Installation Guide

Websense® Web Security
Websense Web Filter

v7

Websense Web Security and Websense Web Filter Installation Guide

Published 2008
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Introduction

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

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

This guide also includes instructions for:

- *Adding or installing individual components*, page 31
- *Configuring Stealth Mode*, page 61
- *Planning for Reporting in Windows*, page 63
- *Troubleshooting*, page 75
- *Contacting Technical Support*, page 81

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*.

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

Note

References to *Websense software* in this guide apply to both Websense Web Security and Websense Web Filter, unless specifically stated otherwise.

Other related documentation

- See the *Websense Deployment Guide* before installing the Web filtering components for network layout.
- Use the *Installation Organizer* to record IP address, port numbers, keys, password, and similar information needed during installation.
- See the *Installation Guide Supplement* for your integration for procedures required to configure Websense to run with that integration.

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

See the Websense Manager Help after installing the Web filtering components for introductory tutorials and information about configuring and customizing Web security and filtering features.

Websense 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**: Manages the Internet protocols that are not managed by your integration product. In an integrated deployment, Network Agent can be used to detect HTTP network activity and instructs the Filtering Service to log this information.

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

  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.
- **DC Agent**: An optional component that works 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.
- **RADIUS Agent**: An optional component that works through a RADIUS Server to transparently identify users and groups who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.
- **eDirectory Agent**: An optional component that works with Novell® eDirectory™ to transparently identify users so that Websense software can filter them according to particular policies assigned to users or groups.
- **Logon Agent**: An optional component that works with a Websense Logon application (`LogonApp.exe`) to transparently identify users as they log on to a Windows domain via client machines.
- **Remote Filtering Server**: An optional component that 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**: An optional component 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.
- **Websense Master Database**: A downloadable list of millions of categorized Internet sites. Protocol definitions are also included in this database.
- **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.

How Websense filtering works

Websense Filtering Service enforces Internet request filtering. Websense software has a flexible, policy-based filtering approach, which allows you to apply different filtering policies to different clients (users, groups, domains/organizational units, computers, or networks) at different times of the day.

Websense software can be integrated with your firewall, proxy server, caching application, or network appliance, or can run without an integration (*Stand-Alone Edition*).

- *Integration*

  When an integration product receives an Internet request from a client, it queries Filtering Service to determine whether the requested site should be blocked or permitted.

- *Stand-Alone Edition*

  When Websense software is installed without an integration, Network Agent detects a client's Internet request and filters HTTP traffic. Network Agent queries Filtering Service to determine if the requested site should be blocked or permitted.

Filtering policies can be applied to individual computers, as defined by an IP address, or to a range of IP addresses defined as a network in Websense Manager. If your integration product supplies user identification, or you implement Websense transparent identification or manual authentication features, you also can apply policies to individual users, groups, domains/organizational units (called directory objects) defined in your organization's directory service. In Websense software, directory objects, computers, and networks are known collectively as **clients**.

When a client makes an Internet request, Filtering Service consults the policy assigned to the client making the request. Each policy defines specific time periods for each day, and identifies how your company wants to handle each category of URLs during those periods. After determining which categories are blocked, Filtering Service checks the Websense Master Database to determine the URL's category. If the site is assigned to a blocked category, Filtering Service sends a block page to the client.

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

The Quota feature is an alternative to full blocking. This feature gives employees time each day to visit sites in categories that you deem appropriate. Quotas help control how much time employees spend on personal surfing and the types of sites they can access. See Websense Manager Help for more information.

If the category is set to Confirm, the Websense block message includes an option to click Continue and view the site briefly for business purposes.

The protocol management feature allows Websense software to filter Internet protocols other than HTTP. This feature allows Websense software to filter Internet

applications and data transfer methods, such as those used for instant messaging, streaming media, file sharing, Internet mail.

Bandwidth Optimizer works with Network Agent to enable Websense software to filter Internet sites, protocols, or applications based on network bandwidth usage.

Websense Web Security includes Instant Messaging (IM) Attachment Manager, which works with Network Agent to allow you to restrict file attachments and file sharing with IM clients. Certain IM traffic can be permitted, while the transfer of attachments by those IM clients is blocked.

Steps for a successful Websense deployment

The following list outlines the tasks for setting up the default Web filtering. Websense Manager Help provides instructions for customizing filtering policies, configuring user- and group-based filtering, and using all features.

1. **Plan the deployment**: Websense components can be deployed in various combinations, depending upon the network layout and volume of Internet requests. Plan the deployment before starting the installation. See the Websense *Deployment Guide* to find guidelines for your environment.
2. **Complete the *Installation Organizer***: Use the *Installation Organizer* to gather IP addresses, port numbers, keys, passwords, and similar information needed during installation.
3. **Install Websense filtering components**: After you plan your deployment, install the selected Web filtering components. See *Chapter 3: Installation Procedures*.

> **Note**
> If the deployment includes an integration 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 prior to installing the plug-in, which allows the integration to communicate with Filtering Service. For more information, see the Websense *Installation Guide Supplement* for your integration.

4. If Websense Manager is installed on a Windows machine, install the reporting components to generate reports within Websense Manager. If Websense Manager is installed on a Linux system, install Websense Explorer for Linux to generate reports through a separate interface.
5. **Perform initial setup tasks**: Perform the post-installation setup tasks in *Chapter 4: Initial Setup*.
6. **Configure authentication or the integration**: Depending on the deployment, you may need to configure user authentication or configure your integration product to work with Websense software. See the *Installation Guide Supplement* for your integration for instructions.

2 Quick Installation

Use the Stand-Alone Edition of Websense filtering software on a single machine to filter a small network to evaluate the product. No integration product (firewall, network appliance, or proxy server) is required for full functionality.

If your network has more than 500 users or you plan to distribute Websense components on different machines, see *Chapter 3, Installation Procedures*.

To install Websense filtering software with an integrated product, see *Chapter 3, Installation Procedures* and the *Installation Guide Supplement* for your integration.

Components in a typical stand-alone installation

When you choose a typical installation of the Stand-Alone Edition, certain components are installed by default. The installer also provides options for installing transparent identification agents for user authentication. You can install one or more of the agents, depending on your network configuration. See *Websense components*, page 6, and the *Deployment Guide* for more information on components, and combining the transparent identification agents.

Operating system	Websense components
Windows (See footnote 1.)	• Policy Broker • Policy Database • Policy Server • Filtering Service • User Service • Network Agent • Usage Monitor • Websense Manager • Log Server (See footnote 2.)

Operating system	Websense components
	• Optional transparent identification agents. – DC Agent, or eDirectory Agent, or Logon Agent, or both DC Agent and Logon Agent – RADIUS Agent, alone or with one of the above agents
Linux (See footnote 1.)	• Policy Broker • Policy Database • Policy Server • Filtering Service • User Service • Network Agent • Usage Monitor • Websense Manager (See note 2.)
	• Optional transparent identification agents. – eDirectory Agent or Logon Agent – RADIUS Agent, alone or with one of the above agents

1. For a list of supported operating system versions, see *Operating systems*, page 12, or the Websense *Deployment Guide*.
2. In a Windows installation, Log Server is installed if you choose the Websense Web Security/Web Filter with Reporting option.
   In a Linux installation, 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.

Requirements for the installation machine

Make sure your installation machine meets or exceeds these system requirements.

Operating systems

- Windows Server 2003 - Standard and Enterprise Editions
- Windows Server 2003, SP2 - Standard and Enterprise Editions
- Windows Server 2003, R2 or R2 SP2 - Standard or Enterprise Editions
- Red Hat Enterprise 3 or 4: AS (Advanced Server)
- Red Hat Enterprise 3 or 4: ES (Enterprise Server)
- Red Hat Enterprise 3 or 4: WS (Workstation)
- Red Hat Enterprise 5 Linux: Server, Advanced Platform, or Desktop

Hardware recommendations

- Quad-Core Intel Xeon processor, 2.5 GHz or greater
- 2 GB RAM, 4 GB if running reporting
- 10 GB of free disk space, 100 GB if running reporting

Supported directory services

You can use any of the following directory services:

- Windows NT directory
- Windows Active Directory® (native or mixed mode)
- Novell Directory Services®/Novell eDirectory v8.51 and later
- Sun Java™ System Directory Server v4.2 or v5.2

Supported database engines

A supported database engine must be installed and running on a separate machine in the network before you install Websense reporting components.

