STEEL-BELTED RADIUS™

Hotspot Edition

Administration Guide

Unix and Windows Versions

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142

617-497-6339
617-491-6503 (Technical Support)

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Introduction

1

Welcome

Thank you for selecting Steel-Belted Radius/Hotspot Edition.

Steel-Belted Radius/Hotspot Edition is a complete implementation of the widely-used IETF standards-track RADIUS (Remote Authentication Dial-In User Service) protocols.

Steel-Belted Radius/Hotspot Edition delivers a complete RADIUS solution, on the scale required by hotspot providers. It interfaces with a wide variety of wireless access points, and easily authenticates customers via proxy RADIUS against a central store of user names and passwords — allowing you to easily set up and manage your hotspot access. Plus, it delivers usage statistics to a central accounting database, so you can track and document how your customers are using the service.

Highlights of Steel-Belted Radius/Hotspot Edition include:

- Flexible, powerful proxy RADIUS features let you easily distribute customer authentication requests to the appropriate RADIUS server for processing.
- Authentication against a local database permits network access by employees.
- High-performance operation guarantees speedy internet access, with no waiting by the customer.
- Support for a wide variety of 802.1x-compliant access points and other network access servers ensures compatibility in your hotspot environment.

System Requirements

Unix

Steel-Belted Radius for UNIX software package includes the server daemon, a Java-based administration user interface, and various dictionary and database files to support authentication.

It requires Solaris 2.60, 7, or later on a SPARC workstation or server with at least 64 megabytes of working memory. Installing Steel-Belted Radius will require 105 megabytes of space on the hard disk; hard disk requirements for running Steel-Belted Radius will depend on your system's product configuration.

The administration UI requires a Java-capable browser that understands signed Java applets. Browsers that meet these criteria include Netscape Navigator 4.08 or later on Windows NT/2000/XP and Solaris, and Internet Explorer 4.0 or later on Windows 95 and NT.

Window NT/2000/XP

Steel-Belted Radius for Windows NT/2000/XP runs as a service on any Windows NT/2000 workstation or server (version 4.0 or later), with TCP/IP properly configured.

Steel-Belted Radius can be administered from the local Windows NT/2000/XP machine on which it is running, or it can be administered remotely from another Windows NT/2000/XP machine.

Licensing

Steel-Belted Radius may be installed on a single workstation or server.

For details about licensing, please refer to the enclosed license agreement or contact Funk Software directly.

Documentation

This manual describes how to install, configure, and administer Steel-Belted Radius for UNIX and Windows NT/2000. Most of the information in this manual is also contained in the on-line help available from the Administrator program.

You may consult our online Vendor Information file for information about using Steel-Belted Radius with many popular brands of Remote Access Server and Firewall. You can access this file by starting the Administrator, choosing the RAS Clients dialog, and clicking the **Vendor Info** button. (In Windows NT, you can also access the file by selecting **Help > Vendor Info** from the **Administrator** menu bar.) For more detailed information about configuring your access servers and firewalls, consult the manufacturer’s documentation provided with each device.

Please also review the readme.txt file, which contains late-breaking information not available in this manual.

Technical Support

If you have any problems installing or using Steel-Belted Radius, there are various resources available to help you.

This manual and the `readme.txt` files provided with the product may contain the information you need to solve the problem you are having. Please re-read the relevant sections. You may find a solution you overlooked.

A range of support options is also available. Refer to the enclosed brochure for information about the support plan that best meets your needs.

If you haven’t already done so, please fill out and return the enclosed Registration Card to ensure that you will be notified of upgrades and of new networking products as they become available.

Reading the Text

In order to make this documentation easy to read, and the text as unambiguous as possible, the following conventions have been adopted.

Software-level text and identifiers

Software-level text and other identifiers (attribute names, values, etc.) will appear in this manual in a plain monospace font, as below. This font will also be used for displaying the contents of computer files, text visible on status messages, and other sorts of technical details.

Consider the following example:

```
[EventDilutions]
SQLConnectFailure=8
```

User interaction

Text that guides the user’s interaction with the software’s user interface will appear in another font. This will be used to specify particular keys on the keyboard (such as **[Esc]**), a string of text (such as “enter **YES**”), programs to invoke from the command line (such as “Now run the installation program by entering **installme** from the command line”), particular buttons or components of the user interface (such as “select the **OK** button” or “click on the **Reboot on disconnect** checkbox”).

Menu commands will be written out as the name of the menu, followed by the **>** sign, and concluding with the name of the command itself. For example, the **Cut** menu command on the **Edit** menu would be written as **Edit > Cut**. If the item on the menu is not a command but a hierarchical menu, the menu chain will be longer. For example, if the **Edit** menu has an entry called **Paste As...** which leads to a hierarchical menu which contains a command called **Text**, this chain of items would be written as **Edit > Paste As... > Text**.

Files, Storage Devices, Web-sites

All files, storage devices, and web-sites will appear in the text shown in the following examples:

> For more information, go to www.tellmemore.com
>
> Now copy SPACEHOG.DAT to your C: drive.

Variable text

There are times when this documentation will have to refer to numerous kinds of variable text. Names, dates, user selections, and so on, can appear in italics in any of the above fonts.

For example, to demonstrate that the user should enter their name and password when prompted to do so on their computer screen, the interaction might be represented as follows:

```
Enter your name: YourName
Password:  YourPassword
```

File names and computer text can also be displayed in italics to indicate that the exact text can change and that it will be up to you to supply it.

For example, the section of the configuration file shown above might be explained as:

```
[EventDilutions]
EventName=DilutionCount
EventName=DilutionCount
...
```

Where *EventName* is the name of a known event and *DilutionCount* is an integer count.

Installation

2

Installing and Starting under Unix

This section describes how to install the Steel-Belted Radius software onto a UNIX server or workstation. Please use the following steps:

1. Review the system requirements and list of documents in Chapter 1.

2. Copy the installation files to the UNIX machine. Set your working directory to the directory to which you’ve copied the files.

3. To display detailed information about the Steel-Belted Radius installation script and its options, type the following command:

   sh install.sh -info

4. Run the install.sh script with the **-all** option:

   sh install.sh -all

5. The script prompts you for the directory where you want to install the Steel-Belted Radius software; this will be known as the *server directory*. Enter a full pathname.

   If the directory does not already exist, the script creates it.

6. The script prompts you to enter a license key. If you have purchased the product, you'll find this number on a sticker affixed to the license agreement in your product package.

   If you type **y** and press **[Enter]**, you will be prompted to enter the license key. Type the number and press **[Enter]**. The script will create the license file and copy it to the server directory.

   If you type **n** and press **[Enter]**, the software will default to 30-day evaluation mode, allowing use of the product's full feature set for that time only.

7. If you type **n** and press **[Enter]**, you will be shown a list of products that may be evaluated on a trial basis.

   Type the number matching the product you wish to evaluate and press **[Enter]**.

8. If you have installed a previous version of this same edition of Steel-Belted Radius on this computer, during the next several steps the install.sh script may detect the following items on the machine:

   - a radius daemon that is already running
   - Steel-Belted Radius configuration files
   - Steel-Belted Radius database files

The script will check for these items prior to copying any files to the server directory. If you have never installed Steel-Belted Radius on this UNIX machine before, you may skip to step 12.

9 The install.sh script checks for a running server:

```
Checking for a running server
```

If the script detects a running radius daemon, the following prompt will be displayed; if not, you may skip to step 10:

```
Server is running with pid x
Stop radius server and unconfig/uninstall before
installing new version
```

If you see the above prompt, complete the following steps before continuing with step 10:

- If you are unsure of the location of the existing server directory, you can find it as follows:

  ps -aef | grep radius

- Change to the existing server directory.
- Stop the server:

  ./S90radius stop

- Unconfigure the previous installation :

  sh install.sh -unconfig

- The script will prompt you to enter the path to the existing server directory:

  ```
  Enter server directory [current_directory/radius]:
  ```

- Type the path and press **[Enter]**.
- Change to the directory into which you want to install the new software.
- Run the install.sh script with the **-all** option:

  sh install.sh -all

10 The install.sh script checks for Steel-Belted Radius configuration files:

```
Checking for previous configuration files
```

If the script detects existing configuration files, the following prompt will be displayed; if not, you may skip to step 11:

```
Previous configuration files exist
Configuration files exist in server_directory
Do you want to discard them? [n]
```

If you type **n** (the default), a directory called OLDCONFIG will be created under the server directory, and the previous configuration files will be moved to this directory. If you type **y**, the installation script will overwrite the previous files.

WARNING: If existing configuration files are overwritten, any network specific information defined there will be lost. It is a good idea to back up all files and subdirectories in the server directory, prior to installing a new version of Steel-Belted Radius.

11 The install.sh script checks for Steel-Belted Radius database files:

```
Checking for database files in server_directory
```

If the script detects existing database files, the following prompt will be displayed; if not, you may skip to step 12:

```
Previous database files exist
Database files exist in server_directory
Do you want to overwrite them? [n]
```

If you type **n** (the default), the database files will not be overwritten and the new version of Steel-Belted Radius will still have the entire administrative database (RAS Clients, Users, and so forth) from the previous installation.

If you type **y**, the database files will be overwritten and all data previously contained in those files will be lost.

WARNING: For this reason, it is a good idea to back up all files and subdirectories in the server directory, prior to installing a new version of Steel-Belted Radius.

12 The install.sh script copies files to the server directory.

13 The install.sh script prompts you for the directory where you want to install the Steel-Belted Radius administration program and online help; this will be known as the *admin directory.* Enter a full pathname.

If the admin directory does not already exist, the script will create it. The script then copies administration and help files to this directory.

14 Steel-Belted Radius includes a Java administration program that may be run locally from a browser on your UNIX machine, served up from a web server, or run remotely from a PC on your network. Consider how you would like to use this program, and set up the method of your choice.

See the "Setting Up the Administrator Program" section below.

15 You may now configure Steel-Belted Radius by running the install.sh script with the **-config** option from the server directory, as follows:

sh install.sh -config

16 The script now runs as configured in the steps above. When it completes configuration, it displays the following message:

```
Admin configuration completed
```

17 To start the radius daemon without waiting for the next system restart, change to the server directory that you chose while installing Steel-Belted Radius, and start the server as follows:

```
cd server-directory
./S90radius start
```

NOTE: If your Solaris system is configured for shadow mode and you plan to use /etc/passwd authentication, you need to run the radius daemon as root. You will also need to run the radius daemon as root if you use a port whose number is less than 1024.

18 You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs.

See the "Configuring the Steel-Belted Radius Server" section below.

Upgrading from a Previous Installation

We recommend that you do the following whenever you upgrade a UNIX installation:

1 Stop the previous version of the radius daemon.

2 Back up the Steel-Belted Radius server directory.

3 Complete the installation procedure as described above.

Restoring the Previous Configuration

Upon installation, old configuration files can be saved to a directory named OLDCONFIG. This practice prevents the loss of configuration information from a previous installation.

The files that are saved to the OLDCONFIG directory are:

- All the .ini files (vendor.ini, account.ini, radius.ini, and so forth)
- Any .eap files (automatic EAP helper (e.g., EAP-TLS) initilization files)

If you do not want to install any new features, copy all the files from the OLDCONFIG directory into the Steel-Belted Radius server directory. If you want to install the new features while maintaining current configuration information, complete the following tasks:

File	Task
account.ini	Modify account.ini in the server's directory with any changes you made in OLDCONFIG/account.ini.
filter.ini	Copy OLDCONFIG/filter.ini to the server directory.
radius.ini	Modify radius.ini in the server directory with any changes you made in OLDCONFIG/radius.ini.
vendor.ini	Insert additional settings from vendor.ini in the server directory into OLDCONFIG/vendor.ini and copy this file to the server directory.
eap files	Insert additional settings from each .eap file file in the server directory into the corresponding file saved in the OLDCONFIG directory and copy these files to the server directory.

Stopping and Starting the radius Daemon

Once installed on the server, the radius daemon will stop and start automatically each time you shut down or boot up the server.

You can stop the radius daemon at any time. Change to the server directory that you chose at installation time, and stop the daemon, as follows:

```
cd server-directory
./S90radius stop
```

To start the radius daemon:

```
cd server-directory
./S90radius start
```

NOTE: If your Solaris system is configured for shadow mode and you plan to use pass-through authentication to UNIX users and groups, you need to start the radius daemon under the root directory.

Setting Up the Administrator Program

The Steel-Belted Radius Administrator program runs as a Java applet within a browser. This program allows you to populate and configure your Steel-Belted Radius server via a graphical user interface. While running the Administrator, you can view online help, get RAS configuration tips, add a license key, import or export RADIUS data, report on the server configuration, and much, much more.

You can deploy the Java Administrator in various ways. For example:

- You can run the Java administrator from within a browser that is installed on the local UNIX machine. Simply launch the browser, browse your local file system and select either the default.htm or the index.html file. Both of these files reside in the java subdirectory under the admin directory (usually found under /radadmin/java).
- You can make the program accessible via a web server. To do this, either:
  - Move (copy or FTP) the Java UI files from the java subdirectory to part of the file system accessible to the web server; *or*
  - Choose a folder that is accessible to the web server. Add to it a symbolic link to the Java UI folder. The symbolic link should point to the java subdirectory.
- You can simply transfer (FTP) the Java UI files from the java subdirectory to a PC on your network and run the program from within a browser installed on that PC. Be sure to move the entire java subdirectory to the PC, keeping the directory structure intact. Once the move is complete, select either the default.htm or the index.html file. This will launch the browser and the Java administrator applet.

Installing under Windows NT/2000

This section describes how to install the Steel-Belted Radius service onto a Windows NT/2000 domain controller, server, or workstation.

1. Review the system requirements and list of documents in Chapter 1.
2. If you have installed a previous version of this same edition of Steel-Belted Radius on this computer, please also read the “Updating a Previous Installation” section below.
3. Log into the Windows NT/2000 server or workstation. Insert the Steel-Belted Radius installation disk, choose **Start > Run**, and enter the drive letter and **Setup** command. For example:

   D:\SETUP *
4. The License Key screen appears.

   Enter the License key printed on your license agreement card, or check the **Install 30-day trial** box, as appropriate.

   Click **Next** to continue.

5. If you checked the **Install 30-day trial** box, another License Key screen appears.

   Select the version of the product you wish to try out.

   Click **Next** to continue.

6. The Software License Agreement screen appears. Before proceeding, make sure that you read and agree with the terms of the license agreement.

   Click **Yes** if you agree. Otherwise, click **No**.

7. The Welcome screen appears.

   Click **Next** to continue.

8. The Select Components screen appears. For a normal installation, make sure both **RADIUS Admin Program** and **RADIUS Server** are checked. You may use the default destination directory for each component you are installing, or click **Browse** to select a different directory.

   Click **Next** to continue.

9. If you are upgrading from a previous installation, a warning screen appears, indicating that existing configuration files will be moved to the `Service\Old` directory.

   Click **OK** to continue.

10. The Select Program Folder screen appears. You can accept the default folder `Steel-Belted Radius` or enter a different folder name.

    Click **Next** to continue.

11. The server will be installed under LocalSystem.

    Click **Next** to continue.

12. The Start Copying Files screen displays the current settings for the installation. Scroll down and make sure the settings are exactly as you want them.

    If the settings are correct, click **Next** to proceed with installation. Otherwise, click **Back** to return to previous screens.

13. Once installation is completed, the Setup Complete screen will appear. This screen gives you the opportunity to view the `readme.txt` file and start the Steel-Belted Radius Administrator.

    Check the options you wish to select, and click **Finish**.

14. Configure the new Steel-Belted Radius server to support your network’s authentication and accounting needs.

See the “Configuring the Steel-Belted Radius Server” section below.

Upgrading from a Previous Installation

We recommend that you do the following whenever you upgrade a Windows NT/2000 installation:

1. Stop the previous version of the Steel-Belted Radius service.
2. Back up the Steel-Belted Radius server directory.
3. Complete the installation procedure as described above.

Restoring the Previous Configuration

Upon installation, existing configuration files will be saved to a directory named Service\Old. This prevents the loss of configuration information from a previous installation.

The files that are saved to the Service\Old directory are:

- All the .ini files (vendor.ini, account.ini, radius.ini, and so forth)
- Any .eap files (automatic EAP helper (e.g., EAP-TLS) initialization files)

If you do not want to install any new features, copy all the files from the Service\Old directory into the Steel-Belted Radius server directory. If you want to install the new features while maintaining current configuration information, complete the following tasks:

File	Task
account.ini	Modify account.ini in the server directory with any changes you made in Service\Old\account.ini.
events.ini	Copy Service\Old\events.ini to the server directory.
radius.ini	Modify radius.ini in the server directory with any changes you made in Service\Old\radius.ini
vendor.ini	Insert additional settings from vendor.ini in the server directory into Service\Old\vendor.ini and copy this file to the server directory

Starting and Stopping the RADIUS Service

Steel-Belted Radius runs as an NT service. By default, it is set to run automatically whenever you start up Windows NT/2000.

If you don’t want it to run automatically, choose **Services** from the Control Panel, select **Steel-Belted Radius** from the **Service** list, click **Startup…** and set the **Startup Type** to **Manual**. You can then use the **Start** and **Stop** buttons to control when it runs.

Upgrading from a 30-Day Trial Installation

If you’ve downloaded Steel-Belted Radius on a 30-day trial basis and want to continue using the product, you do not need to re-install the software. All you need to do is add a license key to your existing installation.

First, purchase the Steel-Belted Radius software, either by contacting your preferred reseller or by contacting Funk Software directly. You will be shipped a product package that will contain a license key.

Next, add the license key, as instructed below. The license key will convert your 30-day trial software to an unlimited version.

Adding a License Key

Depending upon your purchasing arrangements, your Steel-Belted Radius software may require a new license key at some point after its initial installation.

If you are given a new license key by your reseller or by Steel-Belted Radius, you can add the key to an existing Steel-Belted Radius installation as follows:

1. Start the Steel-Belted Radius Administrator program and connect to the server.
2. For **Unix**, click the **License** button at the lower right of the main window.

   For **Windows**, select **File > License**.
3. The Add a License for Server dialog displays. Enter the license key and click **OK**. If you are running Windows and the license key you’ve entered is invalid, the server displays an error message; click **OK** in this message box and try again.
4. Once you’ve entered a valid license key, the server displays a confirmation message and reminds you that you will need to restart the server. When you click **OK** in this message box, the server does not restart itself automatically; you’ll need to restart it manually.
5. The next time Steel-Belted Radius is started, the new license will be loaded.

Configuring the Server

Once you’ve installed the Steel-Belted Radius software on your computer, and have added the appropriate license keys, you must configure the software before it can be used.

The specific steps that you must perform will vary depending on your network’s authentication and accounting needs. However, the basic steps can be summarized as follows:

1. Make sure the computer on which you’re running Steel-Belted Radius has the IP protocol configured.
2. Configure each of your NAS devices to communicate with the server. To do this, you will need to log into each device and run its configuration interface.
3. Run the Steel-Belted Radius Administrator program.
4. Using the Servers dialog, connect to your server (under **Unix** you do this by using the default account **admin** and password **radius**).
5. **Unix only**: Using the Access dialog, change the default administrative account password from **radius** to a password of your choosing.
6. Using the RAS Clients dialog, configure the server to communicate with each of its RADIUS clients (NAS devices).
7. From the Users dialog, identify each of the users or groups of users that are permitted to dial in to the NAS devices. Select user attributes, either by assigning them in the Users dialog or by creating user profiles in the Profiles dialog.

