Using RADIUS Agent for Transparent User Identification

Websense RADIUS Agent works together with the RADIUS server and RADIUS clients in your network to process and track Remote Access Dial-In User Service (RADIUS) traffic.

Websense RADIUS Agent enables TRITON RiskVision to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection (depending on your configuration).

This collection includes the following topics to help you understand how RADIUS Agent works, configure RADIUS Agent, and troubleshoot user identification issues.

Processing RADIUS traffic

RADIUS Agent acts as a proxy that forwards RADIUS messages between a RADIUS client and a RADIUS server (or multiple clients and servers, depending on the network configuration). RADIUS Agent does not authenticate users directly. Instead, the Agent identifies remote users authenticated by a RADIUS server and associates them with IP addresses, so TRITON RiskVision can report on users' activity.

When properly configured, RADIUS Agent captures and processes RADIUS protocol packets of the following types:

- **Access-Request:** Sent by a RADIUS client to request authorization for a network access connection attempt.
- **Access-Accept:** Sent by a RADIUS server in response to an Access-Request message; tells the RADIUS client that the attempted connection is authorized and authenticated.
- **Access-Reject:** Sent by a RADIUS server in response to an Access-Request message; tells the RADIUS client that the attempted connection is rejected.
- **Accounting-Stop-Request:** Sent by a RADIUS client to tell the RADIUS server to stop tracking activity for a specific user.

RADIUS authentication and accounting

Each RADIUS message packet contains attributes that describe the connection attempt, such as user name, password, and IP address of an access server. Websense RADIUS Agent stores user name-to-IP-address pairings in a user map, and provides this information to Websense Filtering Service.

If your RADIUS client supports accounting (user logon tracking), and accounting is enabled, RADIUS Agent is able to extract more details about user logon sessions from the RADIUS messages it receives.

For example, if there is no static IP address for an authenticated remote user, a dynamic IP address is assigned to that user. RADIUS Agent receives the dynamic IP address via an accounting request from the RADIUS client, and then records the resulting user name/IP address entry in its user map.

Stop accounting requests tell the RADIUS server to stop tracking logon activity for a particular user. The stop accounting request process is as follows:

1. RADIUS Agent receives a RADIUS stop accounting message.
2. RADIUS Agent extracts the user name and IP address from the request, and tells the RADIUS Agent service to remove the matching entry from its map.

The RADIUS user identification process

Websense RADIUS Agent works with the RADIUS server and RADIUS client in your network to process and track Remote Access Dial-In User Service (RADIUS) protocol traffic. This enables you to assign particular policies to users or groups of users who access your network remotely, as well as to local users.

Note

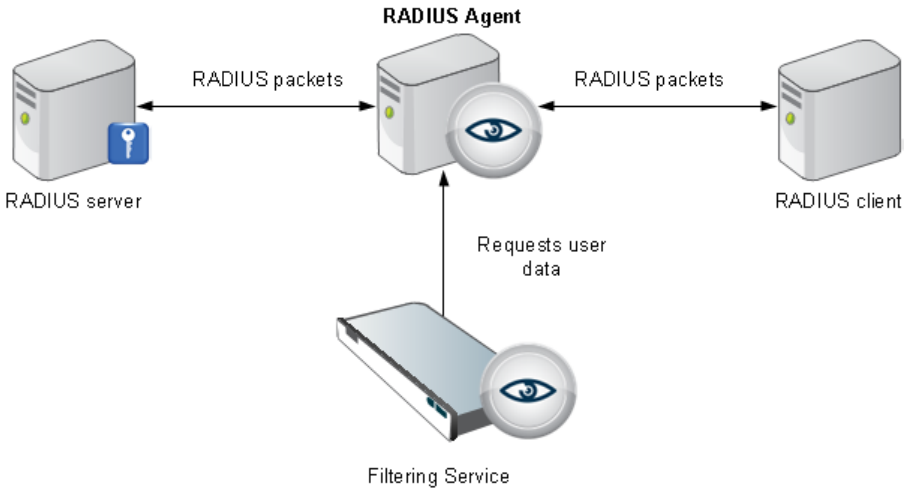
Websense, Inc., recommends installing RADIUS Agent on a machine separate from the RADIUS server machine. This prevents port and IP address conflicts between RADIUS Agent and the RADIUS server.