Windows

- Microsoft SQL Server 2005 SP2 (Workgroup, Standard or Enterprise, or 64-bit edition) - recommended
- Microsoft SQL Server 2000 SP4
- MSDE 2000 SP4 -- suitable for smaller networks

Note

If you do not already have a database engine installed, you can download and install MSDE for free. 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.

Linux

- MySQL 5.0

Non-English languages

A separate installer is available for the non-English languages supported. After choosing a language, the installation screens appear in the selected language, and follow the same sequence as for an English installation. See *Non-English language versions*, page 19, for more information.

Configuration prerequisites

- **Internet access**: The Websense installation machine must be able to download installation files and the Websense Master Database from the Websense Web site. See *Chapter 3, Installation Procedures* for more information.
- **Deployment**: Network Agent is a required component in the Stand-Alone Edition. The machine on which it is installed must be deployed so that Network Agent can monitor all requests sent from clients to the Internet, as well as all replies to those requests.
  - The simplest deployment is to connect the machine running Network Agent to an unmanaged, unswitched hub that is located between an external router and your network.
  - If the machine is connected to a switch or router, Network Agent must be connected to a bi-directional spanning or mirror port. Port spanning or mirroring takes data entering the switch from one or all ports and duplicates that data on a single port. See the switch or router documentation for more information.

Note

If the span port on the switch or router is not capable of bi-directional communication, the machine running Network Agent needs two network interface cards (NICs). One NIC is configured for monitoring, and is attached to the span port. The second NIC is configured for blocking, and is attached to a regular port.

In this scenario, one NIC is receiving data, and one NIC is transmitting data. The required two-way communication is provided by the two NICs in combination. The NICs must be configured for monitoring and blocking, respectively, after installation.

See the Network Agent chapter in the *Deployment Guide* for more information on Network Agent location.

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 support Network Agent and the firewall software.

Installation procedure

1. If you are installing on Windows, ensure that your database engine is running.
2. Log on using administrative privileges:
   - **Linux**: log on as **root**.
   - **Windows**: log on with **domain** and **local** administrator privileges.

   This logon ensures that User Service and DC Agent have administrator privileges on the domain, and Websense software can filter by users and groups. Administrator privileges also can be set after installation. See *Configure domain administrator privileges*, page 58, for instructions.
3. Close all applications and stop any anti-virus software.
4. In Linux, create a setup directory for the installer files. For example:

   ```
   /root/Websense_setup
   ```
5. Download the installer package for your product:
   a. Go to www.websense.com, and navigate to the Downloads page.
   b. Log on to an existing account, or follow the instructions on the page to create a logon account.
   c. Enter your subscription key.
   d. Scroll down to the product that you want to install.
   e. Select the installer package, the operating system, and the language.
   f. Download the installer package to your installation machine.
6. Extract the installer files.
   - **Windows**: Double-click the downloaded file, and click **Extract** when prompted.
   - **Linux**: In the setup directory created in Step 4, 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
     ```
7. Start the installer, if it is not already running. In Windows, the installer starts after the files are extracted. In Linux, the installer must be started manually.
   - **Windows**: If the installation program is not running, double-click `Setup.exe`, located in the directory where the files were extracted.
   - **Linux**: Run the installation program from the `/Websense_setup` directory with the following command:

     ```
     ./install.sh
     ```

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

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

8. Select **Yes** in the **Subscription Agreement** screen, and click **Next**.
9. Select a product to install, and click **Next**.
   - **Websense Web Security/Web Filter**: Installs the core filtering components, and provides options for selecting a transparent identification agent.
   - **Websense Web Security/Web Filter with Reporting**: Available in a Windows installation only, this option installs the same components as above, plus Log Server to provide reporting. Ensure that the database engine is running before installing the reporting option.

     This option is suggested when installing Websense filtering software for evaluation purposes in small network.
   - **Custom**: Allows you to choose individual Websense components to install.
10. Enter a **Password** for the administrative account, WebsenseAdministrator.

    A strong password, containing a combination of lower and upper case letters, plus numbers, is recommended.
11. Select **Stand-Alone** for the Integration Option, and click **Next**.
12. If you are installing the reporting components, you are prompted to provide the location of the database, and an access method.
    - **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.
    - **Windows trusted connection**: Uses a Windows account to log into the database. This account must have administrative access to the database. Websense, Inc., recommends **against** using a Trusted Connection if you run MSDE.
    - **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 (-).

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

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

    Note
    Record the port numbers if you change them from the default settings. These ports numbers are needed when installing other Websense components.

15. Select a network interface card (NIC) for Network Agent communication. All enabled NICs are listed. Then, click **Next**.
16. 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 Websense, Inc., any information that would identify specific users, no matter which Network Agent feedback option is selected.

17. Select an initial filtering option, and click **Next**.
    - **Yes**: Configures Websense software to filter Internet traffic immediately after installation, based on a default policy.
    - **No**: Configures Websense software to monitor Internet traffic only, and permit all Internet requests. Then, use the reporting tools to evaluate network traffic before applying Internet filtering.
18. Select an optional **Transparent User Identification** method to determine how Websense software identifies users, and click **Next**.
    - **eDirectory Agent**: Select this option to use eDirectory Agent to identify users transparently with Novell eDirectory Service.
    - **DC Agent**: Select this option to use DC Agent to identify users transparently with a Windows-based directory service.
    - **Logon Agent**: Select this option to use Logon Agent to identify users transparently when they log on to the domain. For instructions, see *Creating and running the script for Logon Agent*, page 51.
    - **DC Agent and Logon Agent**: Select this option to use both DC Agent and Logon Agent to identify users transparently. This combination increases the accuracy of user identification in some networks.
    - **None**: This option does not install a Websense transparent identification agent. Select this option if your integration product provides user identification, or if you do not plan to apply user and group policies, such as when evaluating Websense filtering software.

    > **Note**
    > You can configure manual authentication in Websense Manager after installation. See Websense Manager Help for instructions.

19. If you have remote users who are authenticated by a RADIUS server, select **Yes** to install the optional Websense RADIUS Agent to transparently identify these users, and click **Next**.
20. If you selected DC Agent, enter a **Domain/User Name** and **Password** with administrative privileges on the domain, and click **Next**.

> **Note**
> This logon ensures that User Service and DC Agent have domain administrator privileges, which are required to filter by users and groups. Administrator privileges also can be set after installation. See *Configure domain administrator privileges*, page 58, for instructions.

21. Accept the default installation path or choose another path, and click **Next**. The default installation paths are listed below.
    - **Windows**: `C:\Program Files\Websense`
    - **Linux**: `opt/Websense`

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

    An installation summary appears.
22. Click **Next** to start the installation.
23. Click **Next** in the **Installation Complete** screen.

    When installation is complete, a Web page provides instructions for launching Websense Manager.
24. If you stopped your anti-virus software, restart it.
25. Launch Websense Manager.
    - 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.

    See *Starting Websense Manager*, page 42, for more information.
26. Run the *New User's Quick Start* tutorial when prompted.

3 Installation Procedures

Install, add, or remove components with the procedures in this chapter.

- *Typical installation*
- *Adding or installing individual components*
- *Removing components*

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.

A separate installation is required for Websense Content Gateway or Websense Web Security Gateway v7. See the *Websense Content Gateway Installation Guide* for instructions.

Websense Web Security/Web Filter can be installed in English and nine other language versions. See *Non-English language versions* to use your Websense software in a non-English language environment.

Non-English language versions

A separate installer package is available for the following languages:

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

Go to www.websense.com, navigate to the Downloads page, and select the multilingual installer package.