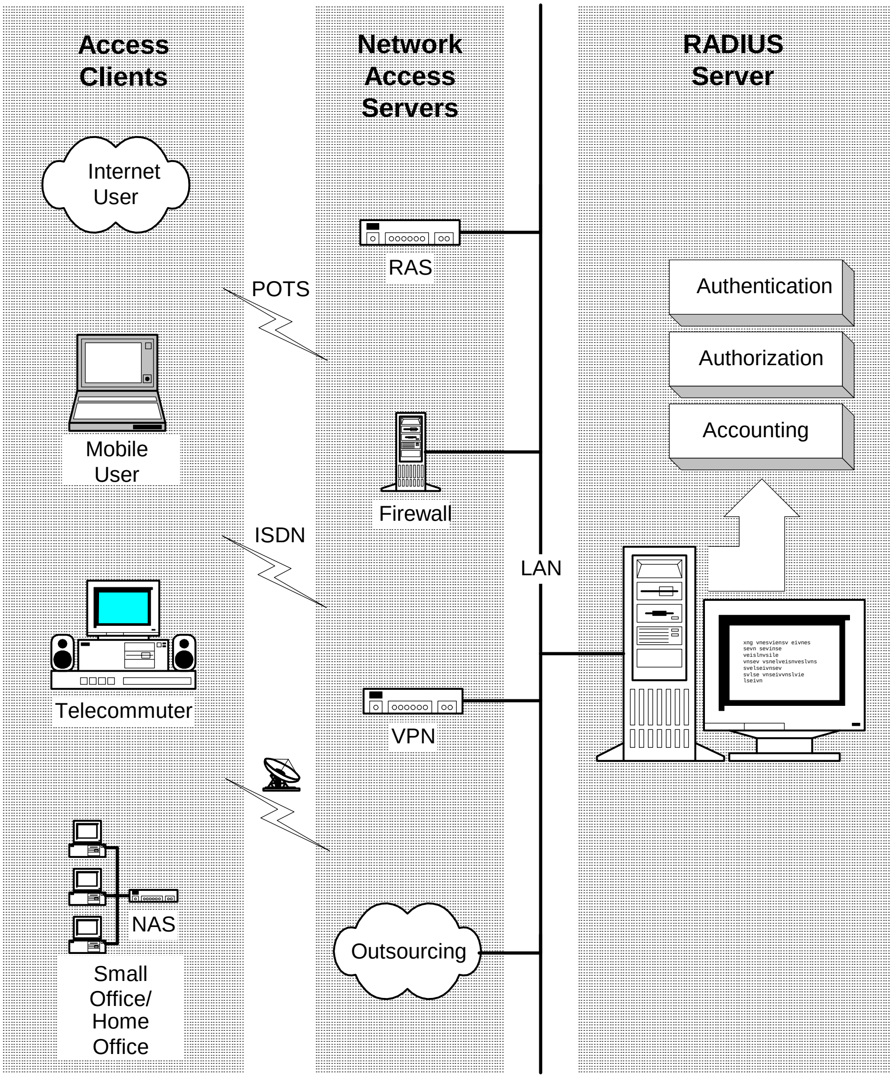
Concepts

3

RADIUS Basics

RADIUS (Remote Authentication Dial In User Service) is a standardized method of information exchange between a device that provides network access to users (the *RADIUS client*) and a device that contains authentication information for those users (the *RADIUS server*).

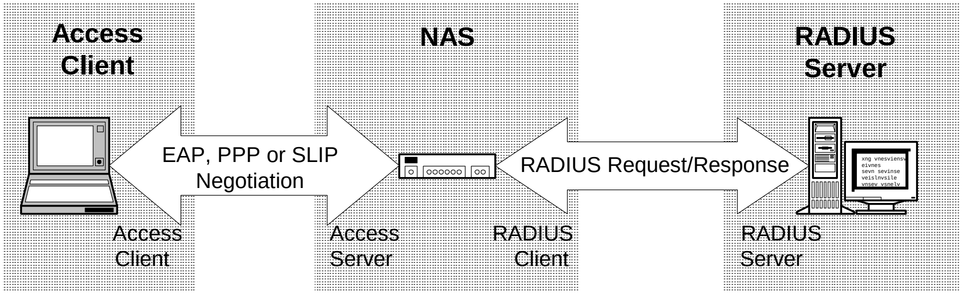
The RADIUS-based remote access environment has three major components: Access Client, Network Access Server, and RADIUS Server.



RADIUS-Based Remote Access Environment

The *Access Client* may be a person dialing into a Service Provider network to connect to various Internet sites (the traditional user role). Alternatively, the Access Client may be a device; it may be an ISDN router or a dial-on-demand router that provides network access to multiple users at a small office/home office.

A *Network Access Server* (NAS) is a device that can recognize and handle connection requests from outside the network "edge." It might be a WLAN Access Point, an ISDN bridge, or a modem pool. When the NAS receives a user's connection request, it may perform an initial access negotiation with the user (EAP, PPP or SLIP). This negotiation will establish certain data (username, password, NAS device identifier, NAS port number, and so on). The NAS will then pass this data to the RADIUS server and request authentication.



Data Exchange between Access Client, NAS, and RADIUS server

The RADIUS server will authenticate the request, and will authorize services over the connection. The RADIUS server does this by matching data from the NAS's request with entries in some well-known, trusted database. In the case of Steel-Belted Radius, the match may be found on the RADIUS server; on some other type of authentication server (ACE/Server or TACACS+); in a SQL or LDAP database; or on some other RADIUS server for which this server is a *proxy.*

If a match can be found, the RADIUS server will accept the user. Otherwise, it will reject the user. Based on this response from the RADIUS server, the NAS will decide whether to establish the user's connection or terminate the user's connection attempt. Finally, the NAS issues accounting data to the RADIUS server to document the transaction; the RADIUS server may store or forward this data as needed to support billing for the services provided.

RADIUS Packets

A RADIUS client and RADIUS server communicate by means of RADIUS packets. RADIUS packets are formatted using conventions outlined in technical documents

RFC 2865 *Remote Authentication Dial In User Service (RADIUS)* and RFC 2866 *RADIUS Accounting*.

To configure the Steel-Belted Radius server, the essential information you'll need to know about RADIUS packets is the following:

- They carry messages between the RADIUS client and RADIUS server.
- They follow a request/response convention: the client sends a request and expects a response from the server. If the response doesn't arrive, the client can retry the request periodically.
- Each packet supports a specific purpose: authentication or accounting.
- A packet may contain values, called *attributes*.
- The specific attributes to be found in each packet depend upon the type of packet (authentication or accounting) and the device that sent it (for example, the specific make and model of NAS device).

If you wish to explore details of packet structure and contents, included in the RFC 2865 is a table of packet types and the attributes to expect in each type of packet. This document also provides exhaustive descriptions of each attribute and its possible values. Refer to the RFC 2866 document for accounting details.

RADIUS Configuration

You must configure a RADIUS client and RADIUS server in order for them to communicate. As shown in the diagram above, if the client is a NAS device, it's probably on the same LAN as the server. If so, the same network administrator will probably have all the data and privileges necessary to configure both sides of RADIUS communications. Under other conditions, you may need to work out configuration details with the administrators of other networks.

RADIUS Server Configuration

You must tell a RADIUS server how to respond to each of its clients. When configuring the Steel-Belted Radius server, you'll need to start the Administrator program, open the RAS Clients dialog, and enter the following information for each RADIUS client:

- The IP address of the client device;
- The RADIUS shared secret to be used by Steel-Belted Radius and the client device; *and*

- The make and model of the client device, selected from a list of devices that Steel-Belted Radius supports. If a specific make/model is not listed, select **- Standard Radius -**.

RADIUS also requires you to specify the UDP ports that you'd like the server to use when sending and receiving RADIUS authentication and accounting packets. Steel-Belted Radius offers default port selections, but if you'd like to configure different choices, you may.

See "RADIUS Ports" on page 25.

RADIUS Client Configuration

You must tell each RADIUS client how to contact its RADIUS server. When configuring a client to work with a Steel-Belted Radius server, you'll need to log into the client device, run its administration program, bring up its RADIUS configuration interface, and enter the following information:

- The IP address of the Steel-Belted Radius server;
- The RADIUS shared secret to be used by the Steel-Belted Radius server and the client device; *and*
- The UDP ports on which the client device wishes to send and receive RADIUS authentication and accounting packets. These must match the ports that Steel-Belted Radius is using for the same purposes.

Multiple RADIUS Servers

The RADIUS workload may be distributed among several servers, as follows:

- You can create specialized servers by separating RADIUS authentication and accounting functionality. To accomplish this, each client device must be configured to send all of its authentication packets to one RADIUS server and all of its accounting packets to another.
- You can provide redundancy by pairing up RADIUS servers to work in tandem. Most NAS configuration interfaces will permit you to designate one server as primary, and another as secondary, for both authentication and accounting purposes.

If both measures for distributing the RADIUS workload are in place, client configuration involves naming the following for each client device: a primary RADIUS accounting server, a secondary RADIUS accounting server, a primary RADIUS authentication server, and a secondary RADIUS authentication server.

RADIUS Shared Secret

The RADIUS *shared secret* is used to validate RADIUS communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.

IMPORTANT: Be careful: Upper- and lowercase letters make a difference!

Configuring Shared Secrets

On the client side, most configuration interfaces will allow you to enter a different shared secret for RADIUS authentication and RADIUS accounting purposes (two secrets). If the interface also permits you to identify primary and secondary RADIUS servers, you may be able to name as many as four secrets (primary accounting, secondary accounting, primary authentication, and secondary authentication).

On the server side, the configuration interface will allow you to create a list of known RADIUS clients (NAS devices). You should be able to identify the authentication shared secret and accounting shared secret that this server uses to communicate with each of the clients on this list.

See “RAS Clients Dialog” on page 55.

See also “Proxy Dialog” on page 67.

You should take steps to ensure that every shared secret is unique across your entire RADIUS configuration.

How Shared Secrets are Used

During an authentication transaction, password information must be transmitted securely between the RADIUS client and the RADIUS server. Password security may be addressed using a variety of protocols such as PAP, CHAP, or MS-CHAP. When PAP is used, the password is encrypted and decrypted using the authentication shared secret.

See “Password Protocols” on page 28.

No encryption is involved in transmitting accounting data between a RADIUS client and RADIUS server. However, the accounting shared secret is used by each device to verify that it can “trust” any RADIUS communications it receives from the other device.

RADIUS Ports

When the RADIUS standard was first written, the standard ports to use for RADIUS authentication and accounting packets were 1645 and 1646, respectively. Then it emerged that these ports had been assigned to another standard. The RADIUS standards group responded by changing the port assignments to 1812 and 1813, but many organizations still use the old assignments.

As with the RADIUS shared secret, any two devices that exchange RADIUS packets must use compatible UDP port numbers. That is, if you are configuring a NAS to exchange authentication packets with a RADIUS server, you must find out which port the server uses to receive authentication packets from its clients (1812, for example). You must then configure the NAS to send authentication packets on the same port (1812). The same is true for RADIUS accounting.

Steel-Belted Radius can listen on multiple ports. In order to provide the best possible compatibility, the server listens to both old and new port standards by default. This means that, as a default setting, ports 1645 and 1812 are assigned to authentication and ports 1646 and 1813 are assigned to accounting. If you wish to reassign ports, you may specify port numbers with the `UDPAuthPort` and `UDPAcctPort` settings in the [Ports] section of the radius.ini file, or edit the services configuration file.

See "services File" on page 158 and "radius.ini [Ports] Section" on page 144.

Authentication

To understand the authentication sequence, you'll need an overview of RADIUS authentication messages. The following table explains the conditions under which each type of message is issued, and the purpose of any RADIUS attributes that the message may contain.

Message Conditions	Purpose of Message Attributes
When a NAS receives a connection request from a user, the NAS authenticates the request by sending an Access-Request to its RADIUS server.	Identify the user. Describe the type of connection the user is trying to establish.
When a RADIUS server is able to authenticate a connection request, it returns a RADIUS Access-Accept to its client (usually the NAS).	Allow the NAS to complete access negotiations. Configure connection details, for example, providing the NAS with an IP address that it may assign to the user. Enforce time limits and other "class of service" restrictions upon the connection.

Message Conditions	Purpose of Message Attributes
When a RADIUS server is unable to authenticate a connection request, it returns an Access-Reject to its client (the NAS).	Terminate access negotiations. Identify the reason for failure.
If initial authentication conditions are met, but additional input is needed from the user, the RADIUS server returns an Access-Challenge to its client (the NAS).	Enable the NAS to prompt the user for more authentication data. Complete the current Access-Request, so the NAS can issue a new one.

Authentication Methods

Each time an Access-Request message arrives at the server, an authentication transaction begins. During this transaction, the server attempts to authenticate the request by trying each of its configured and enabled authentication methods in turn. To know which methods to try, and in which order, the server consults its Authentication Methods list. You can view and edit this list by starting the Administrator program and opening its Configuration dialog.

Native User Authentication

While trying the Native User method (for user accounts stored directly on the server itself), Steel-Belted Radius searches its database for an entry whose User-type is `Native User`, and whose User name matches the username in the Access-Request. If the entry:

- Cannot be found, or if it is found and the Password is invalid, Steel-Belted Radius tries the next enabled method in the Authentication Methods list.
- Is found, but its Check-List doesn’t match attributes found in the Access-Request, Steel-Belted Radius returns an Access-Reject to the NAS.
- Is found, and its Password and Check-List match perfectly, Steel-Belted Radius constructs an Access-Accept using the entry’s Return-List, and returns it to the NAS.

Proxy RADIUS Authentication

Steel-Belted Radius can convey an Access-Request to some other RADIUS server, which then (1) performs authentication according to its own conventions and (2) returns a response. Steel-Belted Radius then relays this response to the NAS. The set of conventions for relaying packets between cooperating RADIUS servers is known as *Proxy RADIUS*.

Configuring the Authentication Sequence

Let’s assume, for the moment, that you’ve configured all of the authentication methods that you want to use on the Steel-Belted Radius server.

If you start the Administrator program and open the Configuration dialog, you’ll find that each authentication method appears as a selection in the **Authentication Methods** list. The methods appear in a specific order from top to bottom. This is the order in which the server will try authentication methods. The names of methods in the list may appear black (enabled) or gray (disabled). During an authentication transaction, the server will skip any disabled methods and continue down the list.

You can enable or disable methods, or re-order methods in the list, by using the control buttons in the Authentication Methods panel. In this way, you directly control the sequence of each authentication transaction.

See “Configuration Dialog” on page 86.

Configuring Authentication Methods

As we’ve seen, Steel-Belted Radius offers several authentication methods. Each method tries to find database entries that match the data in the incoming Access-Request packet. However, methods differ according to:

- The location of the database; *and*
- The conventions required to interact with the database.

Steel-Belted Radius configuration will vary according to the authentication methods you plan to use. The various tasks may be summarized as follows.

Method	How to Configure	Complete Details
Native User	Create Native User entries in the Steel-Belted Radius database.	“Adding a Native User” on page 64
OS Pass-Through Security	This method assumes that you already have users, groups, and passwords defined in your local security database. Create User entries in the Steel-Belted Radius database. Choose User-types as appropriate.	“Users Dialog” on page 59
Proxy RADIUS	Add a single target. You can set up single targets that are not associated with any realm.	“Proxy Dialog” on page 67

Method	How to Configure	Complete Details
EAP-TTLS	This method provides a means for an authentication request to be sent directly from the client to the server via a TLS connection. The act of establishing the TLS connection authenticates the server to the client and the authentication request sent through the tunnel authenticates the client to the server. Create a Steel-Belted Radius ttlsauth.aut file that specifies options for the TLS connection and the manner in which Steel-Belted Radius routes the inner authentication request. Stop and restart the Steel-Belted Radius server. Subsequently, the EAP-TTLS authentication method will appear in the Configuration dialog's Authentication Methods list. You may open the Configuration dialog and enable, disable and re-order the EAP-TTLS methods as required.	"Configuring For EAP-TTLS" on page 169

Password Protocols

During an authentication transaction, password information is transmitted between the NAS and the RADIUS server. This password information originally comes from the user, for example during PPP negotiations between a user and a NAS. Steel-Belted Radius supports four protocols for receiving the password from the NAS. Four are PPP password protocols (PAP, CHAP, MS-CHAP, and MS-CHAP-V2). Steel-Belted Radius also supports *Extensible Authentication Protocol*.

The following table lists supported protocols according to the authentication methods with which each protocol can be used (note that some information is specific to Windows or Unix).

Method	PAP	CHAP	MS-CHAP	MS-CHAP-V2
Native	**Yes**	**Yes**	**Yes**	**Yes**
Proxy RADIUS	**Yes**	**Yes**	**Yes**	**Yes**

PAP

Under PAP (Password Authentication Protocol), the user negotiates with the NAS "in the clear." That is to say, no encryption is used to send the password to the NAS.

Once the NAS has enough information from the user to create an Access-Request, the NAS encrypts the password (using its RADIUS authentication shared secret) before sending an Access-Request packet to Steel-Belted Radius.

Upon receiving the Access-Request, Steel-Belted Radius looks for attributes within the packet that will identify the NAS that sent it. Steel-Belted Radius decrypts the password by matching this NAS with a RAS Client entry stored in its database.

Ultimately, Steel-Belted Radius has the password in clear text form and is able to make use of it for authentication.

All Steel-Belted Radius authentication methods support PAP.

CHAP

CHAP (Challenge Handshake Authentication Protocol) avoids sending passwords in clear text over any communication link.

Under CHAP, during password negotiations the NAS generates a *challenge* (a random string) and sends it to the user. The user's PPP client creates a *digest* (the password concatenated with the challenge), encrypts the digest using one-way encryption, and sends the digest to the NAS.

The NAS sends this digest as the password in the Access-Request.

Because the encryption is one-way, Steel-Belted Radius cannot recover the password from the digest. What it can do is perform the identical digest operation using the NAS's challenge (provided in the Access-Request packet) and its own copy of the user's password. If the two digests match, the password is the same.

Steel-Belted Radius must be able to perform the digest operation in order to support CHAP. Therefore, it must have access to its own copy of the user's password. Native User passwords are stored in the Steel-Belted Radius database. SQL or LDAP BindName authentication retrieves the password via a query to the database; the retrieved password can be used to create a digest if it is in clear text form. A TACACS+ server provides CHAP support, and will handle the digest operation itself once Steel-Belted Radius sends the username and password through. No other authentication method supports CHAP at this time.

MS-CHAP and MS-CHAP-V2

The two varieties of MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) are Microsoft authentication protocols that, like CHAP, avoid sending passwords in clear text. Steel-Belted Radius supports both 40-bit and 128-bit MS-CHAP methods.

Steel-Belted Radius must be able to perform a digest operation similar to CHAP in order to support MS-CHAP. Therefore, it must have access to its own copy of the user's password. Native User passwords are stored in the Steel-Belted Radius database. SQL or LDAP BindName authentication retrieves the password via a query to the database; the retrieved password can be used to create a digest if it is in clear text form.

An NT Domain controller provides MS-CHAP support, and will handle the digest operation itself once Steel-Belted Radius sends the username and password through; however, the user must be on the local domain for the password to be recognized.

MS-CHAP-V2 will communicate users' requests to change their passwords to a RADIUS server. Steel-Belted Radius supports this feature of MS-CHAP-V2, although it must also be supported by whatever application the user is using to log in with.

MS-CHAP and MS-CHAP-V2 effectively operate in the same way, but they use different attributes. An MS-CHAP client won't accept MS-CHAP-V2 attributes, and vice-versa; be careful to use the appropriate set of attributes.

For further details about MS-CHAP and MS-CHAP-V2, see IETF RFCs 2433, 2548 and 2759.

Accounting

To understand the Steel-Belted Radius accounting sequence, you'll need an overview of RADIUS accounting messages. The following table explains the conditions under which each type of message is issued, and the purpose of any RADIUS attributes that the message may contain.

Message Conditions	Purpose of Message Attributes
Accounting data is sent from client to server using an Accounting-Request message The client manufacturer will decide which types of accounting request are sent, and under which conditions. This table describes the most typical conditions. It is also the client's responsibility to ensure that the server receives accounting requests. Most clients will retry periodically for an almost unlimited period of time until the server responds.	Depending on the value of the Acct-Status-Type attribute, the message type is considered to be Start, Stop, Interim-Acct, Accounting-On, or Accounting-Off.
After receiving an Access-Accept from the server, the NAS completes its access negotiation with the user. The NAS then sends a Start message to the server.	Record connection data such as username, NAS identifier, NAS port identifier, port type, and connection start time.
After a connection is terminated, the NAS sends a Stop message to the server.	Record statistics regarding the connection. One message will contain the final value of every statistic that this NAS is capable of recording about this type of connection.

Message Conditions	Purpose of Message Attributes
At intervals of approximately every 6 minutes, the NAS sends an Interim-Acct message to the server.	Record a “snapshot” of statistics regarding the connection. One message will contain the current value of every statistic that this NAS is capable of recording about this type of connection.
Every time a client device comes online, whether after a crash or after an orderly shutdown, it sends an Accounting-On message to the server.	Identify the device that is going online.
Every time a client device experiences an orderly shutdown, before completing its shutdown sequence it sends an Accounting-Off message to the server.	Identify the device that is going online.
Upon receipt of an Accounting-Request message, the server sends an Accounting-Response.	Complete the request/response cycle.

Accounting Sequence

A NAS may issue an Accounting-Request whenever it chooses, for example upon establishing a successful connection. Each time an Accounting-Request message arrives at the Steel-Belted Radius server, an accounting transaction begins. During this transaction, the server handles the message by examining the Acct-Status-Type and other attributes within the message, and taking the appropriate action.

Comma-Delimited Log Files

When the Steel-Belted Radius accounting log is enabled, all of the RADIUS accounting attributes that the server receives are reformatted and logged to a comma-delimited file. A file of this format is easily imported into spreadsheets and database programs for report generation and billing.

Sessions List (Current Users Display)

In addition to simply recording RADIUS accounting data, Steel-Belted Radius also processes the data to gather its own statistics, including a real-time snapshot of currently active connections called the Sessions List (also called the Current Users display). You can view this display at any time by clicking a button on the Administrator program’s Statistics dialog. For every active connection, a line is displayed identifying the user, the NAS, the port number, the assigned IP address, and other information.

