v5.2

Installation Guide for Websense Enterprise v5.2 Embedded on Cisco® Content Engine with ACNS v.5.3

Websense Enterprise Installation Guide

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published May 13, 2005
Printed in the United States of America

NP33-0003CCO

Trademarks

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

Microsoft, Windows NT, Windows 2000, Windows 2003, Windows XP, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc., in the United States and other countries. Sun, Sun ONE and all Sun ONE based trademarks and logos are trademarks of Sun Microsystems, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

The following is a registered trademark of Novell, Inc., in the United States and other countries: Novell Directory Services.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries.

Linux is a trademark of Linux Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (**http://www.apache.org**).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

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

WinPcap

Contents

CHAPTER 1 Introduction

Thank you for choosing to implement Websense Enterprise, which is embedded on the Cisco Application and Content Networking System (ACNS) Content Engine. Websense Enterprise is the leader in Employee Internet Management.

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.

The major components of Websense Enterprise are:

- **Policy Server**—stores all Websense Enterprise configuration information and communicates this data to other Websense services.
- **Filtering Service**—interacts with Cisco Content Engine ACNS v5.3 to provide Internet filtering.
- **User Service**—allows you to apply filtering policies based on users, groups, domains, and organizational units.
- **Websense Enterprise Manager**—administrative interface that communicates with Policy Server to configure and manage the Filtering Service.
- **DC Agent**—an optional component that transparently identifies users for filtering through a Windows directory service.
- **Network Agent**—detects HTTP network activity and calculates the number of bytes transferred. It then instructs the Filtering Service to log this information. You must properly configure Network Agent if you want to use the Bandwidth Optimizer, Protocol Management, and enhanced reporting features.
- **Websense 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.

- **RADIUS Agent**—an optional component that works with RADIUS Server to transparently identify users and groups who use access your network from remote connections. These connections may include dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), and others.
- **eDirectory Agent**—an optional component that works with Novell eDirectory to transparently identify users so Websense can filter them according to particular policies assigned to users or groups.
- **Websense Enterprise Master Database**—the proprietary Websense database, which contains a collection of nearly 4 million Internet sites that represent more than 800 million pages, each categorized by content, and updated daily.
- **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, Websense Enterprise 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 Administrator's Guide* for installation and configuration procedures.

How Websense Works

The Websense Enterprise Filtering Service engine enforces content filtering. You define a flexible policy that identifies filtering parameters, and apply different policy to the various users, groups, network domains, company divisions or departments, workstations, or networks).

When Cisco Content Engine ACNS v5.3 receives an Internet request from a client, it queries Filtering Service to find out whether the requested site should be blocked or not. Filtering Service checks the policy that affects the client machine making the request. Each policy defines specific time periods during the week and lists the category sets that are in effect during those time periods.

After it determines which categories are blocked, Filtering Service consults its comprehensive database of Internet addresses (URLs):

- If the site is assigned to a blocked category, the user receives a block page instead of the requested site.

- If the site is assigned to a permitted category, or belongs to the Miscellaneous set of sites, Websense Enterprise notifies Cisco Content Engine ACNS v5.3 that the employee may access the site. The employee never realizes that a check occurred.

Websense Enterprise filters network applications that use TCP-based protocols and provides filtering and logging support for UDP-based protocols 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.

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

With the Protocol Management feature, Websense Enterprise can filter Internet protocols other than HTTP, HTTPS, and FTP. 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.

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, please refer to the *Quotas* section in your Websense *Enterprise Administrator's Guide*.

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.

Deployment Tasks

The following sequence is recommended for installing Websense Enterprise components and configuring your system to filter Internet traffic with the Cisco Content Engine ACNS v5.3.

1. **Plan the Websense deployment.** Websense components can be deployed in various combinations depending upon the size and architecture of your network. Deciding what Websense components to install and where to put them is your first task. Consult *Chapter 2: Network Configuration* for sample deployment options and to determine the operating systems supported by each Websense Enterprise component.
2. **Configure Cisco Content Engine ACNS v5.3 for NTLM authentication:** You can either enable User Service on Cisco Content Engine ACNS v5.3 or install User Service as an independent component on a separate Windows machine. Regardless of where User Service is running, you will need to configure Windows NTLM for user authentication. For details about this type of configuration, refer to the *Websense Enterprise v5.2 Administrator's Guide*.
3. **Install Websense Enterprise Manager and optional Websense Enterprise components.** Using the appropriate download file for the operating system, install Websense Enterprise Manager on a separate machine in your network. Install optional Websense components on separate machines in your network or together on the same machine as the Manager. Refer to the specific instructions in *Chapter 7: Install Websense Enterprise on Remote Machines*.
4. **Perform the initial setup.** Setup tasks include:
   - **Download the Websense Enterprise Master Database**. Refer to *Configuration via Websense Enterprise Manager*, page 112, for instructions on entering your subscription key and downloading the Websense Enterprise Master Database.
   - **Identify the Filtering Service for block pages.** Refer to *Configure Websense Filtering Service*, page 62, for instructions.
   - **Identify Users.** Refer to *Directory Services*, page 29, for instructions on using the supported directory services.
   - **Identify upstream routers and firewalls in Websense Enterprise.** Refer to *Configure FireWalls or Routers*, page 118, for instructions.
   - **Configure workstation browsers.** Refer to *Browser Access to the Internet via Cisco Content Engine ACNS v5.3*, page 72, for instructions on configuring browsers to send Internet requests through the Cisco Content Engine ACNS v5.3.

Related Documentation

When you install and use Websense Enterprise v5.2 for ACNS, the following documents may be of value.

- *Websense Enterprise v5.2 Reporting Installation Guide*
- *Websense Enterprise v5.2 Administrator's Guide*
- *Websense Enterprise v5.2 Reporting Administrator's Guide*
- *Websense Enterprise v5.2 Explorer Administrator's Guide*
- *Transparent Identification of Users in Websense Enterprise v5.2* (technical white paper)

All Websense Enterprise documents are available at http://ww2.websense.com/global/en/SupportAndKB/ProductDocumentation/.

CHAPTER 2 | Network Configuration

There are numerous ways you can configure Websense Enterprise for Cisco Content Engine ACNS v5.3. This chapter identifies several common deployment options, hardware requirements for component installation, and installation dependencies and specifics.

Identify Deployment Options

When you purchase Cisco Content Engine ACNS v5.3, a number of Websense Enterprise components are embedded on the appliance for an "on-box" solution. You can enable a component on the appliance, or disable it and then install the component elsewhere.

Websense Enterprise installation options are highly flexible. This allows you to enable and/or disable components embedded on Cisco Content Engine ACNS v5.3, to install components on a single remote machine, or to enable some components on Cisco Content Engine and install others on remote machines. To help identify installation options, the next table shows the options for each Websense Enterprise component.

Websense Component	Embedded	Remote Machine	Multiple Instances
Policy Server (required)	Yes [1]	Yes	No
User Service (required)	Yes [1]	Yes	No
Filtering Service (required)	Yes	Yes	Yes [2]
Network Agent (required)	Yes	Yes	Yes [2, 3]
DC Agent (optional)	No	Yes[5]	Yes[4]
eDirectory Agent (optional)	Yes	Yes	Yes [5, 6]
RADIUS Agent (optional)	Yes	Yes	Yes [6]

Websense Component	Embedded	Remote Machine	Multiple Instances
Websense Enterprise Reporter (optional)	No	Yes [7]	No
Real-Time Analyzer (RTA) (optional)	No	Yes [8, 9]	No

[1] Only one instance can be enabled for each logical Websense Enterprise installation. For most deployments, subscribers choose to enable Policy Server on Cisco Content Engine ACNS v5.3.

[2] Must be enabled on Cisco Content Engine ACNS v5.3 with other instances installed on remote Windows machines or other Cisco Content Engine appliances.

[3] Each instance must be assigned a range of IP addresses to identify monitoring responsibilities. IP address ranges cannot overlap.

[4] Must be set to use administrator level access at the installation machine.

[5] Each instance must be able to communicate with a Novell eDirectory Server.

[6] Each instance must be able to communicate with Filtering Service.

[7] Must be installed on a Windows machine, must be the same version as Websense Enterprise, and must be available if you want to use RTA for reporting.

[8] Websense Enterprise Reporter must be installed for this component to work. All components must be the same version.

[9] Either the IIS or Apache Web Server must be installed for this component to work.

Deploy Websense

The network diagrams in this section represent common configurations that provide maximum efficiency. Because Websense Enterprise deployment is flexible, be aware of the following as you plan your installation:

- A number of Websense components are embedded on Cisco Content Engine ACNS v5.3, any of which you can enable or disable.
- If you disable components on Cisco Content Engine ACNS v5.3, you can install the same components at remote machines.
- Some optional components cannot be installed or enabled on Cisco Content Engine ACNS v5.3. These must be installed manually on one or more remote machines.

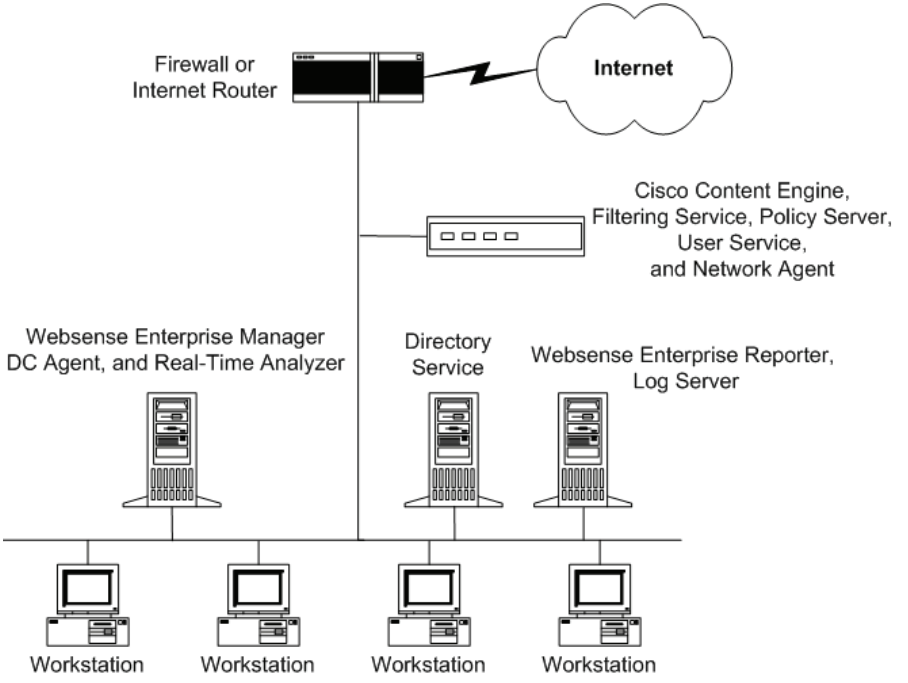
The architecture shown in this section is appropriate for networks with fewer than 1,000 users. For deployment guidelines, read *Embedded Websense Components*, page 22, and *Remote Websense Components*, page 27.

You can achieve load balancing in large environments by installing multiple instances of Filtering Service. For details, read *Websense Enterprise Administrator's Guide.*

Typical configurations include networks with:

- a single firewall, proxy server, or caching appliance
- an array of firewalls, proxy servers, or caching appliances

A common network topology places Cisco Content Engine ACNS v5.3 with Websense Enterprise behind the firewall. Websense Enterprise Manager, RTA, and DC Agent are installed together on a Windows server machine communicating with Policy Server on Cisco Content Engine through TCP/IP. You can also install Websense Enterprise Manager on multiple machines in the network to enable remote configuration of Policy Server.



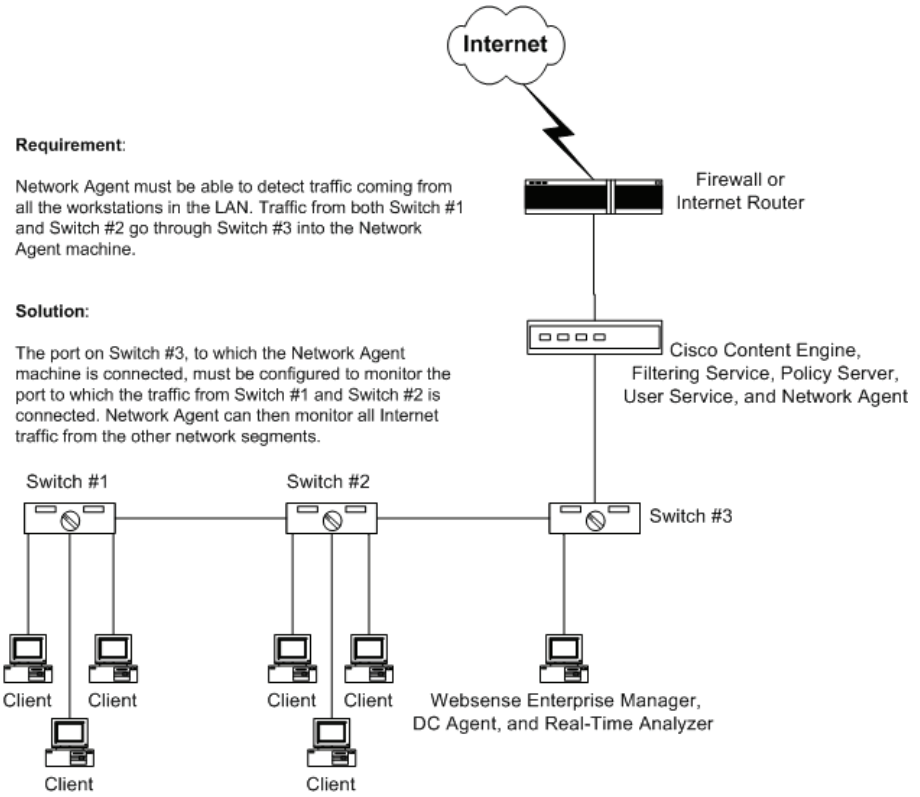
Websense Enterprise, Network Agent, and Cisco Content Engine ACNS v5.3 Behind Firewall

Switched Environments

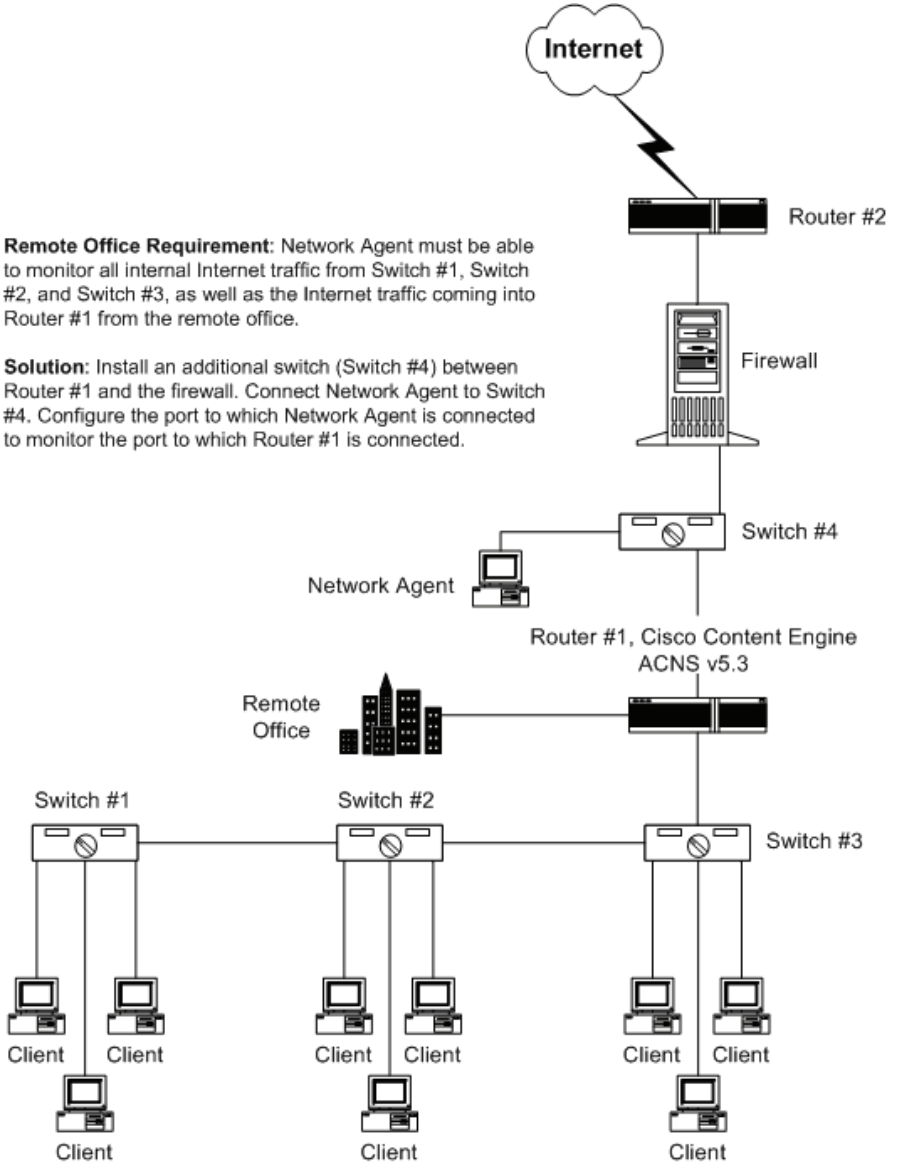
In a switched environment, configure a switch to use *mirroring* or two-way port spanning, so Network Agent can detect Internet requests from all workstations.

NOTE

Contact your switch vendor to determine if your switch is capable of mirroring or port spanning, and for configuration details.



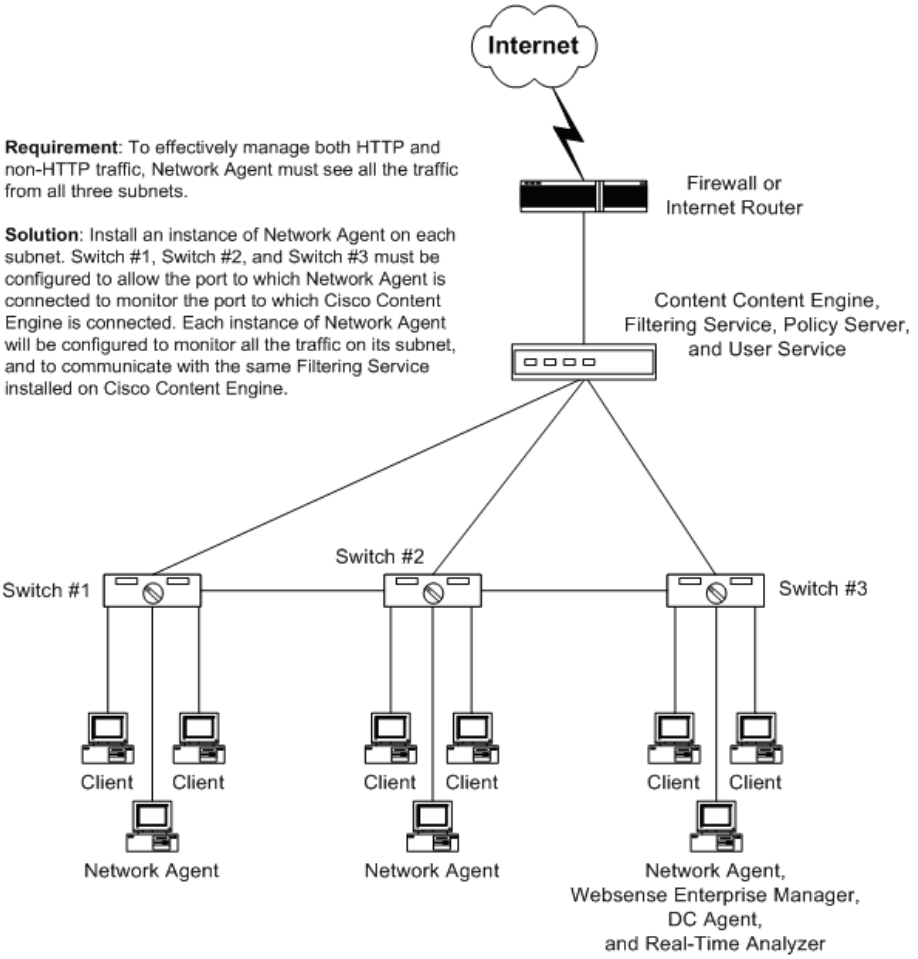
Basic Deployment in a Switched Environment



Switched Environment with a Remote Office Connection

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

- Do not assign overlapping IP address ranges. If IP ranges overlap, network bandwidth measurements will not be accurate and bandwidth-based filtering will not be applied correctly.
- Deploy the instances of Network Agent so they can filter the entire network. Partial deployment results in the loss of log data from network segments that are not watched by Network Agent.