Important

Use the same installer language to install all Websense components.

Select your language at the beginning, and the remaining installation screens appear in that language.

Note

The Subscription Agreement appears in English when you install in Italian, Korean, Brazilian Portuguese, or Traditional Chinese. All other elements of the installation process use the selected language.

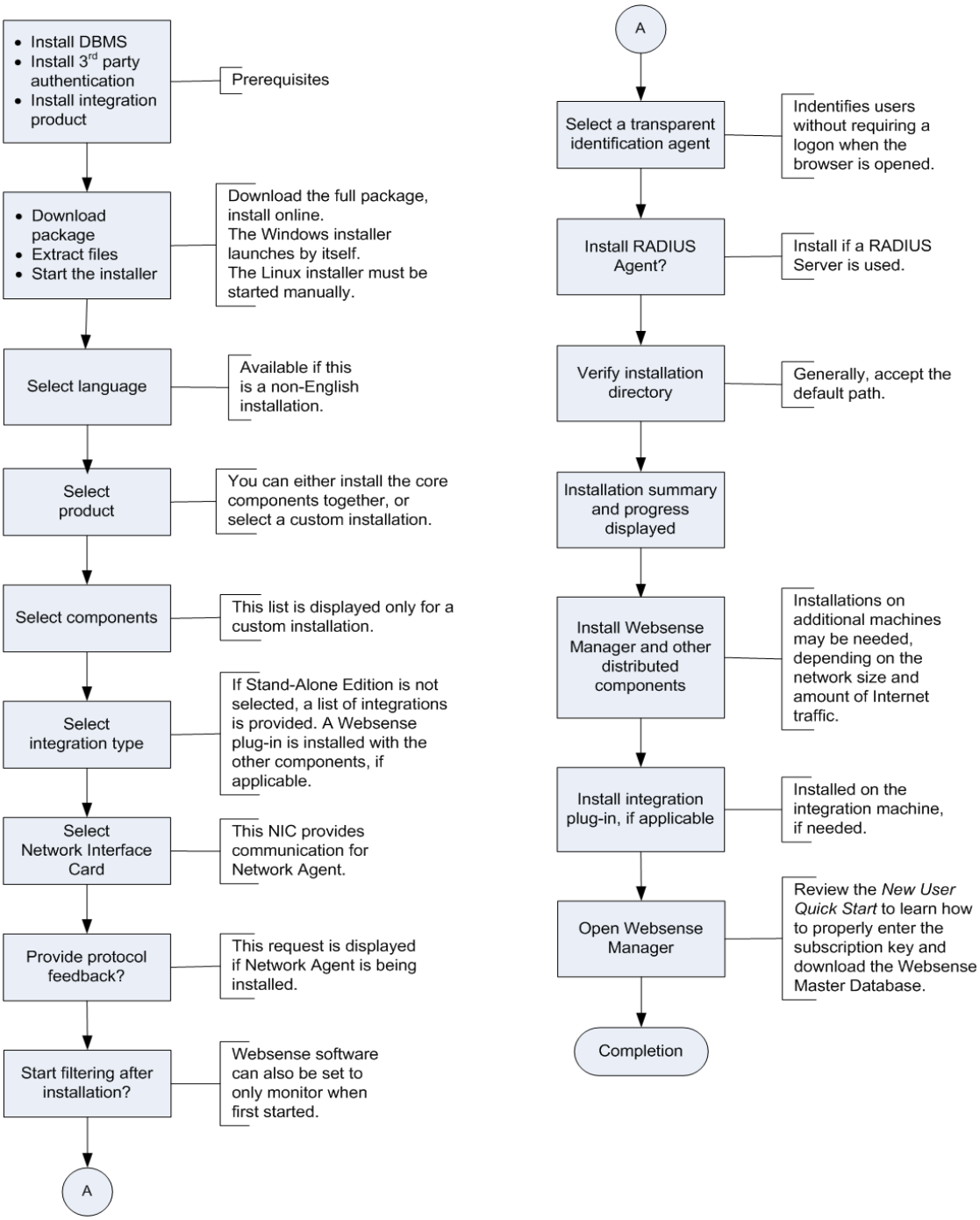
The multilingual installer package converts the following software elements into the selected language.

- Block page files (standard and Citrix-specific)

  These files are placed into a language-specific directory, named with the language code shown in the preceding table.
- Category and protocol names
- System and usage alert messages sent to configured Websense administrators
- RTSU descriptions
- Service descriptions in the Windows Services dialog box
- Network Traffic Detector interface (French, German, Spanish, and Japanese only)

Installation flow

The diagram below provides an overview of the order in which Websense components are installed.



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 determine system requirements and the appropriate location of Websense components.

  You can install the main Websense filtering components on the same machine, or distribute them on separate machines, even with different operating systems. Some components can be installed on 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 *Adding or installing individual components*, page 31.

- **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 Planning, Installation and Upgrade folder under Documentation 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 Planning, Installation and Upgrade folder under Documentation in the Websense Knowledge Base, www.websense.com/docs/.

- **Network Agent**: Network Agent is included as part of a typical installation. The machine on which Network Agent is installed must be deployed so that Network Agent is able to monitor all requests sent from clients to the Internet, and monitor all replies from the Internet to the requesting clients.

  If you install Network Agent on a machine that cannot monitor the targeted traffic, basic HTTP filtering (Stand-Alone Edition) 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 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 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.

  > **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 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 *Testing visibility of Internet traffic to Network Agent*, page 57.

- **Internet access**: For the Websense Master Database download to occur after installation, 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 also installed, shutdown 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 22 for more information.

Downloading and extracting the installation files

1. Log on using administrative privileges to the primary installation machine:
   - Linux—log in as **root**.
   - Windows—use **domain** and **local** administrator privileges.

   Important

   This logon ensures that User Service and DC Agent have administrator privileges on the domain, and Websense software can filter by users and groups. Administrator privileges also can be set after installation. See *Configure domain administrator privileges*, page 58, for instructions.

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

   ```
   /root/Websense_setup
   ```

4. Download the installer package for your product:
   a. Go to www.websense.com, and navigate to the Downloads page.
   b. Follow the instructions on the page to create a logon account, or log on as an existing user, if you already have an account.
   c. Enter your subscription key.
   d. Select the installer package, the operating system, and the language.
   e. Download the installer package to a directory on the installation machine.
5. Extract the installer files.
   - **Windows**: Double-click the downloaded file, and click **Extract** when prompted. The installation program starts automatically
   - **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 related installation files and documents.

Starting the installation program

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

If the installation program is not running:

- **Windows**: If the installation program is not running, double-click `Setup.exe`, located in the directory where the files were extracted. If another program, such as Internet Explorer, is running, the installation screens may be hidden behind that program's window.
- **Linux**: Run the installation program from the `/Websense_setup` directory with the following command:

  ```
  ./install.sh
  ```

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

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

> **Note**
> If the installation program displays error messages that it is having difficulty locating other machines, turn off any firewall installed on the same machine.

Typical installation

When you select a typical installation of Websense software, core components are installed together on one machine. Transparent identification agents also can be installed. These components are listed in the table below.

If Websense software is installed with an integration product, additional components may be installed. The *Websense Installation Guide Supplement* for your integration provides more information. The document is located in the Planning, Installation and Upgrade folder under Documentation in the Websense Knowledge Base, www.websense.com/docs/.

You also can install the product without an integration, as a Stand-Alone Edition. Complete instructions are provided in this *Installation Guide*.

To install components separately, select the Custom option when prompted to select a product. See *Adding or installing individual components*, page 31.

Operating System	Websense Components Installed
Windows (See note 1.)	• Policy Broker • Policy Server • Filtering Service • User Service • Network Agent • Usage Monitor • Websense Manager • Log Server (See note 2.)
	• Optional transparent identification agents: DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent See the *Deployment Guide* for acceptable combinations of agents.
Linux (See note 1.)	• Policy Broker • Policy Server • Filtering Service • User Service • Network Agent • Usage Monitor • Websense Manager (See note 2.)
	• Optional transparent identification agents. eDirectory Agent, Logon Agent, or RADIUS Agent See the *Deployment Guide* for acceptable combinations of agents.