Each server has its own Current Users display. Therefore, when you view this display, it only reflects the activity on the Steel-Belted Radius server that you’ve currently selected for administration (using the Servers dialog). The Current Users display on a specific server will reflect the activity across your entire RADIUS configuration only if (1) all of the clients in your configuration support RADIUS accounting and (2) they've all been configured to send accounting messages to the same server (the one you're viewing).

See "Sessions List" on page 107.

Attributes

You'll work with RADIUS attributes while setting up Users, Profiles, and RAS Clients on the Steel-Belted Radius server. You won't need to memorize the RADIUS standard or work in hexadecimal (that is, "packet") format in order to do this. The Steel-Belted Radius Administrator program will allow you to select RADIUS attributes by name from a predetermined list. For each attribute, the Administrator program will prompt you to enter values using familiar data types such as string, integer, telephone number, or network address.

This section provides all of the background information you'll need to work with attributes on the Steel-Belted Radius server.

Dictionaries

Steel-Belted Radius uses files called *dictionaries* to store lists of RADIUS attributes. The main Steel-Belted Radius dictionary file `radius.dct` lists attributes defined by the RADIUS standard. The `radius.dct` file resides in the same directory as the Steel-Belted Radius service (usually `C:\RADIUS\Service` on Windows computers or `Radius_Home\` on Unix computers).

Vendor-Specific Attributes

In addition to the standard attributes, many NASs use additional, Vendor-Specific Attributes (VSAs) to complete a connection. Steel-Belted Radius supports a large number of specific NAS devices by providing vendor-specific, proprietary dictionary files. These files also reside in the server directory and use the filename extension `.dct`.

Make/model Field

During Steel-Belted Radius configuration, when you make a selection in the RAS Client **Make/model** field, you are telling the server which dictionary file contains the VSAs for this client device. Thereafter, whenever the server receives a RADIUS packet from this client device, it can consult this dictionary file for any non-standard attributes that it encounters in the packet. Standard RADIUS attributes are always defined by the radius.dct file. If you are in doubt as to the Make/model that you should choose for a RAS Client, it's a safe bet to choose the default option, **- Standard Radius -**.

For the most part, the selections currently available in the **Make/model** field are devices whose vendors have worked with Funk Software to provide up-to-date attribute dictionaries. Documentation for these vendors and their products is available online by clicking on the **Vendor info** button on the RAS Clients dialog.

See "RAS Clients Dialog" on page 55.

If you are using a computer running Windows, you can also access product information by selecting **Help > Vendor Info** from the Administrator menu bar.

Updating Attribute Information

If you receive news from your NAS vendor about a new product, a new attribute, or a new value for an attribute, you can add this information to your Steel-Belted Radius configuration. You can edit the dictionary file for that vendor to add new attributes or attribute values, or you can create a new vendor-specific dictionary file that contains new attributes and values.

For detailed instructions see "Dictionary Files" on page 151.

User Attribute Lists

Each User entry in the Steel-Belted Radius database provides the information necessary for the server to try to authenticate a connection request using a specific authentication method. When you view a User entry using the Administrator program, this method is identified in the **User type** field.

There can be more to authentication than a simple username/password pair. If you wish, you may control authentication at a fine level of detail. The Check-List, Return-List, or Profile fields in the User entry in the database provide powerful tools for the authentication and authorization of users. These fields tell the server how to handle RADIUS attributes while authenticating a connection request and can be used to configure the authorization of the session.

NOTE: All of these fields are optional.

Check-List Attributes

The *Check-List* is a list of attributes that must accompany the request for connection and thus could be considered "authentication requirements." The NAS must send attributes that match the Check-List that is “on file” in a User entry; otherwise, Steel-Belted Radius will reject the user even if the user’s name and password are valid.

By including appropriate attributes in the Check-List, a variety of rules could be enforced. For example, only certain users might be permitted to use ISDN connections, or dial-in to a particular NAS. Or, Caller ID could be used to validate a user against a list of legal originating phone numbers.

A Check-List is created by selecting attributes from a list of all RADIUS attributes known to the Steel-Belted Radius server. This list may include a variety of vendor-specific attributes.

During authentication, Steel-Belted Radius “filters” the Check-List based on the dictionary for the Make/model of the specific RAS Client that sent the authentication request. The server ignores any Check-List attribute that is not valid for this device.

Return-List Attributes

The *Return-List* is a list of attributes that Steel-Belted Radius must return to the NAS once authentication succeeds. The Return-List usually provides additional parameters that the NAS needs to complete the connection, typically as part of PPP negotiations. They can thus be considered to be “authorization configuration parameters.”

By including appropriate attributes in the Return-List, a variety of connection policies could be applied. Specific users could be assigned particular IP addresses or IPX network numbers, IP header compression could be turned on or off, or a time limit could be assigned to the connection.

A Return-List is created by selecting attributes from a list of all RADIUS attributes known to the Steel-Belted Radius server. This list may include a variety of vendor-specific attributes.

During authentication, Steel-Belted Radius “filters” the Return-List based on the dictionary for the Make/model of the specific RAS Client that sent the authentication request. The server omits any Return-List attribute that is not valid for this device.

Attribute Values

The value of each RADIUS attribute has a well-defined data type, which may be numeric, string, IP or IPX address, time, or hexadecimal.

For example, Callback-Number is of type string and contains a telephone number. NAS-Port-Type is an item from a list, and may be Sync, Async, and so forth.

Multi-valued Attributes

Attributes may be single- or multi-valued; in other words, certain attributes may appear at most once in the Check-List or Return-List, while others may appear multiple times.

If an attribute appears more than once in the Check-List, this means that any one of the values is valid. For example, you may set up the Check-List to include both Sync and Async values for attribute NAS-Port-Type. This means that the user can dial into a Sync port or an Async port, but not one of the ISDN ports.

If an attribute appears more than once in the Return-List, this results in each value of the attribute being sent as part of the response packet. For example, to enable both IP and IPX header compression for a user, the Framed-Compression attribute should appear twice in the Return-List: once with the value VJ-TCP-IP-header-compression and once with the value IPX-header-compression.

Orderable Attributes

Certain multi-valued Return-List attributes are also orderable; that is, the attribute may appear more than once in a RADIUS response, and the order in which the attributes appear is important.

For example, the Reply-Message attribute allows text messages to be sent back to the user for display. A multi-line message is sent by including this attribute multiple times in the Return-List, with each line of the message in its proper sequence.

System Assigned Values

Some attributes do not allow the administrator to set a value. Steel-Belted Radius will retrieve the appropriate value for this attribute when it is needed.

The Echo Property

Using the echo property, you can force an attribute from the RADIUS request to be echoed in the RADIUS response.

Suppose, for example, you add Callback-Number to the Return-List and select the **echo** checkbox. Steel-Belted Radius will take the value of the Callback-Number it receives in the RADIUS request and echo it back to the client in the RADIUS response; if it receives no Callback-Number, it echoes nothing.

Let us further suppose that you enter `Callback-Number` one or more times into the Check-List. This indicates that one of the callback numbers you supplied must be present in the RADIUS request, and that number should be echoed in the RADIUS response.

Default Values

By selecting **default** for any Check-List attribute, you indicate that if the RADIUS request does not include this attribute, the request should not be rejected. Instead, the value supplied as the default should be used as if it were received as part of the request.

One use for default values is to require that an attribute in a RADIUS request must have one of several values, or must not be present at all.

Another use would be to provide a default value for an attribute in conjunction with the echo property in the Return-List. If an attribute appears once in the Check-List marked as **default**, and the same attribute appears in the Return-List marked as **echo**, this means the following:

- If the attribute does appear in the RADIUS request, the server will echo it in the RADIUS response.
- If the attribute does not appear in the RADIUS request, the server will echo the default value (from the Check-List) in the response.

Note that if you add multiple values of the same attribute to the Check-List, only one of them can be marked as **default**.

Suppose, for example, you add several Callback-Number values to the Check-List and mark one of them as default. Also, you add `Callback-Number` to the Return-List and specify it as **echo**. Here’s what happens:

- If a Callback-Number value is present in the RADIUS request, it must match one of the Check-List values or the user will be rejected.
- If it does match, the user is accepted and the value supplied is echoed in the RADIUS response.
- If no `Callback-Number` is supplied in the request, the user is accepted and the default value is echoed in the response.
- Other Check-List attributes are used to provide configuration for the user, such as time-of-day and concurrent-login-limit information.

Wildcard Support

Steel-Belted Radius supports wildcards (‘?’ and ‘*’) for string-type attributes in checklist items and for IP addresses using a network number.

To allow backward compatibility with checklist items that treat the string literally, a string containing wildcards must be prefixed with a caret (‘^’). When the caret is present, the remainder of the string is parsed using escape rules.

A ‘?’ matches any character and an ‘*’ matches the remainder of the string (but may only appear at the end of a string). Wildcard characters may be treated as literals by using escape codes (for example, ‘\?’). The following non-ASCII characters may also be present in the wildcard string:

Code	Meaning
\a	BEL
\b	BS
\f	FF
\n	LF
\r	CR
\t	HT
\v	VT
\\	Backward backslash
*	Literal ‘*’ (not wildcard)
\?	Literal ‘?’ (not wildcard)
\x*nn*	Where *nn* is a hexadecimal value
\nnn	Where *nnn* is a decimal value

A ‘\’ followed by any other character represents that character’s value.

The following is a wildcard example for string type attributes:

```
Called-Station-ID = ^800*
```

where `Called-Station-ID` indicates any 800 number.

The following is a wildcard example for IP Addresses:

```
NAS-IP-Address = 199.100.10.0
```

where `NAS-IP-Address` indicates any IP address on the 199.100.10.0 network.

Profiles

Steel-Belted Radius lets you define default templates of Check-List/Return-List pairs called *Profiles*. A Profile provides specific attributes for one or both lists. You may define as many Profiles as you wish. This feature provides a powerful means of managing and configuring accounts.

See “Profiles Dialog” on page 65.

When you edit a User entry, you may select a Profile. When you do, Steel-Belted Radius assigns this Profile to the User. That is, this Profile’s Check-List and Return-List attributes become the default settings for the User entry. This saves time (and the risk of typing errors!) compared to editing the lists individually. Profiles thus provide a management solution that is scalable and efficient in terms of time and storage space.

Once you assign a Profile to a User entry, you are free to modify the new entries on the User’s Check-List and Return-List. All of the changes you make are local variations that apply only to this User entry; they do not affect the Profile itself. Assigning a Profile and then overriding individual attributes is a convenient way to leverage Steel-Belted Radius’s features to your advantage.

See “Editing User Settings” on page 60.

If you’d like to change attributes settings across many users at once, you can do so by editing the Profile that you’ve assigned to these users; the changes you make to the Profile are automatically reflected in each user’s Check-List and Return-List.

Resolving Profile and User Attributes

If there are user-specific attributes stored in an external database, the Steel-Belted Radius server determines the final set of attributes for a user by merging the attributes stored in the native database with those retrieved from the external database. This calculation is performed as follows:

1. The attributes from the Profile (or Alias user) assigned to the user are first retrieved.
2. These attributes are then merged with the user-specific modifications to the attributes in the following manner:
   - If the attribute is multi-valued, then the attribute(s) retrieved from the external database is added to the overall list of attributes.
   - If the attribute is single-valued, then the attribute(s) retrieved from the external database replaces any attribute of the same name in the Profile or associated with the alias.

- If the attribute is orderable, then the attribute(s) retrieved from the external database replaces any orderable attribute of the same name in the Profile or associated with the alias.

Proxy RADIUS

Steel-Belted Radius can forward a RADIUS request to another server for processing and relay the other server's result back to its client. We say that Steel-Belted Radius is acting as a *proxy* for the *target* server, and that Steel-Belted Radius is *proxy-forwarding* the request to the target server.

Steel-Belted Radius fully supports Proxy RADIUS, in that every computer running it can act as either proxy or target for either authentication or accounting messages.

Proxy RADIUS Authentication

RADIUS authentication messages are proxy-forwarded as follows:

1 A RADIUS server receives an authentication message.

2 The first RADIUS server (the *proxy*) forwards the message to a second RADIUS server (the *target*).

3 The target performs the authentication services indicated by the message, then returns a response message to the proxy.

4 The proxy relays the response message to its original RADIUS client.

Proxy RADIUS Accounting

RADIUS accounting messages are proxy-forwarded as follows:

1 A RADIUS server receives an accounting request.

2 What the RADIUS server does next depends upon how it is configured for proxy accounting. The options are to:

(a) Forward the accounting message to a target server; *or*

(b) Record accounting attributes locally on the proxy server; *or*

(c) Both (a) and (b).

3 If the proxy server does not receive an acknowledgement of the forwarded packet, it will re-send periodically according to its retry policy.

.

Tunnels

This section provides background information about tunnels and explains how to configure the Steel-Belted Radius server to support them.

NOTE: Steel-Belted Radius does not add tunnel functionality to your network. Steel-Belted Radius is able to support the authentication and accounting needs of any tunnels that you've already set up.

A *tunnel* is a uniquely secure type of remote connection. A tunnel passes data between a remote site and an enterprise site, providing an additional layer of encrypted protocol “wrapper” around the data. A tunnel offers authentication and encryption features that help secure the connection against network vandals and eavesdroppers. In addition, it can provide quality of service features such as guaranteed bandwidth.

All administration and configuration of the tunnel happens at the remote site. This is the side of the connection that will request remote access and open the tunnel. An administrator at the remote site needs to configure the tunnel with various attributes: its destination IP address, what security protocols it supports, its password, and so on. These attributes are stored in a database to be retrieved when needed to set up a connection. It is useful to centralize the information by storing the tunnel attributes on a RADIUS server.

At connection time, the tunnel is established by a NAS device at the remote site. The NAS retrieves the tunnel configuration attributes from the RADIUS server and uses them to open the tunnel into the enterprise. Once the tunnel is open, the user can be authenticated at the enterprise.

A RADIUS server is said to “support tunnels” if it has the ability to store and retrieve the configuration data that a NAS needs to open a tunnel. Steel-Belted Radius fully supports tunnels. It can:

- Determine from the attributes in the incoming Access-Request whether or not the connection request involves a tunnel, and if so, which tunnel.
- Store and retrieve tunnel configuration data.
- Track the number of tunnels currently in use, compare to a maximum number, and refuse the connection if the number is exceeded.

Tunnel Authentication Sequence

The tunnel authentication sequence begins when an Access-Request arrives at the Steel-Belted Radius server:

1 Steel-Belted Radius checks to see if the Access-Request contains a Called-Station-Id attribute. If so, Steel-Belted Radius will search its database for a Tunnel entry that contains the indicated telephone number in its Called-Station-Id list.

NOTE: If realms are in use, Steel-Belted Radius will also search for this number in its realm configuration files. If a match is found, the Access-Request is routed to the realm, and the quest for a tunnel is abandoned. For this reason, it is important to ensure that DNIS numbers are unique across all Tunnel entries and across all realm configuration files.

If a match between the `Called-Station-Id` and a Tunnel entry can be found, Steel-Belted Radius will construct an Access-Accept message using the Attributes list in the matching Tunnel entry. It will then return the Access-Accept to the client NAS.

2 Steel-Belted Radius next checks to see if the Access-Request contains a username in the form *`User<Delimiter>TunnelName`* or *`TunnelName<Delimiter>User`*.

`<Delimiter>` is a single character that must match the server's tunnel delimiter character. The order of the realm name relative to the user name must match the server's tunnel naming convention (`prefix` or `suffix`). Both of these values are determined per server (that is, all tunnels that use this server must follow the same conventions) by entering them in the Configuration dialog.

Steel-Belted Radius will search its database for a Tunnel entry whose Tunnel name matches the incoming TunnelName.

If a match can be found, Steel-Belted Radius will construct an Access-Accept message using the Attributes list in the matching Tunnel entry. It will then return the Access-Accept to the client NAS.

3 If Steel-Belted Radius was able to match the Access-Request with a Tunnel entry, the NAS will use the attributes returned in the Access-Accept message to open a tunnel into the enterprise site. Authentication of the User-Name will now be attempted, usually at the enterprise site. If user authentication succeeds, the connection is complete. Otherwise, the user's connection request is denied.

If no matching Tunnel entry was found in steps 1 or 2, Steel-Belted Radius concludes that a tunnel is not involved in making this connection. It then continues with its User-Name parsing sequence determine a destination for the authentication request.

The following is a wildcard example for IP Addresses:

```
NAS-IP-Address = 199.100.10.0
```

where `NAS-IP-Address` indicates any IP address on the 199.100.10.0 network.

Configuring Tunnel Support

To configure the Steel-Belted Radius server to support a tunnel, you must open the Tunnels dialog in the Administrator program and add a Tunnel entry.

See “Tunnels Dialog” on page 73.

A Tunnel entry allows you to specify a list of connection Attributes such as the tunnel password, the IP address of the NAS at the enterprise site, encryption conventions to use, and so on. You can also enter the maximum number of tunnels that can be open at one time. You’ll need to coordinate with the administrator at the enterprise site to get some of this information.

Called Station Id

DNIS (Dialed Number Information Services) refers to a capability that many NAS devices have to determine and use the telephone number that was dialed to make a connection request. The RADIUS standard supports DNIS by specifying the following attributes:

- `Calling-Station-Id` is the number from which the user originated the request.
- `Called-Station-Id` is the telephone number that was dialed to make the network connection.

When setting up a Tunnel entry for the Steel-Belted Radius database, you can enter a telephone number or list of numbers in the **Called Station Id** list box on the Tunnels dialog. This list box identifies Called-Station-Id attribute values that the server should expect to find in tunnel connection requests.

Dictionaries for Tunnel Support

The Tunnels dialog allows you to create the Attributes list by selecting attributes from a drop-down list. The available selections include attributes from all standard and vendor-specific RADIUS dictionaries installed on the Steel-Belted Radius server.

Whenever the server is able to accept a tunnel connection request, it consults the corresponding Tunnel entry for the list of Attributes to return in the Access-Accept packet. Steel-Belted Radius will always return any standard RADIUS attributes that appear in the Attributes list. It will also return any vendor-specific attributes that are appropriate for the Make/model of the NAS that requested the tunnel connection. Vendor-specific attributes that appear in the Attributes list, but that do not apply to the requesting NAS, are ignored.

IP Address Assignment

Steel-Belted Radius can assign IP addresses in one of the following ways:

- Static assignment. Each time the user connects, the same specific address will be assigned. For example, if the user `Kevin` has the `Framed-IP-Address` attribute set to `123.11.245.123`, then each time Kevin connects to the network, the IP address 123.11.245.123 will be assigned.
- Assignment from a specific address pool. When the user connects, an address will be assigned from a specific pool. For example, if user `Kevin` has `Framed-IP-Address` set to the `Sales` IP address pool, when Kevin connects to the network, the next available IP address from `Sales` will be assigned.
- Assignment from the RAS Client’s IP address pool (or set of IP address pools). When the user connects, an address will be assigned from one of the pools associated with the RAS Client that makes the connection. For example, let’s say that:
    - a RAS Client called `NAS1` uses IP address pool A;
    - a RAS Client called `NAS2` uses IP address pool B; *and*
    - a User entry called `Kevin` has a `Framed-IP-Address` attribute value of `pool associated with RAS Client`.

  In this case, on connecting to the network, if user Kevin gets a port on `NAS1`, an IP address from pool A will be assigned. On the next call, Kevin might connect to `NAS2`; in this case an address from pool B will be assigned.

  Alternatively, if a user has been assigned to a particular NAS-Specific IP Address Pool (and suffix), an IP address from that pool will be assigned.
- Assignment from DHCP server. When the user connects, an address will be assigned (leased) from a DHCP server for a user-configurable period of time. This period should be significant (for example, twenty-four hours).

See "Specifying IP Address Assignment in User/Profile Records" on page 77.

Hints

Steel-Belted Radius can treat the attribute Framed-IP-Address as a *Hint*. This means that if this attribute appears in the Access-Request and the user return list is configured to allocate Framed-IP-Address from a pool, the IP address in the Access-Request is returned instead of the newly-allocated IP address.

This functionality is defined in the [Configuration] section of radius.ini:

```
[Configuration]
FramedIPAddressHint = <yes/no>
```

When hints are enabled, Steel-Belted Radius uses a hint to determine the value of the Framed-IP-Address attribute in the access response. This means that Framed-IP-Address in the Access-Request is returned in the Access-Accept, regardless of the Framed-IP-Address value stored in the user's account.

The default value is no.

The following table details the effect of hints:

Account Configuration	**Framed-IP-Address returned without hints**	**Framed-IP-Address returned with hints**
No Framed-IP-Address	No value	Framed-IP-Address from Access-Request
Static Address	Static address	Static address
Address from Pool	Next address from pool	Framed-IP-Address from Access-Request

NOTE: By using hints, you may assign the same IP address to multiple active accounts.

