



Installation Guide

Websense[®] Web Security
Websense Web Filter

©1996–2009, Websense, Inc.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
All rights reserved.

Published 2008

Printed in the United States of America and Ireland

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

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense, Inc.

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

Trademarks

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

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

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Pentium, Xeon, and Core2 are registered trademarks of Intel Corporation.

This product includes software developed by the Apache Software Foundation (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

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).

Copyright (c) 2005 - 2009 CACE Technologies, Davis (California).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

Chapter 1	Introduction	5
	Other related documentation	6
	Websense components	6
	How Websense filtering works	8
	Steps for a successful Websense software deployment	9
	Technical Support	10
Chapter 2	Installation Procedures	13
	Websense installers	13
	Installation flow	14
	Before installing	15
	Preparing to install	17
	Typical installation	18
	Windows	19
	Linux	19
	Installation procedure: typical installation	20
	Installing individual components	25
	Installation procedure: any component	25
	Modifying an installation	36
	Removing components	36
	Stopping and starting Websense services	40
	Manually stopping and starting services (Windows)	40
	Manually stopping and starting services (Linux)	40
	Stopping principal components	41
Chapter 3	Initial Setup	43
	Starting Websense Manager	44
	Configuring firewalls or routers	46
	Working with Windows Server 2008	46
	Turning on the Computer Browser service	47
	Identifying Filtering Service by IP address	48
	Creating and running the script for Logon Agent	48
	Prerequisites for running the logon script	49
	Websense user map and persistent mode	50
	Deployment tasks	50
	Configuring Network Agent to use multiple NICs	54

Appendix A	Configuring Stealth Mode	55
	Configuring for Stealth Mode	55
	Windows	56
	Linux	56
Appendix B	Planning for Reporting in Windows	57
	Installing reporting in Windows networks	58
	Installation concerns	58
	SQL Server/MSDE installation error messages	60
	Database version error messages	60
	Collation and case-sensitivity error messages	60
	Database creation error messages	61
	Installing with MSDE 2000	63
	Installing with SQL Server 2000 or 2005	63
	Configuring Microsoft SQL Server 2005 user roles	64
	Configuring services for trusted connection	65
Appendix C	Troubleshooting	67
	Websense Manager cannot be accessed	67
Index		73

1

Introduction

Installation and setup information in this guide applies to both Websense Web Security and Websense Web Filter.

Instructions are included for downloading and extracting installation files, and starting and running the installer.

This guide also includes instructions for:

- ◆ *Installing individual components*, page 25
- ◆ *Configuring Stealth Mode*, page 55
- ◆ *Planning for Reporting in Windows*, page 57
- ◆ *Troubleshooting*, page 67
- ◆ *Contacting Technical Support*, page 69

Websense software can be integrated with your firewall, proxy server, caching application, or network appliance, or can run without an integration (Stand-Alone Edition). *Installation Guide Supplements* provide integration-specific information for installing and initial setup:

- ◆ Cisco products
- ◆ Citrix
- ◆ Check Point
- ◆ Network Appliance NetCache
- ◆ Microsoft ISA Server
- ◆ Squid Web Proxy Cache

A *Universal Integrations* supplement is also available for supported integrations that do not have a specific supplement.

For instructions on upgrading from a previous version, see the *Upgrade Supplement*.

The supplements and other installation documents are available from the Websense Knowledge Base at: www.websense.com/docs/.



Note

In this guide, *Websense software* refers to both Websense Web Security and Websense Web Filter, unless specifically stated otherwise.

Other related documentation

- ◆ See the *Deployment Guide* before installing the Web filtering components for network layout.
- ◆ Use the *Installation Organizer* to record IP addresses, port numbers, keys, passwords, and other information needed during installation.
- ◆ If you have integrated Websense software with a firewall, proxy server, or related product or device, see the *Installation Guide Supplement* for that product for important configuration steps.

These documents are available from the Websense Documentation Web site:
www.websense.com/docs/

After installing Websense software, refer to the Websense Manager Help for setup and configuration information.

Websense components

Websense software is made up of several components that work together to provide user identification, Internet filtering, and reporting capabilities. Not all components are required to deploy the software.

Required components

- ◆ **Policy Broker:** Manages requests from Websense components for policy and general configuration information.
- ◆ **Policy Database:** Stores Websense software settings and policy information. This database is installed with Policy Broker, and cannot be installed separately.
- ◆ **Policy Server:** Identifies and tracks the location and status of other Websense components. Stores configuration information specific to a single Policy Server instance. Communicates configuration data to Filtering Service, for use in filtering Internet requests.
- ◆ **Filtering Service:** Interacts with your integration product and Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.
- ◆ **Websense Manager:** Configuration and management interface to Websense software. Websense Manager also serves as a reporting interface in a Windows environment.
- ◆ **User Service:** Communicates with your network's directory services to allow you to apply filtering policies based on users, groups, domains, and organizational units.
- ◆ **Network Agent** (required for Stand-Alone deployment only): Manages the filtering of all protocols, including HTTP, HTTPS, and FTP.

In integrated deployments, Network Agent may optionally be used to filter the Internet protocols not managed by the integration product. Network Agent can

also be used to detect HTTP network activity and instruct Filtering Service to log this information.

Network Agent detects network activity to support the bandwidth filtering and protocol management features, and to log the number of bytes transferred.

- ◆ **Usage Monitor:** Tracks users' Internet activity and sends alerts to Websense administrators when configured threshold values are exceeded.
- ◆ **Websense Master Database:** A downloadable list of millions of categorized Internet sites. Protocol definitions are also included in this database.

Optional user identification components

- ◆ **DC Agent:** With Microsoft Windows® directory services to transparently identify users so that Websense software can filter them according to particular policies assigned to users or groups.
- ◆ **Logon Agent:** Works with the Websense logon application (**LogonApp.exe**) to transparently identify users as they log on to Windows domains.
- ◆ **RADIUS Agent:** Works through a RADIUS Server to transparently identify users and groups who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.
- ◆ **eDirectory Agent:** Works with Novell® eDirectory™ to transparently identify users so that Websense software can filter them according to particular policies assigned to users or groups.

Optional filtering components

- ◆ **Network Agent** (optional in integrated deployments): Manages the Internet protocols that are not managed by your integration product. Can be used to detect HTTP network activity and instruct Filtering Service to log this information.

In a Stand-Alone deployment (no third party integration), Network Agent is used to manage filtering of all protocols, including HTTP, HTTPS, and FTP.

Network Agent detects network activity to support the bandwidth filtering and protocol management features, and to log the number of bytes transferred.

- ◆ **Remote Filtering Server:** Provides Web filtering for clients located outside your organization's network firewall or Internet gateway. The Remote Filtering Server should be installed inside the outermost firewall, but in the DMZ outside the firewall protecting the rest of the corporate network.
- ◆ **Remote Filtering Client:** Is installed on client machines, such as laptop computers, that are used outside of the organization's network firewall or Internet gateway. This component connects with a Remote Filtering Server to filter the remote computers.

Optional reporting components

A wide variety of reports and charts can be generated, depicting your network's Internet usage trends.

In a Windows environment, the following components are installed to make these reports available within Websense Manager, and require that Microsoft SQL Server or Microsoft SQL Server Desktop Edition (MSDE) is installed before installation.

- ◆ **Log Server:** Sends records of Internet activity to the Log Database. It also sends category names, protocol names, and risk class names from the Master Database to the Log Database.
- ◆ **Log Database:** Receives and stores Internet activity data.

In a Linux environment, you can install **Websense Explorer for Linux**, a Web-based reporting application that provides a customizable view into the Log Database. These reports are not viewed within Websense Manager. The MySQL database engine must be installed and running before you install Websense Explorer for Linux.

Integration components

- ◆ **Filtering plug-in:** Enables communication between supported firewalls, proxy servers, caching applications, or network appliances and Filtering Service. See the *Installation Guide Supplement* for your integration for more information.
- ◆ **Linking Service:** Enables communication between Websense filtering software and Websense Data Security Suite. Linking Service gives Data Security Suite access to user name information from User Service and URL categorization information from Filtering Service.

How Websense filtering works

Websense software has a flexible, policy-based filtering approach to Internet request filtering. You create and apply filtering policies, which then determine which types of Web sites and Internet applications clients can access.

Websense software can be integrated with your firewall, proxy server, caching application, or network appliance, or can run as a stand-alone product (*Stand-Alone Edition*).

- ◆ In an **integrated environment**, the integration product receives the client's Internet request, and then queries Websense Filtering Service to determine whether the request should be blocked or permitted.
- ◆ In a **stand-alone environment**, Websense Network Agent detects the client's Internet request, and then queries Filtering Service to determine whether the request should be blocked or permitted.

Filtering policies are applied to **clients**. In all environments, clients can be computers (identified by IP address) or networks (identified by IP address range). If you configure Websense software to communicate with a supported directory service, clients can also be users, groups and domains/organizational units (referred to collectively as **directory clients**).

When a client requests a Web site, Websense Filtering Service identifies which policy currently applies, and which categories have the Block, Confirm, or Quota action

applied by that policy. (More information about the Permit, Block, Confirm, and Quota actions is available in the Websense Manager Help.)

Next, Filtering Service checks the Websense Master Database to find out how the requested site is categorized. If the category is blocked (or has the Confirm or Quota action applied), Filtering Service sends a block page to the client.

Websense Network Agent makes it possible to filter protocols other than HTTP, such as those used by instant messaging, streaming media, and file sharing applications. Network Agent also enables Bandwidth Optimizer functionality, which makes it possible to filter HTTP and non-HTTP access based on bandwidth usage.

Steps for a successful Websense software deployment

Follow these steps to simplify and streamline the installation process.

1. **Plan the deployment.** Websense components can be deployed in many combinations. The optimal deployment for your organization depends on your network layout and the expected volume of Internet requests. Consult the *Deployment Guide* for guidelines and considerations.
2. **Complete the *Installation Organizer*.** This worksheet, available from the [Websense Knowledge Base](#), ensures that you have gathered the IP addresses, port numbers, keys, passwords, and other information needed during installation.
3. **Install Websense filtering components.** Follow your deployment plan to distribute Websense software components appropriately. See [Chapter 2: Installation Procedures](#).



Note

If you are integrating Websense software with a product that requires a Websense plug-in, be sure to install the plug-in on **each** machine running the integration product. Filtering Service must be installed in the network **before** the plug-in. For more information, see the *Installation Guide Supplement* for your integration product.

4. If Websense Manager is installed on a Windows machine, also install Log Server on a Windows machine to enable reporting tools.
If Websense Manager is installed on a Linux machine, install Websense Explorer for Linux to enable reporting.
5. **Perform initial setup tasks.** Post-installation setup tasks are described in [Chapter 3: Initial Setup](#).

For detailed information about post-installation setup and configuration tasks, refer to the Websense Manager Help.

If this is your first time using Websense software, the New User Quick Start tutorial, accessed via Websense Manager, provides a streamlined overview of the key tasks and concepts, with examples.

Technical Support

Technical information about Websense software and services is available 24 hours a day at www.websense.com/support/, including:

- ◆ the latest release information
- ◆ the searchable Websense Knowledge Base
- ◆ Support Forums
- ◆ Support Webinars
- ◆ show-me tutorials
- ◆ product documents
- ◆ answers to frequently asked questions
- ◆ Top Customer Issues
- ◆ in-depth technical papers

For additional questions, click the **Contact Support** tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online **Support Request Portal** at ask.websense.com.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at MyWebsense.

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401

Location	Contact information
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- ◆ Websense subscription key
- ◆ Access to the Websense management console.
- ◆ Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)

Familiarity with your network's architecture, or access to a specialist

2

Installation Procedures

Use the procedures that follow to install or remove Websense software components together or individually.

In general, even in smaller networks, it is recommended that you install filtering and reporting components on separate machines.

- ◆ *Typical installation* describes how to install all filtering components (and, optionally, reporting components) at the same time.
- ◆ *Installing individual components* describes how to install one or more components on a machine, without installing all filtering components together.
- ◆ *Removing components* describes how to remove one or all Websense software components on a machine.

If you are integrating Websense filtering software with another product, combine the steps provided here with the instructions in the applicable *Installation Guide Supplement*.

The documents referenced in this chapter are available from the Documentation section of the Websense Knowledge Base (www.websense.com/docs/).