Multiple Network Agents in a Switched Environment

Embedded Websense Components

A number of Websense components are embedded on Cisco Content Engine ACNS v5.3. You can use the embedded installation of these components or disable the embedded instance and then install the same component on a remote machine or machines. Some components can run at the same time on Cisco Content Engine and remote machines.

Three embedded components must be enabled and/or installed. If these three components are not enabled on Cisco Content Engine or installed on a remote machine, Websense Enterprise will not work. Other components are optional, and support transparent user identification and reporting options.

Required Components

The next table identifies embedded Websense components that are required for operations. The information in the table includes any known requirements and limitations that may impact your Websense installation.

Websense Component	@ Cisco Content Engine ACNS v5.3	@ Remote Machine
Policy Server	Only one Policy Server can be active for each logical Websense installation.	Disable Policy Server on Cisco Content Engine ACNS v5.3 to install Policy Server on a remote machine.
	For Policy Server installations, be aware of the following: • One instance of Policy Server delivers the same policies and category details to the subnet with which it is associated. • The machine where Policy Server runs identifies the locale/language for the Websense Enterprise components. If you need to use multiple languages, you **must** install one instance of Filtering Service, Policy Server, and User Service on a separate machine for **each** language you want to support, where the machine must use operating system for that language.	

Websense Component	@ Cisco Content Engine ACNS v5.3	@ Remote Machine
Filtering Service	In very large networks, this component may be installed/ enabled at more than one Cisco Content Engine ACNS v5.3, or on remote machines to distribute the load.	May be installed on remote Windows machines, in addition to the instance on Cisco Content Engine ACNS v5.3.
User Service	Only one User Service can be enabled for each logical Websense installation. For example, one User Service installation serves all machines on a subnet.	Disable User Service on Cisco Content Engine ACNS v5.3 before you install and enable User Service on a remote machine.

Optional Components

The next table identifies Websense components that are not necessary for operations but are embedded on Cisco Content Engine ACNS v5.3. These optional components provide user identification processes or support reporting functions. You can install these components on a remote machine or machines if you choose. The information in the table includes any known requirements and restrictions that may impact your Websense installation.

<table>
<tr><th>Websense Component</th><th>@ Cisco Content Engine ACNS v5.3</th><th>@ Remote Machine</th></tr>
<tr><td rowspan="2">Network Agent</td><td>You can enable the instance of Network Agent embedded on Cisco Content Engine ACNS v5.3, even if other instances of Network Agent run at remote machines.</td><td>Install any number of instances on remote machines. The operating system may be either be Windows or Linux.</td></tr>
<tr><td colspan="2">When installing/deploying Network Agent, be aware of the following:
Do not install Network Agent on machines running any type of firewall. Network Agent uses WinPcap, a Microsoft architecture that captures and analyzes network packets, and firewalls may interfere with the WinPcap ability to detect HTTP requests.
Make sure Cisco Content Engine ACNS v5.3 or the remote machine where Network Agent runs can see Internet traffic from your network.
Network Agent can run in switched environments. For details, read Switched Environments, page 19.
To distribute excessive load, you can install multiple instances of Network Agent in large networks, where each agent monitors a specific IP address range for your network. For details, check the Websense Enterprise Administrator's Guide.
For installations using multiple instances of Network Agent, make sure that your agents are able to monitor your entire network. If the Network Agents cover only a portion of the network, you will lose data from network segments that are not being monitored.
Do not deploy Network Agent across LANs. If Network Agent and Policy Server communicate across LANs using any combination of switches and routers, communication delays may prevent Network Agent from blocking Internet requests in a timely fashion.
If you are implementing Bandwidth Optimizer, Protocol Management, or reporting functions, you must configure Network Agent.</td></tr>
</table>

Websense Component	@ Cisco Content Engine ACNS v5.3	@ Remote Machine
eDirectory Agent	You can enable eDirectory Agent embedded on Cisco Content Engine ACNS v5.3, even if other instances of eDirectory Agent are running on remote machines.	You can install eDirectory Agent on remote machines, even if you enable the instance at Cisco Content Engine ACNS v5.3. You can install remote instances of eDirectory Agent on machines running Windows, Solaris, or Linux.
	When deploying eDirectory Agent, be aware of the following restrictions: • You **must** have a Novell eDirectory Server able to communicate with all instances of the agent. • You **must** configure each instance of eDirectory Agent to communicate with every Novell eDirectory Server you include in your topography. Refer to *Websense Enterprise Administrator's Guide* for configuration details. • If you install multiple instances of eDirectory Agent, you must configure communications between each instance and Filtering Service. • If you replicate Novell eDirectory Server to improve response time, eDirectory Agent must be able to communicate with the original instance of the Novell eDirectory Server and any machines where you have created a replica of that server.	

<table>
<tr><th>Websense Component</th><th>@ Cisco Content Engine ACNS v5.3</th><th>@ Remote Machine</th></tr>
<tr><td>RADIUS Agent</td><td>You can enable the RADIUS Agent instance embedded on Cisco Content Engine ACNS v5.3, even if other RADIUS Agents run at remote machines. For large networks, multiple agents may be of value.</td><td>Install any number of RADIUS Agents on remote machines. If you install RADIUS Agent on a:
Windows machine, the agent runs as a service.
Linux or Solaris machine, the agent runs as a daemon.</td></tr>
<tr><td></td><td colspan="2">When deploying RADIUS Agent, be aware of the following restrictions:
You must have RADIUS Server installed on a remote machine.
Do not install RADIUS Agent on any remote machine that runs RADIUS Server. If you do, it is possible you will encounter port and IP address conflicts.
If you configure RADIUS Agent to use authenticated communications, you need to know the password you entered during setup, or that which is identified in Websense Enterprise Manager.
If you install multiple instances of RADIUS Agent, you must configure communications to Filtering Service for each instance.</td></tr>
</table>

Remote Websense Components

NOTE

While you can install any Websense Enterprise component on remote machines, the ones identified in this section are available for use **only** if you install them manually, as they a) are not embedded, and b) must run on a remote machine.

Websense installation choices include several optional components that are not embedded on Cisco Content Engine ACNS v5.3. These manually installed components all run on Windows operating systems; some can also run on Linux and Solaris systems.

The next table identifies Websense components that you must install manually if you choose to use the indicated component. The information in the table includes any known requirements and restrictions that may impact the installation.

IMPORTANT

You must access and use Websense Enterprise installers created specifically for Cisco Content Engine ACNS v5.3. If you use other installers, your implementation may fail to work as expected.

Websense Component	Function	Installation Details
Websense Enterprise Manager	System, filtering, and policy configuration	• Installs only on Windows machines • Multiple instances of Websense Enterprise Manager can run at the same time

Websense Component	Function	Installation Details
DC Agent	Transparent user identification	• Installs only on Windows server machines • Must have access to a Windows directory service, which may be Active Directory or NTLM • Only one instance of DC Agent can run in a domain • Multiple instances of DC Agent are supported • May be installed on any network segment if NetBIOS is allowed between DC Agent and the domain controller • DC Agent should not be installed in any network segment that acts as a DMZ
Websense Enterprise Reporter (suite)	• Log Manager receives and saves Internet access data • Websense Enterprise Reporter provides report configuration and scheduling tools • Explorer provides drill-down access to report details	• Installs only on Windows machines • Supports Websense Enterprise Reporter, Real-Time Analyzer, and Websense Enterprise Explorer • Install the same version of Websense Enterprise and Websense Enterprise Reporter--if you do not, you will not be able to generate reports
Real-Time Analyzer (RTA)	Internet access reporting, showing details including protocols and bandwidth use	• Installs only on Windows machines • Requires an Internet Server; which must be either Apache, version 2.x or later, or Microsoft IIS v4.0 or v5.0 • Must have access to an installed instance of Websense Enterprise Reporter

Directory Services

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

- Windows NTLM-based directories
- Windows Active Directory
- SunONE Directory Server v4.2 and v5.1
- Novell Directory Services/eDirectory v8.51, v8.6, and v8.7

For configuration details, see the *Websense Enterprise Administrator's Guide*.

Websense Enterprise can communicate with your directory service whether it runs on the same operating system as Websense Enterprise or not.

You can base filtering on an individual user, group, domain, and/or departmental policy, providing that Websense Enterprise can identify the user making the Internet request. The authentication method you configure must allow Filtering Service to get directory object information from a Windows or LDAP directory. For details, read the *Websense Enterprise Administrator's Guide.*

Websense can use LDAP expressions to classify users for filtering purposes. You can create named groups of users based on any LDAP attribute in your directory service, and add these groups to Websense Enterprise Manager. For details, see the *Websense Enterprise Administrator's Guide*.

NOTE

Websense can filter Internet access using workstation or network policies in any environment. Websense identifies:

- workstations by their IP addresses
- networks by IP address ranges

Websense Enterprise can transparently identify users in a Windows domain if DC Agent is installed on a Windows NT or Windows 2000 Server in the network. The transparent identification feature allows Websense Enterprise to filter Internet requests from users identified in a Windows directory without prompting them to manually authenticate.

Once you configure communications between Filtering Service and DC Agent, DC Agent gets user information from a Windows-based directory service, and then sends it to Filtering Service. When Filtering Service receives the IP address of a machine making an Internet request, it matches the address with the corresponding user name that DC Agent provides. This allows Websense Enterprise to transparently identify users whenever they open a browser that sends Internet requests. For details, read the *Websense Enterprise Administrator's Guide*.

In cases where Websense Enterprise cannot identify users transparently via your directory service, you should also enable manual authentication. This configuration forces users to authenticate requests manually only if they cannot be transparently identified.

You can filter Internet requests using policies assigned to individual directory objects one you have completed the following tasks.

- If you are using a Windows NTLM-based directory or Active Directory:
  1. Configure the Windows directory service within Websense Enterprise.
  2. Install and configure DC Agent so Websense Enterprise can identify users transparently. You must install DC Agent on a Window NT or Windows 2000 server that is on the network where you enable or install Websense Enterprise components.
  3. Enable manual authentication within Websense Enterprise to force users to manually authenticate their request if they cannot be identified transparently via DC Agent. For details, see the *Websense Enterprise Administrator's Guide.*
- If you are using a SunONE or Novell directory service:
  1. Enable the appropriate directory service within Websense Enterprise.
  2. Enable Websense manual authentication so Websense Enterprise can identify users if Websense Enterprise cannot transparently identify them.

Domain Name System

When Websense components are enabled on Cisco Content Engine ACNS v5.3, Websense Enterprise requires a DNS Server. Websense Enterprise uses DNS for Internet filtering requests, user message presentation, and DC Agent functions.

Internet Requests and DNS

URLs must be in the form of IP addresses before Websense filtering can occur. When Websense is integrated with Cisco Content Engine ACNS v5.3, either Cisco Content Engine or the browser performs a DNS lookup. depending on whether or not Cisco Content Engine is in transparent proxy mode.

IMPORTANT

If Cisco Content Engine is acting as a proxy, it **must** have access to the domain server to perform a DNS lookup.

Once Websense Enterprise gets the IP address, it searches Websense Enterprise Master Database and determines the category to which the site belongs. If more than one site is hosted at the same IP address, or if pages within the site are categorized differently, Websense matches the path that follows the domain name to the list of paths associated with the IP address in the Websense Enterprise Master Database, and then filters accordingly.

User Message Page URLs and DNS

When Websense Enterprise blocks an Internet request, the browser is redirected to a user message page hosted by Filtering Service. The user message page URL typically uses the following format:

```
http://<EIMServerIPAddress>:<MessagePort>/cgi-
bin/blockpage.cgi
```

. . . where <EIMServerIPAddress> is the IP address of Cisco Content Engine ACNS v5.3 and <MessagePort> is the message port. The default message port number is 15871.

As long as the URL identifies a machine or appliance by an IP address, a DNS lookup is not needed. However, when Filtering Service is installed on a multi-homed machine, where a single machine has two or more network interface cards (NICs), the machine has two IP addresses, one internal and one external. This may cause the URL to use the following format:

```
http://<EIMServerMachineName>:<MessagePort>/cgi-bin/blockpage.cgi
```

. . . where <EIMServerMachineName> is the name of Cisco Content Engine ACNS v5.3 and <MessagePort> is the message port. The default port number is 15871.

Websense strongly recommends that you identify Filtering Service by an IP address, where the internal IP address is the best choice. Otherwise, employees may receive a blank page instead of a user message. For details, read *Translated User Messages Pages for Cisco Content Engine ACNS v5.3*, page 122.

DC Agent and DNS

DC Agent performs DNS lookup in two cases:

- Whenever an employee logs on to a machine, DC Agent performs DNS lookup to resolve the user's machine name to an IP address. If the network includes a directory service, user names are first matched against directory service entries, and then DC Agent records the user name together with the corresponding IP address of the machine.
- If you identify the DC Agent machine by the host name during configuration, instead of using the IP address, Websense Enterprise performs a DNS lookup to obtain the IP address of DC Agent. This DNS lookup occurs the first time Websense contacts DC Agent, and then according to a pre-defined schedule after that.

CHAPTER 3

System Requirements for Remote Machines

The versions of Cisco Content Engine ACNS v5.3 appliances where Websense components are embedded along with Cisco Content Engine network modules are:

- 500 Series
- 7300 Series

System requirements are listed separately for the Websense Enterprise components not embedded on the Cisco Content Engine ACNS v5.3 or that may be installed separately.

- **User Service**: runs on Windows and Cisco Content Engine ACNS v5.3.
- **Network Agent:** runs on Windows and Cisco Content Engine ACNS v5.3—which uses Linux. You can install multiple instances of Network Agent for larger networks to help with load balancing issues.
- **Websense Enterprise Manager**: runs only Windows machines.
- **DC Agent**: runs only on Windows machines.
- **Real-Time Manager (RTA):** runs only on Windows.

User Service

You can enable User Service on Cisco Content Engine ACNS v5.3, or you can install and run it on Windows. This section lists the requirements.

On Windows machines, User Service requires the following:

- Pentium II or higher
- 512 MB RAM or more
- Supported operating systems
  - Windows NT 4.0 Server, Service Pack 6a
  - Microsoft Windows 2000 Server, Service Pack 2 and higher

Websense Enterprise Manager

IMPORTANT

Make sure you access Websense Enterprise Manager v5.2 for the embedded version for Cisco Content Engine ACNS v5.3. If you do not access the correct installer, you will not be able to run Websense components. Websense Enterprise Manager runs only on Windows machines.

Websense Enterprise Manager runs only on Windows machines and requires the following:

- Pentium II or higher
- 256 MB RAM (or more)
- Supported operating systems
  - Windows 98 (with updated Microsoft Virtual Machine)
  - Windows Millennium Edition
  - Windows XP Professional
  - Windows 2000 Professional or Server, Service Pack 2 and higher
- Web browser with Java support enabled (required to view online Help)
- Color depth set to 8 bit (256 colors) or greater
- 60 MB of disk space

Network Agent

You can enable Network Agent on Cisco Content Engine ACNS v5.3. Alternately, you, or you can install it on a Windows machine. For the most reliable performance, install Network Agent on an Ethernet network.

On Windows machines, Network Agent requires the following:

- Pentium II or higher
- 256 MB of RAM
- Supported operating systems
  - Windows NT 4.0 (Server version) Service Pack 6a
  - Microsoft Windows 2000 (Server version), Service Pack 2 and higher

DC Agent

DC Agent requires the following:

- Pentium II or higher
- 256 MB of RAM
- Supported operating systems
  - Windows NT 4.0 (Server version) Service Pack 6a
  - Microsoft Windows 2000 (Server version), Service Pack 2 and higher

eDirectory Agent

eDirectory Agent requires the following:

- Pentium II or higher
- 256 MB of RAM
- Supported operating systems
  - Windows NT 4.0 (Server version) Service Pack 6a
  - Microsoft Windows 2000 (Server version), Service Pack 2 and higher

RADIUS Agent

RADIUS Agent requires the following:

- Pentium II or higher
- 256 MB of RAM
- Supported operating systems
  - Windows NT 4.0 (Server version) Service Pack 6a
  - Microsoft Windows 2000 (Server version), Service Pack 2 and higher

Real-Time Analyzer (RTA)

RTA runs only on Windows machines, and requires the following:

- Pentium II or higher
- 256 MB of RAM
- Supported operating systems
  - Windows NT 4.0 (Server version) Service Pack 6a
  - Microsoft Windows 2000 (Server version), Service Pack 2 and higher

To install and run RTA, you must have one of the following supported Web servers installed:

- Apache version 2.x and higher
- Microsoft IIS version 4.0 and 5.0

NOTE

If one of the supported Web servers is not on your machine, you can use the Websense installer to load Apache.

Websense Enterprise Reporter

Websense Enterprise Reporter requires the following:

- Pentium II processor (Pentium III with 350 MHz recommended)
- 256 MB of RAM
- Microsoft Windows 98, Windows NT 4.0 Workstation or NT 4.0 Server (Service Pack 5 or 6a), Windows 2000, Professional, Server, or Advanced Server (Service Pack 1), Windows XP Professional, Windows Millennium Edition, Windows 2003
- Monitor: 800 x 600 or better resolution, with at least 256 colors recommended
- Microsoft Internet Explorer version 5.5 or later
- Valid print driver, appropriate to the operating system, selected as default. Check the Technical Support Web site for a list of print drivers that are known to be incompatible with Reporter. *Do not* set one of these as the default print driver on the Reporter machine.

Websense Enterprise Explorer

- Pentium II processor, minimum; Pentium III with 350 MHz recommended
- 256 MB of RAM minimum, 512 MB recommended
- Microsoft Windows 2000 Server SP3, Microsoft Windows 2003 (Web, Enterprise, or Standard editions)
- Monitor: 800 x 600 or better resolution, with at least 256 colors recommended

- Microsoft Internet Explorer version 5.5 or later
  - If you use Internet Explorer version 6.x, you may have problems accessing the Explorer Web Server even though it is an intranet site.
  - If you do use Internet Explorer version 6.x, add the Explorer URLs to the **Trusted Sites** list, and reduce the security for trusted sites to **Medium**.
- Microsoft IIS Web server if you want to set “Departmental Level Reporting.” (Must also use either NTLM or Active Directory as the directory service.

User Workstations

For Websense filtering, a user workstation must access the Internet through Cisco Content Engine ACNS v5.3.

CHAPTER 4 | Before Installing

This chapter contains details to consider before you install Websense Enterprise components. There are a number of considerations that are easier to address now than when you are actually performing an installation.

Installation Restrictions

Before installing Websense Enterprise components, it is important to note the following details.

Requirement	Important Details
Reporting	• To properly generate reports, you **must** use the same version of Websense Enterprise, Websense Enterprise Reporter, and RTA. • To use RTA, you must also install Websense Enterprise Reporter.
Non-English operating systems	Because Websense Enterprise v5.2 installs in English, you need to download Websense Enterprise Language Pack to convert Websense components so they work on non-English operating systems. Installation instructions are provided with the Websense Enterprise Language Pack product. You can download the Websense Enterprise Language Pack from the Websense Web site at: http://www.websense.com/downloads/
LDAP directory	If your directory service information resides in an LDAP directory, you can get LDAP server IP address and port, base domain, and LDAP cache information from the **records.config** file, which is found in the records.
NICs	If you are adding one or more NICs at a machine where you are also going to install Network Agent, install the NIC or NICs before installing Network Agent. If you add the NIC or NICs later, you will need to perform additional configuration for Network Agent.

Websense Installation Overview

For most organizations, a fully embedded Websense installation is appropriate. For a “basic” installation, most Websense components are enabled and installed on Cisco Content Engine ACNS v5.3, with only Websense Enterprise Manager on a remote machine. If you want to add reporting functions, generally Websense Enterprise Reporter, Explorer, and RTA are installed on a single remote machine, often the same one where Websense Enterprise Manager runs.

Basic Websense Installation

If the basic installation is appropriate for your environment, you need only perform the following steps, in the order shown:

1. Decide which user identification method you are going to use. For details, read *User Identification Methods*, page 50.
2. Enable components that will run on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54. For many organizations, most Websense Enterprise components are enabled on Cisco Content Engine.
3. *Select Websense Installers*, page 73.
   - Select `WebsenseManager_5.2_ACNS5.3.exe` to install only Websense Enterprise Manager
   - Select `WebsenseEnterprise_5.2.exe`. to install Websense Enterprise Manager with other Websense components
4. *Access and Unzip Websense Installers*, page 74.
5. *Start a Websense Installation*, page 76.
6. *Install Websense Enterprise on Remote Machines*, page 83.
   - *Websense Enterprise Manager*, page 99 (required for database downloads)
   - Other component installation is optional
7. Set up Websense Enterprise. For details, read *Configuration via Websense Enterprise Manager*, page 112.
8. *Install and Implement Language Pack*, page 108. This step is required only if your Websense installation occurs on non-English operating systems.