Without Websense RADIUS Agent, remote users are authenticated by a RADIUS client (RAS server, VPN server, or firewall).

The authentication process without RADIUS Agent is as follows:

1. A user logs on to the network from a remote machine.
2. The RADIUS client receives an authentication request for that user.
3. The RADIUS client contacts the RADIUS server via the default RADIUS ports (1645 for authentication, and 1646 for accounting), and sends the user name and password to the RADIUS server.
4. The RADIUS server validates the user name/password combination by checking it against the directory service, and then responds to the RADIUS client.

With Websense RADIUS Agent in place in your network, the user authentication process allows the agent to process and transmit remote authentication requests and provide user information to Filtering Service.



The transparent identification process is as follows:

1. RADIUS Agent listens on port 1645 (the RADIUS authentication port) for authentication requests and detects users logging on to domains, or logging on to the RADIUS server directly.

Note

If you are using RADIUS authentication in a specific Windows domain, run the Websense RADIUS Agent service as a domain user, or as the default System account on a machine in that domain.

2. When a remote user logs on to the network, the RADIUS client receives an authentication request and contacts the RADIUS Agent machine via port 1645.

3. RADIUS Agent extracts the authentication request ID (a unique identifier), user name, and originating IP address and stores the data in a user name-to-IP-address map in local memory, and in the **RadiusAgent.bak** file.

Note

If RADIUS Agent receives a new request from an IP address already included in its user map, it **replaces** the existing pair with the new pair.

4. After extracting the required information, RADIUS Agent forwards the authentication request to the RADIUS server.
5. The RADIUS server checks the user name and password entered against the corresponding account in the directory service, and then sends a response to RADIUS Agent indicating the status of the authentication request.

Note

To configure the amount of time RADIUS Agent waits for a response from the RADIUS server before ending a query attempt, modify the **Timeout** parameter in the RADIUS configuration file (**wsradius.ini**).

For more details, see *Custom configuration for a RADIUS Agent instance*, page 11, and *RADIUS Agent initialization parameters*, page 11.

6. RADIUS Agent evaluates the response from the RADIUS server. If the RADIUS message received is an authentication **rejection**, RADIUS Agent removes the corresponding entry from its user map.

   If the RADIUS packet received is an authentication **acceptance**, RADIUS Agent copies the corresponding entry to its main user map (a listing of full domain/user name/IP address entries).
7. RADIUS Agent forwards the authentication response to the RADIUS client.
8. RADIUS Agent sends user names and IP addresses to Filtering Service each time its user map is updated, using port 30800. Filtering Service records user name/IP address pairs to its own copy of the user map in local memory. No confidential information (such as user passwords) is transmitted.

Note

If you configure RADIUS Agent to require authentication, the RADIUS Agent service checks the password provided by Filtering Service against the password you specified on the Settings .> General > User Identification page in the management console. See *Configuring RADIUS Agent settings*, page 8.

9. Filtering Service queries User Service to get group information for user names in its copy of the user map. User Service queries the directory service for group information corresponding to those users, and sends the information to Filtering Service.

10. Filtering Service assigns policies to logged-on users and includes user name information in log records forwarded to Log Server.

Components used for transparent identification with RADIUS Agent

Transparent identification with Websense RADIUS Agent uses the following components.

RADIUS Agent

RADIUS Agent is installed on a Windows Server 2008 R2 or Windows Server 2012 machine.

One instance of Websense RADIUS Agent can support multiple RADIUS clients. Multiple RADIUS Agents can also be used; this may benefit larger networks.

By default, RADIUS Agent listens for authentication requests on the RADIUS authentication port. Filtering Service uses the information provided by RADIUS Agent to apply policies and log requests for remote users logged on to the network.

RADIUS Agent extracts the authentication request ID (a unique identifier), user name, and originating IP address. The Agent stores this data in a user name-to-IP-address map in local memory and in the **RadiusAgent.bak** file.