1. For a list of supported operating system versions, see *Operating systems*, page 12, or the Websense *Deployment Guide*.
2. In a Windows installation, Log Server is installed if you choose the Websense Web Security/Web Filter with Reporting option.
   In a Linux installation, 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

Important

The installation supplement for your integration 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 running the following procedures.

1. Download and extract the installation files, if needed. See *Downloading and extracting the installation files*, page 24.
2. If the installation program is not running, start it. See *Starting the installation program*, page 25.
3. Follow the prompts. Click **Next** through the Welcome screen.
4. Select **Yes** in the **Subscription Agreement** screen, and click **Next**.
5. Select a the type of installation, and 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/Web Filter with Reporting**: Available for a Windows installation only. Installs the same components as above, plus Log Server to provide reporting. Ensure that the database engine is running before installing the reporting option.

     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. Use this option to install Websense components on different machines in your network. For more information, see *Adding or installing individual components*, page 31.
6. If you are not running a Custom installation, you are prompted enter a **Password** for the administrative account, WebsenseAdministrator.

   A strong password, containing a combination of lower and upper case letters, plus numbers, is recommended.
7. Select an Integration Option, and click **Next**.
   - Select **Stand-alone** to install Network Agent as the Internet filtering component of Websense Web Security or Web Filter.
   - Select **Integrate** if you are installing Websense software to work with a firewall, proxy server, cache, or network appliance.

The *Websense Installation Supplement* for your integration includes instructions for selecting an integration and the appropriate options, plus steps for configuring Websense software and the integration to work together.

8. If you selected to install Websense software with reporting, you are prompted to provide the location of the database engine, and an access method.

   If you are not installing reporting at this time, or plan to install Websense Explorer for Linux, skip to Step 10.

   a. **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.

   b. 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 begin or end with a hyphen (-).

      - **Windows trusted connection**—Uses a Windows account to log into the database. This account must have administrative access to the database. Websense, Inc., recommends **against** using a Trusted Connection if you run MSDE.

9. Accept the default location for the Log Database, or select a different location. Then, click **Next**.

10. 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 the port numbers if you change them from the default settings. These port numbers are requested when installing other Websense components.

11. Select a network interface card (NIC) for Network Agent to send block messages and communicate. If the installation machine contains multiple NICs, all enabled NICs with an IP address are listed.

    NICs without an IP address can be set up to monitor Internet requests in stealth mode. See *Appendix A, Configuring Stealth Mode* for more information.

12. 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.

13. Select an optional **Transparent User Identification** method to determine how Websense software identifies users, and click **Next**.
    - **eDirectory Agent**: Select this option to use eDirectory Agent to identify users transparently with Novell eDirectory Service.
    - **DC Agent**: Select this option to use DC Agent to identify users transparently with a Windows-based directory service.
    - **Logon Agent**: Select this option to use Logon Agent to identify users transparently when they log on to the domain.

      Logon Agent receives its user information from an application called `LogonApp.exe` that must be run by a logon script in your network. For instructions, see *Creating and running the script for Logon Agent*, page 51.
    - **DC Agent and Logon Agent**: Select this option to use both DC Agent and Logon Agent to identify users transparently. This combination increases the accuracy of user identification in some networks.
    - **None**: This option does not install a Websense transparent identification agent. Select this option if your integration product provides user identification, or if you do not plan to apply user and group policies, such as when evaluating Websense filtering software.

    > **Note**
    > You can configure manual authentication in Websense Manager after installation. See Websense Manager Help for instructions.

14. Select whether or not to install **RADIUS Agent**.

    If you have remote users who are authenticated by a RADIUS server, select **Yes** to install the optional RADIUS Agent to transparently identify these users. Click **Next** to continue.
15. If you selected DC Agent in the Transparent Identification screen, enter a **Domain/User Name** and **Password** with administrative privileges on the domain, and click **Next**.

    DC Agent accesses directory information to identify users transparently.

> **Note**
> This logon ensures that User Service and DC Agent have domain administrator privileges, which are required to filter by users and groups. Administrator privileges also can be set after installation. See *Configure domain administrator privileges*, page 58, for instructions.

16. 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 Websense Manager Help for details of now 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.
17. Accept the default installation path or click **Browse** to locate another path, and click **Next**. Default paths are:
    - **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 quits 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.
18. Click **Next** to start the installation. An installation progress screen is displayed.

19. Click **Next** in the Installation Complete screen.

    When the installer finishes running, a Web page provides instructions for launching Websense Manager. For more information on starting Websense Manager, see *Starting Websense Manager*, page 42.

20. If you stopped your anti-virus software, restart it.
21. If you stopped a firewall running on a Linux machine:
    a. Open a command prompt.
    b. Enter `service iptables start`.
    c. Enter `service iptables status` to determine if the firewall is running.
22. See *Chapter 4: 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.

Adding or installing individual components

A Custom installation allows Websense components to be distributed onto multiple machines, in the combinations that are most suitable to your environment.

Remote Filtering components can be installed only through a Custom installation. See the *Remote Filtering* technical paper for more information on installing remote filtering. This paper is located in the Planning, Installation and Upgrade folder under Documentation in the Websense Knowledge Base, www.websense.com/docs.

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. Only one instance of Policy Broker can be installed.

Multiple instances of some components may be needed, depending on the network's configuration and volume of Internet traffic. Most components install on both Windows and Linux, 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 Websense Web Security/Web Filter during installation, Policy Broker, Policy Server, User Service, Filtering Server and Network Agent were installed on the same machine. A transparent identification agent was also installed, if selected during the installation. Use the Custom option to install additional instances of some components.

Common component installation procedures

The steps in this section are common to all separate installations of components. Refer to the appropriate sections for the component-specific information.

1. Log onto the installation machine with administrative (Windows) or root (Linux) privileges.
2. Close all applications and stop any anti-virus software.
3. Download the installation package and extract the files. See *Downloading and extracting the installation files*, page 24.
4. Start the installation program if it is not running. See *Starting the installation program*, page 25, for instructions.
5. Follow the prompts. Click **Next** through the Welcome screen.
6. Select **Yes** in the **Subscription Agreement** screen, and click **Next**.
7. Select a procedure:
   - Select **Custom**, and click **Next**, if the installer is running on a machine with no Websense components installed.
   - Select **Add Websense Components**, and click **Next**, if the installer is running on a machine where other Websense components are installed.

   A list of components not installed on the machine is displayed.
8. Select the components to be installed, and click **Next**.

   If Policy Server is installed on a different machine, the installer asks you to enter the IP address and configuration port.

> **Note**
>
> The configuration port shown, 55806, is the default port for Policy Server. If you installed Policy Server with a different port, enter that port number.

If other Websense components are already installed on the same machine as the component being installed, the installer locates existing Websense initialization files and uses this configuration information to locate Policy Server and Filtering Service in the network.

> **Note**
> Fewer steps are needed to install Websense Logon Agent and Remote Filtering components when other components are already installed on the same machine. The installer uses information from the existing initialization files to locate Policy Server and Filtering Service.

9. Enter the IP address of the Policy Server machine, and the port number if it is different than the default setting, and click **Next**.

   Depending on the component and location, the installer may request Filtering Service location, domain administrator credentials, or the IP address or host name and port number for another component.

10. Check the component sections following this procedure for specific instructions needed to install that component.

    - *Websense Manager*, page 34
    - *Policy Broker*, page 35
    - *Policy Server*, page 35
    - *User Service*, page 35
    - *Filtering Service*, page 36
    - *Network Agent*, page 36
    - *DC Agent*, page 37
    - *Usage Monitor*, page 38
    - *RADIUS Agent*, page 39
    - *eDirectory Agent*, page 39
    - *Logon Agent*, page 39
    - *Log Server*, page 40
    - *Remote Filtering Server*, page 41

11. 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.