Resource Management

This section explains how Steel-Belted Radius manages limited resources, such as network addresses, user or tunnel connections, and UDP ports.

Network Address Assignment

The Steel-Belted Radius address pooling feature allows you to set up one or more pools out of which unique network addresses will be assigned dynamically as users require them. Each pool consists of a list of one or more ranges of IP addresses (an IP pool) or IPX network numbers (an IPX pool).

By using this feature, you can avoid allocating specific fixed addresses to individual users. You can make fewer addresses go farther, and you can consolidate address assignment across all your NAS devices.

How Address Assignment Works

Proper operation of address assignment from a pool depends crucially on both RADIUS authentication and RADIUS accounting transactions, as follows:

1. During the RADIUS authentication transaction, if the user's attribute settings specify address assignment from a pool, an address is allocated for that user from that pool.
2. The address is reserved for that user until a RADIUS accounting transaction indicates that the user has terminated the connection.

For this reason, it is essential that the NAS device be configured for RADIUS accounting and that the same Steel-Belted Radius server be specified for both authentication and accounting.

If your NAS is not configured for accounting (or does not support accounting) you cannot use the address pooling feature because addresses would be assigned but never released.

Setting Return-List Attributes

The `Framed-IP-Address` (or `Framed-IPX-Address`) Return-List attribute controls how the user's IP (or IPX) address will be assigned. For each user known to the Steel-Belted Radius Administrator program, the `Framed-IP-Address` or `Framed-IPX-Address` attribute may be set.

Handling Address Leaks

Under optimal conditions, the system will take care of assigning and releasing addresses without any need to intervene. But in some circumstances, you can get *address leakage*; that is, an address is still being reserved for a user even after the user has terminated the connection.

Address leakage occurs when the address has been assigned during the authentication transaction, but the accounting transaction that would have released the address is never received by Steel-Belted Radius. This could occur for a variety of reasons:

- The Steel-Belted Radius server may have been taken down for a period of time during which accounting transactions occurred.
- The NAS device may have been taken down or crashed before the user terminated. (In many cases, however, Steel-Belted Radius may be able to prevent address leakage by recovering the addresses when the NAS starts up again.)
- The NAS may have sent the authentication and accounting transactions to a different RADIUS servers.
- Despite a successful authentication, the user's PPP negotiation with the NAS may have terminated unsuccessfully for a variety of reasons. In such a case, some NAS devices may not initiate a subsequent accounting transaction.
- Routing problems may have prevented the accounting transaction from reaching Steel-Belted Radius.

An address that has "leaked" will remain out of circulation until you manually release it by displaying the Sessions list and deleting the corresponding session.

See "Deleting Entries from the Sessions List" on page 109.

Address Leakage upon Stopping and Starting the Server

Steel-Belted Radius maintains all current address assignments in a persistent database on disk. If you shut down the server and then restart it, all the information about which address is assigned to which user will be retained.

Note that if you leave Steel-Belted Radius turned off for a substantial period of time after addresses have already been assigned, you run the risk of address leakage as described above. When you start the server up again, be sure you review the Current Users dialog and delete any entries you know to be obsolete.

Overlapping Address Ranges

If you have multiple IP or IPX address pools, it is perfectly permissible to duplicate some of the addresses among the pools. Steel-Belted Radius's address tracking mechanism, when it is enabled, ensures that if an IP address appears in more than one pool, once it is assigned out of any pool it will be unavailable through any of the pools until it is released.

You will have to disable this type of address tracking if the server is assigning IP addresses from disjoint networks. In that configuration, two numerically identical IP addresses would signal a conflict, even though they actually belong to two different networks.

Order of Address Assignment

IP or IPX addresses are assigned on a FIFO basis; that is, the address that was first released is the first to be reassigned. This ensures that addresses are out of use for as long as possible prior to reuse.

Concurrent Network Connections

The Steel-Belted Radius Administrator program allows you to limit the number of active connections, on a per-user, or per-tunnel basis.

Concurrent User Connections

You can set a maximum limit on the total number of concurrent connections that a user may have. Subsequently, when the user requests a new connection, Steel-Belted Radius compares the current number of connections to the maximum limit. If a new connection would exceed the limit, Steel-Belted Radius can either:

- Reject the additional connection; *or*
- Allow the connection, but log the event in the Authentication log.

NOTE: When counting connections, Steel-Belted Radius will not distinguish between multi-link connections and new user authentication attempts.

For concurrent connection limits to work, it is essential that each NAS be configured for RADIUS accounting and that the same Steel-Belted Radius server be responsible for both authentication and accounting. These conventions give the server full access to the data it needs to accurately track connections.

The maximum number of concurrent connections may be set individually for any User entry of any User-type. The concurrent connection limit is set in the Users dialog by selecting the **Maximum Concurrent Users** checkbox and entering a number in the accompanying field.

See “Users Dialog” on page 59, especially “Concurrent Connection Limits” on page 63.

For individual users, a limit will apply to the user; for groups, a limit will apply to all members of the group. For example, if GroupA has a connection limit of 2, then users `\\GroupA\userID1` and `\\GroupA\userID2` (on an NT-based server) will each be entitled to 2 concurrent connections.

Authentication methods that do not require User entries must provide alternate mechanisms for supporting concurrent connection limits. For example, if you are using external database authentication there is an alias mechanism you can use in the SQL or LDAP configuration file. Concurrent connection limits can be supported under proxy authentication only if the target server supports them.

NOTE: Concurrent user connections can be tracked across multiple Steel-Belted Radius servers by adding the Concurrency Server package.

Concurrent Tunnel Connections

The Steel-Belted Radius server uses its Sessions list to determine the number of active connections for each Tunnel. The Sessions list summarizes all of the RADIUS accounting data currently available to the server. Tunnel connections appear in the Sessions list using a special display convention that distinguishes them from user connections.

You can set a maximum limit on the total number of concurrent connections that can be open using a specific Tunnel. Subsequently, when a user requests a new connection via that Tunnel, Steel-Belted Radius compares the current number of connections to the maximum limit. If a new connection would exceed the limit, Steel-Belted Radius rejects the additional connection.

For concurrent connection limits to work, it is essential that each NAS that may open a tunnel be configured for RADIUS accounting and that the same Steel-Belted Radius server be specified for both authentication and accounting. This permits the server's Sessions list to be kept up to date and available to every NAS that needs to authenticate tunnel connections.

NOTE: Concurrent tunnel connections cannot be tracked across multiple Steel-Belted Radius servers without the addition of further software extensions. Contact Funk Software for more information.

Phantom Records

The Steel-Belted Radius server allocates certain limited resources to its clients; these resources include IP addresses, IPX addresses, user connections, and tunnel connections.

Each time a client is allocated a resource, the Steel-Belted Radius server generates a *phantom* accounting record for its internal use. Phantom records are not written to the RADIUS accounting database, but they are displayed in the Sessions List window, where they closely resemble accounting start records; the only difference is that the phantom records display `N/A` in the Session-ID column.

See "Sessions List" on page 107.

Once the Steel-Belted Radius server receives the corresponding accounting start request packet from the client, the phantom record is no longer needed. Steel-Belted Radius discards the phantom and, in the Sessions List display, replaces `N/A` with the actual `Session-ID` number returned by the client device.

In some cases, a user may be allocated a resource and a phantom record may be created, but the Steel-Belted Radius server may never receive a corresponding start packet from the client. Since the resource will be tied up from the moment it is allocated to the user, it is desirable to limit the amount of time spent waiting for the start packet to confirm the transaction.

The default time that the Steel-Belted Radius server will wait is 180 seconds. You can modify this time by editing the `radius.ini` file.

See "radius.ini [Configuration] Section" on page 139.

Technical Bulletins

For information about special features that have been added to Steel-Belted Radius, see the Technical Bulletins that appear at the end of this manual.

Administration

4

The Administrator Program

The Steel-Belted Radius Administrator (radadnt.exe under Windows) lets you easily and flexibly control all aspects of Steel-Belted Radius. In minutes you can set up new users, alter standard profiles, or configure new NAS devices from any computer on the network.

NOTE: For large-scale changes to the Steel-Belted Radius database, it may be more convenient to use its LDAP command line interface. See "LDAP Configuration Interface" on page 240.

Running the Administrator

To run the Steel-Belted Radius Administrator program:

- Under **Windows**, double-click the **RADIUS Administrator** icon.
- Under **Unix**, open the index.html or default.htm file in your browser. This file is located in the java subdirectory under the admin directory that you defined when you installed Steel-Belted Radius on the UNIX machine, usually at path /radadmin/java.

The Administrator's main window appears and displays the Servers dialog. A panel of radio buttons to the left of the main window allows you to select the dialogs you want to display. However, you must use the Servers dialog to connect to a specific Steel-Belted Radius server before the other dialogs are enabled.

If you are running **Unix**: When you click **Connect**, you will be prompted to enter an administrative account name and password. Do so and click **OK**.

Dialogs and menu items will be available to you only if the account under which you've connected to the server has the right to access those items.

See "Servers Dialog" on page 53.

Help with the Administrator

To get help with the Steel-Belted Radius Administrator:

- Under **Windows**: Press **[F1]** or select **Help > Topics** from the Administrator menu.
- Under **Unix**: Click the **Help** button at the bottom of any Administrator dialog.

To identify the current version of the Steel-Belted Radius Administrator:

- Under **Windows**: Select **Help > About** from the Administrator menu.

- Under **Unix**: Click the **About** button just beside the **Help** button.

Exiting the Administrator

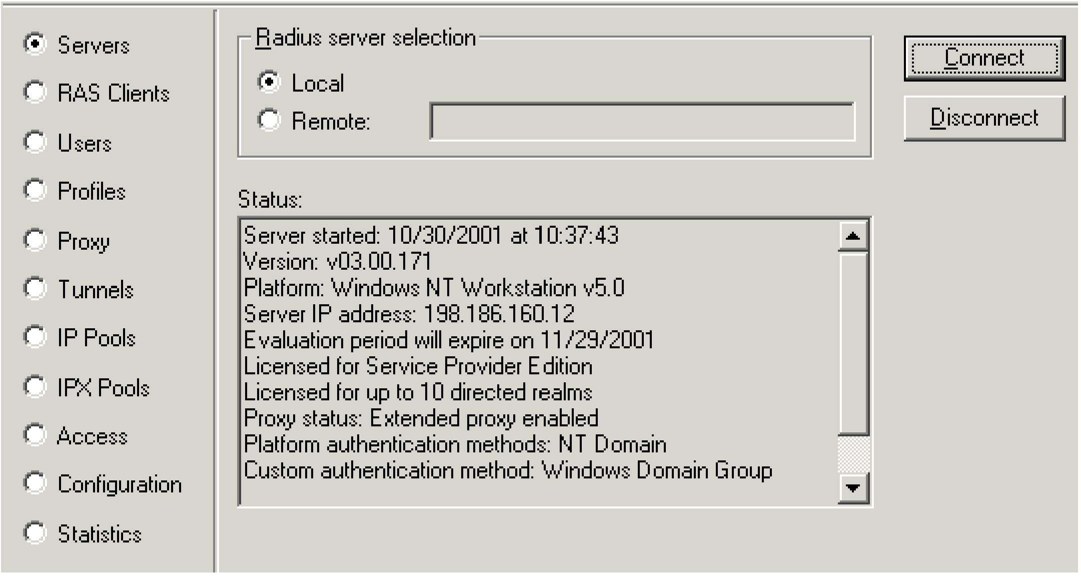
To close the Administrator program:

- Under **Windows**: Select **File > Exit** from the Administrator menu.
- Under **Unix**: Select the Servers dialog and click **Disconnect**. Then close your browser.

Closing the Administrator has no impact on the Steel-Belted Radius service or daemon, which will continue to operate normally.

Servers Dialog

The Servers dialog lets you select which Steel-Belted Radius server to administer within your network.



```
Server started: 10/30/2001 at 10:37:43
Version: v03.00.171
Platform: Windows NT Workstation v5.0
Server IP address: 198.186.160.12
Evaluation period will expire on 11/29/2001
Licensed for Service Provider Edition
Licensed for up to 10 directed realms
Proxy status: Extended proxy enabled
Platform authentication methods: NT Domain
Custom authentication method: Windows Domain Group
```

Servers dialog (Windows version)

Once you've connected to a server, the **Status** panel will list various features of the running server, such as version, platform on which it is running, IP address, available authentication methods, license information, and any initialization errors that may have occurred.

Steel-Belted Radius allows you the administrative rights that have been assigned to the account under which you connect to the server. These rights govern which server settings you may or may not view or change. Based on these rights, you may or may not be able to select some of the Administrator dialog buttons.

Unix

The RADIUS **Server Selection** panel lets you choose which server to administer. To use this panel, either:

- Select the **Local** machine where you’re running the Administrator program and click **Connect**; *or*
- Select **Remote**, enter the name of the machine, and click **Connect**.

When you click **Connect**, the server displays a dialog prompting you to enter an administrative account name and password. This may be:

The default Steel-Belted Radius administrative account (admin), whose password you may configure using the Access dialog; Enter the account name and password in the dialog, then click **OK**.

See “Access Dialog” on page 82.

Windows

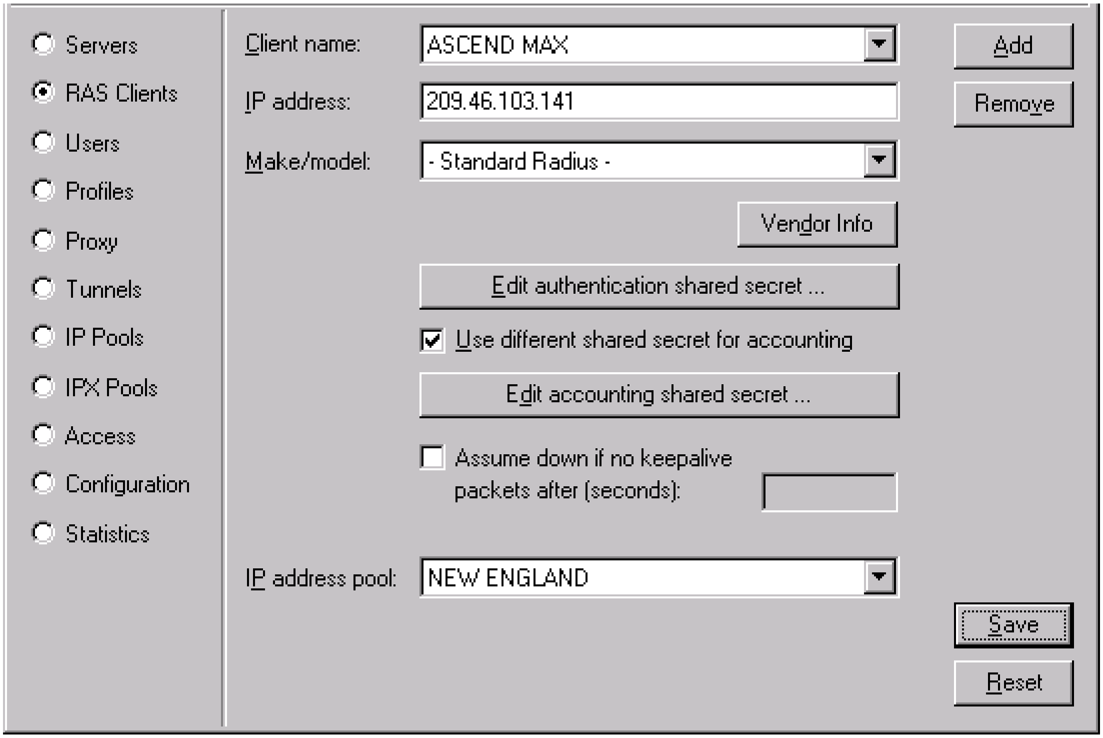
The RADIUS **Server Selection** panel lets you choose which server to administer. To use this panel, either:

- Select the **Local** computer where you’re running the Administrator program and click **Connect**. The Administrator program verifies that the account under which you logged into the local machine has been enabled for Steel-Belted Radius administration using the Access dialog. If so, it permits you to connect; *or*
- Select **Remote** and enter the name of the computer; then click **Connect**. The Administrator program examines the remote machine for an NT user or group account that matches the username and password under which you logged into the local machine. If found, it verifies that this account has been enabled for Steel-Belted Radius administration using the Access dialog. If a match can be found, the Administrator permits you to connect to the remote machine under this account.

See “Access Dialog” on page 82.

RAS Clients Dialog

The RAS Clients dialog lets you identify the devices that you want to be clients of the Steel-Belted Radius server.



○ Servers
● RAS Clients
○ Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

Client name: ASCEND MAX

IP address: 209.46.103.141

Make/model: - Standard Radius -

☑ Use different shared secret for accounting

□ Assume down if no keepalive packets after (seconds):

IP address pool: NEW ENGLAND

Add
Remove
Vendor Info
Edit authentication shared secret ...
Edit accounting shared secret ...
Save
Reset

RAS Clients Dialog (Windows version)

See also "RADIUS Configuration" on page 22.

Adding a New RAS Client

To add a new RAS Client:

1 Click the **Add** button. The Add New RAS Client dialog appears.

2 Enter the name of the RAS Client you'd like to add.

NOTE: Although you can assign any name to a RAS Client entry, it is a good practice to use the device's actual name; this is normally the device's IP host name as well.

3 Click **OK** to return to the RAS Clients dialog.

The name appears in the **Client name** field, with blank settings beneath.

4 Edit the settings, being sure to fill in all required fields.

5 Click **Save** to make your changes permanent.

Editing RAS Client Settings

Once you've edited any of the RAS Client settings, you may click **Save** to make your changes permanent. If you change your mind and want to cancel your edits, click **Reset**.

IP Address

Enter the RAS Client's IP address directly into the **IP Address** field. You can enter the DNS name of the device; the name you entered will be resolved and the corresponding IP address will be entered automatically into the **IP Address** field.

Make/model

The **Make/model** field offers a drop-down list from which you may select the make and model of the client device (Ascend MAX Family, Nortel CVX 1800, and so forth). Your **Make/model** selection tells Steel-Belted Radius the correct dictionary of RADIUS attributes to use when communicating with this client.

See "Dictionary Files" on page 151.

To select the Make/model:

1 For information about the various brands of NAS device supported by Steel-Belted Radius, you may click the **Vendor Info** button to display a detailed help file.

2 Click the **Make/model** drop-down box to bring up a list of the available NAS device makes and models.

3 Scroll through the list and select the item you wish; it will be displayed in the **Make/model** field. If you are not sure which make and model you are using, or if your device is not in the list, select **- Standard Radius -**.

IP Address Pool

The **IP Address Pool** field specifies the pool from which Steel-Belted Radius will select IP addresses when authenticating an access request from this RAS Client. This field is optional and may be left blank.

To associate the RAS Client with an IP address pool:

1 Click the **IP Address Pool** drop-down box to bring up a list of previously configured IP address pools.

2 Scroll through the list and select the item you wish; it will be displayed in the **IP Address Pool** field.

NOTE: Only IP address pools that have been configured, by the IP Pool Dialog and other means, will appear on the list. See "IP Pools Dialog" on page 76.

Shared Secret

See also "RADIUS Shared Secret" on page 24.

To enter the shared secret for authentication:

1 Click **Edit authentication shared secret**. The Shared Secret dialog appears.

2 To enter a shared secret, simply type it into the dialog and click **Set**.

3 For privacy, asterisks will be echoed as you type. But if no one is looking over your shoulder, you can check **Unmask shared secret** to see what you're typing and make sure it is correct.

4 These steps complete configuration of the authentication shared secret on the server side. Be sure to enter the same authentication shared secret when you configure the NAS device.

To enter the shared secret for accounting:

1 If you wish to use the same shared secret for authentication and accounting, ensure that the **Use different shared secret for accounting** box is unchecked before you click **Save** in the RAS Clients dialog.

2 Otherwise, enter a secret for accounting as follows: In the RAS Clients dialog, check the **Use different shared secret for accounting** box and click **Edit accounting shared secret**. Enter the accounting shared secret into the pop-up dialog and click **Set**.

3 These steps complete configuration of the accounting shared secret on the server side. Be sure to enter the same accounting shared secret when you configure the NAS device.

4 If you ever need to verify a shared secret on the Steel-Belted Radius server side, in the RAS Clients dialog click the appropriate **Edit** button, enter the shared secret, and click the **Validate** button. You'll be told whether the shared secret is what you think it is.

Assume Down

If you check the **Assume down if no keepalive packets** box, you can enter a value in the **after (seconds)** field. If the server has not received any RADIUS packets from this client after this number of seconds, it will assume that the client device has gone down.

Steel-Belted Radius will then gracefully close any user or tunnel connections that it has authenticated for this device. That is, Steel-Belted Radius will release any pooled IP or IPX addresses and adjust the counts of concurrent user or tunnel connections appropriately.

WARNING: Give thought to the value that you set for this field. If the after (seconds) value is set too small, valid user or tunnel connections may be lost. For example, during low usage periods, there may be many NAS devices that send no RADIUS packets to the Steel-Belted Radius server; however, these devices are still "up."

