Installation Guide Supplement

for use with

Microsoft® ISA Server

Websense® Web Security
Websense Web Filter

v7

Installation Guide Supplement for Microsoft ISA Server

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

Published 2008
Printed in the United States of America and Ireland.

Trademarks

WinPcap

Contents

1 Microsoft ISA Server Integration

This supplement provides additional information for installing and setting up Websense® Web Security™ or Websense Web Filter™ with Microsoft® Internet Security and Acceleration (ISA) Server.

See the *Websense Web Security and Websense Web Filter Installation Guide* for basic instructions.

An integration with Microsoft ISA Server impacts some Websense components:

- **ISAPI Filter plug-in**: This additional Websense component is installed on the machine running ISA Server. The Websense ISAPI Filter configures ISA Server to communicate with Filtering Service.
- **Filtering Service**: Interacts with ISA Server and Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.

  After the Filtering Service is installed, the ISAPI Filter must be installed on every ISA Server machine in your network.

  If Websense software is installed on the same machine as ISA Server, the Websense ISAPI Filter must be installed on that machine at the same time.
- **Network Agent**: Internet protocols that are not managed by the ISA Server are managed by Network Agent. It can detect HTTP network activity and instruct the Filtering Service to log this information.

  Important

  Do *not* install Network Agent on the machine running ISA Server.

- **Transparent identification agents**: Generally, ISA Server provides user authentication information for Websense software. If ISA Server is not configured to provide user information to Websense software, install the appropriate Websense transparent identification agent. See the *Websense Web Security/Web Filter Deployment Guide* for more information on these agents.

If your environment includes an array of ISA Server machines, the preferred configuration is to install Websense software on a machine outside of the array.

How Websense filtering works with ISA Server

To be filtered by Websense software, a computer must access the Internet through ISA Server.

When ISA Server receives an Internet request from a user, it queries Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service checks the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies ISA Server that the site is not blocked, and the client is allowed to see the site.

Supported integration versions

- Microsoft ISA Server 2004, Standard Edition and Enterprise Edition
- Microsoft ISA Server 2006, Standard Edition and Enterprise Edition

Supported ISA Server clients are:

- Firewall Client for ISA Server
- SecureNAT clients
- Web Proxy clients

Installation

You may install Websense components together with the ISAPI Filter, on the machine running the ISA Server, provided the machine has sufficient resources.

Refer to Chapter 3 of the Websense *Installation Guide* for basic instructions on downloading and installing the Websense software.

When running the Websense installer:

- Leave ISA Server running during the Websense installation.
- Select a **Custom** installation.
- From the components list, select **Filtering Plug-in** and any other Websense components that you would like to install on the ISA Server machine.

  Do **not** install Network Agent on the same machine as the ISAPI Filter. Network Agent must be installed on another machine.

- Select **Integrated** as the integration option, and select **Microsoft Internet Security and Acceleration Server** as the integration product.
- Select an ISA Server installation option:
  - **Install plug-in and other selected Websense components**: Installs Websense components and the ISAPI Filter plug-in together. Choose this option to install Websense filtering components (Policy Broker, Policy Server, Filtering Service, User Service, ISAPI Filter, etc.) on the same machine as ISA Server.

    Important

    Install the Filtering Service and the ISAPI Filter together if you are installing Websense software on the ISA Server machine. You cannot add the plug-in separately once Filtering Service has been installed.

    The installer checks for ISA Server on the installation machine. If ISA Server is detected, the installer continues.

    If ISA Server is not detected, an error message appears advising you that the ISAPI Filter can only be installed on the machine if ISA Server is present. Click **OK** to return to the integration option, or click **Next** to exit the installer.
  - **Install plug-in only**: Installs only the ISAPI Filter on the machine running ISA Server.

    Important

    Install the plug-in on every ISA Server machine in your network.

    In distributed environments, be sure to install the plug-in *after* installing Filtering Service.

  - **Install selected Websense components without plug-in**: Installs only the Websense components that have been selected and not the ISAPI Filter. Choose this option when installing Websense components on machines not running ISA Server.

    Note

    No services are restarted for ISA Server 2004 or ISA Server 2006 *while* the Websense installation is running.