    If the installation machine contains multiple NICs, all enabled NICs with an IP address are listed. NICs without an IP address can be set up to monitor Internet requests in stealth mode. In Linux, do not choose a stealth mode NIC for communicating with other components. See *Appendix A, Configuring Stealth Mode* for more information.

    Select the NIC, and click **Next**.

    See *Network Agent*, page 36, for more information on this component.

12. Accept the default installation path or click **Browse** to locate another path, and click **Next**. The default installation paths are:

    - **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 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.

13. 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.

14. Click **Next** in the Installation Complete screen.

    When the installer finishes running, a Web page provides instructions for launching Websense Manager.

15. If you stopped your anti-virus software, restart it.
16. See *Chapter 4: Initial Setup* for important setup information.

Custom component installation

Each component has special considerations when installed separately.

Websense Manager

Websense Manager provides the administrative interface for Websense software. In a Windows installation, Websense Manager can also provide reporting.

In a Windows installation, due to the amount of processing required to run reports, Websense Manager should be installed on a machine separate from the other components. 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 can connect to a Policy Server on the same or a different operating system.
- Return to Step 11, page 33, to continue with the installation.
- To launch Websense Manager, see *Starting Websense Manager*, page 42.
- In a Windows environment, 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. 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 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.
- Return to Step 11, page 33, to continue with the installation.

Policy Server

Policy Server must be installed second, after 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, multiple Policy Servers may be needed. They are connected 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 other Websense components separately, the installer asks for the location and port number for Policy Server, if it is not installed on the same machine. The default of port 55806 is shown. If you change this port number, the same port must be entered for each component that uses this Policy Server.
- Return to Step 11, page 33, to continue with the installation.

User Service

Each Policy Server requires one User Service. 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 machine on which Policy Server is running.

- When installing User Service, log on with local administrator (Windows) or root (Linux) privileges.

Note

This logon ensures that User Service has administrator privileges on the domain, and Websense software can filter by users and groups. Administrator privileges also can be set after installation. See *Configure domain administrator privileges*, page 58, for instructions.

- Configure User Service to communicate with DC Agent if both components are installed. See the User Identification topic of Websense Manager Help for instructions.
- Return to Step 11, page 33, to continue with the installation.
- 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 Services may be needed. A maximum of ten Filtering Services per Policy Server is recommended.

- 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 those components on a separate machine.
- Return to Step 11, page 33, to continue with the installation.

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.
- 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.

- The installer prompts you to select the NIC that Network Agent can use for communicating. All enabled NICs in the machine are listed.

  Select a NIC and click **Next** to continue.
- 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**.
- Return to Step 12, page 33, to continue with the installation.
- 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 logon 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 *Configure domain administrator privileges*, page 58, for instructions.

- Return to Step 12, page 33, to continue with the installation.
- After installation, configure User Service to communicate with DC Agent by following the instructions in the User Identification topic of Websense Manager Help.

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 requires only one Usage Monitor.

- Return to Step 11, page 33, to continue with the installation.
- After installation, use Websense Manager to configure Usage Monitor to send usage alerts. See the Alerting topic in Websense Manager Help for more information.

RADIUS Agent

RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server.

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.

- Return to Step 12, page 33, to continue with the installation.
- After installation, configure RADIUS Agent and configure your environment to use RADIUS Agent. See the User Identification topic in Websense Manager Help for instructions.

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.
- The installer asks for the Novell eDirectory name and password.

  Enter the **fully distinguished name** and a valid password, and click **Next**.
- Return to Step 11, page 33, to continue with the installation.
- After installation, configure eDirectory Agent and Novell eDirectory. See the User Identification topic in Websense Manager Help for instructions.

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 `LogonApp.exe`, a separate client application that runs only on Windows client machines, and must be run by a logon script.

Logon Agent can be run together 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.
- Set up the required logon script by following the instructions in *Creating and running the script for Logon Agent*, page 51.
- Return to Step 12, page 33, to continue with the installation.
- After installation, configure Logon Agent to communicate with client computers and Filtering Service using the instructions in User Identification topic of Websense Manager Help.

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

Log Server must be installed for Websense reporting to run.

- 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 such as setting up user roles.

  If you do not have a database engine, you can download and download MSDE for free. 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**—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 (-).

  - **Windows trusted connection**—Uses a Windows account to log into the database. This account must have administrative access to the database. 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 Websense Manager Help for details of now 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.

- Return to Step 11, page 33, to continue with the installation.
- After installing Log Server on a separate machine, go to the Websense Manager machine and use the Windows Services dialog box to stop and restart the ApacheTomcatWebsense service.

Important

When installed on a separate machine from Websense Manager, you **must** stop and restart the ApacheTomcatWebsense service on the Websense Manager machine after installing Log Server and before creating scheduled jobs in presentation reports.

Remote Filtering Server

Remote Filtering Server provides Web filtering for user computers, such as laptops, 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 connects to port 55825 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.

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

See the *Remote Filtering* technical paper for information on installing, configuring and using remote filtering. This paper is located in the Planning, Installation and Upgrade folder under Documentation in the Websense Knowledge Base, 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 two supported browsers:

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

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 **tomcat.log** file on the Websense Manager machine (located by default in the `C:\Program Files\Websense\tomcat\logs\` or `/opt/Websense/tomcat/logs/` directory) to verify the port.

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 with the user name of **WebsenseAdministrator** and the password that you entered during the installation.

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 Guide Supplement* for your integration product.

- Add Websense components.

  See *Adding or installing individual components*, page 31, 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.

Important
The Policy Broker and Policy Server services must be running when you uninstall any Websense components. To remove Policy Broker or Policy Server, you must remove all the other components installed on the machine.

Removing Policy Server deletes Websense configuration information, unless it has been properly backed up. See Websense Manager Help for information on using the Websense Backup Utility.

Windows

Notes
- Before removing components, use the Websense Backup Utility to make a backup Websense configuration and initialization files. See Websense Manager Help for instructions.
- Restart the machine, if prompted to do so.

1. Log on with **local** administrator privileges.
2. Close all applications and stop any anti-virus software.

3. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs** to open the Windows Add or Remove Programs dialog box:
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 the Websense Setup starts.

   A list of installed components appears.

   By default, all components are checked for removal. Websense Policy Broker Database is not listed and is not removed by this process.

   Warning

   If components are removed separately, Policy Broker must be removed last.

   Do not remove Policy Server without removing all other Websense components, except 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 be 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 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.

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 a plug-in for an integration product, you may need to restart the integration.

Linux

> **Note**
> Before removing components, use the Websense Backup Utility to back up Websense configuration and initialization files. See the Websense Knowledge Base for instructions.

1. Log on as the **root** user.
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**
> If components are removed separately, Policy Broker must be removed last.
>
> Do **not** remove Policy Server without removing all other Websense components, except 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 be 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 prompt and go to the `/Websense` directory.
   c. Enter `./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 for these components. 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.

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

Principal Websense components must be stopped and started in a prescribed order. Optional components may be stopped and started in any order.

Principal components

The following list is the preferred order for stopping the principal components. Optional components must be stopped before principal components, and started after them.

In Windows, the services are labeled with Websense, such as Websense Policy Server.

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

When restarting Websense services on Windows, reverse the order, starting with the Policy Broker.

In Linux, a single command stops and starts components in the proper order.

Optional components

You can manually start or stop these Websense services in any order.

- eDirectory Agent
- RADIUS Agent
- DC Agent
- Logon Agent
- Usage Monitor
- Remote Filtering Server

Windows

Stop, start, or restart a Websense service within the Services dialog box.

1. If Websense is running with a NetCache integration, disable the ICAP Service Farm.
2. Open the Windows **Control Panel** and select **Administrative Tools** > **Services**.
3. Select a Websense service.
4. From the **Action** menu, select **Start**, **Stop**, or **Restart** or click one of the control buttons in the toolbar (**Stop** ■, **Start** ▶, or **Restart** ■ ▶). **Restart** stops the service, then restarts it again immediately from a single command.