Adding a Wildcard RAS Client

A special RAS Client entry, called `<ANY>`, allows Steel-Belted Radius to accept requests from any NAS or Proxy RADIUS server, as long as the shared secret is correct.

To add an `<ANY>` entry:

1 Click **Add**. The Add New RAS Client dialog appears.

2 Check **Any RAS Client**, then click **OK**. You will now see `<ANY>` in the **Name** field, with blank settings beneath.

3 Update the Make/model and shared secret(s) for this item, then click **Save** to make your changes permanent.

Note that the **IP Address** field cannot be edited. `<ANY>` implies that the server will accept requests from any IP address, provided that the shared secret is correct.

Removing a RAS Client

To remove a RAS Client from the list:

1 Click the **Name drop-down** list and select the RAS Client you would like to remove.

2 In the RAS Clients dialog, click **Remove**.

3 You are prompted to confirm the operation. Click **Yes**.

Users Dialog

The Users dialog lets you configure RADIUS authentication details. Each User entry in the Steel-Belted Radius database identifies one method by which the server can authenticate a specific user. The **User name** field identifies the user; the **User type** field identifies the method.

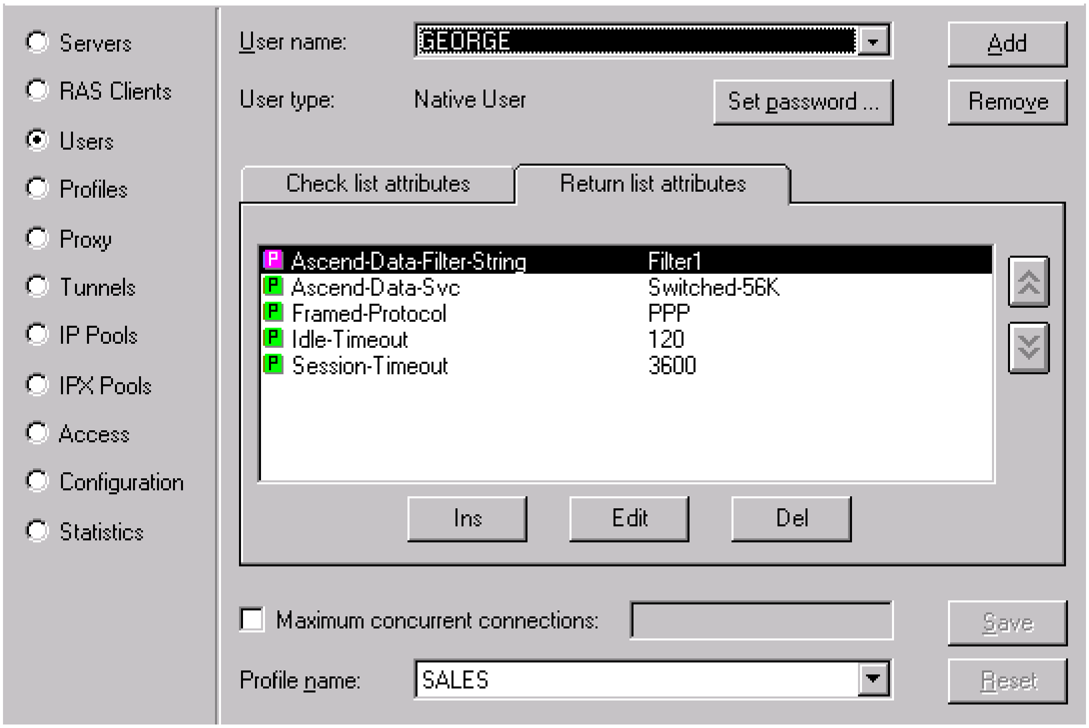
See "Authentication Methods" on page 26 and "Configuring Authentication Methods" on page 27.

There is more than one way to populate the User database for Steel-Belted Radius. You can use the Administrator program, Users dialog, as described in this topic. Alternatively, you can import data from other servers.

See "Import/Export Capabilities" on page 89.

Using the Users Dialog

The Users Dialog allows you to manipulate the records of individual user accounts.



User name: GEORGE

User type: Native User

P Ascend-Data-Filter-String	Filter1
P Ascend-Data-Svc	Switched-56K
P Framed-Protocol	PPP
P Idle-Timeout	120
P Session-Timeout	3600

□ Maximum concurrent connections:

Profile name: SALES

Users Dialog (Windows version)

To create a new User entry, click **Add** and follow the detailed instructions in the next several sections.

Use the button to the right of the **User name** list box to select the User entry you want to view or edit. Users of all local types will be listed together in alphabetical order. You may select a name from the list.

Windows

The name will be displayed in the Users dialog, **User name** field. The user's other settings will be displayed in the remaining fields of the Users dialog.

Unix

The list of users in the **User name** field is not generated until you click the button. To avoid the time required to build the list, if you know the specific name for which you want to search, click the **Find** button instead. A dialog displays in which you may enter the name.

Pay attention to case when typing the name in the Find User dialog, or you may be unable to find the User entry. Native User entries in the Steel-Belted Radius database have all-uppercase names; the names are converted to all-uppercase letters when the Native User entry is created, and they remain all-uppercase for the life of the entry.

For example, a name entered as **realLife1** in the Add User dialog is stored as `REALLIFE1` in the Steel-Belted Radius database. Usernames stored in a database outside Steel-Belted Radius (UNIX, SecurID, TACACS+) retain their case as stored in that database.

After you've entered the name in the Find User dialog, click **OK**. The name will be displayed in the Users dialog, **User name** field. The user's other settings will be displayed in the remaining fields of the Users dialog.

Editing User Settings

This section describes fields that you can set for any User entry, regardless of User type. Useful references include the following:

"User Attribute Lists" on page 33 and "Profiles Dialog" on page 65.

Selecting a Profile

We strongly recommend that you make use of the powerful Profile feature, rather than separately entering Check-List and Return-List attributes and values for each User entry.

To select a Profile for a User entry:

1. Click the **Profile name** drop-down list.
2. Select the profile you’d like to use, or select **<no profile>**.

Adding New Attributes

To add Check-List or Return-List attributes to a User entry:

1. Click the **Check List Attributes** tab or **Return List Attributes** tab.
2. Click **Ins**.
3. The Add New Attribute dialog appears. You will be able to add as many attributes as you want before closing this dialog. The dialog is positioned so that as you add attributes you can see them appear in the list.

   Use the dialog as follows:

   - Select an item from the list of **Available attributes**.
   - You’ll be able to tell whether you can add multiple values for this attribute by noting the state of the **Multi-Valued** indicator.
   - Enter a value for the attribute in the space to the right of the attribute list. The method for entering a value varies with the type of attribute. You may need to enter a string, a numeric value, or select from a list of items.
   - (Check-List attributes only) If you want to set this value as the default value for the attribute in case the attribute is not included in the RADIUS request, check the **Default** box.
   - (Return-List, single-valued attributes only) If you don’t want to specify a particular value, but want to make sure that whatever value of the attribute appears in the RADIUS request is echoed to the client in the RADIUS response, check **Echo**.
   - Click **Add** to add this attribute/value pair to the list.
4. Click **Close** to return to the User dialog.

Setting Attribute Values

To change the value of an attribute already in the Check-List or Return-List for a User entry:

1. Click the **Check List Attributes** tab or **Return List Attributes** tab.
2. Highlight the attribute whose value you’d like to change.

3 Click **Edit** or double-click the attribute. A Change dialog displays.

Depending on the attribute, you may be asked to enter a new value or to select a value from a list. For some attributes, Steel-Belted Radius retrieves the value from the server and you cannot enter a value in this dialog.

4 If prompted, enter or select the new value.

5 Click **OK**.

Removing Attribute/Value Pairs

To remove an attribute/value pair already in the Check-List or Return-List for a User entry:

1 Click the **Check List Attributes** tab or **Return List Attributes** tab.

2 Highlight the attribute/value pair you'd like to remove.

3 Click **Remove**. The value is removed from the list.

Reordering Attributes

Certain attributes are multi-valued and orderable; that is, the attribute/value pair may appear more than once in a RADIUS response, and the order in which the attribute/value pairs appear is important.

To reorder attributes in a User entry:

1 Click the **Check List Attributes** tab or **Return List Attributes** tab.

2 Highlight an attribute/value pair in the list.

3 Click one of the double-up and double-down arrows, as follows.

NOTE: These arrows will be activated only if the attribute you've selected is both multi-valued and orderable; for example the standard RADIUS authentication attribute Reply-List.

Button	Action
⇈	Moves the selected attribute/value up in the list. If the attribute is not orderable, or if this item is already the first value for this attribute, then the button is disabled.
⇊	Moves the selected attribute/value down in the list. If the attribute is not orderable, or if this item is already the last value for this attribute, then the button is disabled.

Changing Attributes Inherited from a Profile

As noted earlier, Check-List and Return-List attributes can be directly entered for any user, or they may be inherited from the profile that has been selected as part of the user's settings.

Attributes that are inherited from a profile may be removed or modified locally; that is, any changes made to profile attributes for this user will not affect other users sharing the same profile.

Items that are inherited from the profile are marked with an icon:

Icon	Meaning
P	Indicates the inherited attribute is unchanged
↑	Indicates the inherited attribute has been changed
⊟	Indicates the inherited attribute has been removed

To change an attribute inherited from a profile, click **Edit** and proceed as you would normally. The modified attribute will be marked with ↑.

To remove an attribute inherited from a profile, click **Remove**. The attribute will not disappear from the display, but will be shown grayed and struck-through, and will be marked with ⊟.

To restore an attribute that you have changed or removed to its original value as specified in the profile, click **Remove**. The attribute will be reset to its unmodified state, and will be marked with P.

NOTE: If you accidentally delete a Profile that is in use as part of a User setting, you will see an error icon displayed on all lines dependent upon this Profile. If this occurs, delete the items in error and re-create the Profile.

Concurrent Connection Limits

See "Concurrent Network Connections" on page 47.

A maximum number of open connections may be set for each User entry by checking the **Maximum Concurrent Users** box and entering a number in the accompanying field. When the user requests access, this user (User name) can be authenticated using this method (User type) only if fewer than this number of connections are currently open for this user.

Adding a Native User

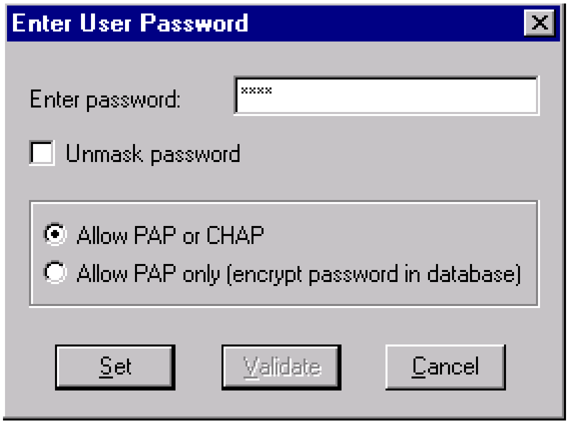
Native User entries require you to enter the user's name and password into the Steel-Belted Radius database. For all other types of User entry, the server relies on another database to confirm the user's password.

- Under **Windows** only: You must define a Native User entry for every user who requires remote access to your network. For example, you can accommodate UNIX- or Macintosh-based users by adding them as Native Users.

To add a new Native User:

1. Click the **Add** button on the right. The Add New User dialog appears.
2. Select the **Native** tab.
3. Enter the User name into the field and click **OK**. The Add New Users dialog closes.

   Back in the Users dialog, the **User name** field displays the name you've just entered. The **User type** field displays the authentication method Native User.
4. Click **Set Password**. The Enter User Password dialog appears.



Enter User Password

Enter password: ****

☐ Unmask password

● Allow PAP or CHAP

○ Allow PAP only (encrypt password in database)

Enter User Password dialog (Windows version)

Use the dialog as follows:

- If you'd like the actual password to be echoed as you type (rather than asterisks) check **Unmask password**. Enter the password for the new user.

  NOTE: The password is case-sensitive.

- If you'd like to enable both PAP and CHAP authentication, check **Allow PAP or CHAP**.
- If you want your password to be stored using *strong encryption* in the Steel-Belted Radius database, check **Allow PAP only (encrypt password in database)**. This option allows the user to authenticate only via PAP. However, the server database will be totally secure even if your server is compromised.
- To verify a password you've already entered, type the password in the dialog and click **Validate**. You'll be told whether the password is what you think it is.
- When you have completed any changes, click **OK**.

5 Back in the Users dialog, edit settings for the new entry.

6 To make your changes permanent, click **Save**.

7 To edit (or add) another User entry, select (or enter) a new User name and User type.

Removing a User Entry

To remove a User entry:

1 Open the Users dialog.

2 Click the **User name** drop-down list and select the user you would like to remove. (Under **Unix**: Click **OK** to proceed.)

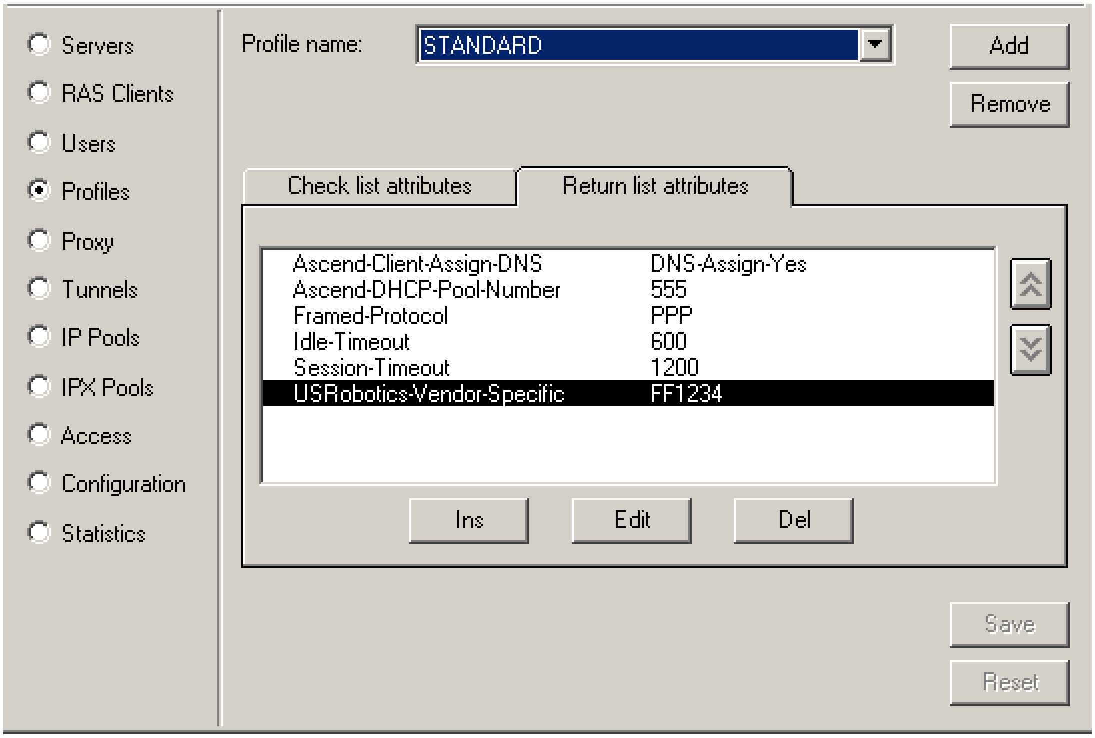
3 In the Users dialog, click **Remove**. You will be prompted to confirm the deletion.

4 Click **Yes**. The user is removed from the list.

Profiles Dialog

The Profiles dialog lets you define standard sets of Check-List and Return-List attributes. Any of these Profiles may then be assigned to a User entry.

See also "User Attribute Lists" on page 33.



Profile name: STANDARD

Ascend-Client-Assign-DNS	DNS-Assign-Yes
Ascend-DHCP-Pool-Number	555
Framed-Protocol	PPP
Idle-Timeout	600
Session-Timeout	1200
USRobotics-Vendor-Specific	FF1234

Profiles Dialog (Windows version)

Adding a Profile

To add a new profile:

1 Click **Add**. The Add New Profile dialog appears.

2 Enter a name for the new profile, and click **OK** to return to the Profiles dialog.

You will now see the name you entered in the Profiles dialog **Name** field, with an empty attribute list below.

3 Add Check-List and Return-List attributes for the new entry.

4 Click **Save** to make your changes permanent.

Editing Profiles

The settings for each Profile entry include Check-List and Return-List attributes. You can add, modify, and remove attributes in the Profile dialog just as you would in the Users dialog.

See “Editing User Settings” on page 60.

Removing a Profile

WARNING: Be sure you don't remove a Profile that is currently included in the settings of a User. You will be warned that the profile name is in use by one or more User entries. If you delete the profile anyway, the attributes defined in the Profile will disappear from that User’s settings; when you next display the User’s settings, you will get an error message asking you to edit and resave those settings.

To remove a Profile from the list:

1 Click the **Name** drop-down list and select the Profile you would like to remove. (Under **Unix**: Click **OK** to proceed.)

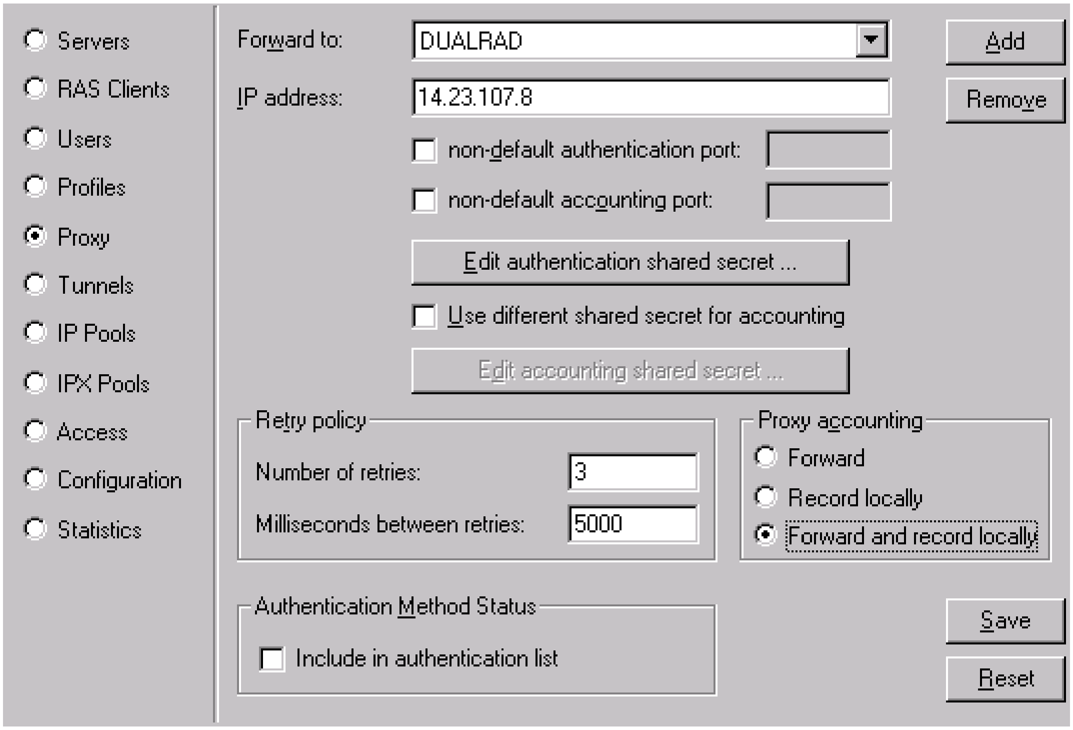
2 In the Profiles dialog, click **Remove**. You will be prompted to confirm the deletion.

3 Click **Yes**. The profile is removed from the list.

Proxy Dialog

The Proxy dialog lets you configure Steel-Belted Radius to forward RADIUS packets to another RADIUS server.

See also “Proxy RADIUS” on page 39.



○ Servers
○ RAS Clients
○ Users
○ Profiles
● Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

Forward to: DUALRAD

IP address: 14.23.107.8

□ non-default authentication port:

□ non-default accounting port:

□ Use different shared secret for accounting

Retry policy

Number of retries: 3

Milliseconds between retries: 5000

Proxy accounting

○ Forward
○ Record locally
● Forward and record locally

Authentication Method Status

□ Include in authentication list

Add
Remove
Edit authentication shared secret ...
Edit accounting shared secret ...
Save
Reset

Proxy Dialog (Windows version)

Adding a New Target

This section explains how to set up proxy forwarding from the Steel-Belted Radius server (the proxy) to another RADIUS server (the target).