Websense installers

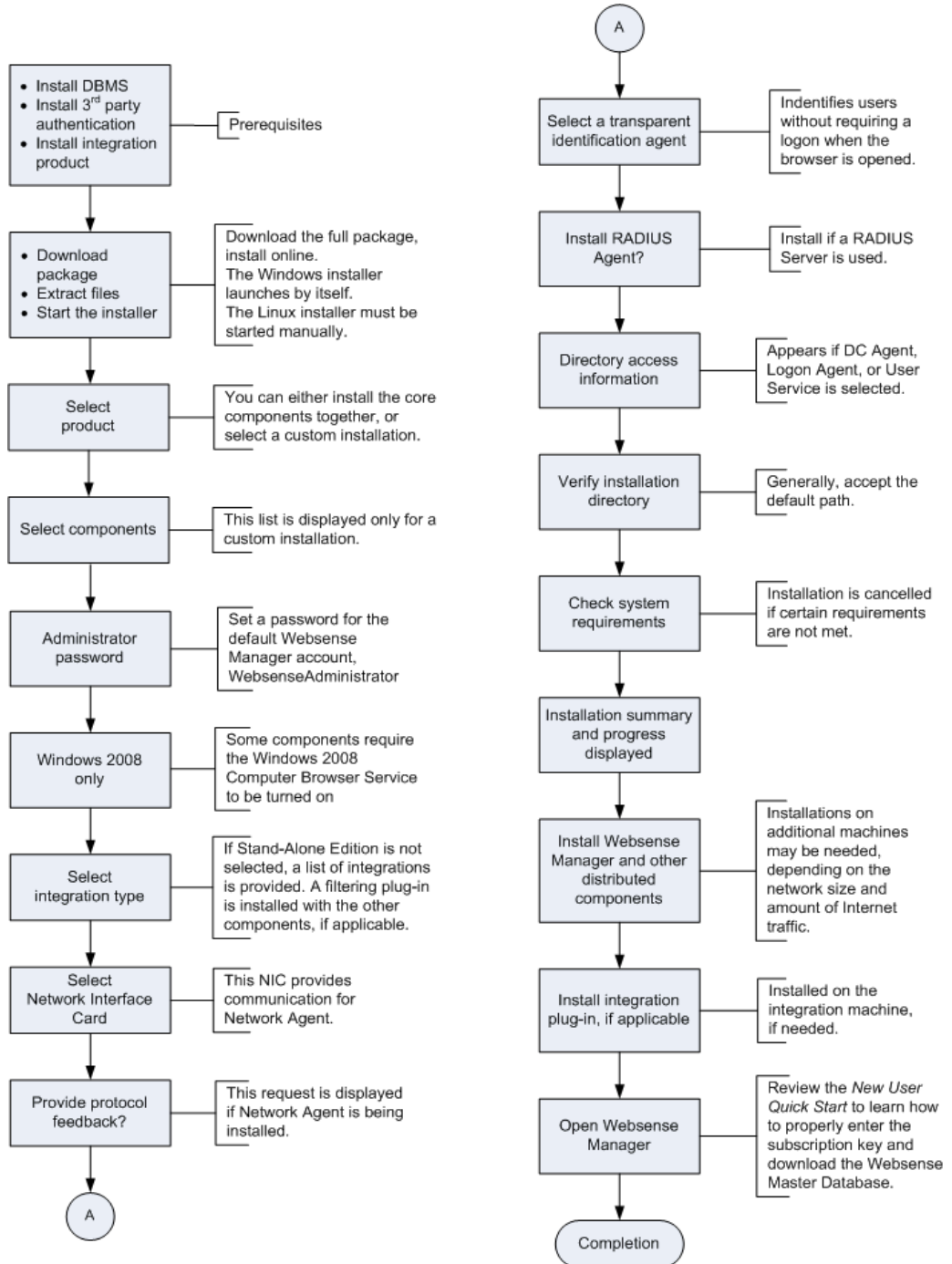
Separate installers are available for Windows and Linux versions of Websense Web Security and Websense Web Filter.

An additional installer is required for the Websense Content Gateway component (a key part of a Websense Web Security Gateway installation). See the *Websense Content Gateway Installation Guide* for instructions.

Installation flow

The following diagram provides an overview of the installation process as a whole.

When you integrate Websense software with some third-party products, additional steps may be required. See the *Installation Guide Supplement* for your integration for more information.



Before installing

Effective planning simplifies your installation, eliminates the need to stop and restart the process because you do not know the information requested by the installer, and reduces post-installation problems.

- ◆ **Deployment Guide:** Use the *Deployment Guide* before starting your installation to make sure that the installation machines meet or exceed system requirements, and that Websense components are distributed appropriately.

You can install the core filtering components on the same machine, or distribute them across multiple machines, even with different operating systems. Multiple instances of some components can be distributed across multiple machines.

If you plan to distribute your Websense components, run the installer on each machine, and select the **Custom** installation option. For instructions, see *Installing individual components*, page 25.

- ◆ **Installation Organizer:** Certain IP addresses, port numbers, keys, passwords, and similar information are requested during the installation. Use the *Installation Organizer* to find and record this information before starting your installation. This document is located in the Documentation > Planning, Installation and Upgrade folder in the Websense Knowledge Base (www.websense.com/docs/).
- ◆ **Computer clock synchronization:** If you are distributing Websense components in your network, synchronize the clocks on all machines where a Websense component is installed.
- ◆ **Remote filtering:** To filter clients outside the network firewall, you must install Remote Filtering components using the **Custom** installation option. For instructions, see the *Remote Filtering* technical paper, located in the Documentation > Planning, Installation and Upgrade folder in the Websense Knowledge Base (www.websense.com/docs/).
- ◆ **Network Agent:** If you are installing Network Agent, ensure that the Network Agent machine can monitor all client Internet requests, and the responses to those requests.

If you install Network Agent on a machine that cannot monitor client requests, basic HTTP filtering (Stand-Alone Edition only) and features such as protocol management and Bandwidth Optimizer cannot work properly. For more information about positioning the Network Agent machine in your network, see the Network Agent chapter in the *Deployment Guide*.



Important

Do not install Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software.

The only exception is a blade server or appliance with separate processors or virtual processors to support Network Agent and the firewall software.

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

On Linux, do **not** choose a NIC without an IP address (stealth mode) for Network Agent communications.



Note

If you install Network Agent on a machine with multiple NICs, after installation you can configure Network Agent to use more than one NIC. See the *Network Configuration* topic in the Websense Manager Help for more information.

After installation, you can run the Network Traffic Detector to test whether the selected NIC can see the appropriate Internet traffic. See the *Network Configuration* topic in the Websense Manager Help for instructions.

- ◆ **Internet access:** To download the Websense Master Database and enable filtering, each machine running Websense Filtering Service must be able to access the download servers at:
 - download.websense.com
 - ddsdom.websense.com
 - ddsint.websense.com
 - portal.websense.com
 - my.websense.com

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

- ◆ **Do not use remote control utilities:** Installation of Websense software with a remote control utility such as Terminal Services is not supported.
- ◆ **Linux firewall:** If Websense software is being installed on a Linux machine on which a firewall is active, shut down the firewall before running the installation.
 1. Open a command prompt.
 2. Enter **service iptables status** to determine if the firewall is running.
 3. If the firewall is running, enter **service iptables stop**.

Websense, Inc., does not recommend installing Network Agent on a machine running a firewall. See the discussion of Network Agent on [page 15](#) for more information.

Preparing to install

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

- **Linux:** log on as **root**.
- **Windows:** log on with **domain** and **local** administrator privileges.

Using administrative privileges at installation ensures that User Service (and, optionally, DC Agent and Logon Agent) is able to apply user-based filtering. If necessary, you can apply administrator privileges after installation (see *Troubleshooting > User Identification* in the Websense Manager Help).

If you are installing Log Server (Windows only), and will use a Windows trusted connection to communicate with the database engine, your logon account must also be a trusted account with local administrator privileges on the database machine.

2. Close all applications and stop any anti-virus software.
3. On Linux, create a setup directory for the installer files. For example:

```
/root/Websense_setup
```

4. Download the installer package for your product from mywebsense.com.
5. Extract the installer files.

- **Windows:** Double-click the downloaded file, and click **Run** when prompted. The installer usually starts automatically.

The installer places the following files in the temporary directory for the current user (by default, C:\Documents and Settings*<user name>*\Local Settings\Temp*<generated name>*.tmp):

File	Description
Setup.exe	Installation program
launch.ini	Configuration information for the installer
Setup	Directory containing additional installation files

- **Linux:** In the setup directory, enter the following commands to unzip and expand the file:

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

For example:

```
gunzip Websense70Setup_Lnx.tar.gz
tar xvf Websense70Setup_Lnx.tar
```

This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup	Archive file containing installation files and documents

6. After extraction, the installation program starts automatically in Windows. It must be started manually in Linux.

If the installation program is not running:

- **Windows:** Go to **Start > Run** and enter **%temp%** to open the directory containing the installer executable. Double-click **Setup.exe** to start the installation. If another program, such as Internet Explorer, is running, the installation screens may be hidden behind that program's window.
- **Linux:** Use the following command to run the installation program from the setup directory:

```
./install.sh
```

A GUI version of the installer is available on English versions of Linux:

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

**Note**

If the installation program displays error messages that it is having difficulty locating other machines, turn off any firewall running on the installation machine.

Typical installation

When you select a typical installation, all core Websense filtering components are installed together. You are also given the option to install one or more transparent identification agents, used to apply user-based filtering without prompting users for logon information. See the *Deployment Guide* for more information about Websense software components, and about combining the transparent identification agents.

Which components are included in a typical installation depends on the operating system of the installation machine, as explained below. For a list of supported operating system versions, see [Operating systems, page 12](#), or the *Deployment Guide*.

If Websense software is integrated with another product, additional components may be installed. The *Installation Guide Supplement* for your integration product (available from the Documentation > Planning, Installation and Upgrade folder of the [Websense Knowledge Base](#)) provides more information.

You also can install Websense software as a stand-alone product. Complete instructions are provided in this *Installation Guide*.

If you want to select which components are installed, see [Installing individual components, page 25](#).

Windows

The following core components are installed as part of a typical Windows installation:

- Policy Broker
- Policy Database
- Policy Server
- Websense Manager (includes required third-party components Apache HTTP Server and Apache Tomcat)
- Transparent identification agents (optional)
 - DC Agent
 - Logon Agent
 - eDirectory Agent
 - RADIUS Agent
- Log Server (installed when you select the Websense Web Security/Web Filter with Reporting option)
- Filtering Service
- User Service
- Network Agent
- Usage Monitor

Linux

The following core components are installed as part of a typical Linux installation.

- Policy Broker
- Policy Database
- Policy Server
- Websense Manager (includes the required third-party component Apache Tomcat)
- Transparent identification agents (optional)
 - Logon Agent
 - eDirectory Agent
 - RADIUS Agent
- Filtering Service
- User Service
- Network Agent
- Usage Monitor

On Linux machines, Log Server and other reporting components are installed separately with Websense Explorer for Linux. See the *Websense Explorer for Linux Administrators Guide* for more information.

Installation procedure: typical installation



Important

The installation supplement for your integration product contains additional information required to install and configure Websense software to run with your firewall, proxy server, caching application, or network appliance. Where indicated, refer to the supplement while performing the following procedures.

1. Make sure that you have followed the steps in [Preparing to install, page 17](#):
 - Log on to the installation machine with appropriate permissions.
 - Close all applications and stop any anti-virus software.
 - Download and start the installer, if needed.
2. Click **Next** on the Welcome screen.
3. Select **Yes** to accept the Subscription Agreement, and then click **Next**.
4. Select an installation type, and then click **Next**.
 - **Websense Web Security/Web Filter**: Installs Filtering Service, Policy Broker, Policy Server, Websense Manager, User Service, Usage Monitor, and Network Agent together on the same machine. The installer gives you the option of installing the following transparent identification agents: DC Agent (Windows only), eDirectory Agent, Logon Agent, and RADIUS Agent.
 - **Websense Web Security with Reporting**: Available for a Windows installation only. Installs the same components as above, plus Log Server to provide reporting.



Important

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

This option is suggested when installing Websense filtering software for evaluation purposes in small network. In larger networks, Websense Manager and the reporting components should be installed on a separate machine.

- **Custom**: Allows you to choose individual Websense components to install. For more information, see [Installing individual components, page 25](#).
5. If you are installing on Windows Server 2008:
 - a. Indicate whether you are using Active Directory to authenticate users in your network.
 - b. If you are using Active Directory, select an option for turning on the Windows Computer Browser service.

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

If you choose not to have the installer turn it on, or if the installer is unable to turn it on, you must turn it on manually after installation. You must also turn on the Computer Browser service on the Active Directory machine, if you use Active Directory 2008 to authenticate users. See [Turning on the Computer Browser service, page 47](#).

6. If you are not running a typical installation, or installing the Policy Broker component in a custom installation, you are prompted to enter a **Password** for the administrative account, WebsenseAdministrator.

A strong password, containing a combination of upper and lower case letters, plus numbers, is recommended.

7. Select an Integration Option, and click **Next**.
 - Select **Stand-alone** to use Network Agent to detect Internet requests.
 - Select **Integrated** if you want Websense software to work with a firewall, proxy server, cache, or network appliance.

If you select Integrate, refer to the *Installation Supplement* for your integration for additional steps and information.

