profile issues, 262
LogonApp.exe
  configuring to run
    Active Directory, 202–204
    Windows NTLM, 204–205
  location of, 198
  script for, 199–202
M
MAC address, 253
Manager, See Websense Manager
manual authentication, 31
Master Database
  description of, 12
  reloading when repairing Policy Server, 186
Master Database download
  and virus scanners, 258
  during installation
    Solaris and Linux, 97, 101
    Windows, 91–92
  during upgrade
    Solaris and Linux, 49, 66
    Windows, 43–44, 61–63
  error message location, 256
  failure of, 257–258
  from the Websense Manager, 192–196
  performing, 192–196
  Messenger Service, 197
  mirroring, 27
  modifying an installation, 164–184
N
NetBIOS, 18
  enabling for logon script, 261
Netscape location, 48, 65
Network Address Translation (NAT), 30
Network Agent
bandwidth optimizer, 85, 97, 110, 149, 169, 173
capture interface, 86, 98, 112, 150, 170, 174
defined, 10
deployment of, 16
feedback on protocol usage, 87, 98
in switched environments, 16, 27
installing separately
  Linux, 148–152
  Solaris, 148–152
  Windows, 109–113
instant messaging attachment manager, 85, 97, 110, 149, 169, 173
multiple installations of, 28
Network Address Translation (NAT), 30
network interface card, 207
on firewall machine, 150
protocol management, 85, 97, 110, 149, 169, 173
proxy server IP address, 205–207
stealth mode NIC, 251–253
network efficiency, 34
network interface cards (NIC)
  configuring for stealth mode
    Solaris or Linux, 253
    Windows, 252
  installation tips, 76
  selecting for Network Agent, 86, 98, 111, 170, 174
Novell Directory Service/eDirectory Agent, 30
Novell Directory Services/eDirectory Agent, 31
NTLM authentication, See authentication

P
  pass phrase for remote filtering, 130, 162
  password
    forgotten, 256
  Policy Server setting, 193
  proxy server/firewall setting, 194
PIX Firewall
  authentication, 226
  commands
    filter except, 222
  filter ftp, 220–222
  filter https, 218–220
  filter url http, 216–218
  show perfmon, 222
  show url-cache statistics, 222
  url-server, 214–216
configuring
  console or TELNET session, 214–225
enhanced caching, 225–226
handing long URLs, 223
help commands, 214
HTTP response buffer, 224
increasing internal buffer, 223
response block buffer, 224
Websense Enterprise configuration
  with, 23–24
Policy Server
  defined, 10
  deployment of, 15
  failure to install, 258
  machine identification, 110, 116, 120
  port number, 97
  repairing, 185–186
port numbers
  Filtering Service, 112, 132, 151, 163
  Policy Server, 110, 116, 120
  port spanning, 27
  protocol block messages, 197–198
  Protocol Management, 10, 13, 85, 97, 110, 149, 169, 173
proxy server
  identifying for Network Agent, 205–207
  settings for Master Database download, 195
Q
  quotas, 13

R
  RADIUS Agent
    defined, 11
    deployment of, 19
    installing separately
      Linux, 154–155
### Index

**Solaris**, 154–155  
**Windows**, 122–123  

**Real-Time Analyzer (RTA)**  
defined, 11  
deployment of, 17  
installing separately, 116–120  
launching, 120, 172  
supported web servers for, 84, 116  

**Remote Filtering Client**  
defined, 11  
deployment of, 21  
installing  
manually, 136  
with third-party tools, 140  
repairing an installation, 144  
uninstalling, 145  
upgrading, 51  
manually, 52  
with third-party tools, 54  

**Remote Filtering Client Pack**  
defined, 104  
installing, 133–135  
upgrading, 51  

**Remote Filtering Server**  
defined, 11  
deployment of, 20  
**External Communication Port**, 129, 138, 141, 161  
firewall configuration for, 210–211  
installing  
**Linux**, 160–164  
**Solaris**, 160–164  
**Windows**, 127–133  
**Internal Communication Port**, 130, 138, 141, 161  
pass phrase, 130, 162  
upgrading, 51  
removing components  
**Linux**, 179–180  
**Solaris**, 179–180  
**Windows**, 176–178  
repairing components  
**Linux**, 183–184  
**Solaris**, 183–184  