IP addresses are the key element in tracking logon sessions, because the same user may log on to the network from different locations. In cases where users share an IP address (as with Windows Terminal Services), Websense software may not always be able to identify users.

A RADIUS Agent installation typically includes the following files:

File name	Location	Functionality
RADIUSAgent.exe	C:\Program Files (x86)\Websense\Web Security\bin\	The Websense RADIUS Agent executable. Automatically sends new entries to Filtering Service, when queried. Allows communication of transparent identification configuration from the management console to RADIUS Agent.
wsradius.ini	Websense\Web Security\bin\	Contains RADIUS Agent initialization parameters.

File name	Location	Functionality
RadiusAgent.bak	Websense\Web Security\bin\	Backup copy of RADIUS Agent's user name-to-IP address map. Read at startup.
ignore.txt (optional)	Websense\Web Security\bin\	Contains list of users, machines, and user/machine pairs for RADIUS Agent to ignore.

User Service

User Service interacts with your directory service to get group information corresponding to logged-on users. It provides this information to Filtering Service.

Filtering Service

Filtering Service receives user logon information from RADIUS Agent as users log on to the network. At each transmission, only the record of logon sessions established since the last transmission is sent back to the server. This includes new users logged on to existing remote machines and new users logged on to new remote machines.

Filtering Service receives user data in the form of user name/IP address pairs (originating from RADIUS Agent's map in local memory). When Filtering Service gets the IP address of a machine making an Internet request, the server matches the address with the corresponding user name provided by RADIUS Agent, allowing users to be identified transparently whenever they make Internet requests.

Filtering Service is the destination for the user information RADIUS Agent gleans from authentication requests. When you are troubleshooting user identification problems, be sure to determine whether Filtering Service is getting the latest and most accurate user data.

RADIUS Client

Typically, the RADIUS client is a Network Access Service (NAS) or remote access server, which acts as the point of contact for remote user logons. The client receives authentication requests as users log on, and sends authentication requests to RADIUS Agent for processing.

The RADIUS client sends authentication requests to the port specified in the management console (go to the **Settings > General > User Identification** page in the TRITON RiskVision manager and click a RADIUS Agent instance to view and configure this setting).

These port values are also stored as **AuthInPort** and **AccInPort** in the RADIUS Agent **wsradius.ini** file (see *Custom configuration for a RADIUS Agent instance*, page 11, and *RADIUS Agent initialization parameters*, page 11).

Important

The RADIUS client and server must be configured to communicate via RADIUS Agent.

RADIUS Server

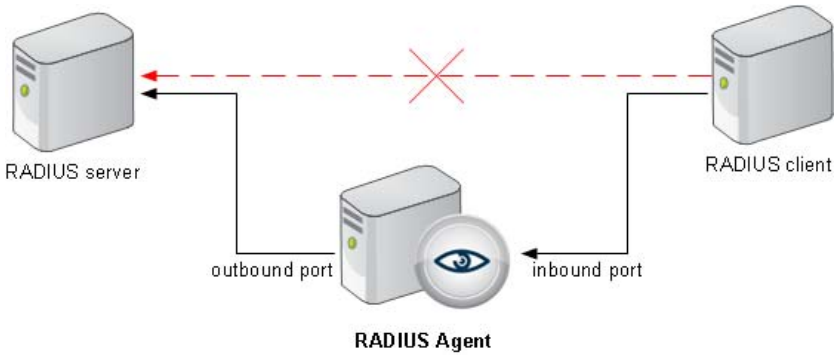
The RADIUS server is typically a service that performs internet authentication, such as the Microsoft Internet Authentication Service (IAS).

The RADIUS server performs the actual user authentication function. The RADIUS server receives authentication requests from Websense RADIUS Agent, and checks the user name and password entered against the corresponding account in the directory service. Finally, the RADIUS server sends a response to RADIUS Agent indicating the status of the authentication request.