To add a new target server:

1 In the Proxy dialog, click **Add**. The Add New Target Server dialog appears.

2 Enter the name of the target server you'd like to add.

You may label a Proxy entry with any name you like. Steel-Belted Radius will use the Proxy entry's **IP Address** field to route the RADIUS packets correctly, so the actual node name of the target server is not important. The only restriction upon the target name is that it must not duplicate any other target name, realm name, or tunnel name in your Steel-Belted Radius configuration.

3 Click **OK**. You will now see the name you entered in the **Forward to** field, with blank settings beneath.

4 Edit the settings for the new target server entry. Be sure you fill in all required fields.

5 Click **Save** to make your changes permanent.

6 Ask the administrator at the target site to log into the target server's RADIUS configuration program and add Steel-Belted Radius as a RADIUS client of the target server. You'll need to provide this administrator with the IP address of the Steel-Belted Radius server.

NOTE: Make sure that the same UDP port and shared secret are entered on both proxy and target sides.

Editing Proxy Settings

The settings for each target server include the target server's IP address and a secret key that is shared between this proxy server and the target server.

Once you've edited the settings, click **Save** to make your changes permanent. If you change your mind and want to cancel your edits, click **Reset**.

IP Address

You can enter the IP address directly into the **IP Address** field. Or, you can enter the DNS name of the target server; the name you entered will be resolved and the IP address will be entered automatically into the **IP Address** field.

UDP Ports

See "RADIUS Ports" on page 25.

You can enter the UDP port on which the target server receives RADIUS authentication traffic. If you do not already have this information, you'll need to acquire it from the administrator at the target site. To enter a port number, check the **non-default authentication port** box and enter a value in the accompanying field. If you do nothing, Steel-Belted Radius will use port 1645.

Similarly, you can enter a **non-default accounting port**. The default is 1646.

Shared Secret

See "RADIUS Shared Secret" on page 24.

To enter the shared secret for authentication:

1 Click **Edit authentication shared secret**. The Shared Secret dialog appears.

2 To enter a shared secret, simply type it into the dialog and click **Set**.

3 For privacy, asterisks will be echoed as you type. But if no one is looking over your shoulder, you can check **Unmask shared secret** to see what you're typing and make sure it is correct.

4 These steps complete configuration of the authentication shared secret on the Steel-Belted Radius side. Be sure to enter the same authentication shared secret when you configure the target server.

To enter the shared secret for accounting:

1 If you wish to use the same shared secret for authentication and accounting, ensure that the **Use different shared secret for accounting** box is unchecked before you click **Save** in the Proxy dialog.

2 Otherwise, enter a secret for accounting as follows: In the Proxy dialog, check the **Use different shared secret for accounting** box and click **Edit accounting shared secret**. Enter the accounting shared secret into the pop-up dialog and click **Set**.

3 These steps complete configuration of the accounting shared secret on the Steel-Belted Radius side. Be sure to enter the same accounting shared secret when you configure the target server.

If you ever need to verify a shared secret on the Steel-Belted Radius side, in the Proxy dialog click the appropriate **Edit** button, enter the shared secret, and click the **Validate** button. You'll be told whether the shared secret is what you think it is.

Retry Policy

When Steel-Belted Radius acts as a proxy, it needs to emulate the typical characteristics of a NAS device. This includes the ability to retransmit a request if it doesn't get a response within some interval of time.

There are two values that can be set:

- **Number of Retries**. This sets the number of times a request will be retransmitted in case an acknowledgment from the target is not received; if the number of retries is exhausted, then the original request will be rejected.
- **Milliseconds Between Retries**. This sets the time interval between each retry in milliseconds (thousandths of a second). For example, a value of 2000 indicates that retries should occur every 2 seconds.

Proxy Accounting

The Proxy Accounting setting lets you control how accounting transactions are handled for authentication requests that are forwarded. There are three options:

- **Forward**. Forward the accounting transaction to the same target server that the authentication transaction was forwarded to.
- **Record locally**. Do not forward the accounting transaction. Log the accounting transaction locally even though the authentication request was forwarded.
- **Forward and record locally**. Do both. Forward the accounting transaction and log the accounting transaction locally.

Proxy Authentication

In the Proxy dialog, the Authentication Method Status panel lets you set up a target server as an authentication method. After you check the **Include in authentication** list box, the target that you've defined using the Proxy dialog will appear in the Configuration dialog's **Authentication Methods** list as `proxy:` *`name`*, where *`name`* is the value you entered in the **Forward to** field.

This option is useful if you already have user records defined on an older RADIUS server and you want to provide a seamless migration to Steel-Belted Radius. You can set up the older server as a Proxy RADIUS target and check the **Include in authentication** list box. RADIUS requests that arrive addressed to this target will be handled by Steel-Belted Radius automatically, without requiring end users to change their addressing conventions.

NOTE: If the target that you're configuring is a member of a Proxy RADIUS realm, you should ensure that the Proxy dialog **Include in authentication list** *box is unchecked*.

Removing a Target

To remove a target server from the list:

1 In the Proxy dialog, click the **Forward to** drop-down list and select the target server you'd like to remove.

2 Click **Remove**.

Steel-Belted Radius as a Target

This section describes how to set up proxy forwarding from some other RADIUS server (the proxy) to the Steel-Belted Radius server (the target):

1 Set up the proxy as a RADIUS client of Steel-Belted Radius.

Add the entry using the RAS Clients dialog. Specify the proxy's name, its IP address, and the shared secret that you want to use for encryption between the proxy and Steel-Belted Radius.

2 Ask the administrator at the target site to log into the proxy's RADIUS configuration program and set up Steel-Belted Radius as a Proxy RADIUS target. You'll need to provide this administrator with the IP address of the Steel-Belted Radius server.

NOTE: Make sure that the same UDP port and shared secret are entered on both proxy and target sides.

Dictionaries when Steel-Belted Radius is the Target

When Steel-Belted Radius receives a proxy-forwarded packet, it consults its RAS Client entry for that proxy server. The **Make/model** field of this entry determines which attribute dictionary Steel-Belted Radius will use.

At various different times, Steel-Belted Radius may receive requests from the same proxy server that have originated from different NAS devices, possibly of different types. The single **Make/model** field that was entered for the proxy may not be adequate to handle the variety of NASs on the "other side" of the transaction.

One way to handle this problem is to add the originating NAS devices to Steel-Belted Radius's list of RAS Clients. Steel-Belted Radius can be configured to examine each proxy-forwarded packet for clues as to the make and model of the originating device. If clues are found, Steel-Belted Radius will do everything it can to map this information to a vendor-specific dictionary, and will use this dictionary in preference to the one for the proxy.

Accepting Packets from Any Proxy

If you'd like Steel-Belted Radius to be able to accept proxy requests from any IP address, you can use the RAS Clients dialog to add a special entry called `<ANY>`, and specify a shared secret. The `<ANY>` entry permits forwarded requests from any proxy to be accepted, provided the shared secret is correct.

NOTE: This feature will succeed only if proxies are configured to use the shared secret you provide in the `<ANY>` *entry.*

Proxy RADIUS as an Authentication Method

Any target server can be configured as a Steel-Belted Radius authentication method. Simply enable the **Include in authentication** list option in the corresponding Proxy database entry.

A target server can be set up as an authentication method even if the end users don't know anything about the target. That is, a user does not need to log in using a decorated username such as `User@TargetName` in order to be authenticated by the target server.

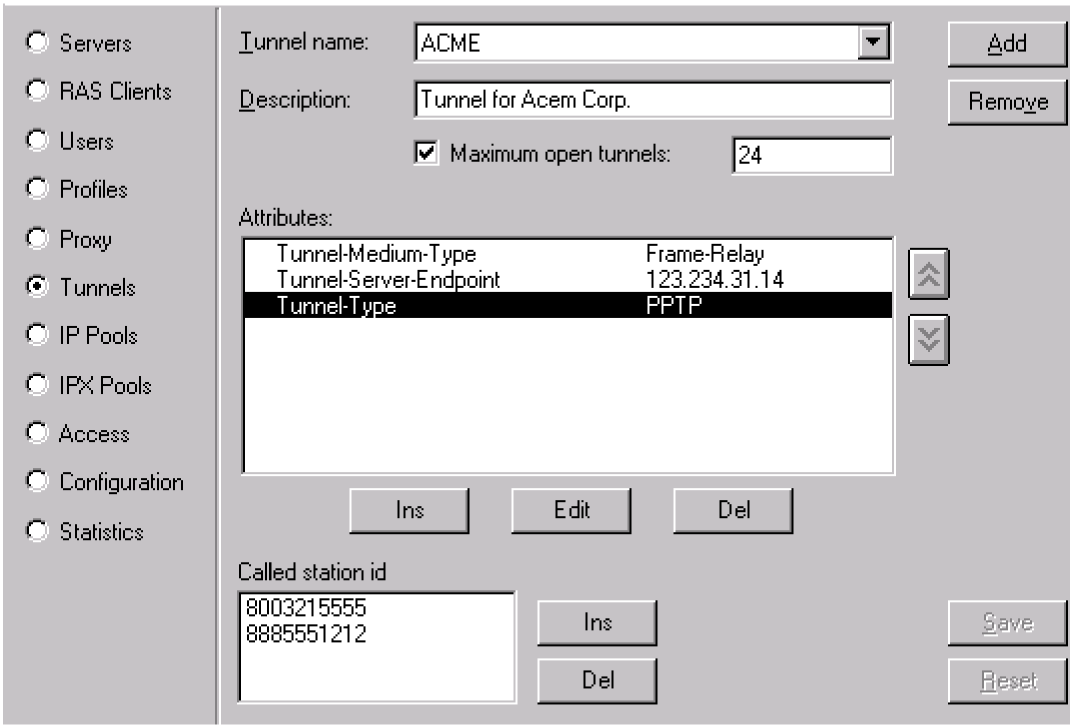
If you prioritize the `proxy:` *`TargetName`* authentication method above the Native User authentication method in the Authentication Methods list, the user can log in as `User` and Steel-Belted Radius will automatically send the request to the target for authentication. The authentication will succeed if the UserName and password are stored on the target, but if not, Steel-Belted Radius will reach the Native User method eventually, and the user can be authenticated then.

This technique is useful as a migration path to Steel-Belted Radius from other RADIUS servers. You can set up Steel-Belted Radius as the proxy and the old RADIUS server as the target. Once proxy authentication is enabled (in the Proxy dialog) and prioritized (in the Configuration dialog), Steel-Belted Radius can authenticate users against the old RADIUS server, either as an automatic "first choice" or as an alternative when authentication against the new server's "native" database fails.

Tunnels Dialog

The Tunnels dialog lets you configure Steel-Belted Radius to support tunnels. When you add a Tunnel entry, you're not creating a tunnel; you're enabling Steel-Belted Radius to support an existing tunnel's authentication and accounting needs.

See also "Tunnels" on page 40.



Tunnel name: ACME

Description: Tunnel for Acem Corp.

☑ Maximum open tunnels: 24

Attributes:

Tunnel-Medium-Type	Frame-Relay
Tunnel-Server-Endpoint	123.234.31.14
Tunnel-Type	PPTP

Called station id

8003215555
8885551212

Tunnels Dialog (Windows version)

Adding a Tunnel

To add a Tunnel entry:

1 In the Tunnels dialog, click **Add**. The Add New Tunnel dialog appears.

2 Enter the Tunnel name and click **OK**.

You may label a Tunnel entry with any name you like. It does not need to match the actual node name of a client tunnel server. The only restriction upon the tunnel name is that it must not duplicate any other target name, realm name, or tunnel name in your Steel-Belted Radius configuration.

You will now see the name you entered in the **Forward to** field, with blank settings beneath.

3 Edit the settings for the new Tunnel entry, as described below. Be sure you fill in all required fields.

4 Click **Save** to make your changes permanent.

Editing a Tunnel

The settings for each Tunnel include the maximum number of concurrent connections using this tunnel, and any attributes that the RAS client needs to complete the tunnel connection.

You can configure these settings using the Tunnels dialog, as follows:

1 Set the **Maximum open tunnels** number.

  See "Concurrent Tunnel Connections" on page 48.

2 Enter a text **Description** of the tunnel, for example the name of the organization that will use it. This text is for administrative use only and does not affect tunnel connections.

3 Each Tunnel entry may provide various Attributes. At the time of connection, these attributes will be filtered according to the Make/model of the RAS Client used to establish the connection.

  You can add, modify, and remove Attributes in the Tunnels dialog using similar techniques as in other dialogs. Use the **Ins**, **Edit**, and **Del** buttons underneath the **Attributes** list box, and the up- and down-arrow buttons to the right of the **Attributes** list box.

  See "Editing User Settings" on page 60, especially "Adding New Attributes" on page 61 and following.

4 To add a telephone number to the **Called station Id** list box, click the **Ins** button to the right of the list box. To delete a number, highlight it in the list and click **Del**.

  See "Called Station Id" on page 42.

5 Click **Save** to make your changes permanent, **Reset** to undo them.

Removing a Tunnel

To remove a Tunnel entry from the Steel-Belted Radius database:

1 In the Tunnels dialog, click the **Name** drop-down list and select the Tunnel you would like to remove. (Under **Unix**: Click **OK** to proceed.)

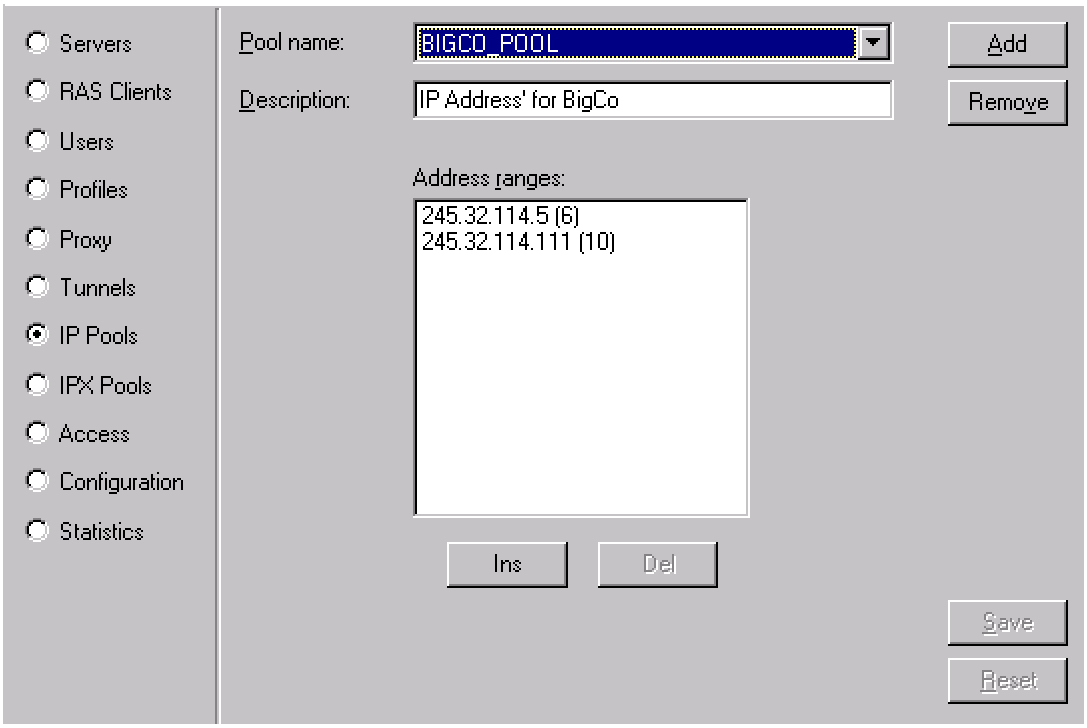
2 Click **Remove**. You will be prompted to confirm the deletion.

3 Click **Yes**. The tunnel is removed from the list.

IP Pools Dialog

The IP Pools dialog allows you to set up one or more pools out of which unique IP addresses will be assigned as users require them. Each pool consists of a list of one or more ranges of IP addresses.

IMPORTANT: Depending on your overall configuration, certain limitations may apply to this feature. See "How Address Assignment Works" on page 45.



● IP Pools

Pool name: BIGCO_POOL

Description: IP Address' for BigCo

Address ranges:

245.32.114.5 (6)
245.32.114.111 (10)

IP Pools Dialog (Windows version)

Adding an IP Address Pool

An IP address pool consists of one or more ranges of IP addresses. You can add or delete ranges and set an optional description for each address pool.

To add a new IP address pool:

1 In the IP Pools dialog, click **Add**. The Add New IP Address Pool dialog appears.

2 Enter the **Pool name** and click **OK**. In the IP Pools dialog, you will now see the name you entered in the **Pool name** field.

3 Enter a text **Description** of the address pool.

4 Each IP Pools entry may provide various **Address ranges**. Add and remove the ranges of IP addresses that make up the pool, as described in the following topic.

5 Click **Save** to make your changes permanent.

Editing an IP Address Pool

To add a new range of IP addresses to an IP address pool:

1 Select the pool from the **Pool name** drop-down list.

2 Click **Ins**. The Add New IP Address Range dialog appears.

3 Enter the starting address and the number of addresses in the new range, then click **Add**.

Repeat for as many address ranges as you'd like to add.

4 When done adding ranges, click **Close** to return to the IP Pools dialog.

To remove a range of addresses from an IP address pool:

1 Select the pool from the **Pool name** drop-down list.

2 Highlight the range in the **Address ranges** list.

3 Click **Del** (not **Remove**).

Removing an IP Address Pool

To remove an IP Pool entry from the Steel-Belted Radius database:

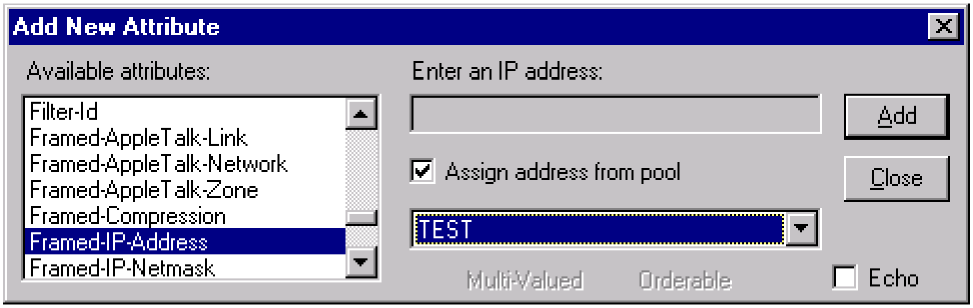
1 In the IP Pools dialog, click the **Pool name** drop-down list and select the IP Pool you would like to remove. (Under **Unix**: Click **OK** to proceed.)

2 Click **Remove**. (Under **Windows**: You will be prompted to confirm the deletion.)

Specifying IP Address Assignment in User/Profile Records

The Framed-IP-Address Return-List attribute controls how the server will assign an IP address to a user making a connection.

When you add or edit the Framed-IP-Address attribute in the Users or Profiles dialog, the Framed-IP-Address dialog appears.



Add New Attribute

Available attributes:

Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Framed-AppleTalk-Zone
Framed-Compression
Framed-IP-Address
Framed-IP-Netmask

Enter an IP address:

☑ Assign address from pool

TEST

Multi-Valued Orderable

□ Echo

Editing the Framed-IP-Address (Windows version)

This dialog allows you to select an IP address assignment option. Either:

- Type an IP address in the **Enter an IP address** field; *or*
- Check the **Assign IP address from pool** box and select the name of the pool from the list.

NAS-Specific IP Address Pools

Steel-Belted Radius allows you to define IP Address Pools that are specific to the NAS from which the user request was received. You can also define a set of suffixes that define categories of pools.

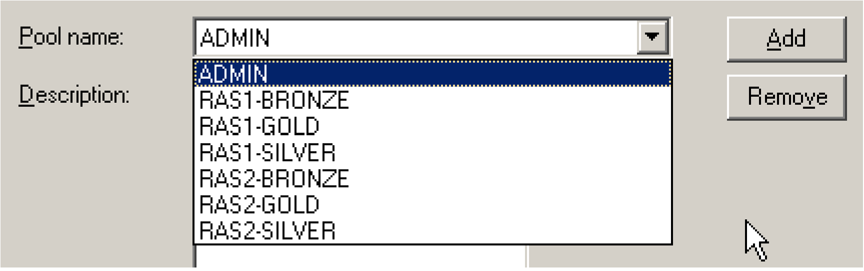
A pool category might correspond, for example, to the kinds of services available to users in that category. You might decide to define categories called `Bronze`, `Silver`, and `Gold`, indicating increasing packet routing priorities.