**Windows**, 180–183  
reporting  
transactions for authentication, 249–250  

**Reporting Tools**  
deployment of components, 22  
supported version, 38, 75  

**S**  
Samba client, 47, 65, 99  
Secure Authentication (ACS), 31  
set up  
**block page URL**, 196–197  
**Master Database download**, 192–196  
**subscription key**, 192–196  
**show perfmon command**, 222  
**show url-cache statistics command**, 222  

**Solaris**  
adding components on, 173–175  
error messages, 256  
removing components on, 179–180  
repairing components on, 183–184  
starting and stopping Websense services, 190  
upgrading Websense Enterprise on, 45–50  
Websense Enterprise installation, 94–102  
**squid log format**, 249  

**Stand-Alone Edition**  
converting to integrated system  
**Solaris and Linux**, 70–72  
**Windows**, 67–70  
upgrading  
**Solaris and Linux**, 63–67  
**Windows**, 57–63  
version information for upgrading, 55  

**stealth mode**, 96  
configuring  
**Solaris or Linux**, 253  
**Windows**, 252  
definition of, 251  
problems with NIC, 259–260  
using with Network Agent, 251  
**subscription key**  
entering, 192–196
Master Database download during installation with, 83, 97
verification and troubleshooting of, 257
Sun Java System Directory Server, 30, 31
switched environments, 16, 27
system requirements, 32
Cisco integrations supported, 33
workstations, 33

T
TCP/IP protocol, 33
technical support
documentation feedback, 267
e-mail, 266
premium support, 265
support website, 265
telephone assistance, 266
Web Portal, 266
TELNET configuration
ASA, 214–225
Content Engine, 228–229
PIX Firewall, 214–225
Traffic Visibility Tool, 208
transparent identification, 31

U
upgrading
changing Cisco integration products, 72–73, 186–187
distributed component, 37
general information, 37–39
manually restarting services, 38
non-English language versions, 37
on Linux, 45–50
on Solaris, 45–50
on Windows, 39–45
Remote Filtering Client, 51
Remote Filtering Server, 51
transferring data to fresh install, 36–37
versions supported, 36
url-server command, 214–216
Usage Monitor
automatic installation during upgrade, 38

defined, 10
deployment of, 17
installing separately
Linux, 152–154
Solaris, 152–154
Windows, 120–121
user identification, 30–32
user profile issues with logon script, 262
User Service
defined, 10
deployment of, 16
required privileges, 78, 105, 165
users
authenticating, 75
authentication query on Content Engine, 246

V
virus scanners, 258

W
Web Cache Communication Protocol (WCCP), 230
Web Security Suite, 9
Websense Enterprise
bypass for specified IP addresses, 222
component configurations, 15–22
components
adding, 164–175
removing, 176–180
converting Stand-Alone system to integrated
Solaris and Linux, 70–72
Windows, 67–70
functional overview, 12–13
installation on
Linux, 94–102
Solaris, 94–102
Windows, 77–93
selecting a NIC for communication, 251
versions supported for upgrade, 36
Websense Enterprise - Corporate Edition, 9
Websense Enterprise Explorer, 12
Websense Enterprise Explorer for Unix, 12
Index

Websense Enterprise Reporter, 12
Websense Manager
  defined, 10
  deployment of, 16
  does not launch, 262
  installing separately
    Linux, 147–148
    Solaris, 147–148
    Windows, 108–109
  launching, 193
Websense Master Database, See Master Database
Websense services
  manually stopping, 188
  starting and stopping
    Linux, 190
    Solaris, 190
    Windows, 188–190
  stopping before upgrading, 38
Websense Web Security Suite, 9
websense.ini file, 37

Websense.log, 256
Windows
  Active Directory, 30, 31
  adding components on, 165–172
  converting Stand-Alone to integrated system, 67–70
  error messages, 256
  NTLM-based directories, 30, 31
  removing components on, 176–178
  starting and stopping Websense services, 38, 188–190
  upgrading Websense on, 39–45
  Websense Enterprise installation, 77–93
Windows NTLM
  group access lists, 247–248
  running logon script from, 204–205
Windows XP SP2 and protocol block messages, 197
winpopup.exe, 198
workstations, 33
WSSEK.dat file, 139