8. If you are installing Websense software with reporting, you are prompted to provide the location of the database engine and an access method, and then asked to specify a location for creating the Websense Log Database.

If you are not installing reporting at this time, or plan to install Websense Explorer for Linux, skip this step.

- a. **Database Engine:** A database engine must be present to continue with the installation of reporting components. Do one of the following:
 - Specify that you want to connect to an existing database engine, and then continue to **step b**.
 - Use the link to find out more about installing the free MSDE database, and then exit setup. Run the installer again once a supported database engine has been configured.
- b. **Database Engine Location:** Enter the name or IP address of the machine on which a supported database engine is running (see [Supported database engines, page 13](#)). If a database engine is not available, you must install one before reporting components can be installed.
- c. Select an access method:
 - **SQL database account:** Enter the user name and password for a SQL Server account that has administrative access to the database. This is the recommended method.



Note

The SQL Server password cannot be blank, or begin or end with a hyphen (-).

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

- d. Accept the default location for the Log Database, or select a different location. Then, click **Next**.
9. The installer assigns default port numbers to Policy Server (55806) and Filtering Service (15868).

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

**Note**

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

10. Select the network interface card (NIC) that Network Agent will use to communicate with other Websense software components. All enabled NICs with an IP address are listed.
On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address.

After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests. See [Appendix A, Configuring Stealth Mode](#).

11. Select a **Network Agent Feedback Option**, and click **Next**.

Selecting **Yes** allows Websense, Inc., to gather information about the use of Websense-defined protocols. This information is used to enhance protocol filtering.

**Note**

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

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

**Note**

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

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

- **eDirectory Agent:** Use eDirectory Agent to identify users transparently with Novell eDirectory Service.

- **DC Agent** (*Windows only*): Use DC Agent to identify users transparently with a Windows-based directory service.
 - **Logon Agent**: Use Logon Agent to identify users transparently when they log on to the domain.
Logon Agent receives its user information from a logon application (LogonApp.exe) that must be run by a logon script in your network. For instructions, see *Creating and running the script for Logon Agent*, page 48.
 - **DC Agent and Logon Agent** (*Windows only*): Use both DC Agent and Logon Agent to identify users transparently. This combination increases the accuracy of user identification in some networks.
 - **None**: Do not install a Websense transparent identification agent. Select this option if your integration product provides user identification, if you do not plan to apply user and group policies, or if you want users to be prompted for logon information before accessing the Internet.
13. If you have remote users that are authenticated by a RADIUS server, select **Yes** to install the optional RADIUS Agent to transparently identify these users, and then click **Next**.
14. If you selected DC Agent for transparent identification, enter a **Domain/User Name** and **Password** with administrator privileges on the domain, and then click **Next**.

**Note**

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

15. If you are installing reporting components on Windows, the Minimizing Database Management screen allows you to set options that affect the size of the Log Database used to generate reports.
- **Logging Web Page Visits**: Log a record of each Web page requested. This selection creates a smaller database and faster reporting.
Deselect this option to log a record of each separate file that is part of a Web page request, including graphic images and advertisements. This selection results in more precise reports, but creates a much larger database and causes reports to generate more slowly.
 - **Consolidating Log Records**: Combine multiple visits by the same user to the same Internet domain (see the Websense Manager Help for details). This selection creates a smaller database, but decreases reporting precision.
Deselect this option to record each visit or hit separately. This selection provides greater reporting precision, and a larger database.
16. Accept the default installation path, or click **Browse** to locate another path, and then click **Next**. The installation path must be absolute (not relative). The default installation path is:

- **Windows:** C:\Program Files\WebSense\
- **Linux:** /opt/WebSense/

The installer creates this directory if it does not exist.



Important

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

The installer compares the installation's system requirements with the machine's resources.

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

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

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

17. Click **Next** to start the installation. An installation progress screen is displayed.

18. Click **Next** on the Installation Complete screen.

On Windows machines, when the installer finishes running, a Web page provides instructions for launching Websense Manager.

For more information, or if you are installing on a Linux machine, see [Starting Websense Manager, page 44](#).

19. If you stopped your anti-virus software, restart it.

20. If you stopped a firewall running on a Linux machine, open a command shell and enter:

```
service iptables start
```

To determine whether the firewall is running, enter:

```
service iptables status
```

21. If your network uses Active Directory 2008 to authenticate users, you must turn on the Windows Computer Browser service on the Active Directory machine. See [Working with Windows Server 2008, page 46](#), for instructions.

22. See [Chapter 3: Initial Setup](#) for important setup information.

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

**Note**

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

Installing individual components

The Custom installation option allows you to distribute Websense components across multiple machines, in the combinations best suited to your environment.

Remote Filtering components can be installed only through a custom installation. See the *Remote Filtering* technical paper (available from the Documentation > Planning, Installation and Upgrade folder in the [Websense Knowledge Base](#)) for more information.

**Important**

When you are installing Websense components separately on the same network, Policy Broker must be installed first, and then Policy Server and Filtering Service. Install only one instance of Policy Broker.

Multiple instances of some components may be needed, depending on your network configuration and the volume of Internet traffic. Components can be installed on both Windows and Linux machines, unless otherwise noted. Check the *Deployment Guide* before beginning an installation to determine the best way to distribute components for your network.

If you chose the **Websense Web Security/Web Filter** option during installation, Policy Broker, Policy Server, User Service, Filtering Service, and Network Agent were installed on the same machine. A transparent identification agent may also have been installed. You can still use the Custom option to install additional instances of some components.

Installation procedure: any component

Use these steps to install any Websense software component. The sections that follow provide additional, component-specific details.

1. Make sure that you have followed the steps in [Preparing to install](#), page 17:
 - Log on to the installation machine with appropriate permissions.
 - Close all applications and stop any anti-virus software.
 - Download and start the installer, if needed.

2. Click **Next** on the Welcome screen.
3. Do one of the following:
 - If no other Websense components are installed on the machine, select **Yes** to accept the Subscription Agreement, and then click **Next**. On the next screen, select **Custom**, and then click **Next** again.
 - If Websense components are already installed on the machine, select **Add Websense Components**, and then click **Next**.

A list of components not installed on the machine is displayed.

4. Select the components to install, and then click **Next**.
5. The screens that follow vary, depending on which components you are installing. Be prepared to provide the following information, if prompted:
 - If you are installing Policy Broker, provide a password for the default **WebsenseAdministrator** account, used to log on to Websense Manager.
 - If you are installing Policy Server only, provide the Policy Broker location.
 - If Policy Server is installed on a different machine, provide the Policy Server IP address and configuration port (55806, by default), if prompted.

If other Websense components are already installed on the machine, the installer locates their initialization files and, if possible, retrieves Policy Server and Filtering Service information from those files.


- If you are installing Network Agent, you are prompted to select the IP address for the NIC for communicating with other components and sending block messages. See [Network Agent, page 29](#), for more information.
- If you are installing Network Agent, Remote Filtering Server, or a plug-in, provide the Filtering Service location.
- If you are installing User Service, DC Agent, or Logon Agent, you are prompted for directory access information. If you are installing any of these components on Windows Server 2008:
 - a. Indicate whether you are using Active Directory to authenticate users in your network.
 - b. If you are using Active Directory, select an option for turning on the Windows Computer Browser service.

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

If you choose not to have the installer turn it on, or if the installer is unable to turn it on, you must turn it on manually after installation. You must also turn on the Computer Browser service on the Active Directory machine, if you use Active Directory 2008 to authenticate users. See [Turning on the Computer Browser service, page 47](#).

6. Check the sections below for component-specific installation instructions, and then return to this procedure.
 - *Websense Manager*, page 28
 - *Policy Broker*, page 28
 - *Policy Server*, page 28
 - *User Service*, page 29
 - *Filtering Service*, page 29
 - *Network Agent*, page 29
 - *DC Agent*, page 31
 - *Usage Monitor*, page 32
 - *RADIUS Agent*, page 32
 - *eDirectory Agent*, page 32
 - *Logon Agent*, page 32
 - *Log Server*, page 33
 - *Remote Filtering Server*, page 34
 - *Remote Filtering Client Pack*, page 35
 - Linking Service
7. Accept the default installation path or click **Browse** to locate another path, and then click **Next**. The installation path must be absolute (not relative). The default installation path is:
 - **Windows:** C:\Program Files\WebSense
 - **Linux:** /opt/WebSense/

The installer creates this directory if it does not exist.

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

The installer compares its system requirements with the machine's resources.

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

A summary shows the installation path and size, and the components to be installed.
8. Click **Next** to start the installation.

If Network Agent was not installed, a message reminds you that features such as protocol management and Bandwidth Optimizer cannot be used unless Network Agent is installed on a machine with direct access to Internet traffic. Click **Next** to continue.
9. Click **Next** on the Installation Complete screen.

When the installer finishes running, a Web page provides instructions for launching Websense Manager.
10. If you stopped your anti-virus software, restart it.
11. See *Chapter 3: Initial Setup* for important setup information.

Websense Manager

Websense Manager is the administrative interface for Websense Web Security and Websense Web Filter. When installed on a Windows machine, Websense Manager can also be used to access reporting tools (optional).

In Windows environments, Websense, Inc., recommends installing Websense Manager and Log Server on a different machine than filtering components. This helps to minimize the impact of report processing on Internet filtering. See the *Deployment Guide* for a list of supported operating systems and deployment recommendations.

- ◆ If Websense Manager is installed on a different machine than Policy Server, it needs network access to the Policy Server machine. Websense Manager and Policy Server do not need to run on the same operating system.
- ◆ For instructions to launch Websense Manager, see [Starting Websense Manager](#), page 44.
- ◆ In a Windows environment that includes reporting:
 - If Websense Manager and Log Server are installed on a different machines, open Websense Manager and verify the Log Server location on the **Settings > Logging** page.
 - If Websense Manager and Log Server are installed on the same machine, make sure that the machine IP address, rather than **localhost**, appears on the **Settings > Logging** page.

See Websense Manager Help for more information.

For more information about installing reporting functions, see [Appendix B, Planning for Reporting in Windows](#).

Policy Broker

Policy Broker manages policy and configuration information required by other Websense components. The Policy Database is installed with Policy Broker to store this information. Only one instance of Policy Broker can be installed.

When you are installing components separately, install Policy Broker first.

Policy Server

Install Policy Server after installing Policy Broker. When you install Policy Server on a separate machine, the installer asks for the location of Policy Broker.

In a very large network, or a network with a large volume of Internet traffic, you may need multiple Policy Server instances. All instances connect to the same Policy Broker.

If multiple Policy Servers are installed, each must be installed before the other components with which it communicates.

When you install Websense components on a separate machine from Policy Server, the installer asks for the Policy Server location and port number. The default port is

55806. The same port must be entered for each component that connects to this Policy Server.

User Service

Each Policy Server requires one User Service instance. User Service is generally installed on the same machine as Policy Server. If you are installing User Service on a separate machine, the installer asks you to identify the Policy Server machine.

- ◆ When installing User Service, log on with local administrator (Windows) or root (Linux) privileges.
This ensures that User Service has the permissions it needs to enable user-based filtering. Administrator privileges can also be configured after installation. See the *Troubleshooting > User Identification* topic in the Websense Manager Help for instructions.
- ◆ After installation, follow the instructions in the *User Identification* section of the Websense Manager Help to configure how Websense software identifies directory clients (users, groups, etc.).
- ◆ If User Service is installed on a Linux machine **and** Network Agent is used for protocol filtering, be sure to install the Samba client (v2.2.8a or later) on the User Service machine so that protocol block messages can be displayed on Windows computers.

Filtering Service

Depending on the size of the network or volume of Internet traffic, multiple Filtering Service instances may be needed. Websense, Inc., recommends a maximum of ten Filtering Services per Policy Server.

- ◆ Filtering Service is installed after Policy Broker and Policy Server.
- ◆ Filtering Service must be installed before the remaining components. The installer asks for the Filtering Service location when you install other components on a separate machine.

Network Agent

Install Network Agent on a machine that can see the Internet requests **from** the internal network as well as the Internet response **to** those requests. By connecting to a span or mirror port on a router or switch, Network Agent can monitor all Internet requests.

In busy networks, filtering performance improves if Network Agent is installed on a separate machine from Policy Broker, Policy Server, and Filtering Service. See the *Deployment Guide* for more information.

To share the load, multiple Network Agents can be installed on separate machines, with each one monitoring a separate IP address range. The ranges combine to cover the entire network, but must not overlap. Overlapping ranges result in double logging of Internet activity. If the entire network is not covered by instances of Network Agent, some machines are not filtered and their Internet traffic not logged.

IP ranges for Network Agent are configured in Websense Manager, after installation. See the Network Configuration topic in Websense Manager Help for instructions.



Important

If you install Network Agent on a machine that cannot monitor the targeted traffic, Websense features such as protocol management and Bandwidth Optimizer cannot perform as expected.