- Follow the onscreen instructions to complete the installation. Refer to the Websense *Installation Guide* for more information.
- Manually restart the ISA Server from its management console after the Websense installation is complete.

Testing visibility of Internet traffic to Network Agent

If you installed Network Agent and have any doubt about its ability to monitor Internet requests from the desired network and to see the replies, you can conduct a traffic visibility test on the Network Agent machine using the Websense Network Traffic Detector. See Websense Manager Help for instructions.

Upgrade

- Upgrade the Filtering Service before upgrading the ISAPI Filter. This ensures proper communication between Filtering Service and ISA Server.
- To upgrade the ISAPI Filter, run the Websense installer on the ISA Server machine and follow the onscreen instructions.
- If you are upgrading your Websense system and migrating from Microsoft Proxy Server to ISA Server, see *Migrating between Microsoft integration products*, page 16.

  This version of Websense software does not support an integration with Microsoft Proxy Server.

Converting to an integrated system

You can convert an existing Websense Stand-Alone Edition to a Websense system that is integrated with ISA Server, without losing any configuration settings. The conversion process preserves such settings as policies, port numbers, and IP addresses.

Tasks

Task 1: Upgrade to the current version of Stand-Alone Edition. See the Websense *Installation Guide* for instructions.

Task 2: Restart the installation machine.

Task 3: Uninstall and reinstall Filtering Service.

If Websense software, including Network Agent, is running on the machine on which ISA Server will be installed, then Network Agent must be moved to another machine.

See the *Installation Guide* for instructions on removing components and installing them separately.

Warning

Use caution when removing Websense components. Removing Policy Server deletes all existing configuration settings. If you accidently remove Policy Server, use the backup files created in the following procedures to restore your system.

Task 4: Convert the Stand-Alone Edition to a system integrated with ISA Server.

The procedure depends on where Websense software is installed:

- If Websense software is running on a different machine than ISA Server, follow the procedures in *Converting to an integrated system on a separate machine*, page 9.
- If Websense software is running on the same machine as ISA Server, follow the procedures in *Converting to an integration on the same machine*, page 11.

Task 5: Complete the setup tasks, as described later in this supplement.

Task 6: Enable authentication so that users can be properly identified and filtered. For instructions, see *Chapter 2: Authentication*.

Converting to an integrated system on a separate machine

After you have upgraded your existing Stand-Alone Edition to the current Websense version, you can convert Websense software to integrate with ISA Server running on a separate machine.

When ISA Server is running on a different machine than the Websense software, you must remove the existing Filtering Service, reinstall it to integrate with ISA Server, and then install the ISAPI Filter on the machine running ISA Server.

See the Websense *Installation Guide* for instructions on backing up files, removing components, and running the installer.

Upgrade Websense and remove Filtering Service

1. If you have not done so, upgrade your Websense software.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See Websense Manager Help for instructions.
3. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
4. Go to **Start >Settings >Control Panel > Add or Remove Programs**.
5. Select **Websense**, and click **Change/Remove**.

   The Websense uninstall program starts.

6. Make sure that only **Filtering Service** is selected in the Remove Components screen, and click **Next**.
7. Follow the prompts to complete the removal process.
8. When prompted, select **Yes** to restart the machine. Then, click **Finish**.

Reinstall Filtering Service

After Filtering Service is removed, reinstall it to integrate with ISA Server.

1. Stop any anti-virus programs on the machine running Filtering Service.
2. Start the Websense installer.
3. Click **Next** in the Welcome screen to access the Add/Remove screen.
4. Select **Add Websense components**, and click **Next**
5. Select **Filtering Service**, and click **Next**.
6. Select **Integrated** as the integration option, and click **Next**.
7. Select **Microsoft Internet Security and Acceleration Server** as the integration type, and click **Next**.
8. Select **Install selected Websense components without plug-in**, and click **Next**
9. Complete the installation on the Websense machine, as described in the *Installation Guide*.
10. After restarting the machine, go to the Windows Services dialog box to verify that Websense Filtering Service has started.
11. If you stopped your anti-virus software, start it again.

Install the Websense ISAPI Filter

Next, install the ISAPI Filter on the ISA Server machine. This plug-in allows Websense software and ISA Server to communicate.