Basic Websense Installation Plus Reporting

If you want to use Websense reporting tools, you can easily add them to a basic Websense installation. This deployment keeps most Websense components enabled and installed on Cisco Content Engine ACNS v5.3, with only Websense Enterprise Manager, Websense Enterprise Reporter, and Real-time Analyzer on remote machines.

If you want to add reporting functions to a basic installation, you need only perform the following steps, in the order shown:

1. Decide which user identification method you are going to use. For details, read *User Identification Methods*, page 50.
2. Enable components that will run on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54. For many organizations, most Websense Enterprise components are enabled on Cisco Content Engine.
3. *Select Websense Installers*, page 73.
   - Select `WebsenseManager_5.2_ACNS5.3.exe` to install only Websense Enterprise Manager
   - Select `WebsenseEnterprise_5.2.exe`. to install Websense Enterprise Manager with other Websense components
4. *Access and Unzip Websense Installers*, page 74.
5. *Start a Websense Installation*, page 76.
6. *Install Websense Enterprise on Remote Machines*, page 83.
   - *Websense Enterprise Manager*, page 99 (required for database downloads)
   - *Real-Time Analyzer (RTA)*, page 93 (optional reporting tool)
   - Other component installation is optional

   IMPORTANT

   After installing these components, you **must** reboot the machine before you can install reporting components.

7. Identify the Policy Server and download the Websense Enterprise Master Database. For details, read *Configuration via Websense Enterprise Manager*, page 112.

8. Real-Time Analyzer. Select `WebsenseReporting_5.2.exe` to install Websense Enterprise Reporting and/or Explorer. The reporting component allows you to schedule and run reports, and is required if you want to run Real-time Analyzer (RTA).
9. *Install and Implement Language Pack*, page 108. This step is required only if your Websense installation occurs on non-English operating systems.

Required Third-Party Applications

There are several third-party applications that may be needed for your Cisco Content Engine ACNS v5.3 installation when you enable Websense Enterprise, and then install Websense Enterprise Manager and Reporter on a remote machine. These third-party programs—and their relationship to Websense Enterprise—appear in the next table.

Requirement	Details
SQL Server or MSDE Database	You must have access to a database if you want to use Websense Enterprise reporting functions. You can use either of the following: • **SQL Server**. Able to handle larger amounts of volume, SQL Server is the choice of most organizations with more than 1,000 machines, or those with a large amount of Internet traffic. Websense reporting tools can create the necessary database on any existing SQL Server. SQL Server must be purchased as a separate package. • **MSDE** (Microsoft Database Engine). Good for small companies or organizations with little Internet traffic, MSDE logs rollover at approximately 1.5 GB. You can generate reports from any archived log. MSDE is available free from Microsoft, and runs on most Microsoft operating systems. If you do not already have a database installed, the Websense installer links to an MSDE download. You can download and install MSDE, and then continue with the reporter installation. For details, read *Install MSDE as Database*, page 44.

Requirement	Details
IIS or **Apache 2.x**	If you install RTA, you must use one or the other of these Web servers: • If you use IIS, you may need to interact with IIS Manager to determine which Web site will be used to run RTA. For details, read Real-Time Analyzer. • If you want to install Apache, you can download the program now at http://httpd.apache.org/download.cgi or you can use the Websense installer to access the Apache download. For details, read *Install Apache as the Web Server*, page 45.
Acrobat Adobe Reader, 5.x or higher	This application allows you to read Websense documentation, which is in PDF format. If you do not have Adobe Reader on the machine where you install Websense Enterprise components, a message reminds you that you need to install it. You can access the free download at http://www.adobe.com/products/acrobat/readstep2.html.
Windows Control panel, Services function	If you are adding new components to an existing installation, upgrading existing components, or removing components, you may need to start and stop Websense services. For details, read *Stop, Start, or Restart Websense Services*, page 46.
Internet Explorer	You must have Internet Explorer v5.5 or higher installed if you want to use Websense Enterprise reporting tools. This program is also required if you want to view online help in Websense Enterprise Manager and Reporter.
RADIUS Server	If you want to use RADIUS Agent for transparent user identification, any installed instances of RADIUS Agent must be able to communicate with the machine where RADIUS Server is installed. RADIUS Server is available as a free download at http://www.freeradius.org/.
eDirectory Server	If you want to use eDirectory Agent for transparent user identification, any installed instances of eDirectory Agent must be able to communicate with the machine where Novell's eDirectory Server is installed. For more information, go to http://www.novell.com/products/edirectory/.

Install MSDE as Database

If you decide to install MSDE to support Websense reporting functions, the selection in the Websense installer and the download from www.microsoft.com/downloads/ does not automatically run MSDE. You need to access and run the files manually.

To install MSDE:

1. Download the MSDE installation file from www.microsoft.com/downloads/ or select it from the Websense installer. (The Reporter installer is described in detail in *Install Websense Enterprise Reporter and Explorer*, page 101.)
2. Once the downloaded file is available, unzip it. By default, the unzipped files are placed at `C:\\sqlksp3`.
3. Go to the directory where the unzipped files are, and then select `MSDE > setup.exe`.
4. Double-click `setup.exe` to run the MSDE installation. Follow all prompts.
5. When the MSDE installation is complete, you need to restart the machine.
6. After restarting the machine, run `setup.exe` from `WebsenseReporter_5.2.exe` to install Websense Enterprise Reporter.

Install Apache as the Web Server

If you want to install RTA or Websense Enterprise Explorer, you need to have a Web server installed at a machine where these reporting components run. If you do not already have a Web server installed, you can install Apache free of cost.

The fastest and easiest way to install your free instance of Apache is to download the installer from http://httpd.apache.org. You can also access a link directly from the Websense installer if system analysis does not find a Web server. If you use the version in the Websense installer, you will need to close the Websense installer, access the Apache installer, and then reopen the Websense installer, and repeat several steps.

IMPORTANT

Because Apache is a third-party tool, provided as a convenience by Websense, Inc., Websense provides installation details based on the version available at the time of the release. If you have questions about the Apache Web Server installation process, please check http://httpd.apache.org/ for the latest details.

To install Apache as the Web server for RTA and/or Explorer:

1. Access the Apache installation files from http://httpd.apache.org or from the Websense installer.
2. Once you have access to the Apache files, unzip and/or run `apache.exe`.
3. When the Apache Installation Wizard opens, the **Welcome** dialog box appears. Click **Next**.
4. Read the subscription agreement, and then click **I accept the terms of the license agreement**.
5. When all buttons become active, click **Next**.
6. When the **Read Me First** dialog box appears, read the information, and then click **Next**.
7. When the **Server Information** dialog box opens, enter the following information:
   a. Identify the network domain.
   b. Enter the server name where you are installing Apache.

c. Enter the email address for the administrator. Usually, this is either your email address or an email address that is accessible by your department.

d. Identify how you want to install Apache. You can:

- install Apache for all users, as a Service on port 80, recommended by Apache.
- only for the current user on port 8080, where Apache must be started manually whenever you want to use it.

e. Click **Next**.

8. When the **Setup Type** dialog box opens, select **Typical**, and then click **Next**.
9. When the **Destination Folder** dialog box opens, either accept the default location, `C:\Program Files\Apache Group\`, or click **Change** to select a different location for installation, and then click **Next**.
10. When the **Ready to Install the Program** dialog box opens, click **Install**.

    Status messages appear as the installation proceeds.
11. When the **Installation Wizard Completed** dialog box opens, click **Finish**.
12. Restart the machine.
13. Run Websense installers as appropriate.

Stop, Start, or Restart Websense Services

At various points during your installation or upgrade, you may need to stop or start a Websense service. For example, you must stop Filtering Service whenever you edit the `eimserver.ini` file or after customizing default user messages.

Stop and Start Websense Services on Cisco Content Engine ACNS v5.3

- Start all services installed on Cisco Content Engine ACNS v5.3 with the following command:

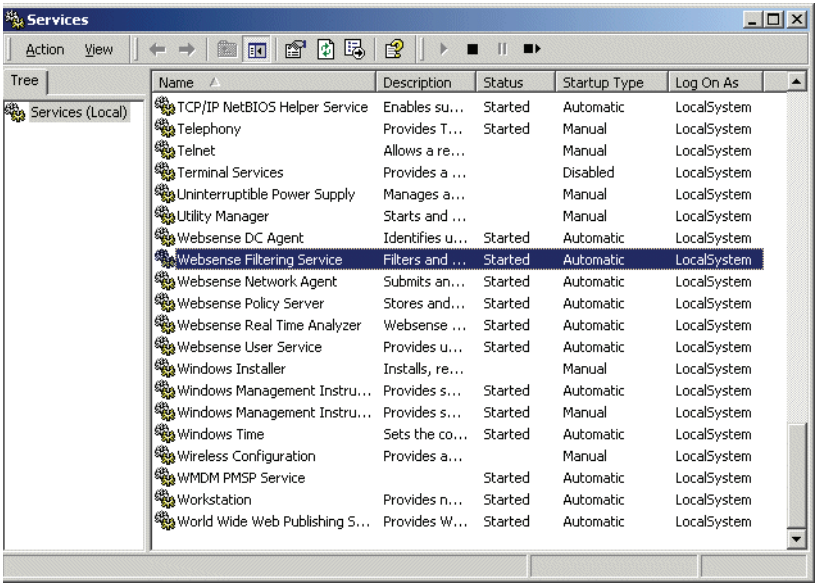
  ```
  websense-server enable
  ```
- Stop all services installed on Cisco Content Engine ACNS v5.3 with the following command:

  ```
  no websense-server enable
  ```

Stop, Start, or Restart a Websense Service on Windows

Although Websense services start automatically when you start the host Windows machine, there are still times when you may need to control those services. To control Websense services on Windows:

1. Access the Windows Control panel.
   - For Windows NT, select **Start > Settings > Control Panel**, and then double-click **Services**.
   - For Windows, select **Start > Programs > Administrative Tools > Services**.
2. Scroll down the list of available services, and then highlight the Websense service you want to manually control.



Windows Services List

3. Right-click the entry, and then select the control you want to impose.
   - Select **Stop** if you want to stop a service that is running.
   - Select **Start** if you want to start a service that is not running.
   - Select **Restart** if you want to stop and then immediately restart the service.

4. Continue controlling Websense services as appropriate. For example, a procedure may require that you stop a service, do something in a file, and then restart the service. You can leave the Services window open so you can return to it.
5. Close the **Services** window when you are done.

Change Access Rights for Components on Windows Machines

You may need to change the access rights for Websense components if you install User Service or DC Agent on a Windows machine using local accounts or any other account that does not have administrator access rights. Without administrator level access, these components may not work as expected. You can change access rights from the Service Manager in Windows.

To change access rights for Websense components on Windows machines:

1. Select **Start > Control Panel > Administrator Tools > Services**.
2. Scroll through the list of services to find the Websense service whose access you need to change.
3. When you find the service, right-click, and then select **Properties** from the drop-down menu.
4. Click the **Log On** tab to access the **Log On** dialog box.
5. Click the radio button for **This account** to activate the needed fields and deactivate the current selection.
6. Select the domain and account that the Websense component will use in the future.

IMPORTANT

You need to have administrator access to the domain you select.

There are two ways to identify the domain for the account.

- If you already know the information, type the domain name and user for the domain in the first field. The format is <domain/<user name>.
- If you need to locate machines and users, click **Browser** and locate the needed information. If you need assistance, use the **What's This?** help option in the various dialog boxes.

7. Enter the password for the account, confirm the password, and then click **OK**.
8. Return to the **Services** pane, right-click the Websense service whose access you just changed, and select **Restart** from the drop-down menu.

Copy Default Web Site Names From IIS Manager

If you are installing the Real-Time Analyzer or Websense Enterprise Explorer, and using IIS as your Web server, you must identify a Web site where the Websense installer creates a *virtual directory*. This is the site where the RTA or Explorer Web-based application will run. The default value is **Default Web Site**, which is correct in most instances.

If you have renamed the default Web site in the IIS Manager or are using a language version of Windows other than English, you must enter a value in the Web site name field that matches an existing Web site name in the IIS Manager. You can open IIS Manager, copy the needed Web site name, and then paste it into the Websense installer.

To access Web site names:

1. Select **Start > Control Panel > Administrative Tools**.
2. Double-click **Internet Services Manager** to open the IIS control screen.
3. Expand the tree under your computer name to view available Web site names.
4. Right-click the Web site in which the installer should create the virtual directory, and then select **Properties** from the pop-up menu.
5. Copy the name of the Web site from the **Description** field to the clipboard.
6. Close IIS Manager.
7. Return to the **Virtual Directory** screen in the Websense installer and replace **Default Web Site** with the name from the IIS Manager.
8. Continue with your Websense installation.

User Identification Methods

Several Websense Enterprise components are available that provide transparent user identification. The various agents--DC Agent, eDirectory Agent, and RADIUS Agent--interact with User Service and Filtering Service to provide user identification for Websense policy enforcement and data logging.

Generally, User Service performs best when you enable or install it in the same location as Policy Server. For Cisco Content Engine ACNS v5.3 integrations, many customers enable Policy Server, User Service, and Filtering Service on the engine, and then install other Websense components on remote machines. When a customer integration differs from this type of deployment, it is generally because the network is larger than 5,000 machines and/or load balancing is an issue due to high volume of traffic.

It is best to select the user identification method you are incorporating before your installation. Take into consideration which agent or agents you want to use, and where you want to enable or install that agent or agents. In large complex systems, you can install multiple agents of a single type on multiple remote machines, run two different agents on the same machine, or any other combination--barring only configuration requirements. To help you determine which agent you want to use--if any--and how you can install the agent or agents you choose, refer to the next table.

Websense Agent	Limitations and Restrictions
(no agent installed)	You can run Websense Enterprise without installing any agents. However, if you do not install at least one of the available agents, any employee who tries to access the network will need to provide his or her user name and a password. If you have multi-user machines, or if users have multiple logon identities, logged information is not always accurate.
DC Agent	• May be installed on remote Windows machines (*DC Agent*, page 95) • Each machine can run only one instance of DC Agent • Multiple instances can be installed, as long as each instance can communicate with Filtering Service • Can be installed on a machine that also runs RADIUS Agent

Websense Agent	Limitations and Restrictions
eDirectory Agent	• May be enabled at Cisco Content Engine ACNS v5.3 (*Install and Enable Embedded Websense Components*, page 54), or installed on remote machines (*eDirectory Agent*, page 98) • Each machine can run only one instance of eDirectory Agent • Multiple instances can be installed, as long as each instance can communicate with Filtering Service • Each instance must have access to Novell's eDirectory Server • Can be installed on a machine that also runs RADIUS Agent
RADIUS Agent	• May be enabled at Cisco Content Engine ACNS v5.3 (*Install and Enable Embedded Websense Components*, page 54), or installed on remote machines (*RADIUS Agent*, page 97) • Each machine can run only one instance of RADIUS Agent • Multiple instances can be installed, as long as each instance can communicate with Filtering Service • Each instance must have access to RADIUS Server • Can be installed on a machine that also runs DC Agent • Can be installed on a machine that also runs eDirectory Agent

Default Port Number Assignment

When you enable embedded components on Cisco Content Engine ACNS v5.3, the components use the following default port number assignments. The data here may be needed when you configure your Websense installation via Websense Enterprise Manager.

Websense component	Default Port
Filtering Service	15868
Configuration Port (communications between Websense Enterprise Manager and Filtering Service)	55806
User Messages port (Block and Continue messages are sent over this port)	15871
Log Server	55805
DC Agent	30600
eDirectory Agent	30700
RADIUS Agent	30800

CHAPTER 5 Working on Cisco Content Engine ACNS v5.3

Logical deployment of Websense components is critical to your installation. You should identify and enable the components you want to run on Cisco Content Engine ACNS v5.3 **before** installing Websense components on remote machines. If you have not done this yet, read *Chapter 2: Network Configuration, page 15*. There are two different ways you can interact with Cisco Content Engine ACNS v5.3:

- Use the Console mode or a Telnet session. For details, read *Cisco Content Engine ACNS v5.3 Command Line Interface*, page 54. Many configuration requirements can only be set using this method.

  NOTE

  You **must** use CLI entries to enable and disable embedded Websense components on Cisco Content Engine ACNS v5.3, and to configure some details.

- Use the Cisco Web-Browser GUI. For details, read *Cisco Content Engine ACNS v5.3 Web-Browser GUI*, page 62. A few configuration requirements can be set using this method. The GUI also provides Websense status details.

Other configuration requirements for Cisco Content Engine ACNS v5.3 include regulating browser access and identifying Filtering Service on appliances with multiple NIC cards.

Cisco Content Engine ACNS v5.3 Command Line Interface

Cisco Content Engine ACNS v5.3 includes a Command Line Interface (CLI) that allows you to enable, disable, start, and/or configure Websense components. You can also enter information that directly affects how Cisco Content Engine handles Websense data. Complete details are available in the Cisco documentation provided with your appliance or from the Cisco Web site at www.cisco.com/univercd/home/home.htm.

NOTE

A complete list of Cisco CLI commands is available at http://www.cisco.com/univercd/cc/td/doc/product/webscale/use/acns50/cref50/14623c50.pdf.

Install and Enable Embedded Websense Components

Once you know how you are going to deploy Websense Enterprise components, you should enable the components that will run on Cisco Content Engine ACNS v5.3. When you begin installing components on remote machines, you may need to point those components to the ones that are enabled and running on the appliance. The next table identifies each embedded component and the CLI command to enable, install, and/or configure that component, where all commands are issued from "Configure Terminal."

WARNING

You **must** first install Policy Server before you can install any other Websense components. If you are running Policy Server on a remote machine, and not on Cisco Content Engine ACNS v5.3, the remote instance of Policy Server must be running and able to communicate with the Websense Enterprise components you are installing.

Embedded Component	CLI Commands

Policy Server	To enable Policy Server, enter:
	`websense-server service policy local activate`
	To point Cisco Content Engine ACNS v5.3 to an instance of Policy Server installed on a remote machine, enter:
	`websense-server service policy remote host <IP address> port <port number>`

Filtering Service	To enable Filtering Service:
	`websense-server service eim activate`
	
	To show status and administrator data for Filtering Service, enter:
	`show websense-server`
	
	This command returns the following information:
	• Status (Running or Stopped)
	• Version number
	• Port numbers
	• Installed components
	• RADIUS Agent configuration
	• eDirectory Agent configuration

User Service	To enable User Service: `websense-server service user activate`
Network Agent	To enable Network Agent: `websense-server service network-agent activate`

Embedded Component	CLI Commands

eDirectory Agent	To configure eDirectory Agent, enter the following commands:
	
	`websense-server service edir-agent edir-host <eDir IP>`
	
	`websense-server service edir-agent edir-server administrative-dn <admin dn>`
	
	`websense-server service edir-agent edir-server administrative-passwd <admin password>`
	
	`websense-server service edir-agent edir-server root-context <root context>`
	
	To enable eDirectory Agent:
	`websense-server service edir activate`

Embedded Component	CLI Commands

RADIUS Agent	To configure RADIUS Agent, enter the following commands:
	`websense-server service radius-agent outgoing host <RADIUS Server IP>`
	`websense-server service radius agent incoming auth-port <AuthInPort>`
	Note: The default port number is 12345
	`websense-server service radius-agent outgoing auth-port <AuthOutPort>`
	Note: The default port number is 1645
	`websense-server service radius-agent incoming accnt-port <AccInPort>`
	Note: The default port number is 12346
	`websense-server service radius-agent outgoing accnt-port <AccOutPort>`
	Note: The default port number is 1646
	To enable RADIUS Agent:
	`websense-server service radius activate`

All components	To start all embedded *and* installed components at the same time, enter: `websense-server enable`

Sample Procedure for Websense Enterprise on Cisco Content Engine

The next procedure shows a basic series of entries required to enable and configure Websense Enterprise on Cisco Content Engine ACNS v5.3:

1. Access Cisco Content Engine from a console connection or a TELNET session at a remote terminal.
2. Use the `configure` command to enter the global configuration mode.