- ◆ Network Agent can be installed at the same time as Policy Server and Filtering Service.
- ◆ If Network Agent is installed on a separate machine, Filtering Service and Policy Server must be running before you install Network Agent. The installation cannot proceed if Policy Server and Filtering Service cannot be located.

When you install Network Agent:

1. The installer asks you to confirm that you want to install Network Agent on this machine, and that the machine is not running a firewall.
 - If the machine is *not* being used as a firewall, select **Yes** to install Network Agent, and click **Next**. Installation continues.
 - If the machine is running a firewall, select **No**, and click **Next**. The installer exits. Install Network Agent on a machine that is not running a firewall.



Important

Do **not** install the Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software.

The only exception is a blade server or appliance with separate processors or virtual processors to separately support Network Agent and the firewall software.

2. The installer prompts you to select the NIC that Network Agent can use for communicating. All enabled NICs with an IP address are listed. On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address. After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests. See [Appendix A, Configuring Stealth Mode](#). Select a NIC and click **Next** to continue.
3. If Filtering Service is installed on a different machine, enter the IP address and filter port, and click **Next**.

**Note**

The **Filter port** shown, 15868, is the default port used by Filtering Service. If you installed Filtering Service with a different port number, enter that number in this dialog box.

- The installer asks if you want to allow Websense, Inc., to gather information about the use of Websense-defined protocols. This information is used to enhance protocol filtering.

**Note**

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

Select a Network Agent feedback option, and click **Next**.

- Go to [Step 7 of *Installation procedure: any component*, page 25](#).

After installation, configure Network Agent for use in your network. See the *Network Configuration* topic in Websense Manager Help for instructions.

DC Agent

DC Agent is a Websense transparent identification agent used in networks that authenticate users with a Windows directory service.

In a large network, you can install multiple DC Agents to provide ample space for files that are continually populated with user information. See the *Deployment Guide* for more information.

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

DC Agent can be installed only on a Windows machine:

- ◆ To retrieve user information from the domain controller, DC Agent must be installed with domain administrator privileges on the network.

Enter the **Domain\user name**, followed by the **Password** for an account with domain administrator privileges, and click **Next**.

**Note**

This account ensures that DC Agent has administrator privileges on the domain, and Websense software can filter by users and groups. Administrator privileges also can be set after installation. See the *Troubleshooting > User Identification* topic on changing User Service, DC Agent, and Logon Agent service permissions in Websense Manager Help for instructions.

After installation, follow the instructions in the *User Identification* topic in the Websense Manager Help to configure Websense software to use DC Agent to identify users without prompting them for logon information.

Usage Monitor

Usage Monitor tracks users' Internet activity and sends alerts when Internet activity for particular URL categories or protocols reaches configured threshold limits. Each Policy Server should have a separate Usage Monitor.

After installation, use Websense Manager to configure Usage Monitor to send usage alerts. See the *Alerting* topic in the Websense Manager Help for more information.

RADIUS Agent

RADIUS Agent enables Websense software to provide user and group filtering by transparently identifying users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection. The agent can be used in conjunction with either Windows- or LDAP-based directory services.

After installation, follow the instructions in the *User Identification* topic in the Websense Manager Help to configure Websense software to use RADIUS Agent to identify users without prompting them for logon information.

eDirectory Agent

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

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

After installation, follow the instructions in the *User Identification* topic in the Websense Manager Help to configure Websense software to use eDirectory Agent to identify users without prompting them for logon information.

Logon Agent

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network. Logon Agent receives logon information from the logon application (**LogonApp.exe**), a separate client application that runs only on Windows machines, and must be run by a logon script.

Logon Agent can be run with DC Agent if some of the users in your network are not being authenticated properly. For example, Windows 98 computers do not permit DC Agent to poll users for identification when they make an Internet request.

- ◆ Do not install Logon Agent on the same machine as eDirectory Agent, because this can cause conflicts.

- ◆ Use the instructions in *Creating and running the script for Logon Agent*, page 48, to set up the logon script.

After installation, follow the instructions in the *User Identification* topic in the Websense Manager Help to configure Websense software to use Logon Agent to identify users without prompting them for logon information.

Log Server

Log Server receives records of Internet filtering activity and sends them to the Log Database, which is installed on a database engine.

If you are installing reporting on Linux, see the *Websense Explorer for Linux Administrators Guide* for installation prerequisites and requirements.

If you are installing reporting on a Windows machine, the supported database engines are:

- ◆ Microsoft SQL Server 2005 - recommended
- ◆ Microsoft SQL Server 2000
- ◆ Microsoft SQL Server Desktop Edition (MSDE) - suitable for smaller networks
MSDE is not supported on Windows 2008 machines.

Log Server must be installed before you can see charts on the Status > Today and Status > History pages, or run presentation or investigative reports.

- ◆ If you use a Windows trusted connection to communicate with the database engine, the logon account used to run the installer must also be a trusted account with local administration privileges on the database machine.
- ◆ The database engine must be installed and running before you install Log Server. See *Appendix B, Planning for Reporting in Windows* for more details on configuring the database engine, including prerequisites.
If you do not have a database engine, you can download and install MSDE for free. MSDE is not supported on Windows 2008 machines. Refer to the Websense Knowledge Base on the Websense Support Portal, www.websense.com/kb for a download link and further instructions. Search for the exact phrase: *Installing MSDE with Websense software, version 7*.
- ◆ You are prompted to provide the location of the database engine, and an access method, and click **Next**.
 - **Database Engine Location**—Enter the name or IP address of the machine on which a supported database engine is running.

Then, select an access method:

- **SQL database account**—Requires the user name and password for a Microsoft SQL Server account that has administrative access to the database. This is recommended.

**Note**

The SQL Server password cannot begin or end with a hyphen (-), and cannot be blank.

- **Windows trusted connection**—Uses a Windows account to log into the database. This account must be a trusted account with local administration privileges on the database machine. Websense, Inc., recommends **against** using a trusted connection if you run MSDE.
- ◆ The Minimizing Database Management screen allows you to set options that affect the size of the Log Database used to generate reports.
 - **Logging Web Page Visits**—Select this option to log a record of each Web page requested. This selection creates a smaller database and faster reporting. Deselect this option to log a record of each separate file that is part of a Web page request, including graphic images and advertisements. This selection results in more precise reports, but creates a much larger database and causes reports to generate more slowly.
 - **Consolidating Log Records**—Select this option to combine multiple visits by the same user to the same Internet domain (see the Websense Manager Help for details of how records are combined). This selection creates a smaller database, but decreases reporting precision. Deselect this option to record each visit or hit separately. This selection provides greater reporting precision, and a larger database.

After installing Log Server on a separate machine, stop and restart the **ApacheTomcatWebsense** and **Apache2Websense** services on the Websense Manager machine.

**Important**

When Log Server is not installed on the Websense Manager machine, you **must** stop and restart the Apache services on the Websense Manager machine before creating scheduled jobs in presentation reports. If you skip this step, scheduled jobs are not saved properly, and will be lost.

Remote Filtering Server

Remote Filtering Server provides Web filtering for machines such as laptops that are located outside the network firewall. A remote computer must be running the Remote Filtering Client to be filtered by the Remote Filtering Server.

Remote Filtering Server is installed on a separate, dedicated machine with the same installer used for other Websense components. Ideally, it should be installed behind

the outermost network firewall, but in the DMZ outside the firewall that protects the rest of the network.

During the installation, Remote Filter Server connects to ports 40000, 15868, 15871, 55880, and 55806 on machine or machines running Policy Server, Policy Broker, and Filtering Service. Also, Policy Server uses port 55825 to communicate with the Remote Filtering machine.

If a firewall is installed between Remote Filtering Server and these other components, open these ports on the firewall. After the installation is complete, ports 15868, 15871, 55880 must remain open.

As part of installation, the installer program requests a pass phrase to use to authenticate connections to Remote Filtering Server. This pass phrase cannot contain spaces.

The Remote Filtering Client is deployed using the Remote Filtering Client Pack.

See the *Remote Filtering* technical paper (available in the in the Documentation > Planning, Installation and Upgrade folder of the [Websense Knowledge Base](#)) for information on installing, configuring, and using remote filtering.

Remote Filtering Client Pack

The Remote Filtering Client Pack is a Windows MSI file (**CPMClient.msi**) used to install the Remote Filtering Client on machines to be filtered when they are outside the network.

The Remote Filtering Client Pack can be installed only on Microsoft Windows machines. When you install Remote Filtering Server on Windows, the Remote Filtering Client Pack is also installed automatically.

Before installing the Remote Filtering Client on Microsoft Windows Vista machines, make sure that User Account Control (UAC) is turned off, and that you are logged on to the machine as a local administrator.

See the Remote Filtering technical paper (available in the in the Documentation > Planning, Installation and Upgrade folder of the [Websense Knowledge Base](#)) for information about deploying the Remote Filtering Client.

Linking Service

Websense Linking Service makes it possible for Websense data security software to access user information and URL categorization details from Websense Web security software.

When installing Linking Service separately, be sure that Filtering Service, User Service, and a transparent identification agent (DC Agent, Logon Agent, or RADIUS Agent) are already installed and running.

Modifying an installation

To change the location of a Websense component or modify the Websense installation, run the installer again and select the appropriate option. The installer detects the presence of Websense components and offers the following choices:

- ◆ Integrate with a firewall, proxy server, or network appliance.

**Note**

For information about converting a Stand-Alone installation to an integrated system, see the *Installation Supplement* for your integration product.

- ◆ Add Websense components.
See *Installing individual components*, page 25, for instructions on running a custom installation to add components.

Removing components

The procedure for removing Websense software components varies according to the operating system on which they are installed.

Refer to the *Installation Supplement* for your integration product for any integration-specific requirements.

**Important**

The Policy Broker and Policy Server services must be running when you uninstall any Websense components. Before removing Policy Broker and Policy Server, remove their distributed components.

To remove Policy Broker or Policy Server, also remove all other Websense components.

Removing Policy Server deletes Websense configuration information, so run a backup before proceeding. See the Websense Manager Help for information about the Websense Backup Utility.

Windows



Notes

- ◆ Before removing components, use the Websense Backup Utility to make a backup of Websense configuration and initialization files. See the Websense Manager Help for instructions.
- ◆ If you are removing components from a Windows Server 2008 machine, log in as the built-in administrator, or run the uninstall program with elevated (full administrator) privileges.
- ◆ After uninstalling components, you may be prompted to restart the machine.

1. Log on with **local** administrator privileges.
2. Close all applications and stop any anti-virus software.
3. Open the Windows Add or Remove Programs dialog box (**Start > Settings > Control Panel > Add or Remove Programs**).
4. Select **Websense** from the list of installed applications.
5. Click **Change/Remove** to launch the Websense Setup program.

There may be a delay of several seconds while Websense Setup starts.

A list of installed components appears.

By default, all components are checked for removal.



Warning

When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.

Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining Websense components and requires the reinstallation of those components.

6. Deselect any components in the list that you do *not* want to remove, and click **Next**.



Note

If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, Setup cannot stop Network Agent and an error message is displayed.

If Policy Server is not running, a message tells you that removing Websense components may require communication with Policy Server.

- a. Exit Setup.
- b. Restart Policy Server from the Services dialog box.
- c. Restart this process at [Step 3](#).



Warning

If Policy Server is not running, the files for the selected components are removed, but configuration information is not updated for these components. Problems could occur later if you attempt to reinstall these components.

7. A list shows the components selected for removal are listed. Click **Next**.
If you are uninstalling Network Agent after Policy Server has already been removed, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.
8. A completion message indicates that components have been removed. Click **Next**.
9. Select a restart option and click **Next** to exit Setup.
The machine must be restarted to complete the removal process.
10. If you stopped your anti-virus software, restart it.
11. If you remove an integration plug-in, you may need to restart the integration. Check the Installation Supplement for your integration.

Linux



Note

Before removing components, use the Websense Backup Utility to back up Websense configuration and initialization files. See Websense Manager Help for instructions.

1. Log on as **root**.
2. Close all applications and stop any anti-virus software.
3. Run the uninstall program from the Websense installation directory (**/opt/Websense** by default):

```
./uninstall.sh
```

A GUI version is available on English versions of Linux. To run it, enter:

```
./uninstall.sh -g
```

The installer detects the installed Websense components and lists them. All components are selected for removal, by default.

**Warning**

When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.

Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining Websense components and requires the reinstallation of those components.

4. Deselect any components you do **not** want to remove, and choose **Next**.

**Note**

If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, Setup cannot stop Network Agent and an error message is displayed.

If Policy Server is not running, a message tells you that removing Websense components may require communication with Policy Server

- a. Exit the uninstaller.
- b. Open a command shell and go to the **Websense** directory (/opt/Websense, by default).
- c. Enter the following command:

```
./WebsenseAdmin start
```
- d. Restart this process at [Step 3](#).

**Warning**

If Policy Server is not running, the files for the selected components are removed, but configuration information is not updated. Problems could occur later if you attempt to reinstall these components.