RADIUS Agent deployment and configuration

To implement transparent user identification via RADIUS Agent:

- Install RADIUS Agent on a Windows Server 2008 R2 or Windows Server 2012 machine.
- Configure Filtering Service to communicate with RADIUS Agent. (For information about securing communication between the agent and Filtering Service, see *Configuring RADIUS Agent settings*, page 8.)
- Configure the RADIUS client to communicate with Websense RADIUS Agent instead of directly with the RADIUS server. The RADIUS client uses RADIUS Agent as the source of responses to authentication requests.



- Configure RADIUS Agent to forward authentication requests from client machines to the RADIUS server.

- Configure the RADIUS server to use Websense RADIUS Agent as a proxy.

Note

If you use Lucent RADIUS Server and RRAS, you must configure the RADIUS server to use Password Authentication Protocol (PAP), and the RRAS server to accept only PAP requests. For more information, see the related product documentation.

- Use the management consoled to apply policies to directory clients.

Configuring RADIUS Agent settings

Use the **Settings** > **General** > **User Identification** page in the TRITON RiskVision manager to review and edit RADIUS Agent configuration information.

To edit settings for a RADIUS Agent instance:

1. Use the Transparent Identification Agents table to select the IP address or host name of the RADIUS Agent instance that you want to configure.

   If you have installed a new RADIUS Agent instance that does not appear in the list, click **Add Agent**, then select **RADIUS Agent** from the drop-down list.
2. Under Basic Agent Configuration, enter the RADIUS Agent **IPv4 address or host name**.

Note

Hostnames must start with an alphabetical character (a-z), not a numeric or special character.

Hostnames containing certain extended ASCII characters may not resolve properly. To avoid this issue, enter an IP address instead of a hostname.

3. Enter the **Port** that RADIUS Agent should use to communicate with other Websense components. The default is 30800.
4. To establish an authenticated connection between Filtering Service and RADIUS Agent, select **Enable authentication**, and then enter a **Password** for the connection.

Next, customize global RADIUS Agent settings. By default, changes that you make here affect all RADIUS Agent instances. Settings marked with an asterisk (*), however, can be overridden in an agent's configuration file to customize the behavior of that agent instance (see *Custom configuration for a RADIUS Agent instance*, page 11, and *RADIUS Agent initialization parameters*, page 11).

1. Under RADIUS Server, enter the **RADIUS server address or name**. If you provide the IP address, use IPv4 address format.

   RADIUS Agent forwards authentication requests to the RADIUS server, and must know the identity of this machine.

2. If your network includes a RADIUS client, enter the **RADIUS client address or name**. If you provide the IP address, use IPv4 address format.

   Websense software queries this machine for user logon sessions.

3. Enter the **User entry timeout** interval, used to determine how often RADIUS Agent refreshes its user map. Typically, the default query value (24 hours) is best.
4. Use the **Authentication Ports** and **Accounting Ports** settings to specify which ports RADIUS Agent uses to send and receive authentication and accounting requests. For each type of communication, you can specify which port is used for communication between:
   - RADIUS Agent and the RADIUS server (authentication default 1645; accounting default 1646)
   - RADIUS Agent and the RADIUS client (authentication default 12345; accounting default 12346)
5. When you are finished making configuration changes, click **OK** to return to the Settings > User Identification page, then click **OK** again to cache your changes. Changes are not saved until you click **Save and Deploy**.

Configuring the RADIUS client

Your RADIUS client must be configured to transmit authentication and accounting requests to the RADIUS server via RADIUS Agent.

Modify your RADIUS client configuration so that:

- The RADIUS client sends authentication requests to machine and port on which RADIUS Agent listens for authentication requests. This is the **Authentication Port** specified during RADIUS Agent configuration.
- The RADIUS client sends accounting requests to the machine and port on which RADIUS Agent listens for accounting requests. This is the **Accounting Port** specified during RADIUS Agent configuration.

The exact procedure for configuring a RADIUS client differs by client type. For details, see your RADIUS client documentation.

Note

The RADIUS client should include the attributes **User-Name** and **Framed-IP-Address** in authentication and accounting messages it sends. RADIUS Agent uses the values of these attributes to interpret and store user name/IP address pairs. If your RADIUS client does not generate this information by default, configure it to do so (see the RADIUS client documentation).