   Console# `configure terminal`

   Console (config)#

3. Decide where you want Filtering Service to run. The service can run on Cisco Content Engine or a remote machine.
   - If you want to enable URL-filtering using Websense Enterprise embedded on Cisco Content Engine, enter the following command.
     ```
     url-filter http websense server local
     ```
   - If you are not using the default port number, or if Filtering Service is to run on remote machine or appliance, add the Filtering Service IP address and port number for communications by entering a command using the following format.
     ```
     url-filter http websense server <filtering IP> port
     <port#> timeout <seconds>
     ```
     where:
     - **filtering IP** is the IP address of the remote machine where Filtering Server is running.
     - **port#** is the port number that Cisco Content Engine will use to communicate with Filtering Service. *Generally, the default port number, 15868, is the best option, as it usually reduces the changes you will need to make during installation and upgrades.*
     - **seconds** is the time that Cisco Content Engine waits for a response from Filtering Service before timing out. The time range is between 1 and 120 seconds.*Generally, the default timeout period, 20 seconds, is the best option for maintaining optimum performance.*

       Cisco Content Engine ACNS v5.3 only permits sites after the timeout is met if the engine is configured to do so.
4. Enable or disable URL filtering.
   - To enable URL filtering, enter:
     ```
     url-filter http websense enable
     ```
   - To disable URL filtering, enter:
     ```
     no url-filter http websense enable
     ```

5. Decide if you want to set a timeout override for Cisco Content Engine. If you do set a timeout override, you are allowing Cisco to permit Web site access if Websense Server times out.

   If you do not enter the following command, Cisco Content Engine will not allow any Web access if Websense Filtering Service times out.

   ```
   url-filter http websense allowmode enable
   command
   ```

6. Enter the following command to exit the global configuration mode.

   ```
   exit
   ```

7. Enter the following command to save your configuration data to permanent memory.

   ```
   write memory
   ```

   This prevents your changes from disappearing if Cisco Content Engine restarts for any reason.

8. Install Websense Enterprise Manager on a remote machine. Read *"Basic" Installation (Websense Enterprise Manager only)*, page 83.

9. Download the Websense Enterprise Master Database.

For detailed instructions that cover *Websense Enterprise Administrator's Guide* for information about configuring Websense for filtering.

Stop and Uninstall Embedded Websense Enterprise Components

There may be times when you need to uninstall a Websense component on Cisco Content Engine ACNS v5.3. For example, you install Network Agent on Cisco Content Engine, but then later decide you want to run a single instance of Network Agent on a remote machine. You therefore stop all Websense Enterprise components, uninstall Network Agent on Cisco Content Engine ACNS v5.2, and then install it on the remote machine.

The next table identifies each embedded Websense component and the CLI command to disable the component.

Embedded Component	CLI Commands
All components	To stop all embedded and installed components at the same time, enter: `no websense-server enable` **NOTE**: You **must** enter this command before you can "uninstall" any embedded Websense Enterprise components. If you do not run this command first, an error message appears.

Policy Server	• To disable Policy Server on Cisco Content Engine ACNS v5.3, enter:
	`no websense-server service policy local activate`
	
	• To stop communication with an instance of Policy Server installed on a remote machine, enter:
	`no websense-server service policy remote host <IP address> port <port number>`
	
	Generally, this entry is not needed, unless your network includes multiple instances of Policy Server.

User Service	To disable User Service: `no websense-server service user activate`

Filtering Service	• To disable Filtering Service:
	`no websense-server service eim activate`
	
	• To disable filtering:
	`no url-filter http websense enable`

Network Agent	To disable Network Agent: `no websense-server service network-agent activate`

Embedded Component	CLI Commands
eDirectory Agent	To disable eDirectory Agent: `no websense-server service edir-agent activate`
RADIUS Agent	To disable RADIUS Agent: `no websense-server service radius-agent activate`

Manage Websense Files

The next table identifies commands that are used to manage files on Cisco Content Engine ACNS v5.3 or show data that are on Cisco Content Engine. The known situations that may require file management appear in this document, and list these commands in the context where they are used

Command	Description
copy disk ftp <remote-ftp-server> <remote directory path> <local file name> <remote file name>	Copies files from Cisco Content Engine ACNS v5.3 to an FTP server, where: • `<remote ftp server>` identifies the remote FTP server using the IP address. • `<remote directory path>` identifies the path where files are to be copied. • `<local file name>` identifies what the local copy of the file is named before the file is copied to a remote machine. • `<remote file name>` identifies the name as it will be shown on the remote machine.

Command	Description
copy ftp disk <remote-ftp-server> <remote directory path> <remote file name> <local file name>	Copies files from an FTP server to Cisco Content Engine ACNS v5.3, where: • `<remote ftp server>` identifies the remote FTP server using the IP address. • `<remote directory path>` identifies the path of the files that are being copied. If you end with this entry, all files in the directory are copied. • `<remote file name>` identifies the file that will be copied by name. • `<local file name>` identifies what the local copy of the file will be named, if different than the remote file name.
delfile <file name>	Delete files that are on Cisco Content Engine ACNS v5.3. The format is `delfile <file name>` where the actual file name appears in place of **<file name>**.

Cisco Content Engine ACNS v5.3 Web-Browser GUI

The Cisco Content Engine ACNS v5.3 GUI provides rapid access if you need to change Filtering Service data or need to see operating details for Websense. While the GUI does not provide numerous configuration options, the operating details can be extremely valuable.

Configure Websense Filtering Service

The Cisco Web-Browser GUI provides rapid access for changing Websense Filtering Service data. The information that populates the GUI is collected from information you provide when you enable and configure Websense components using the CLI.

To change Filtering Service data using the Cisco Web-Browser GUI:

1. Enable the Cisco Content Engine ACNS v5.3 GUI server using the following CLI commands.

```
configure terminal
gui-server enable
```

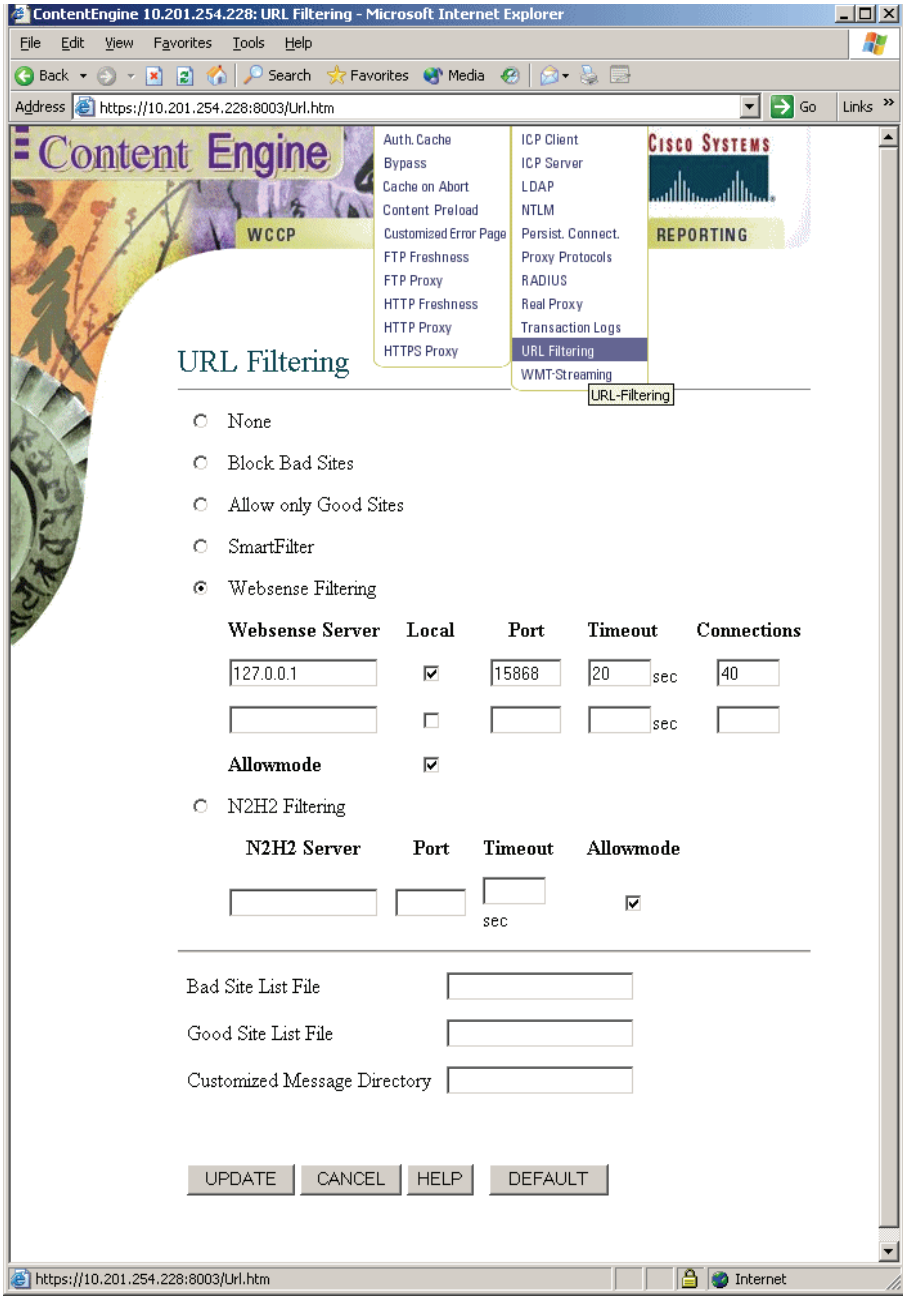
2. Open a Web browser, and then connect to Cisco Content Engine.

   `https://<ip address>:8003`

   . . . where:<ip address> is the IP address of Cisco Content Engine machine. The default port is 8003.

   The **Enter Network Password** dialog box appears.

3. Enter a valid administrator user name and password that allows access to the initial management page.
4. Select **Caching > URL Filtering**. The **URL Filtering** page opens.



Set Filtering Access via Cisco GUI

5. Select **Websense Filtering**, and then enter the appropriate information in the first row of fields. If there are any default settings or known data, that information pre-populates the field. The next table identifies the fields that impact your Websense Enterprise installation.

Field	Description
Websense Server	Enter an IP address that identifies the machine or appliance where Filtering Service is running.
Local	• Mark this checkbox **only** if Filtering Service is on the local Cisco Content Engine ACNS v5.3. • If Filtering Service is on a remote appliance or machine, make sure this check box is not marked.
Port	Enter the port number that Cisco Content Engine ACNS v5.3 will use to communicate with Filtering Service. The default port number is 15868. *For most installations, using the default port number is the recommended entry, as it saves considerable time and effort if you add to your Websense configuration or upgrade to a newer version of Cisco Content Engine ACNS v5.3.*
Timeout	The value you enter must be between 1 and 120, inclusively, and identifies the number of seconds that Cisco Content Engine ACNS v5.3 waits until it identifies Filtering Service as having timed out. The default value is 20 seconds. *For most installations, using the default timeout value is recommended for optimum performance.*
Connections	The number of concurrent connections that Websense allows to open. The default value of 40 connections is recommended.
Allowmode	Mark this checkbox **only** if you want Cisco Content Engine ACNS v5.3 to permit access to Web sites if Filtering Service has timed out.

6. If you have a secondary Websense Filtering Service, hosted on a second machine, enter the data for that machine in the second row of **Websense Filtering** fields.

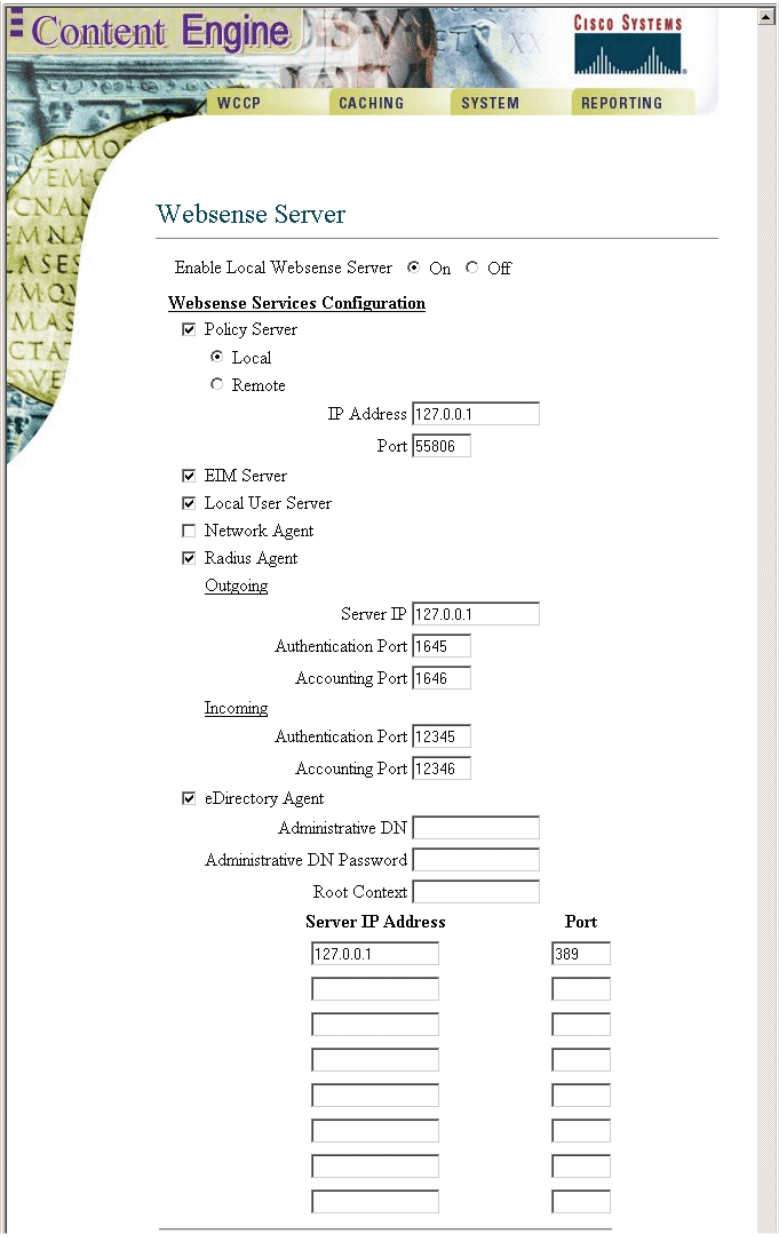
View Websense Operating Data

The Cisco Web-Based GUI provides a snapshot view of Websense component configuration data and operating details. If you want to use Cisco Content Engine ACNS v5.3 GUI to see system configuration and operating data for Websense Enterprise:

- Select **System > Websense Server**. The **Websense Server** page opens. You may need to scroll down to see all the information available, as the page can be long.

The top portion of the **Websense Server** page contains the following data:

- Status of the local Websense Server (On or Off)
- Websense Enterprise Policy Server location (local or remote), IP address, port
- Installation status of Websense Enterprise components (EIM Server, Local User Server, Network Agent)
- Installation status of RADIUS Agent (if installed)
  - (Outgoing) Server IP address, Authentication Port, Accounting Port
  - (Incoming) Authentication Port, Accounting Port
- Installation status of eDirectory Agent (if installed)
  - Administrative DN, Administrative DN Password, Root Context
  - Server IP addresses and ports



Websense Server Configuration Data via Cisco Web-Browser GUI

The middle part of the Websense Server page contains information about your Websense installation.

```
Local Websense Server Information :
-----------------------------------

Websense Enterprise Version : 5.2.0
Websense Enterprise Build   : 1108699513

Websense server components installed :
Policy Server
EIM Server
User Service
Radius Agent
eDirectory Agent

Status of the components:
-------------------------


Websense Filtering Service running...


Websense Policy Server running...


Websense User Service running...


Websense eDirectory Agent running...


Websense RADIUS Agent running...



Websense Server running...

-----------------------------------------
 Sending SERVER_STATUS_REQUEST...
-----------------------------------------

  Status Code = 0
  License Count = 1000
  Elapsed Time = 1 ms

AVG TIME PER REQUEST = 1 ms

Websense Server Port : 15868
Websense Block Message Port : 15871
Websense Config Server Port : 55806
Websense Diagnostics Server Port : 15869
```

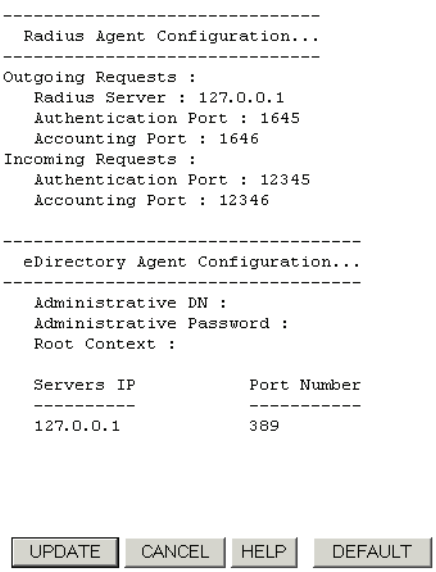
Websense Server Component Data via Cisco Web-Browser GUI

The details in this portion of the Cisco Web-Browser GUI include:

- The Websense Enterprise version number
- The Websense Enterprise build number
- A list of the components that have been installed

- The status of all installed components
- Server status data, including—
  - Status code
  - License Count
  - Elapsed time
  - Average time per Internet request
  - Websense Server Port
  - Websense User message Port
  - Websense Configuration Server Port
  - Websense Diagnostics Server Port

The bottom portion of the Cisco Web-Browser GUI shows configuration details for any agents you install. The exact details vary.



Websense Agent Data via Cisco Web-Browser GUI

Disabled Components and Embedded Files

When you disable eDirectory Agent or RADIUS Agent, information about these components remains in the local `config.xml` file, while entries are removed from other files that control component startup. The entry in the `config.xml` file may cause problems later if you decide to re-enable any disabled component.

WARNING

Because modifying `config.xml` may lead to critical issues, Websense, Inc., strongly recommends you contact Technical Support for assistance if you think you have reason to edit that file.

User Message URLs for Machines with Multiple NIC Cards

When Websense detects an Internet request that is set to block, continue, or quota time, the browser is redirected to a user message page hosted by Filtering Service. The format of the user message page URL typically takes the form:

```
http://<WebsenseServerIPAddress>:<MessagePort>/
cgibin/blockpage.cgi
```

Websense recommends using the IP address to identify the machine where Filtering Service is installed. If you use the machine name, it appears as part of the URL, which may cause users to see a blank page instead of the user 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.

To add an entry to the `eimserver.ini` file:

1. Using FTP, copy the `eimserver.ini` file from the directory on Cisco Content Engine ACNS v5.3 to a folder on your local drive.
2. Open the `eimserver.ini` file on your local drive with any text editor.
3. In the **[WebsenseServer]** area, enter the following command on a blank line:

   ```
   BlockMsgServerName = <IP address>
   ```

   where <IP address> is the correct (typically internal) IP address of the machine running Filtering Service. *Do not* use the loopback address 127.0.0.1.
4. Save the file.
5. Delete the `eimserver.ini` file from Cisco Content Engine. For instructions on deleting files from Cisco Content Engine, refer to *Manage Websense Files*, page 61.
6. Copy the edited version of the **eimserver.ini** file into the directory on Cisco Content Engine.
7. Stop and then restart Filtering Service. For details, read *Stop, Start, or Restart Websense Services*, page 46.

Browser Access to the Internet via Cisco Content Engine ACNS v5.3

Cisco Content Engine ACNS v5.3 can regulate Internet activity either transparently or by requiring manual authentication:

- In transparent mode, the firewall or Internet router sends Internet requests to the Cisco Content Engine, which queries Websense Enterprise. All configuration changes can be performed through Cisco Content Engine and any connected firewalls or routers— special configuration is not required on client machines.

  IMPORTANT

  To regulate Internet access transparently, you must enable Web Cache Communication Protocol (WCCP) on both Cisco Content Engine ACNS v5.3 and the firewall or router. However, if requests are routed through a proxy, you enable WCCP and set transparent mode, Websense is unable to correctly identify User IDs.

- In non-transparent mode, Web browsers on all client machines must be configured to send Internet requests to Cisco Content Engine. Check Cisco Content Engine documentation for instructions.

CHAPTER 6 | Starting a Remote Installation

Once you enable embedded Websense components on Cisco Content Engine ACNS v5.3, you need to begin the process of installing Websense Enterprise components on remote machines. This chapter describes the steps required to install remote Websense components.

Select Websense Installers

There are two primary ways to install Websense Enterprise components on remote machines:

- Install components on a single Windows machine using `WebsenseEnterprise_5.2.exe`. Use the unzipped `setup.exe,` which allows you to install one or more components at a time on a single machine.
- Install components manually at one or more machines. Only Websense Enterprise Manager and Real-time Analyzer (RTA) must be installed on Windows machines. You can use `WebsenseEnterprise_5.2.exe` and select the specific component you want to install, or you can use the individual installer for each component.
  - **WebsenseManager_5.2_ACNS5.3.exe**. The unzipped files include `Setup.exe`, which installs only Websense Enterprise Manager.
  - **WebsenseReporting_5.2.exe.** The unzipped files include `Setup.exe`, which installs only Websense Reporting.
  - **`WebsenseDCAgent_5.2.exe`**. The unzipped files include `Setup.exe`, which installs only DC Agent.
  - **`WebsenseNetworkAgent_5.2.exe`**. The unzipped files include `Setup.exe`, which installs only Network Agent.
  - **`WebsenseEDirectoryAgent_5.2.exe`**. The unzipped files include `Setup.exe`, which installs only eDirectory Agent.
  - **`WebsenseRADIUSAgent_5.2.exe`**. The unzipped files include `Setup.exe`, which installs only RADIUS Agent.