5. A list shows the components selected for removal. Choose **Next**.
If you are uninstalling Network Agent on a remote machine after removing Policy Server, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.
6. A completion message indicates that components have been removed. Exit the installer.
7. If you stopped your anti-virus software, restart it.
8. If you remove an integration plug-in, you may need to restart the integration. Check the *Installation Supplement* for your integration.

Stopping and starting Websense services

By default, Websense services are configured to start when the computer starts.

Occasionally, you may need to stop or start a Websense service. For example, Filtering Service must be stopped and started after customizing default block messages.



Note

When Filtering Service is started, CPU usage can be 90% or more for several minutes while the Websense Master Database is loaded into local memory.

Manually stopping and starting services (Windows)

Use the Windows Services dialog box to stop and start one or more Websense services:

1. If Websense software is running with a NetCache integration, disable the ICAP Service Farm.
2. Open the Windows Services dialog box (Start > Programs > Administrative Tools > Services).
3. Right-click a service name, and then select **Start**, **Stop**, or **Restart**. Restart stops the service, then restarts it again immediately from a single command.

Refer to [Stopping principal components, page 41](#), for the correct order to use when stopping or starting multiple Websense services.



Warning

Do **not** use the **taskkill** command to stop Websense services. This may corrupt the services.

4. If Websense software is running with a NetCache integration, enable the ICAP Service Farm.

Manually stopping and starting services (Linux)

Stop, start, or restart Websense services from the command line on a Linux machine. Restarting stops the services, then restarts them immediately from a single command. If the components are spread across multiple machines, be sure that Policy Broker and the Policy Database are stopped last and started first. See [Stopping principal components, page 41](#), for the preferred stopping and starting order.

1. If Websense is running with a NetCache integration, disable the ICAP Service Farm.
2. Go to the Websense installation directory (`/opt/Websense/`, by default).

3. Use the following commands to stop, start, or restart all Websense services in the correct order:
 - `./WebsenseAdmin stop`
 - `./WebsenseAdmin start`
 - `./WebsenseAdmin restart`
4. View the running status of all Websense services with the following command:
`./WebsenseAdmin status`

**Warning**

Do **not** use the **kill -9** command to stop Websense services. This may corrupt the services.

5. If Websense is running with a NetCache integration, enable the ICAP Service Farm.

Stopping principal components

When stopping individual components on Windows machines, or when stopping components spread across multiple machines, stop the optional components first, and then the principal components, ending with the following, in the order shown:

1. Websense Network Agent
2. Websense Filtering Service
3. Websense User Service
4. Websense Policy Server
5. Websense Policy Broker
6. Websense Policy Database

When starting services, reverse this order. It is especially important that you begin with the following services, in the order shown:

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

Also remember that if you are stopping and starting services on the Websense Manager machine, you may need to stop or start the Apache services used to host Websense Manager and its reporting tools:

- ◆ Apache2Websense (Windows only)
- ◆ ApacheTomcatWebsense

3

Initial Setup

After your installation is complete, review the following setup requirements and complete the steps that apply to your environment.

All sites

- ◆ Configure your firewall or Internet router to allow Websense software to download the Websense Master Database (see [Configuring firewalls or routers](#), page 46). This is required to enable filtering.
- ◆ Launch Websense Manager (see [Starting Websense Manager](#), page 44), and then follow the instructions in the *New User Quick Start* tutorial to enter your subscription key and start downloading the Websense Master Database.
- ◆ Depending on your integration product, you may need to configure Internet browsers on user computers. See the *Installation Guide Supplement* for your integration for instructions.
- ◆ If you subscribe to Websense Web Security, activate your subscription to the Websense Web Protection Services™: SiteWatcher™, BrandWatcher™, and ThreatWatcher™. See the *Getting Started* topic in the Websense Manager Help for more information.
- ◆ If you install certain components on Windows Server 2008, or if your network uses Active Directory 2008 to authenticate users, you may need to perform some additional configuration steps (see [Working with Windows Server 2008](#), page 46).

Block pages

- ◆ If Filtering Service is installed on a machine with multiple NICs, configure Websense software to identify the Filtering Service machine by its IP address rather than host name so that block pages can be sent to users. See [Identifying Filtering Service by IP address](#), page 48, for instructions.

Network Agent

- ◆ If you installed Network Agent, use the Network Traffic Detector to test whether Network Agent can see the Internet activity that you want it to monitor. See the Network Configuration topic in Websense Manager Help for instructions.
- ◆ If you installed Network Agent on a machine with multiple NICs, you can configure the agent to use more than one NIC to monitor and block requests. See the Network Configuration topic in Websense Manager Help for more

information. To configure a stealth mode NIC for monitoring, see [Appendix A: Configuring Stealth Mode](#).

- ◆ All Windows computers being filtered must have the Messenger Service enabled to receive protocol block messages from Network Agent. See the *Protocol Block Messages* topic in Websense Manager Help for instructions.

Transparent identification of users

- ◆ If you installed Logon Agent, create a logon script for your users that identifies them transparently as they log on to a Windows domain. See [Creating and running the script for Logon Agent](#), page 48, for instructions.
- ◆ If you were unable to grant User Service, DC Agent, or Logon Agent administrator privileges during installation, do so now to ensure that they will function correctly. See the *Troubleshooting > User Identification* topic on changing User Service, DC Agent, and Logon Agent service permissions in Websense Manager Help for instructions.

Remote Filtering

- ◆ If you installed the optional Remote Filtering components, some configuration is required. For instructions, see the *Remote Filtering* technical paper, located in the Planning, Installation and Upgrade folder under Documentation on the Websense Support Portal, www.websense.com/docs.

Starting Websense Manager

Websense Manager is the central configuration and management interface used to customize filtering behavior, monitor Internet usage, generate Internet usage reports, and manage Websense software configuration and settings. This Web-based tool runs on these supported browsers:

- ◆ Microsoft Internet Explorer 7
- ◆ Mozilla Firefox 2 or 3

Although it is possible to launch Websense Manager using some other browsers, use the supported browsers to receive full functionality and proper display of the application.

To launch Websense Manager, do one of the following:

- ◆ If installed on Windows, go to the installation machine and double-click the Websense Manager desktop icon, or go to **Start > Programs > Websense > Websense Manager**.
- ◆ At any machine in the network, open a supported browser and enter the following address:

```
https://<IP address>:9443/mng/
```

Substitute the IP address of the Websense Manager machine.

If you are unable to connect to Websense Manager on the default port, refer to the **knownports.properties** file on the Websense Manager machine (located by default in the **C:\Program Files\Websense\bin** or **/opt/Websense/bin/** directory) to verify the port.

- ◆ On Windows machines, look for the **APACHE_HTTPS=** value.
- ◆ On Linux machines, look for the **TOMCAT_HTTPS=** value.

If you are using the correct port, and are still unable to connect to Websense Manager from a remote machine, make sure that your firewall allows communication on that port.

An SSL connection is used for secure, browser-based communication with Websense Manager. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch Websense Manager from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the [Websense Knowledge Base](#) for instructions.

Once the security certificate has been accepted, the Websense Manager logon page is displayed in the browser window. Log on as **WebsenseAdministrator** with the password that you created during the installation.

When you have logged on to Websense Manager, be sure to enter your subscription key and download the Master Database.

1. In the left navigation pane, click the **Settings** tab.
2. Open the **Account** page, and then enter your subscription key.
3. When you are finished making changes, click **OK**. Changes are not implemented until you click **Save All**.
4. In the left navigation tab, click the **Main** tab.
5. Open the **Today** page, and then click the **Database Download** button at the top.
6. Verify that the Master Database download is in progress. If not, click **Update**.



Important

A partial version of the Master Database is installed with your Websense software on each Filtering Service machine. This partial database is used to enable basic filtering functionality from the time you enter your subscription key. You **must** download the full database for complete filtering to occur. See the Websense Manager Help for additional information.

Configuring firewalls or routers

For Internet connectivity, Websense Manager may require authentication through a proxy server or firewall for HTTP traffic. To allow Websense Master Database downloads, configure the proxy or firewall to accept clear text or basic authentication.

See the proxy server or firewall documentation for configuration instructions. See Websense Manager Help for instructions on running the Websense Master Database download.

If you have integrated Websense software with another product or device, see the *Installation Guide Supplement* for your integration for more information.

Working with Windows Server 2008

If you install certain components on Windows Server 2008, or if your network uses Active Directory 2008 to authenticate users, be aware of the issues listed below. In some cases, additional configuration steps are required.



Note

Websense components can be installed only on Windows Server 2008 (x86), a 32-bit operating system.

- ◆ If you run Websense User Service on Windows Server 2008, and your network uses a Windows NT Directory or Active Directory (Mixed Mode), Websense User Service must run as an account that has administrative privileges on the directory. This means that the User Service machine must be joined to the domain before performing the installation.

See the Troubleshooting section of the Websense Manager Help for instructions on checking and changing the User Service account. Look for the topic on changing DC Agent, Logon Agent, and User Service permissions.

- ◆ If you run Websense User Service, DC Agent, or Logon Agent on Windows Server 2008, the Windows Computer Browser service on that machine must be running. If it was not started during installation, see [Turning on the Computer Browser service, page 47](#).
- ◆ If Websense User Service is installed on Windows Server 2008, protocol block messages and popup usage alerts cannot be displayed at client machines.
- ◆ If your network uses Active Directory 2008 to authenticate users, the Windows Computer Browser service on that machine must be running. See [Turning on the Computer Browser service, page 47](#).
- ◆ If you run Websense User Service on Windows Server 2008, Network Agent cannot send protocol block messages to users. The protocol requests are blocked, but no message is displayed.

In addition, usage alert popup messages cannot be displayed to users. The alerts are generated, and other notification methods function normally.

- ◆ All Websense tools and utilities installed on Windows Server 2008, and text editors used to modify Websense configuration files (such as websense.ini), **must** be run as the local administrator. Otherwise, you may be prevented from running the tool or the changes you make may not be implemented.
 1. Open Windows Explorer to the bin subdirectory in the Websense installation directory (the default installation directory is C:\Program Files\Websense).
 2. Right-click the relevant executable file, and then click **Properties**. Following is a list of files for which this should be done.
 - **wsbackup.exe** for Websense Backup and Restore
 - **logserverconfig.exe** for the Log Server Configuration utility
 - executable for any text editor used to modify a Websense configuration file (such as websense.ini)
 3. In the **Compatibility** tab, under **Privilege Level**, select **Run this program as an administrator**. Then, click **OK**.
- ◆ On Windows Server 2008, the Windows Firewall is turned on by default, and Microsoft recommends that it not be turned off.
 - Check the Websense [Knowledge Base](#) for a list of ports that Websense components use for communication. These ports may need to be opened on the Windows Firewall to enable necessary Websense communication.
 - If you are installing User Service, DC Agent, or Logon Agent, note that the Windows Firewall must be turned off for the Computer Browser service to start.

Turning on the Computer Browser service

Websense Setup offers the option to turn on the Computer Browser service during installation of the following components on Windows Server 2008.

- ◆ Websense User Service
- ◆ Websense DC Agent
- ◆ Websense Logon Agent

If you chose not to have it started, or the installer was not successful, you must turn on the service manually.

In addition, if your network uses Active Directory 2008 to authenticate users, the Windows Computer Browser service must be running on the Active Directory machine. Note that the Windows Firewall must be turned off in order for the Computer Browser service to start.

Perform the following procedure on each machine running an affected component:

1. Make sure that Windows Network File Sharing is enabled.
 - a. Go to **Start > Control Panel > Network and Sharing Center**.
 - b. In the **Sharing and Discovery** section, set **File Sharing** to **On**.
2. Go to **Control Panel > Administrative Tools > Services**.
3. Double-click **Computer Browser** to open the Properties dialog box.

4. Set the **Startup type** to **Automatic**.
5. Click **Start**.
6. Click **OK** to save your changes and close the Services dialog box.
7. Repeat these steps on each machine running Windows Server 2008 and an affected component.

Identifying Filtering Service by IP address

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

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

If Filtering Service is installed on a machine with multiple NICs, and Filtering Service is identified by machine host name rather than IP address, users could receive a blank page rather than a block page.

- ◆ If you have an internal domain name server (DNS), enter the Filtering Service machine's IP address as a resource record in your DNS. See your DNS documentation for instructions.
- ◆ If you do not have an internal DNS:
 1. On the Filtering Service machine, go to the Websense bin directory (by default, **C:\Program Files\Websense\bin** or **opt/Websense/bin**).
 2. Make a backup copy of **eimserver.ini** in another directory.
 3. Open the original **eimserver.ini** file in a text editor.
 4. In the **[WebsenseServer]** section, enter the following command:

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

Here, **<IP address>** is the IP address of the Filtering Service machine.



Important

Do not use the loopback address 127.0.0.1.