1. Log on to the ISA Server machine.
2. Run the Websense installer.
3. Select a **Custom** installation, and click **Next**.
4. Select **Filtering Plug-in**, and click **Next**.
5. Select **Microsoft Internet Security and Acceleration Server**, and click **Next**.
6. Enter the **IP Address** for the machine running Filtering Service.

   The **Filter Port** is the port on which Filtering Service communicates. The default port number (15868) is displayed. If a different port was designated for Filtering Service, enter that port number.
7. Follow the onscreen instructions to complete the installation.

Converting to an integration on the same machine

After you upgrade Stand-Alone Edition, you can convert Websense software to integrate with the ISA Server installed on the same machine.

To convert a Websense Stand-Alone Edition to an integrated system, Websense Filtering Service and Network Agent must be removed and then reinstalled after ISA Server is installed. See the Websense *Installation Guide* for complete instructions on running the installer, upgrading, and removing components.

> **Note**
> Internet requests are not filtered until this process is completed.

1. If you have not done so, upgrade your Websense software.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See Websense Manager Help for instructions
3. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
4. Go to Start > Settings > Control Panel > Add or Remove Programs.
5. Select **Websense**, and click **Change/Remove**.

   The Websense uninstall program starts.
6. Make sure that only **Filtering Service** and **Network Agent** are selected for removal, and click **Next**.
7. Follow the onscreen instructions to remove the components.
8. When prompted, select **Yes** to restart the machine. Then, click **Finish**.

After Network Agent and Filtering Service are removed, you can install ISA Server. See the Microsoft documentation for instructions on installing ISA Server.

After ISA Server is installed, run the Websense installer to reinstall Filtering Service and install the plug-in. Then, install Network Agent on a separate machine.

1. On the ISA Server machine, stop any anti-virus programs on the installation machine.
2. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
3. Start the Websense installer.
4. Select **Add Websense Components**, and click **Next**.
5. Select **Filtering Service** and **Filtering Plug-in**, and click **Next**.
6. Select **Integrated**, and click **Next**.
7. Select **Microsoft Internet Security and Acceleration Server**, and click **Next**.

   If prompted, manually stop the Websense services noted.
8. Follow the onscreen instructions to complete the installation.

9. After restarting the machine, go to the Windows Services dialog box to verify that Websense Filtering Service has started.
10. If you stopped your anti-virus software, start it again.
11. On a separate machine, install Network Agent. Follow the instructions for installing individual components in Chapter 3 of the *Installation Guide*.

Initial Setup

- To use Websense filtering in a network that uses SOCKS or WinSOCK proxy server, see *WinSOCK and SOCKS proxy servers*, page 12, for instructions.
- Additional configuration of the Websense ISAPI Filter is required if you are using non-Web proxy clients with ISA Server 2004 or ISA Server 2006. These ISA Server clients include the Firewall Client with proxy server disabled, and SecureNAT clients.

  See *Configuring for ISA Server using non-Web proxy clients*, page 13, for instructions.
- To configure Websense software to ignore certain traffic based on the user name, host name, or URL, see *Configuring Websense software to ignore specific traffic*, page 14, for instructions.
- If Network Agent was installed, configure Network Agent with the IP addresses of all proxy servers through which computers route their Internet requests. See the Network Configuration topic in Websense Manager Help for instructions.

WinSOCK and SOCKS proxy servers

Websense software filters HTTP, HTTPS, and FTP requests sent to ISA Server, but *cannot* filter traffic tunneled over a SOCKS or WinSOCK proxy server.

The Firewall Client replaced these proxy servers after ISA Server 2000. To use Websense filtering in a network that uses a SOCKS or WinSOCK proxy server, you can either:

- Disable the WinSOCK or SOCKS service.
- Use the WinSOCK or SOCKS proxy client to disable the specific protocols that you want Websense software to filter (HTTP, HTTPS, and FTP), then configure browsers on client computers to point to ISA Server for each of these protocols.

  For information about disabling a protocol, see the ISA Server online help.

Note

Ensure that TCP/IP stacks are installed on all the client computers if protocols have been disabled on the SOCKS or WinSOCK proxy server, and sent through the normal proxy server for filtering by Websense software.