To create a NAS-specific address pool, you must follow these steps:

1. If you want NAS-Specific IP Address pools split into categories, define the appropriate suffixes in the [IPPoolSuffixes] section of radius.ini. For example:

```
[IPPoolSuffixes]
-Bronze
-Silver
-Gold
```

2 Define the IP Address Pool with the IP Pools Dialog.



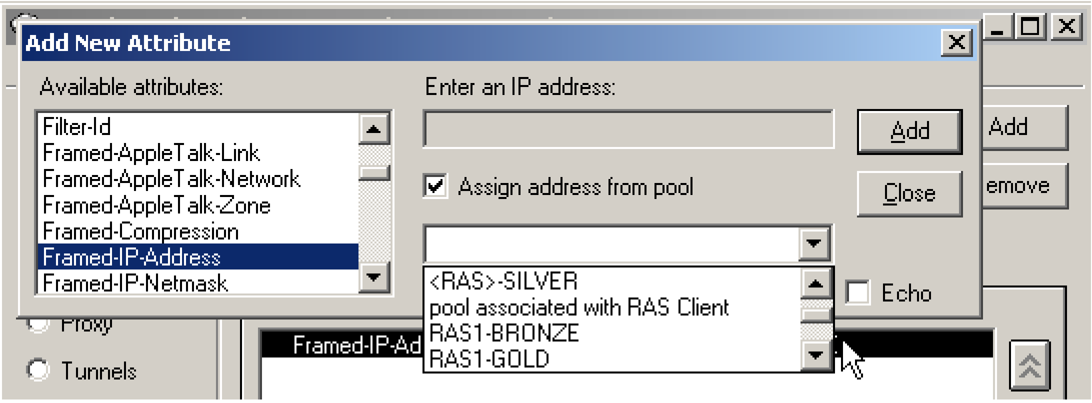
Pool name: ADMIN

Description:

IP Pools Dialog

3 Associate the new IP Address Pool with the appropriate NAS by use of **IP Address Pool** field on the RAS Clients Dialog.

4 You can now assign a user to a NAS-Specific IP Address Pool and suffix. Create this association either with the Users Dialog or the Profiles Dialog.



Add New Attribute

Available attributes:

Enter an IP address:

☑ Assign address from pool

☐ Echo

Associating IP Address Pools with RAS Clients

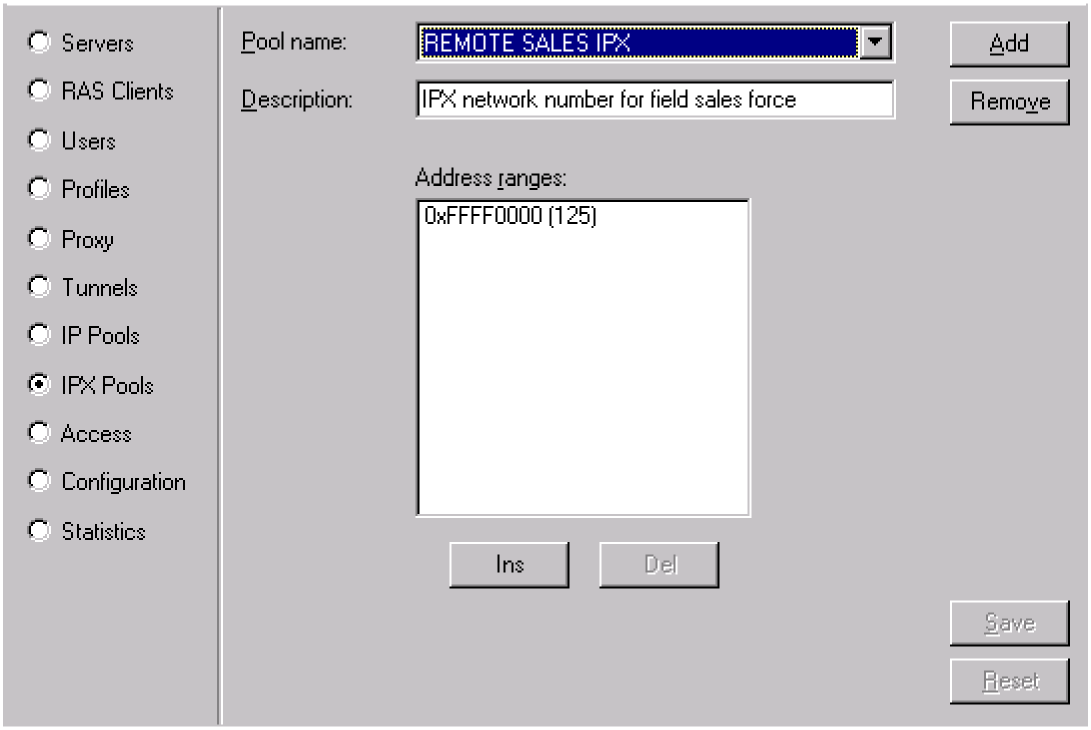
See “radius.ini [IPPoolSuffixes] Section” on page 143.

If user `Bob`, who has been assigned to `<RAS>-Bronze`, logs into RAS1, he will receive an IP Address from the `RAS1-Bronze` address pool. If he logs into RAS2, he will receive an address from the `RAS2-Bronze` address pool. If, however, he logs into RAS3 but `RAS3-Bronze` has not been defined in the IP Pools Dialog, he will not be able to be assigned an IP Address.

IPX Pools Dialog

The IPX Pools dialog allows you to set up one or more pools out of which unique IPX network numbers will be assigned as users require them. Each pool consists of a list of one or more ranges of IPX network numbers.

IMPORTANT: Depending on your overall configuration, certain limitations may apply to this feature. See “How Address Assignment Works” on page 45.



○ Servers
○ RAS Clients
○ Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
● IPX Pools
○ Access
○ Configuration
○ Statistics

Pool name: REMOTE SALES IPX

Description: IPX network number for field sales force

Address ranges:
0xFFFF0000 (125)

IPX Pools Dialog (Windows version)

Adding an IPX Pool

An IPX pool consists of one or more ranges of IPX network numbers. You can add or delete ranges and set an optional description for each address pool.

To add a new pool of IPX network numbers:

1. In the IPX Pools dialog, click **Add**. The Add New IPX Address Pool dialog appears.

2 Enter the **Pool name** and click **OK**. In the IP Pools dialog, you will now see the name you entered in the **Pool name** field.

3 Enter a text **Description** of the address pool.

4 Each IP Pools entry may provide various Address ranges. Add and remove the ranges of IP addresses that make up the pool, as described in the following topic.

5 Click **Save** to make your changes permanent.

Editing an IPX Pool

To add a new range of IPX network numbers to an IPX address pool:

1 Select the pool from the **Pool name** drop-down list.

2 Click **Ins**. The Add New IPX Address Range dialog appears.

3 Enter the starting IPX network number and the number of addresses in the new range, then click **Add**.

Repeat for as many address ranges as you'd like to add.

4 When done adding ranges, click **Close** to return to the IPX Pools dialog.

To remove a range of network numbers from an IPX address pool:

1 Select the pool from the **Pool** name drop-down list.

2 Highlight the range in the **Address ranges** list.

3 Click **Del** (not **Remove**).

Removing an IPX Pool

To remove an IPX Pool entry from the Steel-Belted Radius database:

1 In the IPX Pools dialog, click the **Pool name** drop-down list and select the IPX Pool you would like to remove. (Under **Unix**: Click **OK** to proceed.)

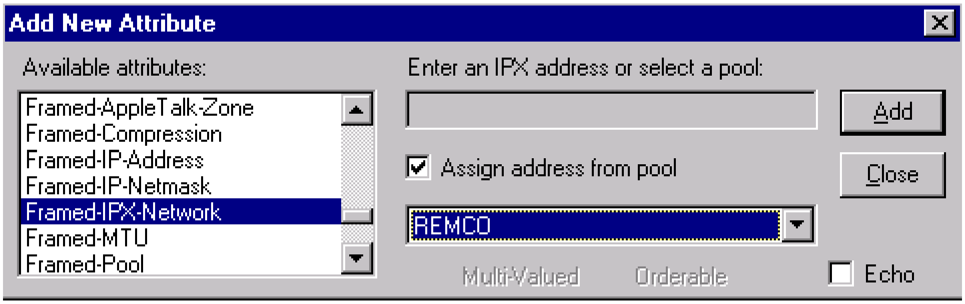
2 In the IPX Pools dialog, click **Remove**.

Specifying Pooled IPX Network Numbers in User/Profile Records

The Framed-IPX-Address Return-List attribute controls how the Steel-Belted Radius server will assign an IPX address to a user making a connection.

When you add or edit the Framed-IPX-Address attribute in the Users or Profiles dialog, the Framed-IPX-Address dialog appears. This dialog allows you to select an IPX address assignment option. Either:

- Type an IPX address in the **Enter an IPX address** field; *or*
- Check the **Assign IPX address from pool** box and select the name of the pool from the list.



☑ Assign address from pool

REMCO

□ Echo

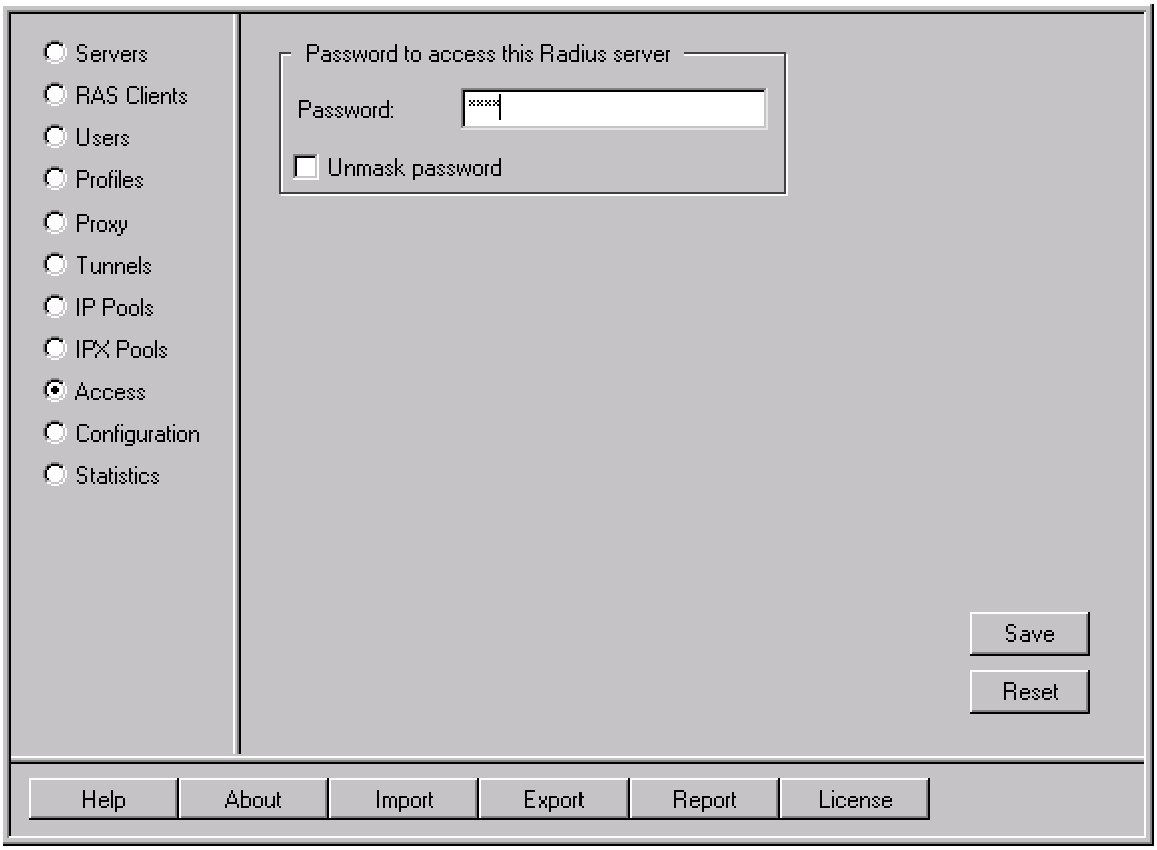
Specifying an IPX Pool for the Framed-IPX-Address Attribute (Windows version)

Access Dialog

Unix Only

Each time you request a connection from the Servers dialog, the Administrator program prompts you to authenticate yourself by entering a Steel-Belted Radius administrative account name and password. If you enter the name of the default, full-service administrative account (`admin`), then you must enter the password defined in the Access dialog. Steel-Belted Radius is shipped with this password set to `radius`.

We suggest you change it immediately after installing the product. To do this, you must start the Administrator program and select the Access dialog.



Password to access this Radius server

Password: ****

□ Unmask password

Access Dialog (Unix version)

Setting the Server Password

To set the password for the default administrative account (admin):

1 In the Servers dialog, select a server name.

2 Choose the Access dialog.

3 Enter a password in the **Password** field.

4 If you want to see the password characters, check the **Unmask password** checkbox. If you want the password concealed as asterisks (********), uncheck the box.

NOTE: There will be no chance to retype the password.

5 Click **Save** to keep your changes, **Reset** to undo them.

You can change this password again at any time.

Resetting the Server Password from the Default

If you forget the password for the default administrative account (`admin`), you can reset it to its default value and then change it to a value of your choice, as follows:

1 Create a new file (even an empty file is fine), name it `resetpwd`, and place it in the Steel-Belted Radius server directory that you defined at installation time.

2 Stop and restart the radius daemon.

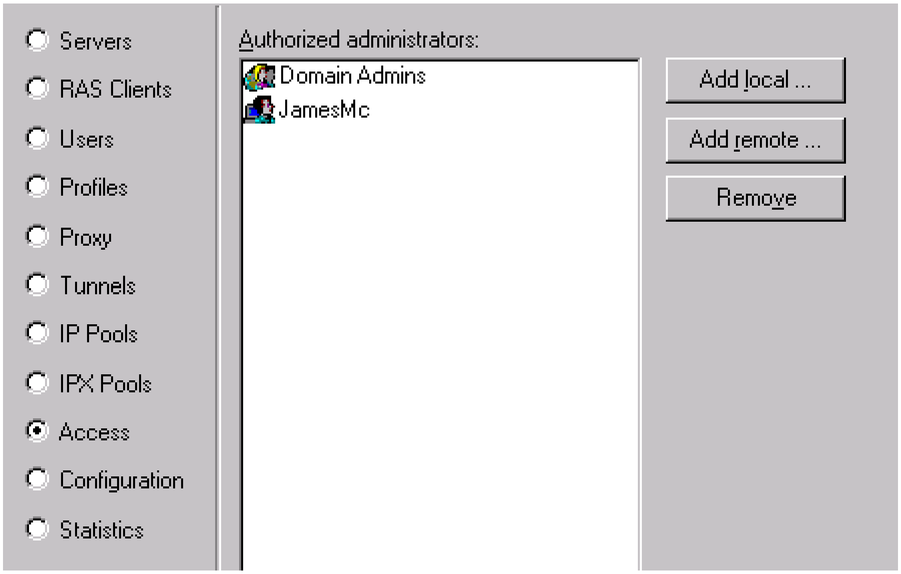
3 Change the password from its installation default (`radius`).

Windows Only

The Access dialog lets you grant and revoke the right to use the Administrator program to configure a Steel-Belted Radius server.

When a Steel-Belted Radius server is first installed, any account that is a member of the NT group `Administrators` on a Steel-Belted Radius server implicitly has the right to use the Administrator program at its default (full) level of access. The Access dialog allows you to selectively grant and revoke the right to use the Administrator program, beginning from this starting point.

In the Access dialog, the RADIUS Administrators list show the users and groups that have been explicitly granted the right to run the Administrator. Local users or groups will be shown with their normal name. Remote users or groups will be shown with the name of the Domain, followed by a backslash and then the name of the Domain user or group.


○ Servers
○ RAS Clients
○ Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
● Access
○ Configuration
○ Statistics

Authorized administrators:
Domain Admins
JamesMc

Access Dialog (Windows version)

Adding a Local Administrator

To grant access to a local administrator:

1 Click **Add local**.

2 A list appears, allowing you to select which users or groups should have Administrator access rights.

3 Select a user or group from the list. Click **Add**. Continue until you are done, and then click **Close**.

To revoke rights, highlight the user or group whose administration rights you'd like to revoke, and click **Remove** in the main Access dialog.

Adding a Remote Administrator

To grant access to a remote administrator within a Domain:

1 Click **Add remote**.

2 A list of Domains appears. Select a Domain name within which you would like to grant access.

3 Select a user or group from the list. Click **Add**. Continue until you are done, and then click **Close**.

To revoke rights, highlight the user or group whose administration rights you’d like to revoke, and click **Remove**.

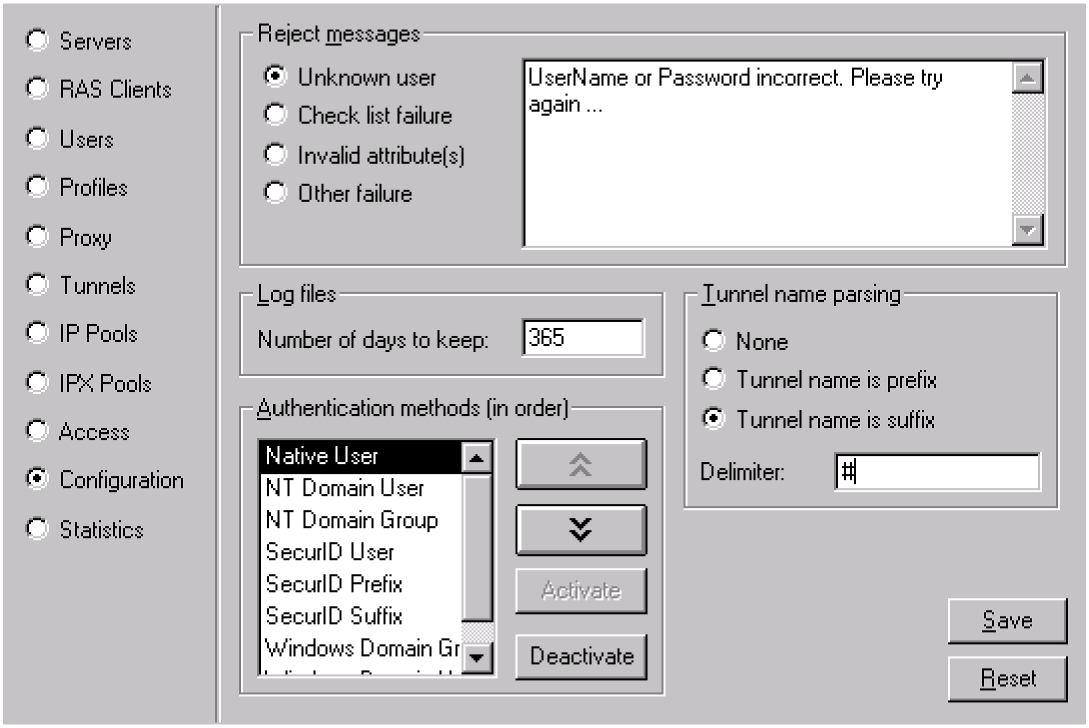
WARNING: Be careful not to revoke your own rights. If you do so, you will no longer have access to RADIUS administrative functions.

Configuration Dialog

The Configuration dialog permits you to define how Steel-Belted Radius will perform authentication and accounting. You can configure:

- The order in which different authentication methods will be attempted.
- The number of days that the RADIUS server should retain authentication and accounting logs before the files are recycled.
- The text of messages that will be sent to the NAS (and possibly to the User) when a RADIUS request is rejected.

- How the server should parse tunnel names; that is, should the tunnel name or user name be first, and which character should separate the names?



○ Servers
○ RAS Clients
○ Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
● Configuration
○ Statistics

Reject messages

● Unknown user
○ Check list failure
○ Invalid attribute(s)
○ Other failure

UserName or Password incorrect. Please try again ...

Log files

Number of days to keep: 365

Authentication methods (in order)

Native User
NT Domain User
NT Domain Group
SecurID User
SecurID Prefix
SecurID Suffix
Windows Domain Gr

Tunnel name parsing

○ None
○ Tunnel name is prefix
● Tunnel name is suffix

Delimiter: #

Configuration Dialog (Windows version)

You can edit information in any of the fields that appear on the screen. To make any changes you have entered permanent, click **Save**, and the new settings will take effect. To revert to the previous settings, click **Reset**.

Reject Messages

When issuing an Access-Reject, Steel-Belted Radius can indicate the reason why the request was rejected. You can configure the message text that will be returned to the client when a particular type of error occurs. This text will be inserted into the standard RADIUS attribute Reply-Message within the Access-Reject response.

The following table lists the errors to which you can assign message text, and the meaning of each error.

Error	Meaning
Unknown User	The username and password authentication failed.
Check List Failure	The user was authenticated but is being rejected because the RADIUS request did not fulfill the requirements of the Check-List.
Invalid Attribute(s)	The request contained an attribute in violation of the RADIUS specification.
Other	Some other error occurred, such as a resource failure.

To modify message text:

1 In the Configuration dialog **Reject messages** panel, select an error type. The current message text displays to the right.

2 In the **message text display** field, edit the current text, or type a new message.

Tunnel Name Parsing

Use the fields in the Tunnel Name Parsing panel to configure a parsing convention for all of the tunnels that use the Steel-Belted Radius server to support RADIUS authentication and accounting. You may set the following options in the Configuration dialog:

- Choose **Tunnel name is suffix** to parse names as *`User<Delimiter>TunnelName`*.
- Choose **Tunnel name is prefix** to parse names as *`TunnelName<Delimiter>User`*.
- Choose **None** to disable tunnel name parsing.