- **`WebsenseLanguagePack_5.2.exe`**. The unzipped files include `Setup.exe`, which installs the Websense Enterprise Language Pack. If you use a non-English language operating system, these files convert components so Websense components operate correctly. There are separate installation files for Windows, Solaris, and Linux.

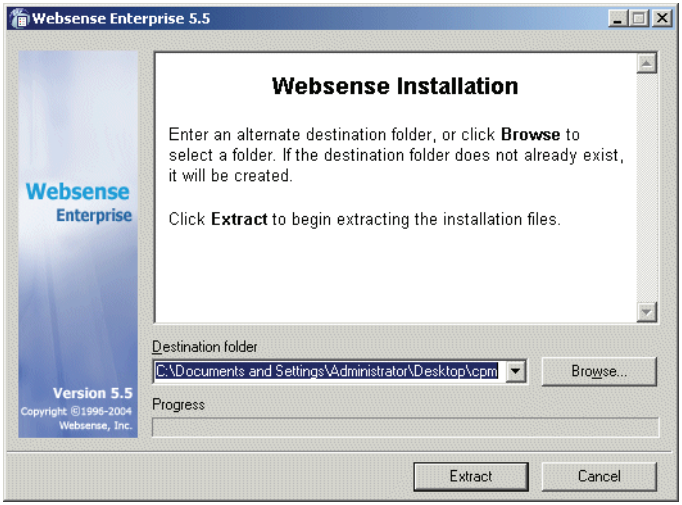
Access and Unzip Websense Installers

Websense, Inc. recommends that you install components directly at the local machine, via CD or download. You may encounter problems if you use Windows Terminal Service or a shared drive. The only exception to this general rule are those components you enable on Cisco Content Engine ACNS v5.3.

To access and unzip Websense installers:

1. Log onto the machine where you want to keep the installation files using local administrator access rights. If you do not have administrator access, you may encounter problems during installation.
2. Close any open applications at the installation machine.
3. Insert the installation CD in the CD-ROM drive or download zipped files from www.websense.com/download/.
   - If you are a new subscriber and want to download from the Web, prompts appear for information about yourself and your company before you can access the download.
   - If you are an existing Websense Enterprise subscriber, be prepared to provide your current subscription key.
   - Make sure you know the operating system of the server where you are installing Websense Enterprise components. When you download files, notice you can select from a full product installer or individual installers for the various components.

   After downloading from the Web, the **Websense Installation** dialog box opens.



Websense Installation dialog box

4. When the **Websense Installation** dialog box opens, accept the default folder or click **Browse** to access the folder where you want to store the installation files.

> **IMPORTANT**
> Do not extract installer files to a folder on your desktop, as this may cause problems as you enter configuration details.

5. Click **Extract** to unzip installation files.
6. If you unzip the files, and then wait until later to install, you must access the folder where you unzipped the files, and then select `setup.exe`.

Start a Websense Installation

After you unzip the installation files, you are ready to install Websense Enterprise components. To support your unique configuration, you may install any combination of components at one time on a single remote machine, or install them individually on one or more machines. The only installation limitations are:

- Policy Server must be running and accessible.
- User Service must be running and accessible.
- Websense Enterprise Manager and RTA must be installed on Windows machines.
- You may need to identify the IP address for a remote Policy Server. Generally, for a "basic" installation, Policy Server is enabled on Cisco Content Engine. If this is the case for your installation, make sure you have the IP address for Cisco Content Engine and the port number that Policy Server will use for communications.

With the exception of information required of new customers or those who are evaluating Websense Enterprise, the steps in this section are required each time you run a Websense installer. To begin installation:

1. Close all open applications and programs.
2. Log on to the installation machine with **domain** and **local** administrator privileges.

WARNING

Always log on with administrator privileges. If you do not have this level of access, you may encounter difficulties during installations.

3. Open the folder where you unzipped your Websense installation files, and double-click on the `setup.exe` file you want to use.
4. When the **Welcome** dialog box opens, click **Next**. The **Subscription** dialog box opens.
5. Read the service agreement, and if you agree to abide by it, click **Yes**, and then click **Next**.

The specific installer you are using determines what you need to do next. For:

- **Websense Enterprise_v5.2.exe**, skip to *Select Components from the "Main" Websense Installer*.
- other Websense installers, skip to the specific topics for the component or components you are installing.

Select Your Integration

If you are installing Policy Server with other components on a remote machine, dialog boxes open and prompt you to identify what installation option you want, and which on-box integration you are using.

IMPORTANT

In most configurations, it makes the most sense to run Policy Server on Cisco Content Engine ACNS v5.3 instead of on a remote machine. If Policy Server is enabled at Cisco Content Engine, communication times are faster and policies enforced more rapidly.

To select your installation method and integration:

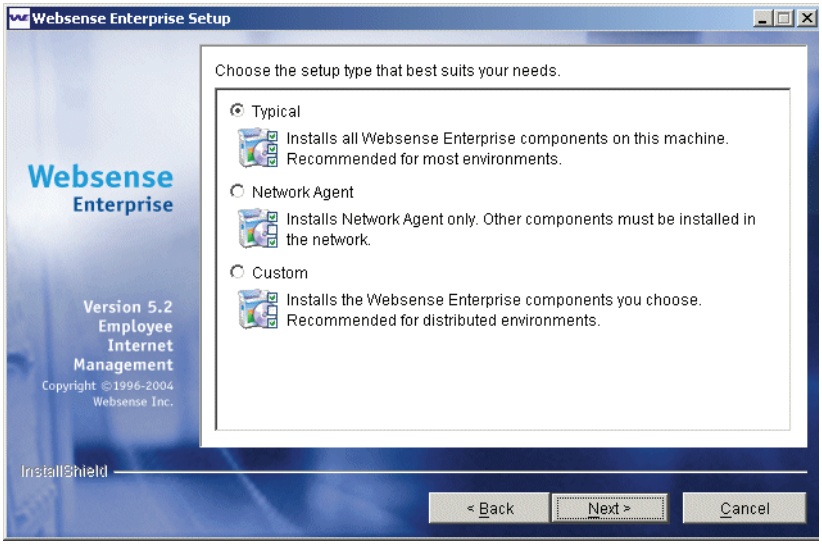
1. When the **Installation Option** dialog box opens, select **Integrated**, and then click **Next**. (The **Stand-alone** option is not a valid selection for an integrated installation.)
2. When the **Integrated Product** dialog box opens, select **Cisco Content Engine**, and then click **Next**.

You are now ready to select Websense Enterprise components for installation. Move to *Select Components from the "Main" Websense Installer*, page 78.

Select Components from the “Main” Websense Installer

Once you log onto the installation machine and indicate your willingness to abide by the service agreement, the `setup.exe` file from `WebsenseEnterprise_v5.2.exe` allows you to select from several Websense products. You can install one or more components at a time on a single machine. To do so:

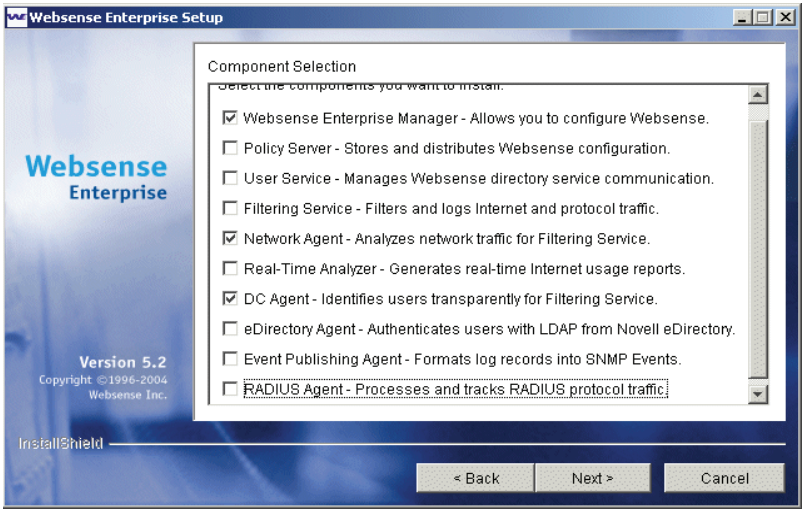
1. When prompted to choose a Websense product for installation, select **Websense Enterprise v5.2,** and then click **Next**.
2. When the **Setup Type** dialog box opens, select one of the following.
   - **Install Network Agent**. Installs only Network Agent. Skip to *Network Agent*, page 91 to complete the Network Agent installation.
   - **Custom**. Allows you to select one or more Websense components for installation. Move to the next step.



Installation Selection dialog box

3. Click **Next**. The **Component Selection** dialog opens.
4. When the **Component Selection** dialog box opens, identify any component or components you want to install, and then click **Next**.

   For a description of the available components, read *Chapter 1: Introduction*.



Component Selection dialog box

When the dialog box first appears, all selections are marked.

- Click a checkbox to remove a checkmark *and* remove the component from the installation list.
- Click a checkbox a second time to checkmark an empty checkbox *and* to add a component to the installation list.

5. Continue following onscreen prompts for the components you select. Refer to the following for specific details.

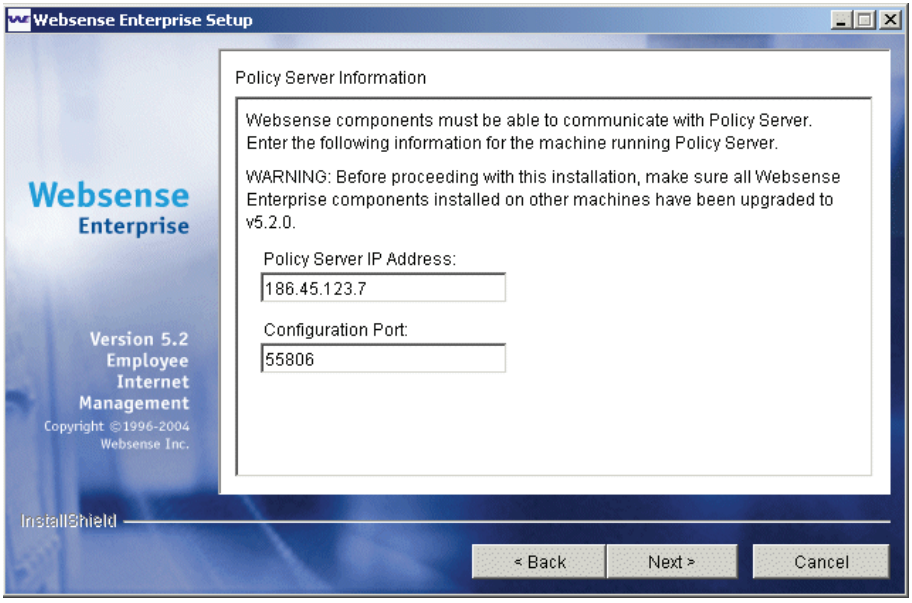
- *Policy Server*, page 87
- *User Service*, page 88
- *Filtering Service*, page 90
- *Network Agent*, page 91
- *Real-Time Analyzer (RTA)*, page 93
- *DC Agent*, page 95
- *RADIUS Agent*, page 97
- *eDirectory Agent*, page 98
- *Websense Enterprise Manager*, page 99

Identify Policy Server

IMPORTANT

You **must** install Policy Server **before** other components. If Policy Server is on another remote machine or installed on Cisco Content Engine ACNS v5.3, that instance of Policy Server must be running to successfully install optional Websense Enterprise components.

Depending on how and where you are installing Policy Server, you may be asked to identify the Policy Server. If you are installing components on remote machines where Policy Server is not running, you may be asked to identify where Policy Server is located. The IP address and port number identify the remote ACNS appliance or machine where Policy Server is either enabled and/or installed.



Policy Server Information dialog box

To identify an instance of Policy Server that is not on the machine or appliance where you are installing other Websense components:

1. Enter the IP address of Policy Server machine. For most configurations, this should be the IP address of Cisco Content Engine ACNS v5.3.
2. Enter the configuration port number.

IMPORTANT

If you enabled Policy Server on Cisco Content Engine ACNS v5.3, the default configuration port number 55806 is the port number assigned to Policy Server. *Do not* change the port number in this dialog box.

If you installed Policy Server on a remote machine, the default configuration port number is valid unless you manually identified a different port. If you changed the default value, you need to use the manually assigned port number.

3. Click **Next** to move to the next dialog box for your installation.

CHAPTER 7 | Install Websense Enterprise on Remote Machines

Once you enable embedded Websense components on Cisco Content Engine ACNS v5.3, you need to install Websense Enterprise Manager, and any optional components you want to use. This chapter describes the processes and steps you need to follow.

"Basic" Installation (Websense Enterprise Manager only)

A "basic" Websense installation is defined as one where:

- Policy Server, User Service, Filtering Service, and any of the transparent agents are enabled on Cisco Content Engine ACNS v5.3
- only Websense Enterprise Manager is on a remote machine

This "basic" installation is appropriate for most organizations if they do not want to include Websense reporting functions.

To perform a "basic" Websense installation:

1. Enable components on Cisco Content Engine ACNS v5.3. For details, read *Working on Cisco Content Engine ACNS v5.3*, page 53.
2. Log on to the installation machine with **domain** and **local** administrator privileges.

WARNING

Always log on with administrator privileges. If you do not have this level of access, you may encounter difficulties during installations.

3. Choose `WebsenseManager_5.2_ACNS5.3.exe` to install only Websense Enterprise Manager. For details, read *Access and Unzip Websense Installers*, page 74.

> **NOTE**
> If you want to install reporting options in addition to Websense Enterprise Manager, select `WebsenseEnterprise_5.2.exe` instead. Read *"Basic" Installation with Websense Reporting Components*, page 84.

4. Follow onscreen instructions to move through the beginning of the Websense installation. For details, read *Start a Websense Installation*, page 76.
5. Navigate through the final dialog boxes to complete the installation. For details, read *Complete a Websense Installation*, page 105.
6. Use Websense Enterprise Manager to identify the instance of Policy Server that is on Cisco Content Engine. For details, read *Add and Connect to Policy Server*, page 112.
7. Use Websense Enterprise Manager to download the Websense Enterprise Master Database. For details, read *Websense Enterprise Master Database Download*, page 113.

"Basic" Installation with Websense Reporting Components

A "basic" Websense installation with reporting tools is defined as one where:

- Some Websense components are enabled on Cisco Content Engine ACNS v5.3.
- Websense Enterprise Manager is installed on a single remote machine.
- RTA is installed at the same time and on the same machine as Websense Enterprise Manager.
- Websense Enterprise Reporter is installed on the same machine as Websense Enterprise Manager, or on a completely different machine. This installation includes Websense Enterprise Explorer.

The next procedure describes a Websense installation with optional components on a single remote machine:

1. Enable components on Cisco Content Engine ACNS v5.3. For details, read *Working on Cisco Content Engine ACNS v5.3*, page 53.
2. Log on to the installation machine with **domain** and **local** administrator privileges.

   WARNING

   Always log on with administrator privileges. If you do not have this level of access, you may encounter difficulties during installations.

3. Choose `WebsenseEnterprise_5.2.exe` to install Websense Enterprise Manager with optional components on a single machine. For details, read *Access and Unzip Websense Installers*, page 74.
4. Follow onscreen instructions to move through the beginning of the Websense installation. For details, read *Start a Websense Installation*, page 76. At a minimum, you will select:
   - Websense Enterprise Manager
   - Real-Time Analyzer
5. Provide the information needed for Real-Time Analyzer. You must identify the following details.
   - Depending on what Web server is installed—if any—you may:
     - select a Web server (IIS or Apache) if both are detected
     - install Apache if the installer does not detect a Web server
     - decide that you do not want to install Real-Time Analyzer
   - If you are using IIS as your Web server, you need to identify a Default Web site for RTA.
   - If you are using Apache as your Web server, you need to permit Apache to shut down, and then restart.

   For complete details, read *Real-Time Analyzer (RTA)*, page 93.
6. Navigate through the final dialog boxes to complete the installation. For details, read *Complete a Websense Installation*, page 105.
7. Use `WebsenseReporter_5.2.exe` to install Websense Enterprise Reporter. When you select components to install, select them all for the best results. For details, read *Websense Reporting Components*, page 100.

8. Use Websense Enterprise Manager to identify the instance of Policy Server that you want to use. Generally, this is on Cisco Content Engine, but may, in this configuration, be on the same, or a different, remote machine. For details, read *Add and Connect to Policy Server*, page 112.
9. Use Websense Enterprise Manager to download the Websense Enterprise Master Database. For details, read *Websense Enterprise Master Database Download*, page 113.

Install Single Components on a Remote Machine

If you decide to install optional components, you can install them all on one remote machine, or you can install them individually on various remote machines. A list of the installers is available in *Select Websense Installers*, page 73.

NOTE

If you want to install more than one component on a single remote machine, read *"Basic" Installation with Websense Reporting Components*, page 84.

If you are installing Websense components individually on any number of machines, and/or any combinations of operating systems, you must install components in the following order—if you do not, you may not be able to complete your installation.

1. *Policy Server*, page 87
2. *User Service*, page 88
3. *Filtering Service*, page 90
4. Other embedded or remote components
   - *Network Agent*, page 91
   - *DC Agent*, page 95
   - *RADIUS Agent*, page 97
   - *eDirectory Agent*, page 98
5. Websense Enterprise Manager, *"Basic" Installation (Websense Enterprise Manager only)*, page 83
6. Reporting components, *Websense Reporting Components*, page 100

Policy Server

IMPORTANT
You **must** install Policy Server **before** you install other Websense Enterprise components. If Policy Server is installed on a remote machine or appliance, it **must** be running before you install other Websense Enterprise components on different remote machines or appliances.

In most embedded environments, installing Policy Server on a remote machine is not necessary, since Policy Server is usually enabled on Cisco Content Engine ACNS v5.3. The common situations where Policy Server is installed on a remote machine occur if you have:

- multiple languages to support. You will install one instance of Policy Server, Filtering Service, and User Service for each language.
- multiple subnets to support. You will install one instance of Policy Server, User Service, and Filtering Service per logical installation.

If you decide to install Policy Server by itself on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If necessary, disable Policy Server on Cisco Content Engine if you do not want to use that instance. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.
3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select the `WebsenseEnterprise_5.2.exe` installer, and then unzip the files. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.
    a. When prompted to choose a Websense product for installation, select **Websense Enterprise v5.2,** and then click **Next**.
    b. When the **Setup Type** dialog box opens, select **Custom**, and then click **Next**.
    c. When the **Component Selection** dialog box opens, select only **Policy Server**, and then click **Next**.

6. When the **Initial Filtering** dialog box opens, identify how you want Websense to filter Internet access immediately after installation, and then click **Next**. Your choices are as follows:
   - Select **Yes** to allow Websense Enterprise to filter Internet traffic immediately after installation, based on a default policy.
   - Select **No** to allow Websense Enterprise to monitor Internet traffic while permitting all Internet requests. You can select this option, and then install a Websense Enterprise reporting tool if you want to evaluate your network before applying custom Internet filtering policies.
7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.
8. Make sure you note the IP address of the remote machine where you installed Policy Server, as you will need to point other components to it.

User Service

NOTE

The machine where you install User Service **must** be able to connect to the machine or appliance where Policy Server is enabled, installed, and/or running.

In most configurations, User Service is embedded and enabled on Cisco Content Engine ACNS v5.3. The common situations where Policy Server is installed on a remote machine occur if you have:

- multiple languages to support. You will install one instance of Policy Server, Filtering Service, and User Service for each language.
- multiple subnets to support. You will install one instance of Policy Server, User Service, and Filtering Service per logical installation.

To install a single instance of User Service on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If necessary, disable User Service on Cisco Content Engine if you do not want to use that instance. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.

3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select the `WebsenseEnterprise_5.2.exe` installer, and then unzip the files. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.
   a. When prompted to choose a Websense product for installation, select **Websense Enterprise v5.2,** and then click **Next**.
   b. When the **Setup Type** dialog box opens, select **Custom**, and then click **Next**.
   c. When the **Component Selection** dialog box opens, select only **User Service**, and then click **Next**.
6. When the **Policy Server Identification** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.
7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.