Configuring the RADIUS server

To enable proper communication between Websense RADIUS Agent and your RADIUS server:

- Add the IP address of the RADIUS Agent machine to your RADIUS server's client list. For instructions, see your RADIUS server documentation.
- Define shared secrets between the RADIUS server and all RADIUS clients that use the agent to communicate with the RADIUS server. Shared secrets are usually specified as authentication security options.

  Configuring a shared secret for RADIUS clients and the RADIUS server provides secure transmission of RADIUS messages. Typically, the shared secret is a common text string. For instructions, see your RADIUS server documentation.

Note

The RADIUS server should include the attributes **User-Name** and **Framed-IP-Address** in authentication and accounting messages. RADIUS Agent uses the values of these attributes to interpret and store user name/IP address pairs. If your RADIUS server does not generate this information by default, configure it to do so (see the RADIUS server documentation).

Configuring RADIUS Agent to ignore certain user names

The method that some Windows services use to contact domain controllers from user machines can cause the users logged on to those machines to be misidentified. For example, problems can be caused by:

- The internal user names (Local Service and Network Service) that Windows XP assigns for processes to use for communication with domain controllers
- Running Systems Management Server (SMS) on a client machine.

To prevent or work around possible misidentification, configure your transparent identification agent to ignore logon names that are not associated with actual users.

1. Use the Windows Services tool to stop **Websense RADIUS Agent**.
2. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin, by default).
3. Use a text editor to either create or open **ignore.txt**.
4. Populate the file as follows. Place each entry on a separate line.
   - Add each **user name** that should be ignored on its own line. Websense software ignores these users, regardless of which machine they use.
   - To add a **user name/machine pair**, enter the user name, followed by a comma, and then the machine host name or IP address (ypark,YPARK-WS1). In this case, Websense software ignores the specified user only on the specified machine.
   - To add a **machine**, enter an asterisk (*), followed by a comma, followed by the machine host name, IP address, or IP address range.

   The following example shows correctly formatted entries:

   ```
   anonymous logon
   admin,WKSTA-NAME
   *, WKSTB-NAME
   ```

```
*, 10.209.34.56
*, 10.203.34.1-10.203.34.255
```

In this example, the Windows 7 service account **anonymous logon** is ignored on all machines, the user name **admin** is ignored only when associated with machine **WKSTA-NAME**, and logons for **WKSTB-NAME**, **10.209.34.56**, and the network range **10.203.34.1** to **10.203.34.255** are ignored.

5. When you are finished making changes, save and close the file.
6. Start RADIUS Agent.

Custom configuration for a RADIUS Agent instance

The transparent identification agent configuration settings in the management console are global, and apply to all instances of the agent you have installed. If you have multiple instances of any agent, however, you can configure one instance independently of the others.

Settings specified for a particular agent instance override the global settings in the TRITON console. Note that not all settings can be overridden.

1. Use the Windows Services tool to stop **Websense RADIUS Agent**.
2. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin, by default) and open the **wsradius.ini** file in a text editor.
3. Add or modify parameters and values in the file, as needed (see *RADIUS Agent initialization parameters*, page 11).
4. When you are finished, save and close the INI file.
5. Start RADIUS Agent.

RADIUS Agent initialization parameters

After configuring RADIUS Agent behavior in the management console, you can customize the behavior of a specific RADIUS Agent instance in **wsradius.ini**, the agent's initialization file.

- Some RADIUS Agent settings can only be configured via the management console.
- Some settings can only be configured via the initialization file.

Some parameters can be modified either via the management console or via **wsradius.ini**; these parameters are marked with an asterisk (*).

The parameters and values described here are case-sensitive.

Before making changes to the initialization files, please consider that the default values are designed to maximize accuracy and efficiency in most environments. In most cases, Websense, Inc., recommends leaving the default values as they are.

AccInPort*

Port over which RADIUS Agent accepts accounting requests from RADIUS clients.

Default	12346
Options	1024 through 65535
Required	No
Synopsis	If your RADIUS environment is configured to support RADIUS accounting (user tracking), RADIUS Agent receives accounting requests from client machines over this port.

AccOutPort*

Port over which the RADIUS server listens for RADIUS accounting messages.