Configuring for ISA Server using non-Web proxy clients

If you are using non-Web proxy clients with ISA Server 2004 or ISA Server 2006, additional configuration is required so that Websense software can filter Internet requests correctly. The term non-Web proxy clients refers to:

- Firewall Client with the proxy server disabled
- SecureNAT clients

Firewall Client

If you are using Firewall Client with ISA Server 2004 or ISA Server 2006, and the proxy server is enabled (default setting), Websense software filters Internet requests normally.

However, if the proxy server is disabled, Websense software cannot filter Internet requests without additional configuration.

Check the Firewall Client machine to see if the proxy server is disabled.

1. Open the Firewall Client configuration screen, and select the **Web Browser** tab.
2. View the **Enable Web browser automatic configuration** check box.
   - If it is marked, the proxy server is enabled. Websense software requires no additional configuration.
   - If it is cleared, the proxy server is disabled. See *Configuring the ISAPI Filter*, page 13, for additional configuration steps.

SecureNAT Clients

SecureNAT clients require that you configure the default gateway so that all traffic to the Internet is sent through the ISA Server. If you need information about configuring and using SecureNAT clients, see your ISA Server online help.

See *Configuring the ISAPI Filter*, page 13, for additional configuration steps.

Configuring the ISAPI Filter

If you are using the ISA Server Firewall Client with the proxy server disabled, or SecureNAT clients, the ISAPI Filter must be configured to ignore requests going directly to the ISA Server and to filter only those requests going out to the Internet.

1. On the ISA Server machine, create a file called `ignore.txt` in the `WINDOWS\system32` directory.
2. Enter the host name or IP address of the ISA Server machine in the text file.

   Host names must be entered in ALL CAPS. Entries that are not in all capital letters are not used.

3. If the ISA Server hosts multiple Web sites, add the names of all the Web sites being hosted. For example: `webmail.rcd.com`.

   If only one Web site is hosted, do not add it to this file.

4. Restart the ISA Server machine.

Configuring Websense software to ignore specific traffic

You can configure the ISAPI Filter to bypass both filtering and logging for certain traffic, based on the user name, host name, or URL. This may be used for a small group of Web sites or users, or for machines in a complex proxy array or proxy chaining configuration.

To prevent filtering and logging of this traffic, add the user names, host names, and URLs that you do not want Websense software to filter to the `isa_ignore.txt` file.

1. On the ISA Server machine, open the `isa_ignore.txt` file in a text editor. This file is located in the `WINDOWS\system32` directory.

   Important

   The default `isa_ignore.txt` file installed during a Websense upgrade or installation contains the following URL:

   ```
   url=http://ms_proxy_intra_array_auth_query/
   ```

   Do **not** delete this URL. It is used by ISA Servers in a CARP array for communication. This URL must be ignored by Websense software to allow filtering and logging to work properly when multiple ISA Servers are deployed in an array.

2. Enter each user name, host name, or URL that you want Websense software to ignore. Enter each item on its own line in the file, using the formats below.

   Important

   You must enter each user name, host name, or URL in the exact same format that ISA Server passes it to Filtering Service.

   - **User name**: Enter the name of a user whose Internet requests should not be filtered or logged by Websense software:

     `username=`<*`user_name`*>

     Examples:

     `username=jsmith`

     `username=domain1/jsmith`

- **Host name**: Enter a destination host name that Websense software should not filter or log user visits to:

  hostname=<*host_name*>

  Example:

  hostname=yahoo.com

- **URL**: Enter a URL that Websense software should not filter or log user visits to:

  url=<*URL*>

  Example:

  url=http://mail.yahoo.com/

  url=mail.yahoo.com/

> **Note**
> To assure that the correct format is available for all situations, it is recommended that you enter the same name in all available configurations. For example, make 2 entries for user name: one with and one without the domain. Make 2 entries for URL: one with and one without the protocol.

3. Restart the ISA Server machine.

Client computer configuration

Internet browsers on client computers should be configured to use ISA Server to handle HTTP, HTTPS, and FTP requests.

An exception to this configuration is browsers in an ISA Server environment using Firewall Clients or SecureNAT. These browsers must point to the same port, 8080, that ISA Server uses for each protocol.