5. Save the file.
6. Restart the Filtering Service. See [Stopping and starting Websense services](#), page 40.

Creating and running the script for Logon Agent

If you installed Websense Logon Agent, you must create a logon script for clients that identifies them to Websense software when they log on to a Windows domain. The Websense Logon application, **LogonApp.exe**, provides a user name and IP address to

the Logon Agent each time a Windows client connects to a Windows Active Directory or a Windows NT directory service.

During Logon Agent installation, the logon application and script files are placed in Websense **bin** directory (by default, C:\Program Files\Websense\bin in Windows or /opt/Websense/bin).

- ◆ **LogonApp.exe** (Windows only): The Websense executable that communicates user information to the Logon Agent.
- ◆ **Logon.bat**: The batch file containing sample logon and logout scripts.
- ◆ **LogonApp_ReadMe.txt**: A summary of the procedures for creating and running the Websense logon script and optional logout script.

See [Logon Agent, page 32](#), for installation instructions.

Prerequisites for running the logon script

Logon Agent requires running the logon application on Windows machines.

- ◆ If the logon script runs the logon application in persistent mode, configure your Active Directory server **not** to run scripts synchronously.
- ◆ Be sure that all computers can connect to the shared drive on the domain controller containing **logon.bat** and **LogonApp.exe**. You must copy both of these files from the machine running Logon Agent to both the **logon** and **logout** directories on the domain controller.

To determine if a Windows machine has access to the domain controller, run the following command from a command prompt:

```
net view /domain:<domain name>
```

- ◆ The TCP/IP NetBIOS Helper Service must be running on each Windows 2000, Windows XP, Windows Vista, Windows Server 2003, and Windows NT client machine that is identified by Logon Agent.
- ◆ The logon application on client machines must use NTLM authentication to communicate with Logon Agent. By default, Windows Vista machines use NTLM v2.

To change this setting globally, for all machines in the network, modify the default domain Group Policy Object (GPO) to require use of NTLM authentication:

1. On the domain controller machine, go to Start > Run, and then enter **mmc**.
2. In the Microsoft Management Console, go to **File > Add/Remove Snap-In**, and then click **Add**.
3. Select **Group Policy Management Editor**, and then click **Add**.
4. Select the default GPO (for example, Default domain policy), and then click **Finish**.
5. Click **Close** and then **OK** to close the open dialog boxes.
6. In the navigation pane of the Console window, expand the Computer Configuration > Policy > Windows Settings > Security Settings > Local Policies node, and then select **Security Options**.

7. In the content pane, select **Network Security: LAN Manager authentication level**, and change the setting to **Send NTLM response only**.
8. Save and close the Console file.

To change this setting on individual Windows Vista machines, change the default setting for **Network security: LAN Manager authentication level** as follows:

1. Open the Windows **Local Security Settings** window. See the Windows online Help for assistance.
2. Go to **Security Settings > Local Policy > Security Options**, and double-click **Network security: LAN Manager authentication level**.
3. In the Properties dialog box that appears, select **Send NTLM response only**.

Websense user map and persistent mode

When Logon Agent identifies a user, the user name and IP address are stored in a user map. The length of time this information is stored without reverification depends on whether the logon application is running in *persistent* mode or *non-persistent* mode. If LogonApp.exe is running in persistent mode, the update time interval is configured in Websense Manager.

In non-persistent mode, user map information is created at logon and is not updated. The use of non-persistent mode creates less traffic between Websense software and the clients in your network.

In Active Directory, you can use a logout script to clear the logon information from the Websense user map before the interval defined in Websense Manager. See [Task 1: Prepare the scripts](#), page 51, for more information.

For detailed information about configuring Logon Agent in Websense Manager, see the User Identification topic in Websense Manager Help.

Deployment tasks

- ◆ [Task 1: Prepare the scripts](#)
Edit the parameters in the sample script file (Logon.bat) to suit your network.
- ◆ [Task 2: Configure the scripts to run](#)
You can run your logon script from a Windows Active Directory or Windows NT directory service using group policies.
The Websense executable and logon batch file must be moved to a shared drive on the domain controller that is visible to all clients. If you use Active Directory, you also can create and deploy an optional logout batch file on the shared drive.
- ◆ [Task 3: Configure Logon Agent in Websense Manager](#)
After the logon scripts and application have been deployed, configure Logon Agent in Websense Manager.

Task 1: Prepare the scripts

A batch file, called **Logon.bat**, is installed with Logon Agent in the Websense **bin** directory (by default, C:\Program Files\Websense\bin or /opt/Websense/bin).

This file contains instructions for using the scripting parameters, and two sample scripts: a logon script that runs the logon application (LogonApp.exe), and a logout script. The logout script removes user information from the Websense user map when the user logs out. Only Active Directory can use both types of scripts.

Script parameters

Construct a logon or logout script using the samples provided and the parameters in the table below.

The required portion of the logon script is:

```
LogonApp.exe http://<server>:<port>
```

This command runs LogonApp.exe in persistent mode (the default).



Note

You can edit the sample, or create a new batch file containing a single command.

Parameter	Description
<server>	IP address or name of the Websense Logon Agent machine. This entry must match the machine address or name entered in Websense Manager in Task 3.
<port>	The port number used by Logon Agent (default 15880).
/NOPERSIST	Causes the logon application to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user's data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours, and can be changed in Websense Manager. If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, residing in memory on the domain server and updating the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes, and can be changed in Websense Manager.
/COPY	Copies the logon application to the %USERPROFILE%\Local Settings\Temp directory on users' machines, where it is run by the logon script from local memory. This optional parameter helps to prevent your logon script from hanging. COPY can be used only in persistent mode.

Parameter	Description
/VERBOSE	Debugging parameter that must be used only at the direction of Technical Support.
/LOGOUT	Used only in an optional logout script, this parameter removes the user's logon information from the Websense user map when the user logs off. If you use Active Directory, this parameter can clear the logon information from the user map before the interval defined for Logon Agent has elapsed. Use this optional parameter in a logout script in a different batch file than the one containing the logon script. See the Examples below.

Examples

The sample logon script sends user information to the Logon Agent at logon only. The information is not updated during the user's session (NOPERSIST). The information is sent to port 15880 on the server identified by IP address 10.2.2.95.

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

With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This option is not available with Windows NTLM.) Create a companion logout script in a different batch file, and place it into a different directory than the logon script.

Copy the logon batch file and rename it **Logout.bat**. Edit the script to read:

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

Task 2: Configure the scripts to run

You can configure your logon script to run with a group policy on Active Directory or on Windows NT Directory. The logout script only runs with Active Directory.



Note

The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense, Inc., cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, see the links provided.

Active Directory

If your network uses Windows 98 client machines, go to the Microsoft Web site for assistance.

1. Make sure your environment meets the conditions described in [Prerequisites for running the logon script, page 49](#).
2. On the Active Directory machine, go to the Windows Control Panel and select **Administrative Tools > Active Directory Users and Computers**.

3. Right-click the domain, and then select **Properties**.
4. On the **Group Policy** tab, click **New** and create a policy called **Websense Logon Script**.
5. Double-click the new policy or click **Edit**.
6. In the tree structure displayed, expand **User Configuration**.
7. Go to **Windows Settings > Scripts (Logon/Logoff)**.
8. In the right pane, double-click **Logon**.
9. Click **Show Files** to open this policy's logon script folder in Windows Explorer.
10. Copy two files into this folder:
 - **Logon.bat**, your edited logon batch file
 - **LogonApp.exe**, the application
11. Close the Explorer window.
12. Click **Add** in the Logon Properties dialog box.
13. Enter **Logon.bat** in the **Script Name** field or browse for the file.
14. Leave the **Script Parameters** field empty.
15. Click **OK** twice to accept the changes.
16. (Optional) If you have prepared a logout script, repeat [Step 6](#) through [Step 15](#). Choose **Logoff** at [Step 8](#), and use your logout batch file when you are prompted to copy or name the batch file.
17. Close the Group Policy Object Editor dialog box.
18. Click **OK** in the domain Properties dialog box to apply the script.
19. Repeat this procedure on each domain controller in your network, as needed.

**Note**

You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users are prompted for a user name and password when opening a browser. Ask your users to notify you if this problem occurs.

To enable manual authentication, see the *User Identification* topic in the Websense Manager Help.

For additional information about deploying logon scripts to users and groups in Active Directory, go to the Microsoft TechNet site (technet2.microsoft.com/), and search for the exact phrase: *Logon Scripts How To*.

Windows NT directory or Active Directory (mixed mode)

1. Make sure your environment meets the conditions described in [Prerequisites for running the logon script](#), page 49.

2. Copy the **Logon.bat** and **LogonApp.exe** files from the Websense installation directory on the Logon Agent machine (by default, C:\Program Files\Websense\bin or /opt/Websense/bin) to the **netlogon** share directory on the domain controller machine.

C:\WINNT\system32\Repl\Import\Scripts

Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.

3. In the Control Panel of the domain controller, select **Administrative Tools > User Manager for Domains**.
4. Select the users for whom the script must be run, and double-click to edit the user properties.
5. Click **Profile**.
6. Enter the path to the logon batch file in the **User Profile Path** field (see [Step 2](#)).
7. Enter **Logon.bat** in the **Logon Script Name** field.
8. Click **OK**.
9. Repeat this procedure on each domain controller in your network, as needed.

**Note**

You can determine if your script is running as intended by configuring your Websense software to use manual authentication when transparent identification fails. If transparent authentication with Logon Agent fails for any reason, users are prompted for a user name and password when opening a browser. Ask your users to notify you if this problem occurs.

To enable manual authentication, see the User Identification topic in Websense Manager Help.

Task 3: Configure Logon Agent in Websense Manager

After the logon/logout scripts and the logon application have been deployed and configured on the domain controllers, you must enable authentication in Websense Manager. See the Logon Agent instructions under the User Identification topic in Websense Manager Help for instructions.

Configuring Network Agent to use multiple NICs

Each Network Agent must use at least one designated NIC, but is capable of using multiple NICs. Network Agent can use one NIC for monitoring traffic, and another NIC to send blocking information.

See the *Deployment Guide* for more information, and the Websense Manager Help for configuration instructions.

A

Configuring Stealth Mode

Websense software can inspect all packets with a monitoring NIC (network interface card) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. Security and network performance are improved with this configuration. Removing the IP address prevents connections to the NIC from outside resources and stops unwanted broadcasts.

Configuring for Stealth Mode

If the Network Agent is configured to use a stealth mode NIC, the installation machine must have multiple NICs. If Network Agent is installed on a separate machine, a second, TCP/IP-capable interface must be configured to communicate with Websense software for filtering and logging.

When installing on Windows, stealth mode interfaces do not display as a choice for Websense communications.



Important

On Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

Make sure you know the configuration of all the interfaces in the machine before attempting an installation.

Stealth mode for the Network Agent interface is supported on Windows and Linux.

Windows

Configure a NIC for stealth mode as follows.

1. Go to **Start > Settings > Network and Dial-up Connection** to display a list of all the interfaces active in the machine.
2. Select the interface you want to configure.
3. Select **File > Properties**.
A dialog box displays the NIC connection properties.
4. Clear the **Internet Protocol (TCP/IP)** checkbox.
5. Click **OK**.

Linux

To configure a NIC for stealth mode in Linux, disable the Address Resolution Protocol (ARP), which breaks the link between the IP address and the MAC address of the interface. Run the following commands, replacing *<interface>* with the NIC's name, for example, **eth0**.

- ◆ To configure a NIC for stealth mode, run this command:

```
ifconfig <interface> -arp up
```
- ◆ To return the NIC to normal mode, run this command:

```
ifconfig <interface> arp up
```



Important

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file, **/etc/sysconfig/network-scripts/ifcfg-*<adapter name>***.

B

Planning for Reporting in Windows

Although you can install reporting components on Windows or Linux machines, a Windows installation integrates all reporting features into Websense Manager, offering the greatest flexibility and usability.



Note

If Websense Manager is installed on a Linux machine, Websense Explorer for Linux must be installed separately to provide reporting. Websense Explorer for Linux requires a MySQL database engine. See the *Websense Explorer for Linux Administrator's Guide* for installation instructions and more information.

Before Websense reporting components can be installed on a Windows machine, one of the following supported database engine must be installed and running:

- ◆ Microsoft SQL Server 2005 SP2 or SP3 - recommended
- ◆ Microsoft SQL Server 2000 SP4
- ◆ Microsoft SQL Server Desktop Edition (MSDE) SP4 - suitable for smaller networks

MSDE is not supported on Windows 2008.

See the Microsoft documentation for Microsoft SQL Server and MSDE installation instructions.

If you do not have a database engine, and do not plan to host the database on a Windows 2008 machine, you can download and install MSDE for free. Refer to the [Websense Knowledge Base](#) for a download link and further instructions. Search for the exact phrase: *Installing MSDE with Websense software, version 7*.