Warning

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

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

Linux

You can 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 is stopped last and started first. See *Principal components*, page 47, 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` directory.
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 procedure may corrupt the services.

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

4 Initial Setup

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

- Launch Websense Manager and enter your Websense subscription key to start a download of the Websense Master Database. The Master Database is needed to enable filtering. See the *New User Quick Start* when you first start Websense Manager.
- If the Filtering Service is installed on a machine with multiple NICs, identify the Filtering Service by its IP address in your network so that Websense block messages can be sent to users. See *Identifying the Filtering Service for the block page URL*, page 50, for instructions.
- If you installed Network Agent on a machine with multiple NICs, you can configure Network Agent after installation to use more than one NIC. See the Network Configuration topic in Websense Manager Help for more information. To set a NIC for monitoring in stealth mode, see *Appendix A: Configuring Stealth Mode*.
- If you installed Network Agent, use the Network Traffic Detector to test whether Network Agent can see the user Internet traffic that you want it to monitor. See the Network Configuration topic in Websense Manager Help for instructions.
- All Windows computers being filtered must have the Messenger Service enabled to receive protocol block messages. See Websense Manager Help for instructions.
- 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 51, for instructions.
- If you were unable to grant User Service or DC Agent administrator privileges during installation, do so now to ensure that they will function correctly. See *Configure domain administrator privileges*, page 58.
- Configure your firewall or Internet router appropriately. See *Configuring firewalls or routers*, page 59, for more information.
- 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 purchased Websense Web Security, activate your subscription to the Websense Web Protection Services™: SiteWatcher™, BrandWatcher™, and ThreatWatcher™. See Websense Manager Help for instructions.

- If you installed the optional Remote Filtering components, some configuration is required before filtering can start. 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.

For additional Websense configuration information, see Websense Manager Help.

Identifying the Filtering Service for the block page URL

If Filtering Service is installed on a machine with multiple NICs, identify Filtering Service by its IP address so that Websense block pages can be sent to users. Block pages tell users that the site is blocked, and why.

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

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

If the Filtering Service machine name, rather than the IP address, is contained in the block page URL, a blank page could be displayed instead of the block message.

- If you have an internal DNS server, enter the Filtering Service machine's IP address as a resource record in your DNS server. See your DNS server documentation for instructions.
- If you do not have an internal DNS server:
  1. On the Filtering Service machine, go to the `\bin` subdirectory under the Websense installation directory. By default, the installation directory is `C:\Program Files\Websense\bin` in Windows, or `opt/Websense/bin` in Linux.
  2. Make a backup copy of the `eimserver.ini` file and move the copy to 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>`

     where `<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 46.

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 transparently to Websense software when they log on to a Windows domain. Identification is accomplished by the Websense Logon application, `LogonApp.exe`. This application provides a user name and IP address to the Logon Agent each time a Windows client connects to an Active Directory or a Windows NT or Active Directory (mixed mode) directory service.

During the installation of Logon Agent, the Logon application and script files are placed to the same machine. See *Logon Agent*, page 39 for installation instructions.

The logon script. `Logon.bat`, must be modified for your network. Both the script and the `LogonApp.exe` application files must then be copied to a shared drive on the domain controller.

Prerequisites for running the logon script

Logon Agent requires running LogonApp.exe on the computers that are filtered. This runs on Windows, only.

- If the logon script runs LogonApp in persistent mode, configure your Active Directory server to **not** run scripts synchronously.
- Be sure that all computers can connect to the shared drive on the domain controller where the `logon.bat` and `LogonApp.exe` are placed. 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 computer has access to the domain controller, run the following command from a Windows command prompt on the computer:

  ```
  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.
- On client machines running Windows Vista, 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**.

File location

These files are located in Websense installation directory on the Logon Agent machine. By default, the installation directory is either `C:\Program Files\Websense\bin` in Windows, or `opt/Websense/bin` in Linux:

- `LogonApp.exe`: 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.

Websense user map and persistent mode

User identification provided at logon by `LogonApp.exe` is stored in the Websense user map. This information is updated periodically if `LogonApp.exe` is run in persistent mode. The update time interval for the persistent mode and the interval at which the user map is automatically cleared of logon information are configured in Websense Manager.

In Active Directory, if you decide to clear the logon information from the Websense user map before the interval defined in Websense Manager, you can create an accompanying logout script. You cannot configure a logout script for Windows NTLM.

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

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 logon script*

  Edit the parameters in the sample script file (`Logon.bat`) to match your network.
- *Task 2: Configure the scripts to run*

  You can run your logon script from an Active Directory, Active Directory (mixed mode), or Windows NT directory service using group policies. You must configure the script to run for the users to be filtered.

  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, you must configure Logon Agent in Websense Manager.

Task 1: Prepare the logon script

A batch file, called `Logon.bat`, is installed with Logon Agent in the Websense installation directory. By default, the installation directory is `C:\Program Files\Websense\bin` in Windows or `opt/Websense/bin` in Linux.

This file contains instructions for using the scripting parameters, and two sample scripts: a logon script that runs `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. You must have `.bat` files with different names to run both scripts.

Script parameters

Construct a script using the samples provided (`Logon.bat`) and the parameters in the table below.

The required portion of the script is:

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

This command runs `LogonApp.exe` in persistent mode (the default), which sends user information to the Logon Agent at predefined intervals.

Note

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

Parameter	Description
<*server*>	IP address or name of the machine running the Websense Logon Agent. This entry must match the machine address or name entered in Websense Manager in Task 3.
<*port*>	The port number used by Logon Agent. Enter **`15880`** if you plan to accept the default port number when configuring the Logon Agent in Websense Manager in Task 3.
/NOPERSIST	Causes `LogonApp.exe` to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user's data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours, and can be changed in Websense Manager in Task 3. If the NOPERSIST parameter is omitted, `LogonApp.exe` operates in persistent mode. In persistent mode, `LogonApp.exe` resides in memory on the domain server and updates the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes, and can be changed in Websense Manager in Task 3.

Parameter	Description
/COPY	Copies the `LogonApp.exe` 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.
/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 following examples is the command for a logon script.

- **Logon Script:** In this example, the edited `Logon.bat` file contains this single command:

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

This sample 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`.

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.

- **Logout Script:** Copy the logon batch file and rename it `Logout.bat`. Edit the script in `Logout.bat`:

  ```
  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, Active Directory (mixed mode), or on a Windows NT directory service. 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 51.
2. On the Active Directory machine, go to the Windows Control Panel and select **Administrative Tools** > **Active Directory Users and Computers**.
3. Right-click on the domain and select **Properties**.

   The domain Properties dialog box appears.
4. Select the **Group Policy** tab.
5. Click **New** and create a policy called **Websense Logon Script**.
6. Double-click the new policy or click **Edit**.

   The Group Policy Object Editor dialog box appears.
7. In the tree structure displayed, expand **User Configuration**.
8. Expand the **Windows Settings** structure.
9. Select **Scripts (Logon/Logoff)**.
10. In the right pane, double-click **Logon**.

    The Logon Properties dialog box appears.
11. Click **Show Files** to open this policy's logon script folder in Windows Explorer.
12. Copy two files into this folder:
    - `Logon.bat`, your edited logon batch file
    - `LogonApp.exe`, the application
13. Close the Explorer window.
14. Click **Add** in the Logon Properties dialog box.

    The Add a Script dialog box appears.
15. Enter the file name of the logon batch file (`Logon.bat`) in the **Script Name** field or browse for the file.
16. Leave the **Script Parameters** field empty.

17. Click **OK** twice to accept the changes.
18. (Optional.) If you have prepared a logout script, repeat Step 7 through Step 17. Choose **Logoff** at Step 10, and use your logout batch file when you are prompted to copy or name the batch file.
19. Close the Group Policy Object Editor dialog box.
20. Click **OK** in the domain Properties dialog box to apply the script.
21. 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 Websense Manager Help.