Default	1646
Options	1024 through 65535
Required	No
Synopsis	If your RADIUS environment supports RADIUS accounting, the RADIUS server receives accounting messages from client machines over this port.

AuthInPort*

Port over which RADIUS Agent accepts authentication requests from RADIUS clients.

Default	12345
Options	1024 through 65535
Required	No
Synopsis	Used to configure the port on which RADIUS Agent receives authentication requests from the RADIUS client as users log on to the network.

AuthOutPort*

Port on which the RADIUS server listens for authentication requests.

Default	1645
Options	1024 through 65535
Required	No
Synopsis	RADIUS Agent processes the authentication requests it receives from the RADIUS client, and then forwards them to the RADIUS server over this port.

DebugLevel

Determines the detail level of the RADIUS Agent diagnostic activity. (See definition for *DebugMode*.)

Default	0
Options	0, 1, 2, 3
Required	No
Synopsis	Specifies the level of log file detail provided for debugging purposes, from none (0) to high (3). Any value outside the range of 0-3 is interpreted as 0. Diagnostic output with a detail level of 3 includes all RADIUS transactions involved in a user logon.

DebugMode

Controls the RADIUS Agent diagnostic activity.

Default	Off
Options	On, Off
Required	No
Synopsis	Enables or disables RADIUS Agent's built-in diagnostic (logging and debugging) capabilities.

LogFile

Output file for RADIUS Agent diagnostic messages.

Default	N/A
Options	Any string of characters valid for your operating system
Required	No
Synopsis	If you have enabled *DebugMode*, specify a name for the text file in which RADIUS Agent stores diagnostic (log) output.

RADIUSHost*

IP address of the RADIUS server machine.

Default	None
Options	Valid IP address in the format 123.123.123.123
Required	Yes
Synopsis	RADIUS Agent forwards authentication and accounting requests to the RADIUS server, and must therefore know the location of the RADIUS server machine.

RRASHost*

IP address of a machine running Microsoft RRAS.

Default	N/A
Options	Valid IP address in the format 123.123.123.123
Required	No
Synopsis	*(Windows)* If Microsoft RRAS is in use, Websense software queries the machine running RRAS for user logon sessions. If no IP address is entered, no query occurs.

Timeout

Amount of time to wait for a response from the RADIUS server.

Default	1000 [milliseconds = 1 second]
Options	Integers greater than 500
Required	Yes
Synopsis	RADIUS Agent waits for a response to an authentication request from the RADIUS server for a specified amount of time before ending a query attempt.

RADIUS Agent troubleshooting

Use the following troubleshooting topics to help identify and resolve RADIUS Agent transparent user identification issues:

- *Enabling RADIUS Agent diagnostics*, page 14
- *RADIUS Agent: VPN issues*, page 16
- *RADIUS Agent fails to start*, page 16
- *RADIUS server Event Log warnings or error messages*, page 16
- *RADIUS agent: The correct policy is not being applied to remote users*, page 17

Enabling RADIUS Agent diagnostics

RADIUS Agent has built-in diagnostic capabilities, but these are not activated by default. To activate RADIUS Agent logging and debugging:

1. Use the Windows Services tool to stop **Websense RADIUS Agent**.
2. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin, by default) and open the **wsradius.ini** file in a text editor.
3. Locate the **[RADIUSAgent]** section.
4. To enable logging and debugging, change the value of **DebugMode** to **On**:

   ```
   DebugMode=On
   ```

5. To specify the log detail level, modify the following line:

   ```
   DebugLevel=<N>
   ```

   N can be a value from 0-3, where 3 indicates the most detail.

6. Modify the **LogFile** line to indicate the name of the output file:

   ```
   LogFile=filename.txt
   ```

   By default, log output is sent to the RADIUS Agent console. If you are running the agent in console mode (see *Running RADIUS Agent in console mode*, page 15), you can optionally keep the default value.

7. Save and close the **wsradius.ini** file.

8. Start RADIUS Agent.

If remote users are not being identified, the likely cause is communication problems between RADIUS Agent and your RADIUS server. Check your RADIUS Agent logs for errors to determine the cause.