See the browser online help for configuration instructions.

Firewall configuration

To prevent users from circumventing Websense filtering, configure your firewall or Internet router to allow outbound HTTP, HTTPS, and FTP requests only from ISA Server.

Contact your router or firewall vendor for information about configuring access lists on the router or firewall.

Important

If Internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

Migrating between Microsoft integration products

You can migrate from Microsoft Proxy Server to ISA Server, and keep your Websense configuration settings. This must be done prior to installing or upgrading Websense software. This version of Websense does not support an integration with Microsoft Proxy Server.

- If Websense software is not already installed:
  - Complete the installation of ISA Server before beginning the Websense installation.
  - Install Websense software following the instructions in the Websense Installation Guide, plus the instructions in this supplement. See *Installation*, page 6.
- If a previous version of Websense is installed:
  - Follow the migration procedures in the *Websense Installation Guide for use with Integrated Microsoft Products* for the installed version.
  - Follow the upgrade procedures for the new version of Websense software.

2 Authentication

Authentication is the process of identifying an individual within a network who has an account in a directory service. Depending on the authentication method selected, ISA Server can obtain user identification and send it to Websense Filtering Service with the Internet request. Filtering Service can filter requests based on policies assigned to individual directory objects, defined as either a user or group of users.

> **Note**
>
> In any environment, Websense software can filter based on computer or network policies. computers are identified in Websense software by their IP addresses, and networks are identified as IP address ranges.

To filter Internet access for individual directory objects, Websense software must be able to identify the user making the request. To implement user-based filtering, do one or more of the following.

- Enable an authentication method within ISA Server so that it sends user information to Websense software.
- Enable Websense software to identify users transparently, if it does not receive user information from ISA Server. You can install one of the Websense transparent identification agents: DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent.

  See the Websense *Deployment Guide* and the User Identification topic in Websense Manager Help for more information.
- Enable manual authentication within Websense software. If users cannot be identified transparently, they are prompted to log on when opening a browser.

  See the Manual Authentication topic in Websense Manager Help for more information.

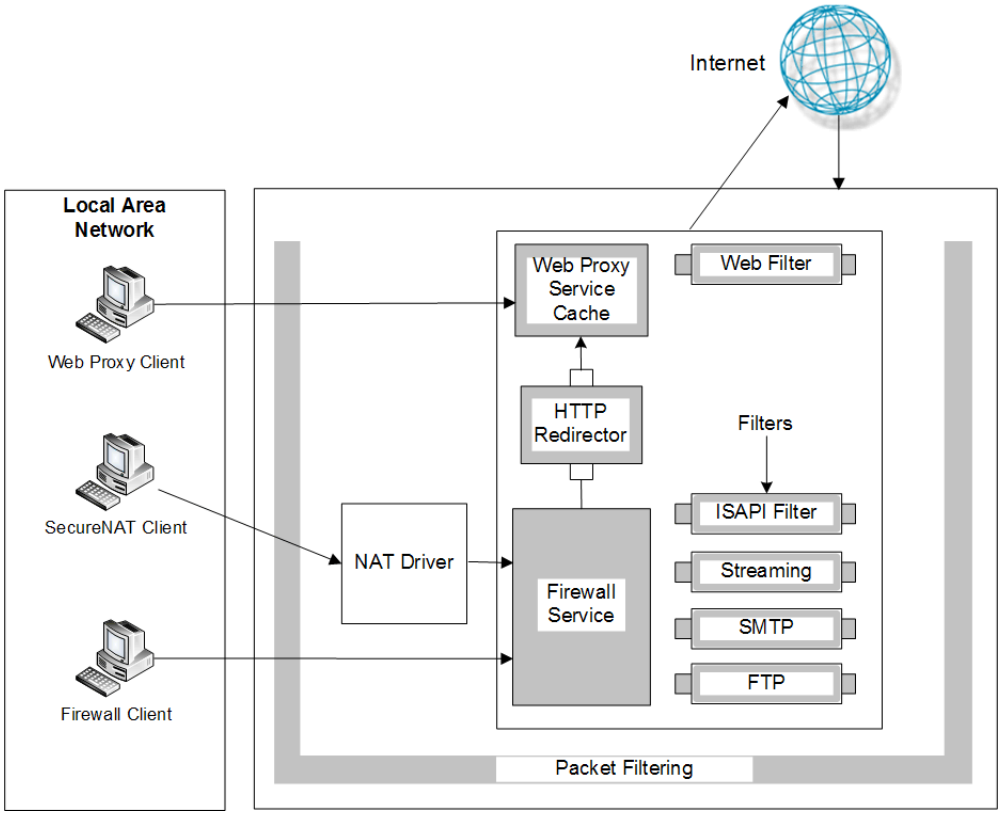
This chapter discusses authentication methods available within ISA Server. It also provides instructions for enabling an authentication method that identifies users transparently and sends the information to Websense software along with the Internet request.