WARNING

If you disable User Service on Cisco Content Engine ACNS v5.3, and then install it on a remote Windows machine, you **must** configure Cisco to enable a remote instance of User Service. For details, read *Install and Enable Embedded Websense Components*, page 54.

Filtering Service

> **NOTE**
> The machine where you install Filtering Service **must** be able to connect to the machine or appliance where Policy Server is enabled, installed, and/or running.

In most configurations, Filtering Service is enabled and running on Cisco Content Engine ACNS v5.3. The common situations where Filtering Service is installed on a remote machine occur if you have:

- multiple languages to support. You will install one instance of Policy Server, Filtering Service, and User Service for each language.
- multiple subnets to support. You will install one instance of Policy Server, User Service, and Filtering Service per logical installation.

To install a single instance of Filtering Service on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If necessary, disable Filtering Service on Cisco Content Engine if you do not want to use that instance. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.
3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select the `WebsenseEnterprise_5.2.exe` installer, and then unzip the files. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.
    a. When prompted to choose a Websense product for installation, select **Websense Enterprise v5.2,** and then click **Next**.
    b. When the **Setup Type** dialog box opens, select **Custom**, and then click **Next**.
    c. When the **Component Selection** dialog box opens, select only **Filtering Service**, and then click **Next**.

6. When the **Policy Server Identification** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.
7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.
8. Make a note of the IP address and the port number you identified for Filtering Service. You need this information for installing any of the Websense transparent ID agents.

Network Agent

In most configurations, Network Agent is enabled and running on Cisco Content Engine ACNS v5.3. The common situations where Filtering Service is installed on a remote machine occur if you have a large network that requires multiple instances of Network Agent, each of which will monitor a specific range of IP addresses for load balancing.

To install Network Agent on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If you only want to use one instance of Network Agent, disable Network Agent on Cisco Content Engine if necessary. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.
3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select `WebsenseNetworkAgent_5.2.exe` installer, and then unzip the files. Alternately, you can use `WebsenseEnterprise_5.2.exe` to install Network Agent. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.

NOTE

If you use `WebsenseEnterprise_5.2.exe` to install Network Agent, when the **Setup Type** dialog box opens, select **Network Agent**, and then click **Next**.

6. When the **Policy Server Information** dialog box opens, the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.
7. When the **Network Agent** dialog box opens, determine if Network Agent should be installed or not, and then click **Next**.
   - Select **Test Traffic Visibility** if you do not know if the machine can "see" Internet traffic. Move to Step 8 in this procedure.
   - Select **Install Network Agent** if you already know the machine can "see" Internet Traffic. Move to Step 9 in this procedure.
   - Select **Do not install** if you know the machine cannot "see" Internet traffic. The installer closes.
8. If you choose to test traffic, the **Test Traffic Visibility** dialog box opens. Choose one of the following actions.
   - Select the NIC you want to test from the **Network Card** drop-down menu., and then click **Start**.
   - If you do not see the NIC you want to test, click **Add**, and then enter the network ID and, if desired, the network mask.

   If the Test Traffic Visibility tool finds that the machine can "see" Internet traffic, you need to return to the **Network Agent** dialog box, and then select **Install Network Agent**.
9. When the **Network Agent and Firewalls** dialog box opens, choose the description that best fits the machine where you are installing Network Agent, and then click **Next**.
   - Select **Yes** if there is a firewall on the machine. The installer closes and does not install Network Agent.
   - Select **No** if there is not a firewall on the machine. The installer continues.
10. When the **Network Card Selection** dialog box opens, choose the NIC you know can see Internet traffic, and then click **Next**. If only one NIC card appears, you must select it before proceeding.
11. When the **Filtering Service Information** dialog box opens, you need to set HTTP reporting options, and then click **Next**.
    - Enter the IP address of the machine where Filtering Service is enabled and/or installed.
    - Enter the port number that Network Agent will use to communicate with Filtering Service.

12. When the **Reporting Option** dialog box opens, decide if you want to activate HTTP reporting or not, and then click **Next**.
    - Select **Yes** to enable HTTP reporting if Network Agent can "see" the network.
    - Select **No** if you do not want to enable HTTP reporting. You can set this later, if you want, via Websense Enterprise Manager.
13. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.

Real-Time Analyzer (RTA)

Websense Real-Time Analyzer provides Web-based reports that can be accessed directly from Websense Enterprise Manager. RTA includes drill-down functionality, and tracks Web access and bandwidth usage. For complete details, read *Websense Enterprise Real-Time Analyzer Administrator's Guide.*

If you install RTA, you must first:

- Enable and/or install Websense components. The components that are mandatory are—
  - Policy Server, User Service, Filtering Service, and Network Agent (usually enabled on Cisco Content Engine)
  - Websense Enterprise Manager (on a remote Windows machine)
  - Websense Enterprise Reporter (on a remote Windows, Solaris, or Linux machine)

  RTA must be able to directly communicate with Policy Server, Filtering Service, and any browser that will be used to view the reports.
- Have IIS or Apache 2.x installed on the machine where you are installing RTA. If you do not have a Web server currently installed, you can install Apache **before** you install RTA, or as part of the Websense installation. For details, read *Install Apache as the Web Server*, page 45.

RTA is extremely flexible and ideal for nearly instant access to employee Internet usage data. RTA also includes functions that allow administrators to view system health and statistics for Filtering Service and the RTA Server.

To install RTA:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.

2. Log on to the remote installation machine with **domain** and **local** administrator privileges.
3. Select `WebsenseEnterprise_5.2.exe` installer, and then unzip the files. For details, read *Access and Unzip Websense Installers*, page 74.
4. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.
   a. When the **Component Selection** dialog box opens, select **Real-Time Analyzer**, and then click **Next**.

   NOTE
   You may select other components if you want to install them on the same machine.

   b. If the **Policy Server Information** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.
   c. Select a directory where RTA files will be installed.
5. The installer checks for an installed Web server, which may be IIS or Apache. Depending on what the installer finds, you may or may not see prompts and selections.
   - If the installer detects only one of the supported Web servers, the installer accepts that Web server for that instance of RTA instance, and then continues. The process is automatic--you do not receive any messages.
   - If the installer opens the **Select Web Server** dialog box, read *Select a Web Server*, page 104.
   - If the installer does not detect a Web server, you will be asked if you want to install Apache. For details, read *Install Apache as the Web Server*, page 45.

   NOTE
   If you install Apache, the Websense installer starts the Apache installer, and then closes. Websense components are not installed. You will need to rerun the Websense installer again after you restart the machine.

6. If you use Apache Web server for your RTA installation, the **Restart Apache Web Server** dialog box opens. To enable RTA functions, you need to stop and then restart the Web server. Select one of the following options, and then click **Next**. Your choices are:
   - **Yes, stop and restart the Apache Web Server now**. *This is the recommended selection*.
   - **No, I will manually restart later**. You will need to restart either the machine or the service at a later time.
7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.
8. Install Websense Enterprise Reporter. For details, read *Install Websense Enterprise Reporter and Explorer*, page 101.

DC Agent

You **must** install DC Agent if you are using a Windows NTLM-based or Active Directory directory service to identify users and groups. If your network is large, you can install multiple instances of DC Agent on various machines in your network, to provide ample space for the DC Agent files that are continuously populated with Internet access information.

To install DC Agent on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If you only want to use one instance of DC Agent, disable DC Agent on Cisco Content Engine if necessary. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.
3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select `WebsenseDCAgent_5.2.exe` installer, and then unzip the files. Alternately, you can use `WebsenseEnterprise_5.2.exe` to install DC Agent. For details, read *Access and Unzip Websense Installers*, page 74.

5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.

> **NOTE**
>
> If you used `WebsenseEnterprise_5.2.exe` to install Network Agent, when the **Setup Type** dialog box opens, select **Network Agent**, and then click **Next**.

6. If the **Policy Server Information** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.
7. When the **Directory Access** dialog box opens, enter a user name and password, and then click **Next**. The user name for the domain must have full administrator privileges for DC Agent to work.
8. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.

RADIUS Agent

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

To install an instance of RADIUS Agent on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If you only want to use one instance of RADIUS Agent, disable RADIUS Agent on Cisco Content Engine if necessary. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.

WARNING

If you use a Windows NT LAN Manager-based directory service, you **must** disable RADIUS Agent on Cisco Content Engine ACNS v5.3, and then install a separate instance of RADIUS Agent on a remote machine in your network.

3. Log on to the remote installation machine with **domain** and **local** administrator privileges.
4. Select `WebsenseRADIUSAgent_5.2.exe` installer, and then unzip the files. Alternately, you can use `WebsenseEnterprise_5.2.exe` to install RADIUS Agent. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.

NOTE

If you use `WebsenseEnterprise_5.2.exe` to install RADIUS Agent, when the **Setup Type** dialog box opens, select **RADIUS Agent**, and then click **Next**.

6. If the **Policy Server Information** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.

   The default port number, 55806, is the port number used by Cisco Content Engine for Policy Server. You need to change this value only if you manually changed the port number when you set up embedded components on Cisco Content Engine.

7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.
8. Run **RADIUS Setup** from **Start > Programs > Websense Enterprise** and follow on-screen instructions.

eDirectory Agent

Websense Enterprise eDirectory Agent works with Novell eDirectory to identify users transparently, so Websense can filter them by policies assigned to users or groups. You can install eDirectory Agent on remote machines if you need. However, most customers enable the instance on Cisco Content Engine ACNS v5.3.

To install an instance of eDirectory Agent on a remote Windows machine:

1. Enable embedded components on Cisco Content Engine ACNS v5.3. For details, read *Install and Enable Embedded Websense Components*, page 54.
2. If you only want to use one instance of eDirectory Agent, disable eDirectory Agent on Cisco Content Engine if necessary. For details, read *Stop and Uninstall Embedded Websense Enterprise Components*, page 59.

WARNING

If you use a Windows NT LAN Manager-based directory service, you **must** disable RADIUS Agent on Cisco Content Engine ACNS v5.3, and then install a separate instance of RADIUS Agent on a remote machine in your network.

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

4. Select `WebsenseEDirectoryAgent_5.2.exe` installer, and then unzip the files. Alternately, you can use `WebsenseEnterprise_5.2.exe` to install eDirectory Agent. For details, read *Access and Unzip Websense Installers*, page 74.
5. Run the installer, and respond to the prompts as they appear. For details, read *Start a Websense Installation*, page 76.

> **NOTE**
>
> If you use `WebsenseEnterprise_5.2.exe` to install eDirectory Agent, when the **Setup Type** dialog box opens, select **eDirectory Agent**, and then click **Next**.

6. If the **Policy Server Information** dialog box opens, enter the IP address and communications port number that identifies the machine or appliance where Policy Server is installed, and then click **Next**.

   The default port number, 55806, is the port number used by Cisco Content Engine for Policy Server. You need to change this value only if you manually changed the port number when you set up embedded components on Cisco Content Engine.
7. Follow onscreen prompts to complete the installation. For details, read *Complete a Websense Installation*, page 105.
8. Run **eDirectory Setup** from **Start > Programs > Websense Enterprise** and follow onscreen instructions.

Websense Enterprise Manager

The procedure provided for a "basic" Websense installation on Windows is the same as installing Websense Enterprise Manager separately. For details, read *"Basic" Installation with Websense Reporting Components*, page 84.

Websense Reporting Components

WARNING

Installing Websense Enterprise Reporter is a completely different procedure than installing other Websense Enterprise components. This section does not attempt to provide detailed information, as the installation and use of Websense Enterprise Reporter is documented elsewhere.

If you want to install Websense Enterprise Reporter and Explorer, Websense, Inc. strongly suggests reading the *Websense Enterprise Reporting Installation Guide* before you continue the installation.

Other useful documents for Websense Enterprise reporting tools are:

- *Websense Enterprise Reporter Administrator's Guide*
- *Websense Enterprise Explorer Administrator's Guide*

These documents are available at www.websense.com/support. Make sure you access documents for Websense Enterprise v5.2.

Websense Enterprise Reporter supports three different ways to view data:

- Websense Enterprise Reporter allows users to schedule and email reports. This component must be installed for Websense Enterprise Explorer and/or Websense Real-time Analyzer (RTA) to work. The installation file is `WebsenseReporter_5.2.exe`.
- Websense Enterprise Explorer is an optional component selection during the reporting installation. To work, Explorer requires that IIS or Apache 2.x is installed on the machine. Websense Enterprise Reporter must also be installed. The installation file is `WebsenseReporter_5.2.exe`.
- Websense Real-time Analyzer (RTA) is an optional component. Both Websense Enterprise Manager and Websense Enterprise Reporting must be installed before you can install RTA.
  - RTA must have access to an IIS or Apache 2.x Web server. The installation file is `WebsenseManager_5.2_ACNS5.3.exe`.
  - RTA can be installed with Websense Enterprise Manager.

Websense Reporting Tools and Databases

You can install Websense Enterprise Reporter any time after you have installed Websense Enterprise Manager. The reporting functions require either an MSDE or SQL Server database for operations. *The database must be installed and accessible before you can install Websense Enterprise Reporter.* If you do not have MSDE or SQL Server installed already, you can:

- purchase and install SQL Server. For details, go to www.microsoft.com/sql/. If your organization already has an instance of SQL Server that is accessible to the machine where you install Websense Enterprise Reporter, you can use that instance for Websense reporting functions.
- download and install MSDE **before** installing Websense reporting components. The free download is available at www.microsoft.com/downloads/. MSDE runs on most Windows operating platforms. For details, read *Select Websense Installers*, page 73.
- download and install MSDE **while** installing Websense reporting components. The installer includes the needed links, however, this installation method stops the Websense installer, and then starts the MSDE installer. You have to rerun the Websense installer after the MSDE installation is complete.

Install Websense Enterprise Reporter and Explorer

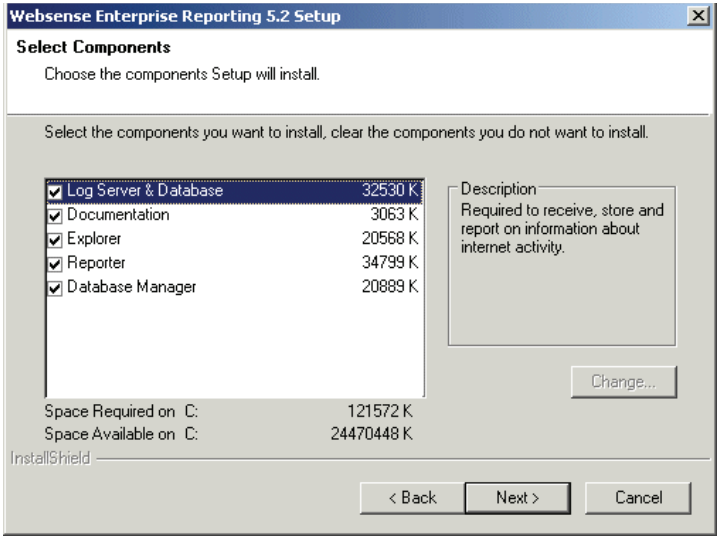
To install Websense Enterprise Reporter and Explorer:

1. Install Websense Enterprise Manager. For details, read *"Basic" Installation (Websense Enterprise Manager only)*, page 83.
2. Select `WebsenseReporter_5.2. exe` to install Websense Enterprise Reporter. For details, read *Select Websense Installers*, page 73.
3. Access and unzip the installer for Websense Enterprise Reporter. For details, read *Access and Unzip Websense Installers*, page 74.
4. Complete the dialog boxes presented at the beginning of the installation. For details, read *Start a Websense Installation*, page 76.
5. When the **Select Components** dialog box opens, select the components you want to install, and then click **Next**. Your choices are:
   - **Log Server & Database**. *Required*. This component **must** be installed somewhere on your network for reporting components to work.

- **Documentation**. *Optional*. If selected, this places PDF documents for Websense Enterprise Reporter and Websense Enterprise Explorer on your desktop. The default file location is `C:\\Program Files\Websense\bin\documents`.
- **Explorer**. *Optional*. If selected, drill-down reports provide rapid access to Internet traffic reports. This is a Web-based component, and IIS or Apache 2.x must be installed and running.

> **NOTE**
> If you want access to Explorer, you must install this component. If you are not sure, you can always install it later.

- **Database Manager**. *Optional*. Database Manager provides tools for managing the size of Log Database. If you select this component, you must also install **Log Server & Database** somewhere on your network.



Select Components dialog box for Websense Enterprise Reporter

6. Follow onscreen prompts as they appear.
7. When the **Install Shield Complete** dialog box opens, click **Finish** to close the installer. Various messages appear as the wizard completes operations.

Define Apache Access Rights for Explorer

> **NOTE**
> If you are installing Explorer, and using Apache as your Web server, you need to complete this series of dialog boxes.

To define access rights for Explorer when you use Apache as your Web server:

1. If the Websense installer detects an installation of Apache as your Web server, a dialog box opens that describes the three access levels for Explorer. When you are done reading the information, click **OK**.

   The three access levels for Apache are:

   - **Administrator**. Can make changes to the database and run any Explorer report.
   - **HR User**. Can run any report, and view any data available in the report, including user and machine names.
   - **Restricted User**. Can run any report but sees only ID numbers that Explorer substitutes for user and machine names.

   More than one person can assume each role. The user name and password applies to the role, not to individual users.

2. As dialog boxes titled **Enter User Name and Password** open, identify a different user name and password for each role, and then confirm the password.

   > **NOTE**
   > If you do not want to use a particular access level, leave all fields blank, and then click **Next**.

3. Click **Next** to move to the next installation screen.

Select the IIS Virtual Directory Location

If you are installing RTA or Explorer, and want to use IIS as your Web server, you need to identify the default database location. In most instances, the *Default Web Site* selection is appropriate. The installer also detects any other valid Web sites that available to your network. You can select any other valid Web site to which you have access, if appropriate.

To select the default Web site for the IIS Web site:

- To accept the default Web site, simply click **Next**.
- To select a Web site other than the default, click the field arrow, select the alternate Web site you want to use, and then click **Next**.

Select a Web Server

If you have both Microsoft IIS and Apache installed on the machine where you are installing RTA or Explorer, the Websense installer opens a dialog box that allows you to select the Web server you want to use.

To select the Web server:

1. When the **Select Web Server** dialog box opens, choose either **IIS** or **Apache**.
2. Click **Next** to move to the next dialog boxes for your installation.

You will see additional dialog boxes that are specific to the Web server you choose.

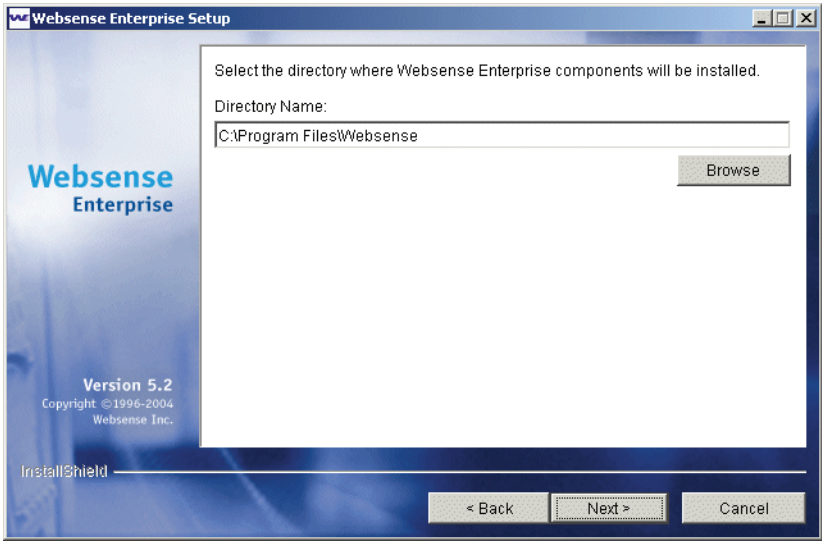
- If you are using Apache as your Web server, read *Define Apache Access Rights for Explorer*, page 103.
- If you are using IIS as your Web server, read *Select the IIS Virtual Directory Location*, page 104.

Complete a Websense Installation

When all configuration options for installation are complete, a series of dialog boxes open that provide the final information the installer needs. These dialog boxes appear for installations using `WebsenseEnterprise_5.2.exe` and each of the individual installers.

To complete your Websense installation:

1. When the Websense Directory location dialog box opens, accept the default path **C:\Program Files\Websense**, or click **Browse** to locate a different installation folder.