For additional information about deploying logon scripts to users and groups in Active Directory, got 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 51.
2. Copy the `Logon.bat` and `LogonApp.exe` files from the Websense installation directory on the Logon Agent machine to the `netlogon` share directory on the domain controller machine.

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

   By default, the Websense installation directory is `C:\Program Files\Websense\bin` in Windows, or `opt/Websense/bin` in Linux.

   Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.
3. In the Control Panel of the domain controller, select **Administrative Tools > User Manager for Domains**.
4. Select the users for whom the script must be run, and double-click to edit the user properties.

   The User Properties dialog box appears.
5. Click **Profile**.

   The User Environment Profile dialog box appears.
6. Enter the path to the logon batch file in the **User Profile Path** field (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 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 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 to Filtering Service.

If you install Network Agent on a machine with multiple NICs, you can configure Network Agent after installation to use more than one NIC. See the *Websense Deployment Guide* for more information on this configuration. See Websense Manager Help for more instructions.

Testing visibility of Internet traffic to Network Agent

The monitoring NIC for Network Agent must be able to see two-way Internet traffic for Network Agent to filter properly.

To determine if Network Agent can monitor Internet traffic for a desired network, you can run a traffic visibility test on the Network Agent machine using the Websense Network Traffic Detector.

1. Open the Network Traffic Detector tool:
   - **Windows**: Go to **Start** > **Programs** > **Websense** > **Utilities** > **Network Traffic Detector** to launch the tool.
   - **Linux**: Open a command prompt and run `./TrafficVisibility.sh` from the Websense installation directory (`/opt/Websense` by default).

     To start a GUI version, run `./TrafficVisibility.sh -g`

2. Select a network card from the **Network Adapter** drop-down list.
3. Check the addresses that appear in the **Monitored Network Ranges** list to verify that all appropriate subnetworks are listed.
4. Use the **Add Subnetwork** and **Remove Subnetwork** buttons to change which parts of the network are tested.
5. Click **Start Monitoring**.

   The Network Traffic Detector detects computers in the network by monitoring the information they send across the network. The **Number of Computers Detected** list shows a running count of computers detected.
6. To see specific information about the computers detected by the tool, select a subnetwork in the Monitored Network Ranges list, and then click **View Detected Computers**.

   If a specific computer is not listed, verify that it is generating network traffic. To do this, go to the machine, launch a browser, and navigate to a Web site. Then return to the Network Traffic Detector and see if the computer appears in the **Detected Computers** dialog box.
7. When you have finished testing network traffic visibility, click **Stop Monitoring**.

If some computers are not visible:

- Review the network configuration and NIC placement requirements. See the Hardware configuration instructions in the Network Configuration topic in Websense Manager Help.
- Verify that you have properly configured the monitoring NIC. See the Configuring NIC settings instructions in the Network Configuration topic in Websense Manager Help.

Configure domain administrator privileges

User Service and DC Agent must have administrator privileges on the network to retrieve user logon information from the domain controller. If you were not able to grant these privileges during installation, do so now.

This procedure may vary slightly, depending upon the version of Windows you are using.

1. From the Windows Control Panel on the installation machine, select **Administrative Tools > Services**.
2. In the Services dialog box, double-click **Websense User Service**.
3. Select the **Log On** tab in the Properties dialog box.
4. Select **This account** and enter a valid domain\user name and password for an account with **domain** administrator privileges in your network.
5. Click **OK**.
6. If DC Agent was installed, repeat the process for the **Websense DC Agent** service.

Configuring firewalls or routers

For Internet connectivity, Websense Manager may require authentication through a proxy server or firewall for HTTP traffic. To allow downloads of the Websense Master Database, 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 Websense software is installed with an integration, see the *Installation Guide Supplement* for your integration for more information.

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 the central Websense software for filtering and logging.

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

Important

In 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 in 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

You can install reporting components on a Windows server or a Linux server. A Windows installation provides reporting functionality within the Websense Manager interface, and offers the greatest flexibility and usability. The information in this appendix specifically addresses the configuration with Websense Manager and reporting components installed on a Windows server.

> **Note**
> If Websense Manager is installed on a Linux system, Websense Explorer for Linux can be installed separately to provide reporting. Websense Explorer for Linux runs with My SQL. 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 server, a database engine must be installed and running. The following database engines are supported:

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

See the Microsoft documentation for SQL Server installation instructions.

If you do not have a database engine, you can download and download MSDE for free. 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`.

In a Windows environment, most Websense functionality is included as part of the Websense Manager installation. This functionality is activated when you install Log Server, the only additional Websense component needed to run reports on Windows.

Installing reporting in Windows networks

Reporting can be installed when other Websense components are installed, or it can be installed separately. See *Chapter 3: Installation Procedures,* for instructions.

- To install reporting at the same time as other components on Windows, select **Websense Web Security /Web Filter with Reporting** in the Installation Type screen. This option installs Log Server with the other components.

  This option is suggested when installing Websense filtering software for evaluation purposes or in small network. In larger networks, Websense Manager and the reporting components should be installed on a separate machine. See the Websense *Deployment Guide* for more information.
- If Websense Manager is already installed on Windows, go to the reporting machine and run the Websense installer. Select **Custom** in the Installation Type screen, and select **Log Server**. See *Log Server*, page 40.
- To install both Websense Manager and Log Server on the same Windows machine, select **Custom** in the Installation Type screen, and then select **Websense Manager** and **Log Server** from the component list.

Follow the onscreen instructions and provide the information requested. See *Adding or installing individual components*, page 31, for installing components separately.

Installation concerns

Your installation options and procedures vary, based on locations and components.

> **Note**
>
> The name of the Websense Log Database 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 66.

The Websense installer verifies that the database engine installation is configured appropriately for use with Websense reporting. If it encounters a problem, an error message appears. The error messages are documented in *SQL Server/MSDE installation error messages*, page 66, which includes instructions for resolving the errors.

Collation and case-sensitivity

To provide highly accurate reports, Websense reporting tools use *case-insensitive* collation functions for database searches. If your SQL Server 2000/2005 instance uses *case-sensitive* collation, reporting components cannot be installed. This problem can occur if other applications use the same instance of SQL Server.

Before continuing with this installation, you must install another SQL Server instance set to use the default, case-insensitive settings. See *Collation and case-sensitivity error messages*, page 67 for instructions to correct the problem.

Database engine location

1. Log on to the Websense reporting installation machine with an account that has local administrator privileges and privileges to create, modify, and delete databases.

   When prompted by the Websense installer, enter the IP address where the database engine is installed. **Localhost** can be used, if the database is installed on the same machine, and the machine has only one NIC. Contact your database administrator for assistance.

   If you installed SQL Server with an instance name other than the default of MSSQLServer, enter the IP address of the SQL Server machine, followed by the instance name:

   `<IP address>\<instancename>`

   For example:

   `10.200.1.1\ReporterSql`
2. Enter a logon name and password for an account that has rights to create a database. The default logon name is **sa**.
3. Click **Next**.

Minimizing database size

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 Websense Manager Help for details of now 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.

Database location

Specify the location for installing the Log Database, and the access method according to your network setup. 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.

1. **Database Engine Location**—Enter the name or IP address of the machine on which a supported database engine is running.

   Important

   You need to create a path to the database before installing Log Server. Problems can occur during installation if the path is nonexistent, and the Log Server and SQL Server are on different machines.

2. 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 begin or end with a hyphen (-).

   - **Windows trusted connection**—Uses a Windows account to log into the database. This account must have administrative access to the database.

     Websense, Inc., recommends **against** using a trusted connection if you run MSDE.

SQL Server/MSDE installation error messages

Before installing Websense reporting files, the installer checks your SQL Server or MSDE configuration. If any configuration issue is found, the an error message describes the problem.

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

The following topics describe the issues that may cause the installation to fail, and provide information for correcting the problems.

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

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. If a database engine is not found during installation, 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`. The database size limit for MSDE is 2 GB.
- SQL Server is available from Microsoft. Check the Microsoft Web site for purchase information.