ISA clients

These ISA clients are supported:

- Firewall
- SecureNAT
- Web Proxy

The term *clients* in this environment refers to computers or applications that run on computers and rely on a server to perform some operations. In the following diagram of Microsoft ISA Firewall architecture, the relationship between ISA Server and the Firewall, SecureNAT, and Web Proxy clients is shown.



Microsoft ISA Firewall Architecture

Each type of client can be configured so that Websense software can obtain user identification and filter Internet requests based on user and group policies.

Firewall and SecureNAT clients

Firewall and SecureNAT clients cannot identify users transparently without special settings. These clients require a Websense transparent identification agent to authenticate users. To enable user-based filtering policies with these clients, select one of these options:

- Configure computer browsers to access the Internet through ISA Server. This configuration allows Firewall and SecureNAT clients to also work as Web Proxy clients.

  If you choose this option, see *Web Proxy clients* for more information.

- If you are using a Windows-based directory service, disable all authentication methods within ISA Server and use Websense transparent identification. This method allows Websense Filtering Service to obtain user identification from the network's domain controllers or directory services.

  See *Transparent identification*, page 22 for more information.

- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither the ISA Server nor a Websense transparent identification agent provides the information.

  See the Manual Authentication topic in Websense Manager Help for more information.

Web Proxy clients

After the browser is configured to use the ISA Server as a proxy server, Web Proxy clients send Internet requests directly to the ISA Server. You can assign individual user or group policies with one of the following methods.

- If your network uses only Microsoft Internet Explorer® browsers, version 5.0 or later, you can enable Integrated Windows Authentication within ISA Server to identify users transparently.
- If you are using a Windows-based directory service with various browsers, you can identify users transparently by disabling all authentication methods within ISA Server and implementing Websense transparent identification.

  See *Transparent identification*, page 22, for more information.

- If the network uses a mixture of browsers, you can enable one or more of ISA Server's authentication methods. Some of these methods may require users to authenticate manually for certain older browsers.

  See *Authentication Methods*, page 20, for more information.

- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither ISA Server nor a Websense transparent identification agent provides the information.

  See the Manual Authentication topic in Websense Manager Help for more information.

Authentication Methods

ISA Server provides four methods of authentication:

- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication*
- *Client Certificate authentication*

Microsoft Internet Explorer, version 5.0 and later, supports all of these authentication methods. Other Web browsers may support only the Basic authentication method. By default, ISA Server has Integrated Windows authentication enabled.

You can configure both incoming and outgoing request properties within ISA Server. Client Web browsers must be able to use at least one of the authentication methods that you specify in an array's incoming and outgoing Web request dialog boxes. Without this authentication, the client cannot access the requested Internet site.

When no authentication method is enabled in the ISA Server, it cannot receive any information about who is making the Internet request. As a result, Websense software does not receive user information from ISA Server. When this problem occurs, you can:

- Filter with computer and network policies.
- Enable Websense manual authentication to permit user-based filtering.

  See the Manual Authentication topic in Websense Manager Help for more information.
- Enable Websense transparent identification to permit user-based filtering.

  See *Transparent identification*, page 22, for more information.

Basic authentication

Basic authentication prompts users to authenticate (log on) each time they open a browser. This authentication allows ISA Server to obtain user identification, regardless of the browser, and send the information to Websense software, which filters Internet requests based on individual user and group policies.

If Basic authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted to for a user name and password.