Running RADIUS Agent in console mode

To start RADIUS Agent in console mode (as an application), enter the following at the Windows command prompt:

```
RadiusAgent.exe -c
```

To stop the agent at any time, press **Enter** again. It may take a couple of seconds for the agent to stop running.

RADIUS Agent accepts the following command-line parameters:

Parameter	Description
-i	Installs RADIUS Agent service.
-r	Runs RADIUS Agent service.
-s	Stops RADIUS Agent service.
-c	Runs RADIUS Agent as an application process instead of as a service. When in console mode, RADIUS Agent can be configured to send log output to the console or to a text file.
-v	Displays the version number of RADIUS Agent.
-? -h -help <*no option*>	Displays usage information on the command line. Lists and describes all possible command line parameters.

RADIUS Agent: VPN issues

The VPN client is not successfully logged onto the VPN network

To verify that RADIUS server is authenticating clients, check the RADIUS server's log file for the user name in question.

For Microsoft IAS, go to the IAS management console and see **Remote Access Logging** to find out where the log file is. (Set which actions are logged via the **Properties** panel).

RADIUS Agent fails to start

If RADIUS Agent does not start, check your RADIUS Agent logs for the following message:

```
Cannot bind to port: 10048
```

The usual cause is that another application (for example, a second instance of RADIUS Agent, or the RADIUS server) is currently running on the RADIUS Agent machine and using the same port RADIUS Agent is defined to use. Ensure that each RADIUS application on the RADIUS Agent machine uses a different port.

RADIUS server Event Log warnings or error messages

The RADIUS server Event Log can be helpful in determining the cause of VPN connection or authentication problems, and in distinguishing whether the problem lies in RADIUS Agent or VPN setup.

RADIUS Accounting is not enabled on the RADIUS server

With some RADIUS servers (Microsoft IAS for example), RADIUS Accounting must be enabled so that RADIUS Agent can get the IP address of the RADIUS client.

The RADIUS server should include the attributes **User-Name** and **Framed-IP-Address** in authentication and accounting messages. RADIUS Agent uses the values of these attributes to interpret and store user name/IP address pairs. If your RADIUS server does not generate this information by default, configure it to do so. See your RADIUS server documentation for instructions.

RADIUS Agent has not been added as a client to the RADIUS server

Configure your RADIUS server to use Websense RADIUS Agent as a proxy. This involves adding RADIUS Agent as a client to the RADIUS server.

See your RADIUS server documentation for instructions on configuring a proxy.

- If you have multiple RADIUS servers, each server must be configured separately.
- Failure to configure RADIUS Agent as a proxy results in a RADIUS connection failure.

Is RADIUS Authentication for Windows domain users in use?

If you require the RADIUS server to authenticate Windows domain users, the RADIUS server may need to reside in the same Windows domain as these users. See your RADIUS server documentation for information on domain user authentication.

Is Livingston RADIUS server in use?

Lucent RADIUS Server must be configured to use Password Authentication Protocol (PAP), and the RRAS server must be configured to accept only PAP requests. For instructions, see your respective product documentation.

Is Microsoft Routing and Remote Access Server (RRAS) in use?

Run RADIUS Agent with administrative rights on an RRAS server. This ensures that when it is restarted, RADIUS Agent can retrieve all currently logged-on users from the RRAS server. In most cases, domain administrative rights are sufficient.

To verify that RADIUS Agent is retrieving all currently logged-on users, check the RADIUS Agent log file for the following entry:

```
WsRadiusApp::StartAgent()
WsRRASInspector::Inspect(127.0.0.1, 151ff24)
Adding RRAS entry to user map: ip=C0A8030C,
user=SOFIA\radiustest
```

RADIUS agent: The correct policy is not being applied to remote users

If no policy or the wrong policy is being applied to remote users, check your RADIUS Agent logs for the message **Error receiving from server: 10060** (Windows).

This usually occurs when the RADIUS server does not recognize RADIUS Agent as a client (source of RADIUS requests). Make sure that the RADIUS server is configured properly (see *Configuring the RADIUS server*, page 9).