To enable reporting functionality in a Windows environment, install both Websense Manager and Log Server on Windows machines. If you install the components on separate machines, install Websense Manager first.

Installing reporting in Windows networks

Reporting can be installed when other Websense components are installed, or it can be installed separately. See [Chapter 2: Installation Procedures](#), for instructions.

Keep in mind that if you plan to use a Windows trusted connection to communicate with the database engine, the logon account used to run the installer must also be a trusted account with local administration privileges on the database machine.

- ◆ If you are installing Websense software for evaluation purposes, or if you are running in a very small network, use the **Websense Web Security / Web Filter with Reporting** option to install all filtering and reporting components at the same time.

In all but the smallest networks, Websense Manager and Log Server should be installed on a separate machine from filtering components to improve performance. See the *Deployment Guide* for more information.

- ◆ If Websense Manager is already installed, run the installer on the reporting machine and select a **Custom** installation. When prompted, select **Log Server** as the component to install.
- ◆ To install both Websense Manager and Log Server on the same machine, select a **Custom** installation. When prompted, select **Websense Manager** and **Log Server** from the component list.

Follow the onscreen instructions and provide the information requested. See [Installing individual components](#), page 25, for installing components separately.

Installation concerns

Installation options vary, based on which components you install and where you place them.



Note

The Websense Log Database name for version 7 is **wslogdb70**. Every time the database rolls over, a new database partition is created, and a number is appended to the end (for example, wslogdb70_1). This number increments each time.

Be sure you do not have an existing database with this name, otherwise the installation fails. For troubleshooting, see [SQL Server/MSDE installation error messages](#), page 60.

The installer verifies that the database engine is configured appropriately for use with Websense reporting and displays an error if it encounters a problem. See [SQL Server/MSDE installation error messages](#), page 60, for information about possible error messages and instructions for addressing them.

Collation and case-sensitivity

To provide highly accurate reports, Websense reporting tools use case-insensitive collation functions for database searches.

If your Microsoft SQL Server or MSDE instance uses case-sensitive collation (which may be required by other applications using the database engine), reporting components cannot be installed.

To resolve this issue, install another SQL Server instance that uses case-insensitive settings (see *Collation and case-sensitivity error messages*, page 60), and then run the installer again.

Database engine location

When the installer asks for the location of the database engine:

- ◆ If the database is installed on the current machine, and the machine has only one NIC, you can enter **Localhost**.
- ◆ If you installed SQL Server with an instance name other than the default (MSSQLServer), include the instance name when you enter the IP address of the SQL Server machine:

`<IP address>\<instancename>`

For example:

`10.200.1.1\ReporterSql`

Database location and access

When the installer requests a location and access method for the Log Database, keep in mind that:

- ◆ **Path**—Create a path to the database before installing Log Server. Problems can occur during installation if the path does not exist, and Log Server and SQL Server are on different machines.
- ◆ **Disk space**—Make sure there is enough free disk space (at least 3 GB) on the specified drive for the Log Database, including space for future growth. Depending on the number of users and your network setup, your Log Database can grow very rapidly.
- ◆ **Access via SQL database account**—Enter the user name and password for a SQL Server account that has administrative access to the database. This is the recommended method.



Note

The SQL Server password cannot begin or end with a hyphen (-), or be blank.

- ◆ **Access via Windows trusted connection**—Uses a Windows account to log on to the database. This account must be a trusted account with local administration

privileges on the database machine. Websense, Inc., recommends **against** using a trusted connection if you use MSDE as the database engine.

SQL Server/MSDE installation error messages

Before installing Websense reporting component, the installer checks your SQL Server or MSDE configuration. If any problems are found, an error message is displayed. Common problems and solutions are described in the sections that follow.

To avoid the need to stop and restart the installation, configure SQL Server before running the installer.

Database version error messages

To install Websense reporting components (Log Server), the installation machine must be able to access a supported database engine:

- ◆ Microsoft SQL Server 2005 SP2 - recommended
- ◆ Microsoft SQL Server 2000 SP4
- ◆ Microsoft SQL Server Desktop Edition (MSDE) SP4 - suitable for smaller networks

MSDE is not supported on Windows 2008.

If you have an older version of SQL Server or MSDE, upgrade the database engine before running the Websense installer. (SQL Express is not supported.)

- ◆ MSDE is free (but not supported on Windows 2008). The database size limit for MSDE is 2 GB.

If a database engine is not found during installation, refer to the [Websense Knowledge Base](#) for a download link and further instructions. Search for the exact phrase: *Installing MSDE with Websense software, version 7*.

- ◆ SQL Server is available from Microsoft. Check the Microsoft Web site for purchase information, and installation or upgrade documentation.

If you try to install Log Server with an unsupported Microsoft SQL Server or MSDE version, or without access to a supported database engine, an error message appears. The installer terminates and does not install reporting components.

Install a supported database engine, and make sure it is running. Then, run the Websense installer again.

Collation and case-sensitivity error messages

Websense reporting tools use **case-insensitive** collation functions for database searches to provide highly accurate reports. If your Microsoft SQL Server instance uses **case-sensitive** collation, reporting components cannot be installed. This problem generally occurs if other applications are using the same instance of SQL Server.

To resolve this issue, install another SQL Server instance that uses case-insensitive settings. During installation, the Collation Settings dialog box provides options from which to select the correct setting.

You can check (but not change) the case setting of SQL Server via SQL Enterprise Manager:

1. Make sure you have administrator access to SQL Server.
2. Open the SQL Server Enterprise Manager: **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
3. If you are running SQL Server 2000:
 - a. In the navigation pane, expand the Microsoft SQL Servers > SQL Server Group node, and then right-click the server icon for the machine running the SQL instance you want to use.
 - b. Select **Properties** from the drop-down menu.
 - c. On the General tab (selected by default), look for the **Server collation** value, then skip to step 5.
4. If you are running SQL Server 2005:
 - a. In the navigation pane, click the appropriate server IP address.
 - b. Right-click, and select **Properties > General**.
 - c. Select **Collation Settings** in the content pane, and review the setting. For example:
5. The collation string looks like this:


```
SQL_Latin1_General_CP1_CS_AS
```

 - **CS** indicates the collation setting is case-sensitive.
 - **CI** indicates the collation setting is case-insensitive.

```
SQL_Latin1_General_CP1_CI_AS
```
6. Click **OK** to close the Properties dialog box, and then close SQL Server Enterprise Manager.
7. If the collation setting is case-sensitive, install a new instance of SQL Server with the default case-insensitive setting.

Database creation error messages

Reporting component installation requires both the database creation rights associated with the **dbcreator** role and SQL Agent permissions. With SQL Server 2000, the dbcreator role includes SQL Agent permissions. With SQL Server 2005, add the SQL Agent permissions separately ([Configuring Microsoft SQL Server 2005 user roles](#), page 64).

Whether you plan to use a SQL Server account or a Windows trusted connection to access database, the account must have the appropriate rights.

- ◆ [Setting database creation rights](#), page 62
- ◆ [Using osql utility to set database creation rights](#), page 62

In addition, if you are using a trusted connection, the account used to run the installer must be a trusted account with local administration privileges on the database machine.

Setting database creation rights

1. Log on or connect to the Microsoft SQL Server machine with administrative rights.
2. If you are using SQL Server 2000, open the SQL Server **Enterprise Manager** (Start > Programs > Microsoft SQL Server > Enterprise Manager).
 - a. In the navigation pane, expand the following trees, in the order listed.
 - Microsoft SQL Servers
 - SQL Server Group
 - The machine entry for SQL Server
 - Security
 - b. Under Security, double-click **Server Roles**.
The Server Roles pane opens with the full names of the available server roles.
 - c. Right-click **Database Creators**, and then select **Properties**.
3. If you are using SQL Server 2005, open the **SQL Server Management Studio** (Start > Programs > SQL Server 2005 > SQL Server Management Studio).
 - a. In the navigation pane, expand the **Security > Server Roles** node.
 - b. Select **dbcreator**, then right-click and choose **Properties**.
4. Click **Add**. The Add Members dialog box appears, showing all existing SQL Server accounts.
5. Highlight the account to which you are adding database creation rights, and click **OK**. The Add Members dialog box closes.
6. Verify that you have updated the correct logon, and then click **OK**.
7. Close SQL Enterprise Manager.

Using osql utility to set database creation rights

On the MSDE machine:

1. Open the Windows Services dialog box and verify that the MSDE instance is running.
2. Open a Windows command prompt (**Start > Run > cmd**).
3. To connect to the named instance of MSDE using Windows Authentication (a trusted connection), enter the following command:

```
osql -E -S servername\instancename
```

In the above command:

- for *servername*, substitute the actual name of the MSDE Server.
- for *instancename*, substitute the actual name of the MSDE instance.

4. Verify the prompt in the command prompt window is **1>**. This shows you are connected to the MSDE server.

**Note**

If the prompt does not say **1>**:

- ◆ Verify that MSDE is running.
- ◆ Verify that the service and instance names are correct.
- ◆ Run the command in [Step 3](#) again.

1. Enter the following command to grant rights for database creation.

```
1> EXEC sp_addsrvrolemember N'user_logon',N'dbcreator'  
2> GO
```

Replace *user_logon* with the account being assigned database creation rights.

2. Check the results. An entry of **0** in the command prompt window indicates success.
3. Enter **EXIT** to close the **osql** utility.
4. Run the Websense installer again.

Installing with MSDE 2000

**Note**

If you are replacing a previous MSDE installation or changing from an English to a non-English MSDE version, you must uninstall the previous version before installing the new version.

If the proper version of MSDE is not installed, refer to the [Websense Knowledge Base](#) for a download link and further instructions. Search for the exact phrase: *Installing MSDE with Websense software, version 7.*

**Important**

You must restart the MSDE machine before installing Log Server.

Installing with SQL Server 2000 or 2005

Microsoft SQL Server must be purchased separately. If it has not been installed in your network, see Microsoft documentation for system requirements and installation instructions.

1. Install SQL Server 2000 or 2005 according to Microsoft instructions, if needed.
2. Make sure SQL Server is running.
3. Make sure SQL Server Agent is running.
4. Obtain the SQL Server logon ID and password for a SQL Server Administrator, or for an account that has rights to create, modify, and delete databases and tables.
You need this logon ID and password when you install Websense components.
5. Restart the SQL Server machine after installation, and then install Log Server on an appropriate machine (see *Installation procedure: any component*, page 25).



Note

You must restart the machine after installing Microsoft SQL Server 2000 or 2005 and before installing Log Server.

6. Make sure the Log Server machine and the Websense Manager machine can recognize and communicate with SQL Server.
7. Install the SQL Server client tools on the Log Server and Websense Manager machines. Run the SQL Server installation program, and select **Connectivity Only** when asked what components to install.
8. Restart the machine after installing the connectivity option. See Microsoft SQL Server documentation for details.

Configuring Microsoft SQL Server 2005 user roles

Microsoft SQL Server 2005 defines SQL Server Agent roles that govern accessibility of the job framework. The SQL Server Agent jobs for SQL Server 2005 are stored in the SQL Server msdb database.

To install Websense Log Server successfully, the user account that owns the Websense database must have membership in one of the following roles in the msdb database:

- ◆ SQLAgentUserRole
- ◆ SQLAgentReader Role
- ◆ SQLAgentOperator Role



Note

The SQL user account must also be a member of the **DBCreator** fixed server role.

Go to Microsoft SQL Server 2005 to grant the SQL Server user account the necessary permissions to successfully install the Websense reporting components.

1. On the SQL Server machine, go to **Start > Programs > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**.
2. Select the **Object Explorer** tree.
3. Select **Security > Logins**.

4. Select the login account to be used during the installation.
5. Right-click the login account and select **Properties** for this user.
6. Select **User Mapping** and do the following:
 - a. Select **msdb** in database mapping.
 - b. Grant membership to one of these roles:
 - SQLAgentUserRole
 - SQLAgentReader Role
 - SQLAgentOperator Role
 - c. Click **OK** to save.
7. Select **Server Roles**, and then select **dbcreator**. The dbcreator role is created.
8. Click **OK** to save.

Configuring services for trusted connection

When you choose a Windows trusted connection for communication with the database engine during installation of Websense reporting components, the installer automatically configures Log Server with the proper credentials.



Note

Websense, Inc., recommends **against** using a trusted connection with MSDE.

Additionally, you must manually configure the services listed below with the Windows user name and password needed to enable communication with the database engine. This may require access to multiple machines, depending on how the components are distributed.

- ◆ Websense Explorer Report Scheduler (Websense Manager machine)
- ◆ Apache2Websense (Websense Manager machine)
- ◆ ApacheTomcatWebsense (Websense Manager machine)
- ◆ Websense Reporter Scheduler (Log Server machine)

If components are distributed on different machines, go to the machine running the service to be configured, and follow these steps.

1. At the machine running the affected service, go to **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Right-click one of the applicable service names in the list, and then click **Stop**.
3. Double-click the same service name to open the Properties dialog box.
4. Open the **Log On** tab, and select **This account**.