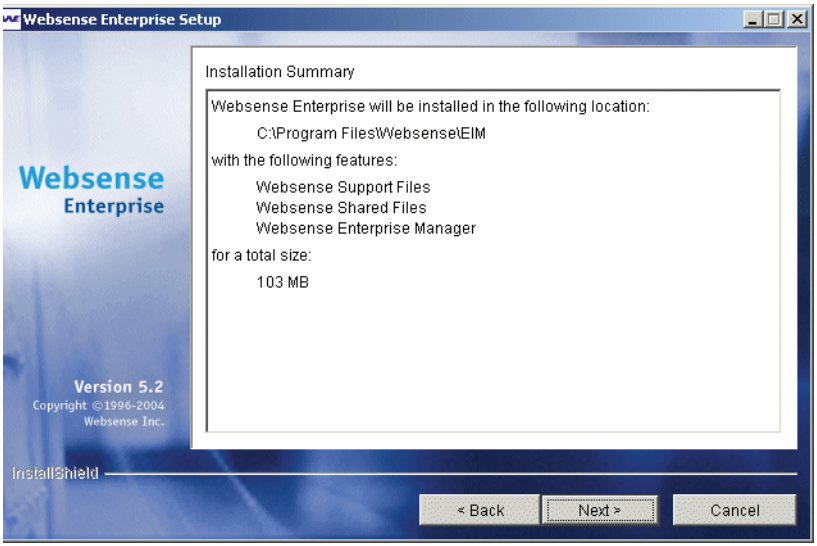
File location dialog box

2. Click **Next**. The **Systems Requirements** dialog box may open, but only if resources at the machine do not meet minimum requirements. If this dialog.
   - If the machine does not have enough disk space, the selected components do not install, and the Websense installer closes.
   - If the machine does not have the recommended amount of memory, the installation continues and all components are installed. The machine may or may not be able to successfully run the installed components.

     WARNING
     Upgrade the memory to the recommended minimum to ensure the best performance of the components you are installing.

   Details show what discrepancies exist between the minimum requirements and the actual resources at the machine. When the **System Requirements** dialog box appears:
   a. Review the data provided, and make note of the discrepancies. You can fix the problems at a later time.
   b. If the amount of memory is at issue, you can continue the installation by clicking **Next**. (If there is not enough disk space, the installer closes.)

   The **Installation Summary** dialog box opens in most cases.
3. When the **Installation Summary** dialog box opens, check the details.
   - If the directory location or any of the listed components are wrong, click **Back** until you get to the appropriate dialog box. Correct the problem, and then click **Next** to move forward and return to the **Installation Summary** dialog box.
   - If the directory location and the list of components is correct, click **Next**.



Installation Summary dialog box

The actual installation of Websense files and components begins. A progress bar at the bottom of the installer tracks the progress of the installation.

4. If the **Network Agent Features** dialog box opens, review the data, and then click **Next**.

   This dialog box may or may not appear, depending on the components you are installing, and whether or not the Websense installer detects an instance of Network Agent at the local machine.

5. When the **Installation Complete** dialog box opens, click **Finish**. The installer closes.

6. Restart the machine where Websense components have been installed.

   - Although some Websense installations do not prompt you to restart the machine where you installed components, it a good idea to do so. By restarting the machine, configuration entries are saved and any open processes closed, and then restarted.
   - If you want to install, add, repair, or remove components, you need to run the Websense installer again. If you have not restarted the machine, a prompt informs you that the Websense installer will not run until you do so.

Install and Implement Language Pack

Websense Enterprise Language Pack translates your English Websense Enterprise system to one of the supported languages:

Chinese Simplified	French	Japanese	Spanish
Chinese Traditional	German	Korean	
English	Italian	Portuguese (Brazil)	

Run Websense Enterprise Language Pack from a remote machine to update Policy Server on Cisco Content Engine ACNS v5.3 with non-English language keys. For instructions on applying the Websense Enterprise Language Pack remotely, refer to the documentation accompanying the Websense Enterprise Language Pack.

NOTE

Installing the Websense Enterprise Language Pack changes the language from English to the language you select for:

- User messages
- Websense categories
- Report data

Websense Enterprise Language Pack does *not* change the language in Websense Enterprise Manager, Websense Enterprise Reporter, Explorer, or RTA screens and dialog boxes.

To install Websense Enterprise Language Pack:

1. Locate `WebsenseLanguagePack_5.2.exe`. For details, read *Access and Unzip Websense Installers*, page 74.

NOTE

Websense Enterprise Language Pack installers are available for Windows, Solaris, and Linux operating systems. For most Cisco Content Engine ACNS v5.3 installations, you need to choose the Windows version.

2. Access and unzip setup files. For details, read *Access and Unzip Websense Installers*, page 74.
3. Begin running the Websense installer. For details, read *Start a Websense Installation*, page 76.
4. When the **Language Selection** dialog box opens, select the language you need, and then click **Next**.
5. Continue responding to prompts as they appear, and then click **Finish** to close the installer.
6. To finalize this process, you **must** install translated pages on Cisco Content Engine. For details, read *Translated User Messages Pages for Cisco Content Engine ACNS v5.3*, page 122.

CHAPTER 8 | Initial Setup Procedures

Once you enable embedded Websense components on Cisco Content Engine ACNS v5.3, install Websense Enterprise Manager, and any other optional remote components, you need to complete the installation. The mandatory tasks are:

1. **Add and connect to Policy Server**. The first thing you must do is to install and connect to a Policy Server. For details, read *Add and Connect to Policy Server*, page 112**.**
2. **Download the Websense Enterprise Master Database:** You must enter your Websense Enterprise subscription key on the **Database Download** screen of the **Settings** dialog box and download the Websense Enterprise Master Database. See *Add and Connect to Policy Server*, page 112 for instructions.
3. **Identify Cisco Content Engine ACNS v5.3 by IP address:** If Cisco Content Engine is multihomed (multiple network interface cards), identify the appliance by its IP address in your network so that Websense block messages can be sent to users. See *User Message URLs for Machines with Multiple NIC Cards*, page 70.
4. **Configure your firewall or Internet router.** If you are using an upstream network device such as a firewall or Internet router, you must configure it to permit traffic from Cisco Content Engine. See *Configure FireWalls or Routers*, page 118 for details.
5. **Configure your network** to regulate browser access to the Internet in transparent or nontransparent mode. For details, refer to *Browser Access to the Internet via Cisco Content Engine ACNS v5.3*, page 72.

Configuration via Websense Enterprise Manager

Websense Enterprise Manager provides an attractive and easy-to-use interface for configuring your Websense installation for Cisco Content Engine ACNS v5.3. You can set some of these parameters using the Cisco Command Line Interface (CLI), documented in *Cisco Content Engine ACNS v5.3 Command Line Interface*, page 54. Other parameters can be set only in Websense Enterprise Manager.

The following mandatory configuration procedures must be set for your Websense Enterprise solution to work.

1. *Add and Connect to Policy Server*, page 112
2. *Websense Enterprise Master Database Download*, page 113
3. *Define Winix Settings for Windows-based Directory Services*, page 116 (These settings are necessary only if you are using a Windows-based Directory Service, and User Service is enabled on Cisco Content Engine.)

Add and Connect to Policy Server

When you first open Websense Enterprise Manager, you must identify a Policy Server if it is not installed on that machine, and then connect to it. For most organizations, Policy Server is enabled on Cisco Content Engine ACNS v5.3.

To add a Policy Server:

1. Select **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.
2. When Websense Enterprise Manager opens, right-click in the navigation pane, and then select **Add Policy Server** from the drop-down menu.
3. Identify the appliance or machine where you installed Policy Server, and then click **OK**. Enter the following to identify Policy Server.
   a. Enter the IP address. For most installations, this is the IP address of the Cisco Content Engine.
   b. Enter the port number. For most installations, the default port number, 55806, is appropriate.

   A “server” icon and the IP address you entered appear in the navigation pane.

4. Double-click the **Policy Server** icon to access the **Set Websense Password** dialog box.
5. Enter a password, confirm it, and then click **OK**.The password should be between 4 and 25 characters in length

> **NOTE**
> Write this password down for future reference. You need the password whenever you connect to the selected Policy Server, and any time that you stop and then restart Policy Server.

Websense Enterprise Manager opens.

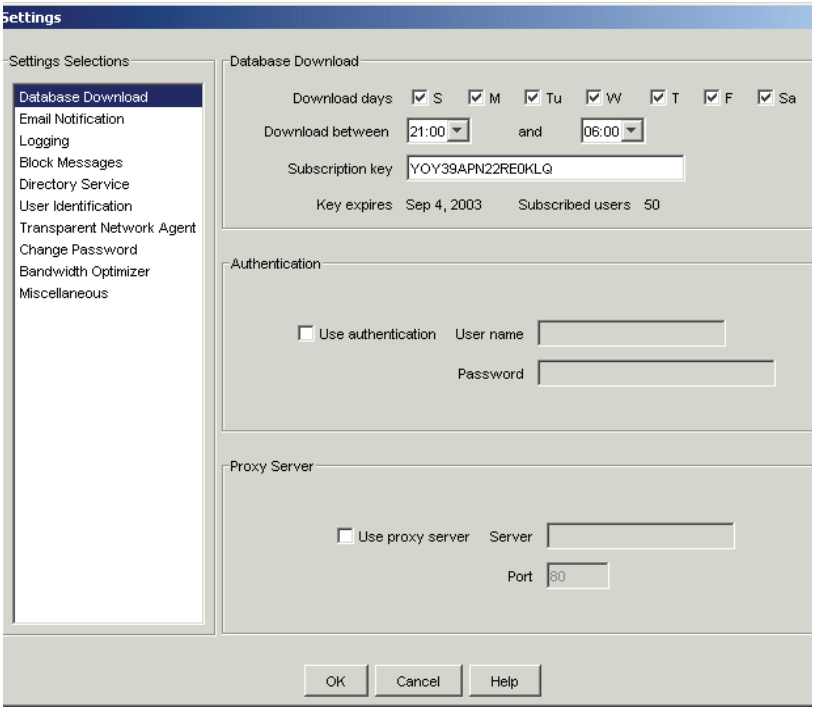
Websense Enterprise Master Database Download

The Websense Enterprise Master Database provides the information needed for filtering. Websense, Inc., updates the database daily, and most organizations download the database in the middle of the night to avoid impacting normal business operations.

To configure the Websense Enterprise Master Database and define downloads:

1. Select: **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.
2. Log on to the appropriate Policy Server.
   - If you have not already done so, add a Policy Server, and then connect to it. For details, read *Add and Connect to Policy Server*, page 112.
   - If you have already added a Policy Server—
     a. double-click the **Policy Server** icon in the navigation pane.
     b. When the **Password** dialog box opens, enter the password, and then click **OK**.
     c. Enter the IP address or the name of Cisco Content Engine on which Policy Server is installed, and the configuration port established during installation. The default port number is 55806.
     d. Click **OK**. The server's IP address or machine name appears in the Manager’s navigation pane.

3. Double-click the **Policy Server** icon in the navigation pane.
   - For first time access, the **Set Websense Password** dialog box appears.
     - If prompted, enter a password that contains between 4 and 25 characters. Confirm the password, and then click **OK**.
   - For subsequent access, enter the password, and then click **OK**.
4. Access the **Settings** dialog box.
   - For first time access, the **Settings** dialog box opens automatically.
   - If you have opened Websense Enterprise Manager before, select **Server > Settings** to access the **Settings** dialog box.



Database Download dialog box

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

> **NOTE**
> When the database download completes, the value in the **Subscribed users** field updates automatically.

6. If your installation includes an upstream firewall or proxy server that handles Internet access and requires authentication, you need to enter that data for downloading the Websense Enterprise Master Database. In the **Authentication** panel on the **Database Download** screen:
   a. Check **Use authentication**.
   b. Enter the **User name** required by the upstream proxy server or firewall to download the Websense Enterprise Master Database.
   c. Enter the **Password** required by the upstream proxy server or firewall.

   WARNING
   Be sure to configure the upstream proxy server or firewall to accept clear text or basic authentication. If you do not, Websense Enterprise Master Database may not download properly.

7. In the **Proxy Server** panel on the **Database Download** screen:
   a. Check **Use proxy server**.
   b. Enter the **IP address** of the upstream proxy server or firewall.
   c. Enter the **Port** of the upstream proxy server or firewall. The default entry is 80.

   IMPORTANT
   If your network requires browsers to use an upstream proxy server to reach the Internet, Websense must use the same proxy settings that are in use at the browser.

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

   NOTE
   If Filtering Service is on the same remote machine as Websense Enterprise Manager, database downloads to local memory may push CPU usage to 90% or higher.

9. When the **Saving Data** dialog box opens, click **Done**.

Define Winix Settings for Windows-based Directory Services

If User Service is enabled on Cisco Content Engine ACNS v5.3, and you are using Windows NT or Active Directory (Mixed Mode), or Active Directory (Native Mode) as your directory service, you need to define Winix NTML settings. Winix is proprietary Websense code that supports communications between Cisco Content Engine and Directory Services at a machine using a Windows operating system.

To define Winix settings:

1. Open Websense Enterprise Manager on the machine where it is installed by selecting **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.
2. In the navigation pane, double-click the Policy Server you want to work with, and then enter associated password.
3. Select **Server > Settings > Directory Services**.
4. Select the directory service you are using, which must be either—
   - Windows NT / Active Directory (Mixed Mode)
   - Active Directory (Native Mode)

   Only the above selections activate the **Winix NTML Settings** panel.
5. Identify an administrative user with access to the domain. Without this data, Winix is unable to function.
   - Enter the user name in the **Administrative User** field.
   - Enter the password for the administrative user in the **Password** field.
   - Enter the domain for which the administrative user has access in the **Administrative Domain** field.
   - Enter the Wins server IP address, if there is a Wins server. If there is not, leave the **Wins Server** field empty.
6. Click **OK**.

Set HTTP Reporting and Protocol Management Use for Network Agent

If you install Network Agent, the installation automatically enables HTTP logging and Protocol Management. If you decide to disable either of these options, use Websense Enterprise Manager to edit Network Agent settings.

To disable HTTP logging or Protocol Management:

1. Open Websense Enterprise Manager on the machine where it is installed by selecting **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.
2. In the navigation pane, double-click the Policy Server you want to work with, and then enter associated password.
3. Select **Server > Settings > Network Agent**.
4. When the **Network Agent** screen opens, click **Local Settings**. The **Settings: Network Agent: Local** dialog box opens, and lists all machines where an instance of Network Agent is installed.
5. Select the instance of Network Agent you want to modify, and then click **Edit**. The local settings for that instance of Network Agent open.
6. Clear the respective checkbox to disable **HTTP reporting** and/or **Protocol monitoring** in the **Activities** area.
7. Stop and restart Network Agent. For details, read *Stop, Start, or Restart Websense Services*, page 46.

Configure User Identification Agents

If you are using DC Agent, eDirectory Agent, or RADIUS Agent, you need to set up configuration in Websense Enterprise Manager. The process is complex, and settings in Websense Enterprise Manager must reflect settings defined on the Cisco appliance. For details, read:

- *Transparent Identification of Users in Websense Enterprise v5.2* (technical white paper)
- *Websense Enterprise v5.2 Administrator's Guide,* Chapter 2, *User Identification*

Configure FireWalls or Routers

To prevent users from circumventing Websense Enterprise, configure your firewall or Internet router to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from Cisco Content Engine. Contact your router or firewall vendor for information on configuring access lists on the router or firewall.

IMPORTANT

If Websense Enterprise Manager requires authentication through a proxy server or firewall for HTTP traffic, you must configure the proxy server or firewall to accept clear text or basic authentication. to enable the Websense Enterprise Master Database download.

CHAPTER 9 | Modify, Upgrade, Downgrade, and Uninstall Websense

This section describes the processes necessary to modify, upgrade, downgrade and uninstall Websense components.

Modify an Existing Websense Installation

Generally, organizations modify an existing Websense Enterprise installation to accommodate changes in environment, personnel, or new bandwidth or traffic requirements. In some cases, components may be disabled or uninstalled at one machine or appliance, and then installed on another. To modify an existing Websense installation, use the same installer you initially used to install remote Websense components.

Add Remote Websense Components

To add components in a remote Windows environment:

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

IMPORTANT

User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense Enterprise cannot filter by users and groups.

If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation by using the Windows Services **Properties** dialog box. For details, see *Change Access Rights for Components on Windows Machines*, page 48.

2. Select `WebsenseEnterprise_5.2.exe` as your installer, and then unzip the files. Alternately, you can choose a separate installer for some Websense components.
   - For details about the available installers, read *Select Websense Installers*, page 73.
   - For details about accessing and unzipping installers, read *Access and Unzip Websense Installers*, page 74.
3. Run the installer, and navigate through the opening dialog boxes. For details, read *Start a Websense Installation*, page 76.
4. When the **Add/Remove/Repair** dialog box appears, choose **Add Websense components**, and then click **Next**.
5. When the **Add Websense Enterprise Components** dialog box appears, choose components you want to add, and then click **Next**.
6. Continue navigating through dialog boxes as they appear.
   - If you are installing Network Agent, you may need to test access to Internet traffic, and select a network interface card (NIC) you want to use for capturing traffic. For more information, read *Network Agent*, page 80.
   - If you are installing Real-Time Analyzer—
     - and using IIS as your Web server, identify a virtual directory in IIS Manager. The default value is **Default Web Site**, which is correct in for most installations. If you have renamed the default Web site in IIS Manager, or your operating system is a non-English version of Windows, you must enter a value in the Web site name field that matches an existing Web site name in IIS Manager. For details, read *Copy Default Web Site Names From IIS Manager*, page 49.
     - and using Apache as your Web server, you need to allow the Websense installer to stop and then restart the Apache service.
7. Complete the installation. For details, read *Complete a Websense Installation*, page 93.

Repair Remote Websense Components

Generally, organizations repair an existing Websense Enterprise installation if a component did not install correctly, is not functioning as it should, or if the company has received notification that hotfix rollups are available from Websense, Inc.

This repair process does not troubleshoot components, but simply overwrites all installed components, using the original installation data retrieved from the configuration file. To repair an existing Websense installation, use the same installer you initially used to install remote Websense components or the version for the hotfix rollup.

To repair Websense components on remote Windows machines:

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

   IMPORTANT

   User Service and DC Agent must have administrator privileges on the network to retrieve user login information from the domain controller. Without this information, Websense Enterprise cannot filter by users and groups.

   If you cannot install these components with such privileges, you may configure administrator privileges for these services after installation by using the Windows Services **Properties** dialog box. For details, see *Change Access Rights for Components on Windows Machines*, page 48.

2. Select `WebsenseEnterprise_5.2.exe` as your installer, and then unzip the files. Alternately, you can choose a separate installer for some Websense components.
   - For details about the available installers, read *Select Websense Installers*, page 73.
   - For details about accessing and unzipping installers, read *Access and Unzip Websense Installers*, page 74.
3. Run the installer, and navigate through the opening dialog boxes. For details, read *Start a Websense Installation*, page 76.

4. When the **Add/Remove/Repair** dialog box appears, choose **Repair Websense components**, and then click **Next**.
5. Select **Repair existing Websense Enterprise components**, and then click **Next**.
6. When the **Repair** dialog box opens, click **Yes** to indicate that you understand the components you are repairing are actually being installed again, and then click **Next**.
7. When the **Stopping Services** dialog box opens, click **Next** to stop any components that are running.
8. Complete the installation. For details, read *Complete a Websense Installation*, page 93.

Change User Messages

You can change user messages as needed. Changes may include localization, text changes within the actual message, and changes to font styles such as bold and italic.

Translated User Messages Pages for Cisco Content Engine ACNS v5.3

Before employees receive translated user message pages, you must install Websense Enterprise Language Pack on any machine using Windows, Solaris, or Linux as the operating system, as long as that machine can communicate with Cisco Content Engine ACNS v5.3.

Once Language Pack is installed, you can localize Websense Enterprise block messages by copying non-English language versions of the default user message pages from the machine where you install Websense Enterprise Language Pack to Cisco Content Engine.

To apply translated user message pages:

1. Run Websense Enterprise Language Pack. For details, read *Install and Implement Language Pack*, page 108.
2. Stop Filtering Service.
   - If Filtering Service is on Cisco Content Engine ACNS v5.3, use CLI, and enter the following command line to stop all embedded Websense services.

     ```
     no websense-server enable
     ```

- If Filtering Service is on a remote Windows machine, read *Stop, Start, or Restart Websense Services*, page 46.

3. Move to Cisco Content Engine ACNS v5.3.
   - If you have already installed translated block messages for the language of choice, delete any files with the same name as the files you are going to copy to Cisco Content Engine. The files are at:

     `Websense Enterprise/EIM/BlockPages/<language code>/Default.`

     NOTE

     You cannot overwrite or delete files on Cisco Content Engine ACNS v5.3 using FTP.

   - If this is the first time you are installing translated block messages for the language of choice, create the following directory structure.

     `WebsenseEnterprise/EIM/BlockPages/<language code>/Default`

   For the language code, select the appropriate value from the following table.