Digest authentication

Digest authentication is a secure authentication used in Windows Server 2003 domains. The features are the same as Basic authentication, but the user name and password are scrambled when they are sent from the browser to the ISA Server. The user can authenticate to ISA Server without the user name and password being intercepted. User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

If Digest authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, ISA Server obtains user identification transparently from browsers using Microsoft Internet Explorer 5.0 and later. User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Integrated Windows authentication, or Digest and Integrated Windows authentication. In either configuration:

- Users with Microsoft Internet Explorer browsers are identified transparently.
- Users with other browsers are prompted for a user name and password.

Note

To transparently identify all users in a mixed browser environment, you can disable Basic or Digest authentication and use Websense transparent identification (see *Transparent identification*, page 22) in conjunction with Integrated Windows authentication.

Client Certificate authentication

Client Certificate authentication identifies users requesting information about a Web site. If Client Certificate is used, ISA Server requests the certificate and verifies that it belongs to a client that is permitted access, before allowing the Internet request.

> **Note**
>
> To use Websense transparent identification, you must disable Client Certificate authentication.
>
> Before changing authentication methods, consider the impact of the change on other ISA Server functions.

For more information about ISA Server authentication and how to configure these authentication methods, see your ISA Server online help.

Transparent identification

Websense transparent identification allows Websense software to filter Internet requests from users identified in a directory service, without prompting them to authenticate manually. If the authentication method enabled within ISA Server does not send user information to Filtering Service, you can use a Websense transparent identification agent to identify users.

For example, if ISA Server is configured to obtain user identification from the browser, and you want to use Network Agent to filter protocols by user or group name, use a Websense transparent identification agent to identify users for protocol traffic.

Install and configure Websense transparent identification agents to transparently identify users from a directory service. DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent can be installed on the same machine as Filtering Service, or on a different machine. See the Websense *Deployment Guide* more information.

Websense also offers secure manual authentication with Secure Sockets Layer (SSL) encryption to protect user names and passwords being transmitted between client computers and Filtering Service. By default, secure manual authentication is disabled. See the Secure Manual Authentication topic in Websense Manager Help for more information and instructions on activating this feature.

After Filtering Service is configured to communicate with a transparent identification agent, user information is obtained from a supported directory service and sent to Filtering Service. When Filtering Service receives the IP address of a computer making an Internet request, the address is matched with the corresponding user name provided by the transparent identification agent.

See the Websense *Installation Guide* for instructions on installing individual Websense components. See the User Identification topic in Websense Manager Help for information about configuring transparent identification agents.

A Troubleshooting

SecureNAT clients are not being filtered

If you are using non-Web proxy clients (i.e., Firewall Client with proxy server disabled, or SecureNAT clients) with ISA Server 2004 or ISA Server 2006, additional configuration of the Websense ISAPI filter is required. Follow the instructions in *Configuring for ISA Server using non-Web proxy clients*, page 13.

Internet requests are not filtered after the Websense ISAPI Filter is installed

Users are still not being filtered after the Websense ISAPI Filter has been installed on the machine running the ISA Server.

- If the ISAPI Filter is the only Websense component installed on the integration machine, the plug-in may not be communicating with the Websense filtering components installed on other machines. Verify that the ISAPI Filter is pointing to the correct IP address and port for the machine running Filtering Service.
  1. In the `C:\windows\system32` directory, look at this file: `wsMSP.ini`.
  2. In the `[initSection]`section, check the `EIMServerIP` and `EIMServerPort` parameters. For example:

     ```
     [initSection]
     EIMServerIP=10.203.136.36
     EIMServerPort=15868
     ```

     The default port number is 15868.
- If other Websense components are installed on the same machine as ISA Server and the plug-in, try restarting the Microsoft Firewall service.

  Verify an ISA firewall rule allows access to Filtering Service on the Filter port (default 15868).
- If some Websense components are installed on the integration machine, while others are installed on a separate machine, be sure the proper ports are open for communication.

  Refer to the help in the ISA Server Management console for instructions on setting a port.

  Refer to the Websense Knowledge Base on the Websense Support Portal, www.websense.com/SupportPortal/, for a list of default port numbers. Search for the exact phrase `default port numbers`.

Index

U

V

W