5. In the text box, enter the user name for an account with appropriate access rights to the Log Database. (Some environments require this to be entered as domain\user name. For example: Websense\jdoe.)
6. Enter and confirm the Windows password for this account.
7. Click **OK** to close the Properties dialog box.
8. Right-click **Websense Log Server** in the Services list, and then click **Start**.
9. Repeat these steps once for each of the services listed above.

C

Troubleshooting

This appendix provides troubleshooting information for the following installation and initial configuration issues:

- ◆ *Websense Manager cannot be accessed, page 67*
- ◆ *Where can I find download and error messages?, page 68*
- ◆ *I am having trouble running the installer on a Linux machine, page 68*
- ◆ *I forgot my WebsenseAdministrator password, page 68*
- ◆ *The Master Database does not download, page 69*
- ◆ *Policy Server fails to install, page 69*
- ◆ *Network Agent on Linux fails to start with stealth mode NIC, page 69.*
- ◆ *Windows 98 computers are not being filtered as expected, page 70*
- ◆ *Network Agent cannot communicate with Filtering Service after it has been reinstalled, page 70*
- ◆ *A General Exception error occurs while installing on Linux, page 70*

For issues not related to installation or communication between Websense software components, see the Websense Manager Help.

For other possible solutions, see the Websense Knowledge Base (kb.websense.com).

If you still need to contact Technical Support, see *Technical Support, page 10*.

Websense Manager cannot be accessed

When you attempt to access Websense Manager, a browser error message states that the page cannot be found.

Websense Manager requires access to certain ports for operation. Depending on your environment, you may use the default ports, or configure alternative ports during installation. If there is a firewall between the browser machine and the Websense Manager machine, and that firewall blocks any of the required ports, Websense Manager may not work properly. The firewall must be configured to allow communication on these ports.

Refer to the [Websense Knowledge Base](#) for a list of default port numbers. Search for the exact phrase *default port numbers*.

Where can I find download and error messages?

To find error or status messages related to Master Database downloads and other key Websense software events:

- ◆ On Windows machines, use the Event Viewer (Start > Programs > Administrative Tools > Event Viewer).
- ◆ On Windows or Linux machines, check the **Websense.log** file, located in the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).

The **Websense.log** file is updated whenever there are errors to record, and can be viewed in a standard text editor. This file is located on the Policy Server machine.

I am having trouble running the installer on a Linux machine

If Websense software is being installed on a Linux machine that is running a firewall, shut down the firewall before running the installer.

1. In the command shell, enter the following command to determine if the firewall is running:

```
service iptables status
```

2. If the firewall is running, enter the following command:

```
service iptables stop
```



Important

Do not install Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software.

The only exception is a blade server or appliance with separate processors or virtual processors to support Network Agent and the firewall software.

Remember to restart the firewall when the installation is complete.

1. Enter the command:

```
service iptables start
```

2. To verify that the firewall is running, enter the command:

```
service iptables status
```

I forgot my WebsenseAdministrator password

Log on to MyWebsense.com and use the v7 Password Reset tool to set a new WebsenseAdministrator password.

The Master Database does not download

The disk partition on the Filtering Service machine may be too small to accommodate the Websense Master Database. Increase the size of the partition to 3 GB.

If that does not resolve the issue, there may be problems with the subscription key, Internet access, or restriction applications that prevent database downloads.

See the Websense Manager Help for troubleshooting instructions.

Policy Server fails to install

If you attempt to install Websense software on a machine with insufficient resources (RAM or processor speed), Policy Server may fail to install.

Certain applications (such as print services) can bind up the resources that the installer needs to install Policy Server. If Policy Server fails to install, the installer exits.

If you receive the error message: *Could not install current service: Policy Server:*

- ◆ Install Websense software on a different machine. See the *Deployment Guide* for system recommendations.
- ◆ Stop all memory-intensive services running on the machine and then run the installer again.

Network Agent on Linux fails to start with stealth mode NIC

This problem can be caused by either of the following:

IP address removed from Linux configuration file

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file. Network Agent does not start if you have bound it to a NIC configured for stealth mode, and then removed the IP address of the NIC from the Linux configuration file (`/etc/sysconfig/network-scripts/ifcfg-<adapter name>`).

An interface without an IP address does not appear in the list of adapters displayed in the Websense installer or in Websense Manager, and is unavailable to use. To reconnect Network Agent to the NIC, restore the IP address in the configuration file.

Stealth mode NIC selected for Websense communications in Linux

NICs configured for stealth mode in Linux are displayed in the Websense installer as choices for communications. If you have accidentally selected a stealth mode NIC for communications, Network Agent cannot start, and Websense services cannot work.

1. Go to the Websense **bin** directory on the Network Agent machine (`/opt/Websense/bin`, by default) and open the **websense.ini** file in a text editor.
2. Change the value of **LocalServerIP** to the IP address of a NIC in normal mode.

3. Navigate to the Websense directory (/opt/Websense/, by default) and run the following command:

```
./WebsenseAdmin restart
```

Windows 98 computers are not being filtered as expected

If you are running DC Agent for user identification, your Windows 98 computer machine names must not contain any spaces. Blank spaces in the machine name could prevent DC Agent from receiving a user name when an Internet request is made from that computer. Check the machine names of any Windows 98 computers experiencing filtering problems and remove any spaces you find.

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

When Filtering Service has been uninstalled and reinstalled, Network Agent does not automatically update the internal identifier (UID) for the Filtering Service.

See the Network Configuration topic in Websense Manager Help for more information.

A General Exception error occurs while installing on Linux

As the installer is configuring Policy Server, an error message is displayed with a value of **null**. After you press Enter, a message states that the installation completed successfully.

To resolve this problem:

1. To stop all Websense services, navigate to the Websense directory and run the following command:

```
./WebsenseAdmin stop
```

2. Navigate to the root directory, and then use the following command to remove the **/opt/Websense** directory:

```
rm -fr /opt/Websense
```

If you were installing Websense software in another directory, substitute the appropriate directory name.

3. Navigate to the **/etc** directory and use the following command to delete the **Websense** file:

```
rm /etc/Websense
```

4. Kill all Websense processes:

- a. Locate all processes that include “Websense” in their name:

```
ps -ef | grep Websense
```

- b. Also locate the **BrokerService** and **postgres** processes. If Remote Filtering Server is installed on the machine, include **SecureWISPProxyApp**, as well.

- c. Run **kill -9** on all of these processes used by Websense software.

5. Run this command:

```
hostname -f
```

If the value comes back as “unknown hostname,” modify the **hosts** file:

- a. Enter a line like this:

```
ipaddress mymachinename.mydomain.com mymachinename
```

Here, *ipaddress* is the machine's IP address, and *mymachinename* and *mydomain* are the machine's name and domain.

To find the IP address, run this command: `ifconfig`

- b. Save the `hosts` file.

6. Run the **hostname** command:

```
hostname mymachinename.mydomain.com
```

7. Restart the network service:

```
service network restart
```

8. Run the Websense installer again.

Index

A

- accessing Websense Manager, 44
- Active Directory
 - running logon script from, 52–53
- Address Resolution Protocol (ARP), 56
- authentication
 - RADIUS Agent, 32

B

- Bandwidth Optimizer, 7, 9, 15, 30
- basic authentication, 46
- block page URL, 48
- bytes transferred, 7

C

- clear text, 46
- components, 6
 - adding, 25
 - removing, 36
- creation rights
 - database
 - setting with OSQL utility, 62
- customer support, 10

D

- database
 - creation error messages, 61
 - creation rights
 - setting with OSQL utility, 62
 - engine location, 59
 - location, 59
 - SQL Server
 - setting creation rights, 62
- database download, *See* Master Database download
- DC Agent
 - defined, 7
 - installing separately
 - Windows, 31–32
 - required privileges, 31
 - required privileges for, 17

- deployment
 - task list, 9
- directory path for installation
 - Linux, 24, 27
 - Windows, 24, 27
- DNS server, 48
- documentation
 - product guides and applicability, 6
 - Websense documentation Web site, 6
- domain administrator privileges, 17, 23, 29, 31
- download
 - extracting installation files, 17

E

- eDirectory Agent
 - defined, 7
 - installing separately, 32
- eimserver.ini file
 - identifying Filtering Service for block page URL, 48
- engine
 - database engine location, 59
- error messages
 - case-sensitivity, 60
 - collation, 60
 - database version, 60
 - installation, 60
 - location of, 68
 - table creation, 61
- extracting installation files, 17

F

- Filtering Service
 - defined, 6
 - identifying for block page URL, 48
 - port number, 22

I

- installation

- Custom option, 15
- DC Agent
 - Windows, 31–32
- eDirectory Agent, 32
- Filtering Service port, 22
- Logon Agent, 32
- Network Agent
 - Windows, 29–31
- Policy Server port, 22
- RADIUS Agent, 32
- Remote Filtering Server, 34
- separate machine, 25–35
- Usage Monitor
 - Windows, 32
- Websense Manager, 28
- installing
 - concerns, 58
 - with MSDE 2000, 63
 - with SQL Server 2000/2005, 63
- IP addresses
 - defining ranges for Network Agent, 30
 - disabling for stealth mode, 56
 - stealth mode, 55
- L**
- launching Websense Manager, 44
- Linux
 - error messages, 68
 - removing components, 38–39
 - starting and stopping Websense services, 40–41
- Logon Agent
 - defined, 7
 - installing separately, 32
- LogonApp.exe
 - configuring to run
 - Active Directory, 52–53
 - Windows NTLM, 53–54
 - location of, 49
 - script for, 51–52
- M**
- MAC address, 56
- Manager, *See* Websense Manager
- Master Database
 - description of, 7
 - download
 - failure, 69
 - Master Database download
 - error message location, 68
 - messages
 - case-sensitivity errors, 60
 - collation error messages, 60
 - database creation errors, 61
 - database version errors, 60
 - installation error messages, 60
 - modifying an installation, 36–38
 - MSDE
 - database version error messages, 60
 - installation error messages, 60
 - installing with MSDE 2000, 63
- N**
- Network Agent
 - bandwidth optimizer, 15, 30
 - capture interface, 30
 - defined, 6, 7
 - feedback on protocol usage, 22
 - installing separately
 - Windows, 29–31
 - network interface card, 54
 - on firewall machine, 15, 30, 68
 - protocol management, 30
 - stealth mode NIC, 55–56
- network interface cards (NIC)
 - configuring for stealth mode
 - Linux, 56
 - Windows, 56
 - installation tips, 16
 - selecting for Network Agent, 22
- O**
- OSQL utility
 - database
 - setting creation rights, 62
- P**
- password, forgotten, 68
- Policy Broker defined, 6
- Policy Database defined, 6
- Policy Server
 - defined, 6

- failure to install, 69
 - machine identification, 26
 - port number, 22
 - port numbers
 - Policy Server, 26
 - Protocol Management, 7, 15, 30
- R**
- RADIUS Agent
 - defined, 7
 - installing separately, 32
 - Remote Filtering Client
 - defined, 7
 - Remote Filtering Client Pack
 - defined, 35
 - Remote Filtering Server
 - defined, 7
 - installing, 34
 - removing components
 - Linux, 38–39
 - Windows, 37–38
 - Reporting
 - components, 7
 - installation concerns, 58
 - running Websense Manager, 44
- S**
- setup
 - block page URL, 48
 - SQL Enterprise Manager
 - database
 - setting creation rights, 62
 - SQL Express, not supported, 60
 - SQL Server
 - database
 - setting creation rights with Enterprise Manager, 62
 - database version error messages, 60
 - installation error messages, 60
 - installing with, 63
 - stealth mode
 - configuring
 - Linux, 56
 - Windows, 56
 - definition, 55
 - problems with NIC, 69–70
 - using with Network Agent, 55
- T**
- technical support, 10
- U**
- Usage Monitor
 - defined, 7
 - installing separately, 32
 - User Service
 - defined, 6
 - required privileges, 17, 29
- W**
- Websense communications
 - selecting a NIC for, 55
 - Websense Explorer for Linux, 8
 - Websense Manager, 44
 - defined, 6
 - installing separately, 28
 - launching, 44
 - Websense Master Database, *See* Master Database
 - Websense services
 - manually stopping, 40
 - starting and stopping
 - Linux, 40–41
 - Windows, 40
 - Websense software
 - components, 6
 - Websense Web Filter
 - components
 - overview, 6–8
 - removing, 36
 - functional overview, 8
 - initial configuration, 43
 - Websense Web Filter components,
 - adding, 25
 - Websense Web Security
 - components
 - overview, 6–8
 - removing, 36
 - components, adding, 25
 - functional overview, 8
 - initial configuration, 43
 - Websense.log, 68
 - Windows

error messages, 68
installation, 21–24
removing components on, 37–38

starting and stopping Websense
services, 40
Windows NTLM
running logon script from, 53–54