Language	Code	Language	Code
Chinese simplified	zh_CN	Italian	it
Chinese traditional	zh_TW	Japanese	ja
English	en	Korean	ko
French	fr	Portuguese (Brazilian)	pt_BR
German	de	Spanish	es

   For example, the structure for French user message pages would be:

   `WebsenseEnterprise/EIM/BlockPages/fr/Default`

4. Download translated user message pages into the `/<language code>/Default` folder on Cisco Content Engine using either the Command Line Interface or FTP.
   - If you are using the CLI, at Cisco Content Engine, enter—
     ```
     copy ftp disk <remote FTP server IP address>
     <remote directory path> <remote file name <local
     file name>.
     ```
   - If you are using FTP, the next example shows the series of commands necessary for uploading translated Japanese files.
     ```
     ftp 10.201.21.25
     cd local1/WebsenseEnterprise/EIM/BlockPages/
     mkdir ja
     cd ja
     mkdir Default
     cd Default
     bin
     mput *.*
     ```
   - When prompts appear, answer **y** for **yes** to every file transfer question.
5. Restart Filtering Service.
   - If Filtering Service is on Cisco Content Engine use the Command Line Interface and enter the following command, which restarts all Websense embedded components.
     ```
     websense-server enable
     ```
   - If Filtering Service is on a remote Windows machine, read *Stop, Start, or Restart Websense Services*, page 46.

The Websense Enterprise Master Database reloads automatically.

Create Custom User Message Pages

You can create custom user message pages by modifying the default user message pages provided with Websense Enterprise. The default English block message files are in the following folder on Cisco Content Engine ACNS v5.3. `WebsenseEnterprise/EIM/BlockPages/en/Default`

IMPORTANT

Do **not** change the contents of the **Default** folder.

The table below shows user message pages by file name and a description of each.

File Name	Description
block.html	Text for the top frame of the block message, indicating that access is restricted. When seen by a user, the block message shows which site was requested, and the reason why that site is blocked.
blockframe.html	Contains text and buttons that appear in the bottom frame when a user requests access to a site that is in a category whose filtering option is set to **Block**.
blockStyle.css	Contains the code necessary for resolving user message text to the presentation format.
continueframe.html	Contains text and buttons that appear in the bottom frame when a user requests access to a site that is in a category whose filtering option is set to **Continue**.
master.html	The master frame that appears in the postpone, continue, and quota block messages. This message is replaced by a custom message if you enter an alternate URL in Websense Enterprise Manager. To access the appropriate dialog box, select **Server > Settings > Block Messages**.
messagefile.txt	Contains the actual text that appears in the various user messages.

File Name	Description
moreinfo.html	Contains content for the page that appears when a user clicks the **More Information** link on any Websense message.
quotaframe.html	Contains text and buttons that appear in the bottom frame when a user requests access to a site that is in a category whose filtering option is set to **Limit by Quota**.

To create custom user message pages:

1. Stop Filtering Service. For details, read *Stop, Start, or Restart Websense Services*, page 46.
2. Copy the user message page files you want to customize from the `WebsenseEnterprise/EIM/BlockPages/<language code>/Default` folder on Cisco Content Engine to a location on the local drive of a remote machine.

   Refer to Real-Time Analyzer for instruction on how to manage files.
3. Open each file in a text editor and make the desired changes.

   The files contain comments that help guide you in editing the text. Observe the following cautions when editing these files:

   - **Do not** modify tokens, which are enclosed by **$*** and ***$** symbols, or the general structure of the HTML code as it relates to tokens. The tokens enable Websense to display specific information in the user message.
   - **Do not** change the names of customized user message page files. Websense looks for user message page files by name.

   IMPORTANT

   Websense uses the user message page files you place in the `Websense\EIM\BlockPages\<language code>\Custom` folder, not default pages with the same name located in the **Default** folder.
4. Save, and then close the file.

5. Add the customized user message page files to the `WebsenseEnterprise/WW/BlockPages/<language code>/Custom` directory on Cisco Content Engine.

   You can use the Cisco CLI or FTP to accomplish this.

6. Restart Filtering Service. For details, read *Stop, Start, or Restart Websense Services*, page 46. From this time forward, employees will receive these new customized user messages.

Restore Original User Message Pages

To restore the original user message pages if you experience errors after implementing custom user message pages:

1. Stop Filtering Service. For details, read *Stop, Start, or Restart Websense Services*, page 46.
2. Delete all files from the `WebsenseEnterprise/EIM/BlockPages/<language code>/Custom` directory.
3. Restart Filtering Service.

Upgrade a Websense Installation

When you upgrade Cisco Content Engine from ACNS v5.2 to ACNS v5.3:

- previously embedded Websense Enterprise components upgrade automatically. These are Policy Server, User Service, and Filtering Service.
- eDir Agent and RADIUS Agent can be installed along with other embedded Websense Enterprise components. These components were not previously supported for Cisco Content Engine.
- you must upgrade any Websense Enterprise components installed on remote machines.

Refer to *Chapter 7: Install Websense Enterprise on Remote Machines* for procedures on installing and configuring separately installed components.

Before Upgrading

Before you upgrade Websense Enterprise components, be aware of the following conditions that may affect your upgrade.

Concern	Upgrade information
Backup files	After you stop Websense services, back up the latest information by copying `config.xml`, `websense.ini`, and `eimserver.ini`. • For Windows machines, the default location of these files is: `Program Files\Websense\EIM\bin`. • For Cisco Content Engine ACNS v5.3, the default location of these files is: `/local1/WebsenseEnterprise/EIM/bin`.
Distributed components	Run `setup.exe` from `WebsenseEnterprise_v5.2.exe` at each machine where the older version of a Websense component is located. The installer automatically detects what is installed and upgrades components accordingly.
Non-English operating systems	Upgrading Websense components converts them to English. Install Websense Enterprise Language pack on the machine where Websense components are installed to convert them back to the language used by the operating system.

Upgrade Websense Enterprise

Although both Cisco Content Engine ACNS v5.2 and ACNS v5.3 include Websense Enterprise v5.2, Websense, Inc. repackaged Websense Enterprise v5.2 for Cisco Content Engine ACNS v5.3. The repackaged Websense Enterprise includes hotfixes and newly enabled components for Cisco Content Engine. Examples of these changes include:

- eDirectory Agent
- RADIUS Agent
- Linux NTLN directory support

WARNINGS

Be aware of the following critical details when you upgrade to Cisco Content Engine ACNS v5.3:

1. Upgrade all remote Websense Enterprise components to Websense Enterprise v5.2—other Websense Enterprise versions are **not** compatible with Cisco Content Engine ACNS v5.3.
2. If multiple Websense Enterprise components run on one remote machine, use the installer to upgrade them at the same time. If you upgrade Websense Enterprise components individually when they are on the same remote machine, you may corrupt files associated with the previous version of Websense Enterprise.
3. If you uninstall Websense Enterprise components from Cisco Content Engine, you lose all previous configuration files that may be stored on the appliance. To avoid losing previous data, Websense, Inc. recommends you disable Websense Enterprise components instead of uninstalling them.

The "main" Websense installer, `WebsenseEnterprise_5.2.exe`, is used as the installer in the next procedure. The procedure covers only components that are running on the same remote machine. Refer to *Chapter 7: Install Websense Enterprise on Remote Machines* for procedures on installing separately installed components.

To upgrade Websense Enterprise components installed on remote Windows machines:

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

IMPORTANT

DC Agent must have administrator privileges to the network. Without this level of access, user log in data cannot be retrieved from the domain controller. Without this information, Websense Enterprise cannot filter by users and groups.

If you cannot install DC Agent with administrator privileges, you can configure it after installation. Use the **Properties** dialog box, available from the Windows **Services** panel. For details, read *Change Access Rights for Components on Windows Machines*, page 48.

2. Close all open applications.
3. Stop all Websense services on the remote machine. For details, read *Stop, Start, or Restart Websense Services*, page 46. If these services have run without interruption for several months, they may take a long time to stop. It is possible the upgrade process may time out.
4. Download the Websense Enterprise installer, `WebsenseEnterprise_5.2.exe`, and then unzip it. For details, read *Access and Unzip Websense Installers*, page 74.
5. Begin the Websense installation. For details, read *Start a Websense Installation*, page 76.
6. When prompted, select **Upgrade Websense Enterprise**, and then click **Next**.
7. A message opens that warns you to upgrade any other Websense modules that may be dependant on the system you are upgrading. Click **Next** to continue.

WARNING

Upgrade all Websense Enterprise components to the same version, and at the same time. If you do not, you could corrupt operating or historical files.

8. Respond to screen prompts as they appear. If you need information about the data necessary for a particular component, locate the component installation procedure in *Install Single Components on a Remote Machine*, page 86.
9. Finish your Websense upgrade. For details, read *Complete a Websense Installation*, page 105.

Downgrade Cisco Content Engine ACNS v5.3

Websense Enterprise does not support downgrading. Downgrading Cisco Content Engine from ACNS version 5.3 to ACNS version 5.2 downgrades Websense Enterprise v5.2 (enhanced) to Websense v5.2 (original) and results in the following:

- You lose all v5.2 (enhanced) Websense Enterprise configuration data. The version of Websense Enterprise v5.2 (original) embedded on ACNS v5.2 uses a format for the configuration file that is incompatible with the v5.2 (enhanced) version of Websense loaded on ACNS v5.3.
- Websense Enterprise v5.2 (enhanced) is incompatible with the downgraded Websense v5.2 (original) installation on Cisco Content Engine ACNS v5.3. You must uninstall the v5.2 (enhanced) components, and replace them with the v5.2 (original) components. The v5.2 (original) components must then be configured to communicate with other Websense components.

Backup Configuration Files

All server configuration and policy settings are stored in `config.xml` and all `*.ini` files in the `WebsenseEnterprise/EIM/bin` directory on Cisco Content Engine ACNS v5.3. Before making changes to the Websense Enterprise configuration or downgrading your Cisco Content Engine operating system, back up `config.xml` to a safe location. This file is critical if you need to restore those settings in the future. Be sure to date backups of the configuration file.

IMPORTANT

If `config.xml` becomes extremely large, it could impact performance in some environments. If this occurs in your environment, contact Websense Technical Support.

Before Downgrading Cisco Content Engine ACNS v5.3

Before you downgrade Cisco Content Engine ACNS v5.3, copy the v5.2 configuration files (`config.xml, eimserver.ini`, and `webserver.ini`) found in the `WebsenseEnterprise/EIM/OldConfig/5.2.` folder on Cisco Content Engine to a different network drive.

The copies of `config.xml`, `eimserver.ini`, and `webserver.ini` files in the `WebsenseEnterprise/EIM/OldConfig/5.2` folder were saved during the ACNS v5.3 upgrade. When you downgrade Cisco Content Engine, the `WebsenseEnterprise/EIM/OldConfig/5.2` folder is removed, and copies of `config.xml`, `eimserver.ini`, and `webserver.ini` files are deleted.

IMPORTANT

If you upgrade Cisco Content Engine ACNS v5.2 to ACNS v5.3 again, you can copy these files into the upgraded Websense Enterprise v5.2 system to restore your pre-downgrade configuration settings.

Restore a Websense Enterprise v5.2 (Original) System

To restore a Websense v5.2 (original) installation after an ACNS v5.3 downgrade to ACNS v5.2:

1. Contact Websense Technical Support for the appropriate installers.
2. Stop all Websense components on Cisco Content Engine ACNS v5.3. For details, read *Stop, Start, or Restart Websense Services*, page 46.
3. Replace the v5.2 (enhanced) configuration files (`config.xml`, `eimserver.ini`, and `webserver.ini`) in the `Websense Enterprise/EIM/bin` folder on Cisco Content Engine with the copy you saved to the safe location described in *Before Downgrading Cisco Content Engine ACNS v5.3*, page 132. By replacing these files, your pre-upgrade configuration settings, from your v5.2 (original) Websense installation are restored.
4. Start all Websense components on Cisco Content Engine ACNS v5.3.

5. Uninstall remote Websense Enterprise v5.2 (enhanced) components by running the Websense Enterprise v5.2 (enhanced) installer on each remote machine where Websense components have been installed, select **Remove** components when prompted, and follow the on-screen instructions. For details, read *Uninstall Websense Remote Components*, page 133.
6. Unzip the contents of any installation files you received from Websense Technical Support. For details, read *Access and Unzip Websense Installers*, page 74
7. Run `setup.exe` to install the Websense Enterprise v5.2 (original) components. You may install them on a Windows machine as a group or individually.

NOTE

If you upgrade Cisco Content Engine ACNS v5.2 to v5.3 again, you must also upgrade all Websense Enterprise components on remote machines in your network to v5.2 (enhanced). Refer to the appropriate installation procedures documented in this guide in *Chapter 7: Install Websense Enterprise on Remote Machines*.

Uninstall Websense Remote Components

If you need to uninstall Websense Enterprise components that are installed on remote machines, follow the next procedure.

NOTE

- Policy Server **must** be running to uninstall other Websense Enterprise components.
- Do **not** use the Windows **Add/Remove Program** function to remove Websense Enterprise components. You may encounter unremoved files or registry keys.

To remove installed Websense Enterprise components in a Windows environment:

1. Log on to the installation machine with **local** administrator privileges.
2. Close all open applications.

3. Access the installer you first used to load Websense Enterprise on the Windows machine. If you need, you can download it from www.mywebsense.com.
4. Run the installer. For details, read *Start a Websense Installation*, page 76.
5. When prompted, select **Remove Websense Enterprise Components,** and then click **Next**.
6. When the **Select Components** dialog box opens, clear the check boxes for any components you do **not** want to remove, and then click **Next.**
7. Finish running the installer. For details, read *Complete a Websense Installation*, page 105.

APPENDIX A | Troubleshooting

You may encounter a situation while installing Websense Enterprise components and configuring Cisco Content Engine ACNS v5.3 that is not addressed in the previous chapters. This appendix troubleshoots installation situations that have been called in to Websense Technical Support. Please check this chapter for information before you contact Technical Support, in case the solution to your situation is described.

If you still need to contact Technical Support, please see *Appendix B Technical Support* for contact information. The situations addressed in this chapter are as follows:

What if I forget my Websense Filtering Service password

Contact Websense Technical Support for assistance. You can find contact information in *Appendix B Technical Support* .

Where can I find download and error messages?

Windows NT

Check the Windows Application Event log for any listings about the database download as well as other error or status messages. Access the Application

Event log by choosing **Start > Programs > Administrative Tools > Event Viewer**. Select **Log > Application**.

Windows 2000

Check the Windows Application Event log 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, Linux, and Cisco Content Engine ACNS v5.3

Websense creates **Websense.log** and **ufpserver.log** (located in **WebsenseEnterprise/EIM/bin)** when there are errors to record. This log records error messages and messages pertaining to database downloads.

Why won't Websense Enterprise Master Database download?

There are several reasons why you might have difficulty receiving Websense Enterprise 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). 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

Cisco Content Engine ACNS v5.3 must have access to the Internet via HTTP, and must be able to receive incoming transmissions.

To verify Internet access:

1. Determine whether Websense Enterprise is accessing the Internet through a proxy server by checking the **Database Download** screen of the **Settings** dialog box in Websense Enterprise Manager.
2. Open a Web browser (either Internet Explorer or Netscape).
3. Set up the browser to access the Internet with the same proxy settings as Filtering Service.
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 Enterprise logo appears, along with a message indicating that it will redirect you to the Websense home page. This means that the Filtering Service's proxy settings are correct, and the Filtering Service should have appropriate HTTP access for downloading.
   - If you are not able to reach the download site and the system requires proxy information, the Filtering Service proxy settings must be corrected. If no proxy information is required, use the **nslookup** command (at the command prompt) with the address of your download site to make sure the Filtering Service machine is able to resolve the download location to an IP address. For example:

     nslookup asia.download.websense.com

     If this does not return an IP address, you must set up the machine running Websense Enterprise to access a DNS server.

   If you need assistance, contact Websense Technical Support (see *Appendix B 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.

What do I do if protocol filtering does not work?

Problem: The Websense Enterprise Master Database has been downloaded, but the browser has no Protocol filtering.

Solution: The browser is pointing to the ACNS machine where there is no Protocol filtering. Network Agent also is not automatically set with default settings. You must set these yourself.

To set up Network Agent with default settings:

1. Make sure Network Agent service is running by entering this command:
   a. For Windows 2000 enter:

      Manager > Settings > Network Agent settings.

   b. For Linux or Solaris enter:

      ./WebsenseAdmin status
2. Make sure the Network Interface Card (NIC) has the ACNS proxy server selected.

   This allows Network Agent to see the Internet traffic through the NIC on the ACNS machine.

What do I do if URL filtering does not work?

Problem: The Websense Enterprise Master Database has been downloaded and the browser is pointing to the ACNS machine, but there is no URL filtering.

Solution: Sometimes Policy Server takes a while to load the database. However, there are some things you can check:

1. On the ACNS machine, enter the following to make sure the Websense services are running:

   show websense-server

   -or-

   If filtering services are running, enter: **show config**
2. Make sure Websense Filtering Service is enabled. Enter:

   <config> url -filter http websense enable <port>

   Note: An optional default port to use is 15868.
3. On the ACNS machine, enter the following to make sure the URL requests are redirected correctly to the Websense filtering:

   <config> url -filter http websense server local

   -or-

   If filtering on another machine, enter:

   <config> url -filter http websense server <Filtering server IP>

Why do I see a “couldn’t delete container” message?

When you install, and then uninstall eDirectory Agent or RADIUS Agent, you may receive a message within the text generated from your Telnet session that states “could not delete container.” This message and the situation that causes it does not have any impact on Websense Enterprise functionality.

Configuration data remains in the `modules.txt` file for ACNS installations. Although you used Websense Enterprise `setup.exe` to uninstall eDirectory Agent or RADIUS Agent, the `modules.txt` file continues to reference that agent. To resolve this issue, contact Technical Support.

Why aren't user-based filters applied even though I installed RADIUS Agent or eDirectory Agent?

If you install and enable RADIUS Agent or eDirectory Agent for Websense Enterprise v5.2 , you may observe one or both of the next behaviors:

- the User Identification entry in Websense Enterprise Manager v5.2 does not show the IP address of the machine where you installed RADIUS Agent or eDirectory Agent
- filters are not applied to employee internet access

The problem may be that host machine IP addresses are not registered in DNS. To use Websense Enterprise Manager to resolve the problem quickly:

1. Log on to Websense Enterprise Manager.
2. Select **Server > Settings** to open the **Settings** page.
3. In the navigation pane, select **User Identification**.
4. When the **User Identification** pane opens, look at the field at the top of the pane. Any machine identified by the machine name may fail to filter properly. You need to add a new entry for every machine in the field that uses a machine name for identification.
5. To add a new entry for a machine or appliance that uses a machine name for identification,
   a. Click **Add** to open the **Add Transparent Agent Identification** dialog box.
   b. In the **Server** field, enter the IP address of a machine where RADIUS Agent or eDirectory Agent is installed and enabled.
   c. In the **Port** field, enter the port number for the agent installed at the machine identified in the **Server** field.
      - For RADIUS Agent, enter **30800**

- For eDirectory Agent, enter **30700**

> **NOTE**
> Make sure you enter the correct value for the agent installed at the machine. Websense filtering may fail if port identification is not correct.

d. Click **OK** to close the **Add Transparent Agent Identification** dialog box.

6. Repeat step 5 for every machine that is identified by a machine name.
7. When all changes are complete, delete the entries that use a machine name as identification.
   a. Select an entry that uses a machine name for identification.
   b. Click **Remove**.
   c. When the message dialog box appears, click **OK** to delete the entry.

8. Repeat step 7 for every machine that is identified by a machine name.
9. To close the **Settings** dialog box when you are done, click **OK**.

For more details about Websense Enterprise v5.2 RADIUS Agent and eDirectory Agent, read:

- Transparent Identification of Users in Websense Enterprise v5.2
- *Chapter 5: User Identification* in the *Websense Enterprise v5.2 Administrator's Guide*

To register IP addresses for DNS servers, read vendor documentation.

APPENDIX B | 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. If you need assistance on the Cisco Content Engine ACNS v5.3, be sure to contact your Cisco technical support team.

Websense Technical Services Support Center

Technical information about Websense Enterprise is available 24 hours a day on the Internet at:

http://ww2.websense.com/global/en/SupportAndKB/ProductDocumentation/

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

Fee-based Support

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

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

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

Support Options

Websense Technical Support can be requested 24 hours a day.

Web Portal

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

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

Email Questions

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

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

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

Telephone Assistance

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

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

For severe problems, additional information may be needed.

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

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

Improving Documentation

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

Index

R

S

T

U