  For installation and upgrade details, see the Microsoft documentation.

If you try to install Websense with an MSDE or SQL Server version that is not supported, 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 then run the Websense installer again to install Log Server.

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 2000 or 2005 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.

Install another SQL Server instance set to use the default, case-insensitive settings. During installation, the Collation Settings dialog box provides options from which to select the correct setting.

You can check the case setting of SQL Server via SQL Enterprise Manager, although you cannot change the setting.

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, proceed as follows:
   a. In the navigation pane, expand the following trees, in the order listed.
      - Microsoft SQL Servers
      - SQL Server Group

b. Right-click the server icon for the machine where the SQL instance you want to use is installed, and select **Properties** from the drop-down menu.

c. Select the **General** tab and look for the text **Server collation**. For example:

`SQL_LATIN1_General_CP1_CS_AS`

In this string, the bold text indicates case sensitivity.

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

4. If you are running SQL Server 2005, proceed as follows:

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:

`SQL_LATIN1_General_CP1_CS_AS`

In this string, the bold text indicates case sensitivity.

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

5. Click **OK** to close the Properties dialog box.
6. 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

To install reporting components, you must have access rights that allow you to create databases. These rights are associated with a fixed server role. You need to create the DBCreator role to gain access to the appropriate rights.

If you are planning to use a trusted connection (Windows Authentication) for communication between Log Server and the Log Database, you must be logged on to the installation machine as a user who has the appropriate rights. If you plan to use a SQL Server account for access to the database, the selected account must have the appropriate rights.

- *Using SQL Enterprise Manager to set database creation rights*
- *Using osql utility to set database creation rights*, page 69

Using SQL Enterprise Manager to set database creation rights

If Microsoft SQL Server is your database engine, use the following procedure to set these rights.

1. Log on with administrator access to SQL Server.
2. Open the SQL Server Enterprise Manager: **Start** > **Programs** > **Microsoft SQL Server** > **Enterprise Manager**.
3. If you are using SQL Server 2000:

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**. The Servers Role Properties- dbcreator dialog box appears.

4. If you are using SQL Server 2005

   a. In the navigation pane, expand the following trees, in the order listed.
      - Security
      - Server Roles

   b. Select **dbcreator**, then right-click and choose **Properties**.

5. Click **Add**. The Add Members dialog box appears, showing all existing logons for SQL Server.
6. Highlight the logon to which you are adding database creation rights, and click **OK**. The Add Members dialog box closes.
7. In the Servers Role Properties - dbcreator dialog box, verify that you have updated the correct logon, and click **OK**.
8. Close SQL Enterprise Manager.

Using osql utility to set database creation rights

If MSDE 2000 is your database engine, use the MSDE user interface, `osql`, to add the dbcreator role.

1. Go to the machine where the MSDE 2000 instance is running.
2. Open the Windows Services dialog box and verify that the MSDE 2000 instance is running.
3. Open a Windows command prompt (go to **Start** > **Run**, and enter **cmd**).
4. Connect to the named instance of MSDE 2000 using Windows Authentication, 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.

5. 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 *servername**instancename* entries are correct.
   - Run the command in Step 4 again.

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

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

   In the above command, replace *user_logon* with the SQL Server or Windows user logon to whom you are assigning database creation rights.

7. Check the results. An entry of **0** in the command prompt window indicates success.
8. Enter `EXIT` to close the `osql` utility.
9. Run the Websense installer again.

Installing with MSDE 2000

Note

If replacing a previous installation of MSDE or changing from an English to a non-English language version of MSDE 2000, you must uninstall the English version of MSDE before installing the non-English version of MSDE.

If the proper version of MSDE is not installed, 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`.

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 *Common component installation procedures*, page 32.

> **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 trusted connection (Windows Authentication) to 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 when MSDE as the database engine.

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 installation and initial configuration issues that have been submitted to Websense Technical Support. Review this appendix for information about your problem before contacting Technical Support.

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

For other possible solutions, see the Websense Knowledge Base: www.websense.com/kb.

If you still need to contact Technical Support, see *Appendix D: Contacting Technical Support* for contact information.

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 on the Websense Support Portal, www.websense.com/kb, for a list of default port numbers. Search for the exact phrase `default port numbers`.

Where can I find download and error messages?

Windows

Check for any listings about the Master Database download and other error or status messages in the Windows Application Event log, or the `Websense.log` file, located in `<install_path>\bin`. The default installation path is `C:\Program Files\Websense`.

1. Access the Application Event log by choosing **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
2. Expand the **Event Viewer** tree.
3. Click **Application Log**.

The `Websense.log` file can be viewed in a standard text editor.

Linux

Websense software creates `Websense.log` (located in `opt/Websense/bin`) when there are errors to record. This log file records error messages and messages pertaining to database downloads. `Websense.log` is located on the Policy Server machine only.

The `Websense.log` file can be viewed in a standard text editor.

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. Open a command prompt on the Linux machine.
2. Enter `service iptables status` to determine if the firewall is running.
3. If the firewall is running, enter `service iptables stop`.

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 support Network Agent and the firewall software.

Remember to restart the firewall when the installation is complete.

1. Open a command prompt.
2. Enter `service iptables start`.
3. Enter `service iptables status` to verify that the firewall is running.

I forgot my WebsenseAdministrator password

Go to www.websense.com/forgotmypassword for assistance.

The Master Database does not download

The disk partition on the download 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 are preventing Websense Master Database downloads.

See Websense Manager Help for instructions on resolving these problems.

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 try another Websense installation.

Network Agent in Linux fails to start with stealth mode NIC

Possible causes and solutions for this problem are described below.

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 accidently selected a stealth mode NIC for communications, Network Agent cannot start, and Websense services cannot work.

1. Open the `websense.ini` file in a text editor. The file is located in Websense installation directory, `opt/Websense/bin`, by default.
2. Change the IP address to that of a NIC in normal mode.
3. Open a command prompt and navigate to the `/Websense` directory.
4. Run this 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. This situation 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 running the installation on Linux

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

To resolve this problem:

1. Stop all Websense services:
   a. From a command prompt, go to the `/Websense` directory.
   b. Run this command: `./WebsenseAdmin stop`
2. Navigate to the root directory.
3. Delete the `/opt/Websense` directory by running the following command:
   `rm -fr /opt/Websense`
4. Navigate to the `/etc` directory.
5. Delete the `Websense` file by running this command:
   `rm /etc/Websense`
6. Kill all Websense processes:
   a. Locate all Websense processes: `ps -ef | grep Websense`
   b. Run `kill -9` on all Websense processes.
7. 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`*
      where *`ipaddress`* is the machine's IP address, and *`mymachinename`* and *`mydomain`* are the machines name and domain.
      To find the IP address, run this command: `ifconfig`
   b. Save the `hosts` file.
8. Run the `hostname` command.
   `hostname` *`mymachinename.mydomain`*`.com`
9. Restart the network service:
   `service network restart`
10. Run the Websense installer again.

D Contacting Technical Support

Websense, Inc., is committed to providing excellent service worldwide. Our goal is to provide professional assistance in the use of our software wherever you are located.

Online Help

Select the **Help** option within the program to display detailed information about using the product.

Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

Technical Support

Technical information about Websense products is available online 24 hours a day, including:

- latest release information
- searchable Websense Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the Web site at:

www.websense.com/SupportPortal/

For additional questions, fill out the online support form at:

www.websense.com/SupportPortal/Contact.aspx

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.

Location	Contact information
North America	+1 858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 57 32 32 27
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 51 70 93 47
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
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	Contact your Websense Reseller.

For telephone requests, please have ready:

- Websense subscription key
- Access to Websense Manager
- Access to the machine running Filtering Service, the machine running reporting tools, and the database server (Microsoft SQL Server or MSDE)
- Permission to access the Websense Log Database
- Familiarity with your network's architecture, or access to a specialist
- Specifications of machines running Filtering Service and Websense Manager
- A list of other applications running on the Filtering Service machine

Index

I

L

M

N