  If you choose this option, the tunnel authentication sequence will be bypassed for each Access-Request; the server will use the standard username/password authentication sequence only.
- You can choose a <*`Delimiter`*> character other than ‘@’ (the default).

You cannot set these options per tunnel, only per server.

Authentication Methods Configuration

When Steel-Belted Radius receives a user name, it does not know in advance to which authentication category this user will belong. It must try each method that it currently has configured and enabled. The Authentication Methods list allows you to fine-tune the sequence of authentication attempts.

See "Configuring Authentication Methods" on page 27.

To change the order in which the methods are tried:

1 Highlight the method in the list box.

2 Click one of the arrow buttons as follows:

Button	Action
︽	Moves the selected method up one slot in the list. If the selected method is already first in the list, then the button is disabled.
︾	Moves the selected method down one slot in the list. If the selected method is already last in the list, then the button is disabled.

To remove a method from the search list entirely:

1 Highlight the method in the list box.

2 Click the **Deactivate** button.

Log Files

Steel-Belted Radius records all transactions to log files. There are separate logs for authentication transactions and accounting attributes.

See "Authentication Log File" on page 96.

See also "Accounting Log File" on page 97.

Each day at midnight, the previous day's log files are completed, and new log files are created for the new day's transactions. In order to prevent the log files from continuously depleting available disk space Steel-Belted Radius retains the log files for some period of time and then automatically deletes them. To specify the number of days to retain log files, enter a value in the **Days to Keep** field.

Import/Export Capabilities

Steel-Belted Radius's Import/Export feature lets you export database information from any Steel-Belted Radius server and import it into another. This gives you a head start if you are configuring multiple servers.

Import and Export are selective; that is, you are given the opportunity to select exactly which items to export or import.

Steel-Belted Radius uses a specially formatted text file called a RADIUS Information File (`.rif`) for export and import.

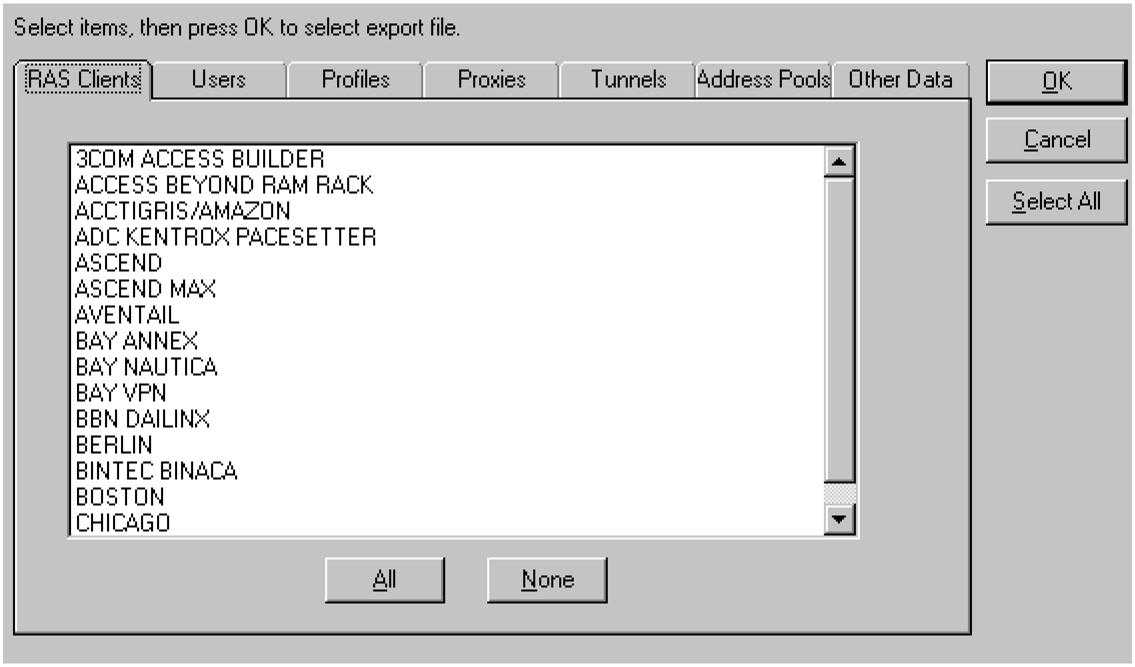
In addition to the native `.rif` format, Steel-Belted Radius permits importing of user data from the file format used in older, freeware implementations of the RADIUS standard, commonly deployed on UNIX systems. Different vendors' variations of this file format are supported via dictionaries.

Exporting to a RADIUS Information File

To export Steel-Belted Radius database information to a RADIUS Information File:

1. Run the Administrator program.
2. Depending on your platform:
   - Under **Windows**: Select the **File Export** command.
   - Under **Unix**: Click the **Export** button that appears at the bottom of the Administrator display.

A dialog appears. Each tab in the dialog lists items of a particular category that you can export.



3COM ACCESS BUILDER
ACCESS BEYOND RAM RACK
ACCTIGRIS/AMAZON
ADC KENTROX PACESETTER
ASCEND
ASCEND MAX
AVENTAIL
BAY ANNEX
BAY NAUTICA
BAY VPN
BBN DAILINX
BERLIN
BINTEC BINACA
BOSTON
CHICAGO

Export Dialog (Windows version)

3 For each category, select the appropriate tab and click each item you'd like to export. To select all items in the category, click **All**.

To select all items in all categories, click **Select All**.

4 Once you've selected all the items you want, click **OK**.

5 Depending on your platform:

- Under **Windows**: A file browsing dialog appears. Specify an export file and click **Save**.
- Under **Unix**: The Select File dialog appears. Specify the full pathname of an export file and click **OK**.

Importing from a RADIUS Information File

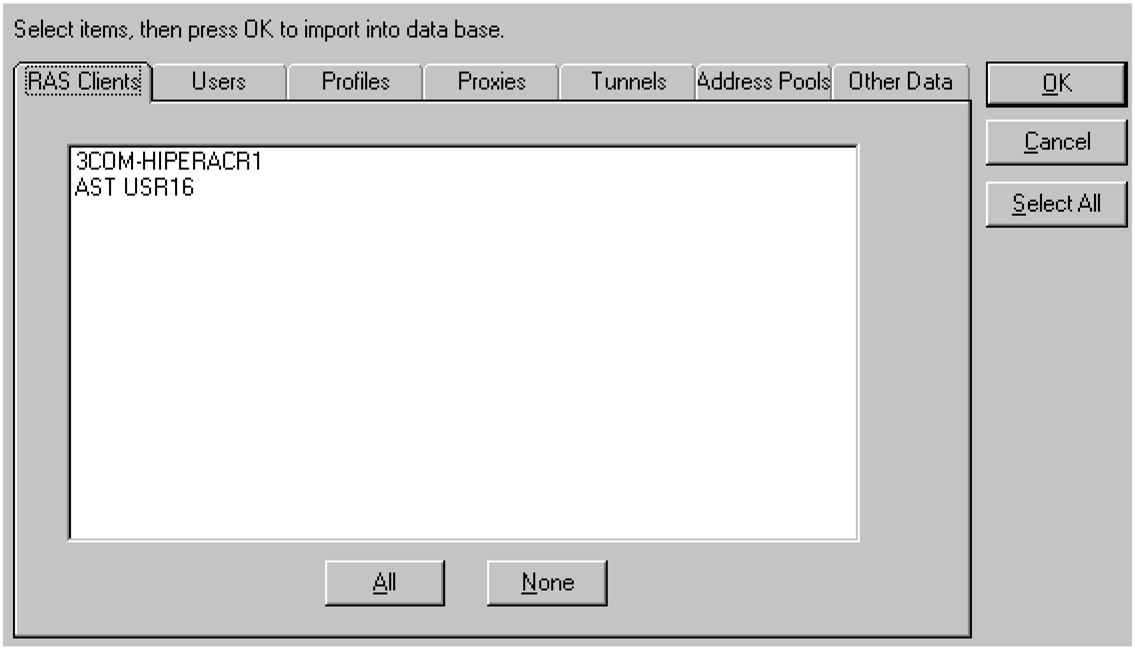
To import from a RADIUS Information File into your Steel-Belted Radius database:

1 Run the Administrator program.

2 Depending on your platform:

- Under **Windows**: Select the **File Import** command. A file browsing dialog appears. Make sure the file type indicates RADIUS Information File (`*.rif`). Select an import file and click **Open**.
- Under **Unix**: Click the **Import** button that appears at the bottom of the Administrator display. The Select File dialog appears. Specify the full pathname of an export file and click **OK**.

3 The Import (or, under Unix, the Import/Export) dialog appears, with each tab listing items of a particular category that are available for import from the selected file.


Select items, then press OK to import into data base.

3COM-HIPERACR1
AST USR16

Import Dialog (Windows version)

4 For each category, select the appropriate tab and highlight each item you'd like to import. To select all items in the category, click **All**.

To select all items in all categories, click **Select All**.

5 Once you've selected all the items you want, click **OK**. The items you selected will be added to the Steel-Belted Radius database.

If an import item already exists, you will be given the opportunity to confirm that you'd like to replace the existing entry with the entry from the import file.

Importing from Other File Formats

There are many RADIUS implementations currently deployed, mostly UNIX systems that are based on source code from Livingston Enterprises and Ascend. These implementations store data in a specially formatted text file normally called users.

To import user data from a users file into your Steel-Belted Radius database:

1 Run the Administrator program.

2 Depending on your platform:

- Under **Windows**: Select the **File Import** command. A file browsing dialog appears. Select a file type of **External User Data File (*.*)**. Select an import file and click **Open**.
- Under **Unix**: Click the **Import** button that appears at the bottom of the Administrator display. The Select File dialog appears. Specify the full pathname of the users file and click **OK**.

3 The Import Options dialog appears. Modify as desired:

- Set **File format** based on the NAS that the originating RADIUS server was meant to work with. This allows Steel-Belted Radius to correctly interpret the attribute naming conventions of a particular vendor.
- If you check **Ignore attributes**, only names and passwords will be imported. Check-List and Return-List attributes that may be present in the imported file will be excluded from the copied entries.
- Select the Steel-Belted Radius Profile to be applied to each imported user entry, or leave the entry set to **<no profile>**. If you do select a profile, ensure that **Ignore attributes** is checked.
- Select **Allow PAP or CHAP** or **Allow PAP only** depending on how you’d like to store passwords in the database.
- When you are satisfied with the settings, click **OK**.

4 The Import dialog appears, showing each user entry available for import from the selected file.

Highlight each user you’d like to import. To select all users, click **All**. Once you’ve selected all the users you want, click **OK**.

The users you selected will be added to the Steel-Belted Radius database as Native users. If a user is already present in the database, you’ll be given the opportunity to confirm that you’d like to replace the existing user with the new user entry from the import file.

When you wish to import user data from a users file into your Steel-Belted Radius database, and the users file contains attributes that you wish to be imported along with the usernames and passwords, it is important to note the following:

- You must have at least one RAS Client entered in the Steel-Belted Radius Administrator. This allows a dictionary file of some type to be associated with the Steel-Belted Radius database, which in turn allows the attributes being imported from the users file to be recognized by the Steel-Belted Radius database.
- Even with a RAS Client entered, all of the attributes from the users file may not be recognized by Steel-Belted Radius due to the different versions of these RADIUS implementations and the fact that attribute names may be different in each.

To help with these differences, Steel-Belted Radius includes three dictionary import files. These files reside in your Steel-Belted Radius server directory and have a .dci extension. The files are named annex.dci, ascend.dci, and portmstr.dci. One of these three files should be a close match to your users file.

When attributes are involved, the best approach to importing from other file formats is the following:

1. Add a RAS Client in the Steel-Belted Radius Administrator.
2. View the users file to see what attributes are associated with the users and compare them with the attribute names in the appropriate dictionary import file.

   For example, if the users file contains the attribute `User-Service-Type`, and the users file is from a Livingston Portmaster, then view the portmstr.dci file in your server directory and you will note that the same attribute is named `Service-Type`. This difference in name would cause the import process to log an error and after the import was complete, the attribute in question would not be associated with the appropriate user(s). To avoid this, edit your portmstr.dci file so that `Service-Type` is globally changed to `User-Service-Type`. The attribute name in the portmstr.dci file will now match the attribute name in the users file and allow for an error-free import. Repeat this for any attribute names that do not match.
3. Once Step 2 is completed, proceed with a normal import from the Steel-Belted Radius Administrator (as described above). Be sure to select the appropriate dictionary import file type when prompted at the Select Import Options dialog.

Logging, Monitoring, and Reporting

5

A Window on Operations

Steel-Belted Radius provides a variety of diagnostic features:

- Authentication and accounting log files record the details of every RADIUS transaction on the Steel-Belted Radius server.
- The Administrator program’s Statistics dialog and the LDAP Configuration Interface allow you to quickly view ongoing counts of the most significant statistics relating to authentication, accounting, and Proxy RADIUS transactions on the Steel-Belted Radius server.
- The Sessions list provides a record of all currently active sessions that were authenticated by this Steel-Belted Radius server.
- Tabular reports allow you to view selected contents of the Steel-Belted Radius database in written form
- **Windows only**: Windows NT Performance Monitor (perfmon) counters let you collect and interpret statistics about the Steel-Belted Radius service.
- **Windows only**: Windows NT events help you detect and solve system-related problems with the service.

Authentication Log File

Each time a RADIUS authentication event occurs it is recorded in the authentication log file. The following are typical log entries:

- `Sent accept response for user USERNAME to client RAS-Client-Name`
- `Unable to find user USERNAME with matching password`
- `Sent reject response`
- `Shutting down RADIUS Authentication Server ...`
- `Starting RADIUS Authentication Server ...`

Authentication log files are in ASCII format, and are intended for viewing by the network administrator. Each line of the authentication log file contains a line with the date and time, followed by event information.

Authentication log files are located in the RADIUS database directory area by default, although you can specify an alternate destination directory in the [Configuration] section of radius.ini. Authentication log files are named *yyyymmdd*+'.'+*suffix*, where *yyyy* is the 4-digit year, *mm* is the month, and *dd* is the day on which the log file was created, and the file *suffix* is LOG.

Authentication log files are kept for the number of days specified in the Configuration dialog. After that time, older log files are deleted from the server in order to conserve disk space.

The current log file can be opened while Steel-Belted Radius is running.

Level of Logging Detail

You can control the level of detail recorded in authentication log files by use of the LogLevel, LogAccept, and LogReject settings.

The LogLevel setting determines the level of detail given in the log file. The LogLevel may be the number 0, 1, or 2, where 0 is the least amount of information, 1 is intermediate, and 2 is the most verbose. It is specified in the [Configuration] section of radius.ini and in the [Settings] sections of .aut files.

The LogAccept and LogReject flags allow you to turn on or off the logging of Access-Accept and Access-Reject messages in the authentication log file. These flags are set in the [Configuration] section of radius.ini. They are 1 (so that these messages are logged) by default, but can be set to 0 (not logged). An Accept or Reject is only logged if LogAccept or LogReject, respectively, is enabled *and* the LogLevel is "verbose" enough for the message to be recorded.

The TraceLevel setting specifies whether packets should be logged when they are received and being processed, and what level of detail should be recorded in the log.

Accounting Log File

Each time a RADIUS accounting event occurs it is recorded in the accounting log file. Accounting events include:

- START messages, indicating the beginning of a connection.
- STOP messages, indicating the ending of a connection.
- INTERIM messages, sent at regular intervals from a NAS to indicate that a user connection is still active.

Accounting log files use comma-delimited, ASCII format, and are intended for import into a spreadsheet or database program. Log file format is as described below.

Accounting log files are located in the RADIUS database directory area by default, although you can specify an alternate destination directory in the [Configuration] section of `account.ini`. Accounting log files are named *yyyymmdd*.ACT, where *yyyy* is the 4-digit year, *mm* is the month, and *dd* is the day on which the log file was created.

Accounting log files are kept for the number of days specified in the Configuration dialog. After that time, older log files are deleted from the server in order to conserve disk space.

The current log file can be opened while Steel-Belted Radius is running.

Accounting Log File Format

The first six fields in every accounting log entry are provided by Steel-Belted Radius for your convenience in reading and sorting the file:

- `Date` - the date when the event occurred
- `Time` - the time when the event occurred
- `RAS-Client` - the name or IP address of the RAS Client sending the accounting record
- `Record-Type` - START, STOP, INTERIM, ON, or OFF, the standard RADIUS accounting packet types
- `Full-Name` - the fully distinguished name of the user, based on the authentication from the RADIUS server
- `Auth-Type` - a number that indicates the class of authentication performed:

  0 - Native
  6 - Windows NT Domain User
  7 - Windows NT Domain Group
  8 - Windows NT Host User
  9 - Windows NT Host Group
  10 - SecurID User
  11 - SecurID Prefix
  12 - SecurID Suffix
  13 - UNIX User
  14 - UNIX Group
  15 - TACACS+ User
  16 - TACACS+ Prefix
  17 - TACACS+ Suffix
  100 - Tunnel User
  200 - External Database
  (other) - Proxy

By default, all of the standard RADIUS attributes appear next.

See “Standard RADIUS Accounting Attributes” on page 100.

These may be followed by several vendor-specific attributes, depending on the device that sent the accounting packet.

See “Vendor-Specific Attributes” on page 32.

You can edit the account.ini initialization file to eliminate, add, or change the order in which standard RADIUS or vendor-specific attributes are logged.

See “account.ini File” on page 127.

First Line Headings

The first line of the accounting log file lists the names of all the attributes that have been enabled for logging, in the order in which they’ll be logged. This first line serves as a complete set of column headings for the remaining entries in the file.

The following example of a first line shows required headings in bold italic, standard RADIUS headings in bold, and vendor-specific headings in regular text:

```
"Date","Time","RAS-Client","Record-Type","Full-Name",
"Auth-Type","User-Name","NAS-Port","Acct-Status-Type",
"Acct-Delay-Time","Acct-Input-Octets","Acct-Output-Octets",
"Acct-Session-Id","Acct-Authentic","Acct-Session-Time",
"Acct-Input-Packets","Acct-Output-Packets",
"Acct-Termination-Cause","Acct-Multi-Session-Id",
"Acct-Link-Count","Acc-Err-Message",
"Nautica-Acct-SessionId","Nautica-Acct-Direction",
"Nautica-Acct-CauseProtocol","Nautica-Acct-CauseSource",
"Telebit-Accounting-Info","Last-Number-Dialed-Out",
"Last-Number-Dialed-In-DNIS","Last-Callers-Number-ANI",
"Channel","Event-Id","Event-Date-Time",
"Call-Start-Date-Time","Call-End-Date-Time",
"Default-DTE-Data-Rate","Initial-Rx-Link-Data-Rate",
"Final-Rx-Link-Data-Rate","Initial-Tx-Link-Data-Rate",
"Final-Tx-Link-Data-Rate","Sync-Async-Mode",
"Originate-Answer-Mode","Modulation-Type",
"Equalization-Type","Fallback-Enabled","Characters-Sent",
"Characters-Received","Blocks-Sent","Blocks-Received",
"Blocks-Resent","Retrains-Requested","Retrains-Granted",
"Line-Reversals","Number-Of-Characters-Lost",
"Number-of-Blers","Number-of-Link-Timeouts",
"Number-of-Fallbacks","Number-of-Upshifts",
"Number-of-Link-NAKs","Back-Channel-Data-Rate",
"Simplified-MNP-Levels","Simplified-V42bis-Usage",
"PW_VPN_ID"
```

Comma Placeholders

It’s possible that not all the attributes expected in the first line of the accounting log file have had data returned for them by the currently logged event. If this is the case, when Steel-Belted Radius writes the event to the accounting log file, it uses a comma “placeholder” to mark the location of each empty entry, so that all entries remain correctly aligned with their headings.

For example, based on the “first line” of headings described above, the following is a valid accounting log entry, in which the value of the Acct-Status-Type attribute is 7:

```
"12/23/1997","12:11:55","RRAS","Accounting-On",
,,,,7,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,
```

Standard RADIUS Accounting Attributes

As a handy reference to use while working with the accounting log file, *yyyymmdd*.ACT, and its configuration file, `account.ini`, we’ve listed the standard RADIUS accounting attributes below:

- `User-Name` - the name of the user as received by the client.
- `NAS-Port` - the port number on the client device.
- `Acct-Status-Type` - a number that indicates the beginning or ending of user service:

  1 - Start
  2 - Stop
  3 - Interim-Acct
  7 - Accounting-On
  8 - Accounting-Off
- `Acct-Delay-Time` - how many seconds the client has been trying to send this record; can be subtracted from the time of arrival on the server to find the approximate time of the event generating this request.
- `Acct-Input-Octets` - number of bytes (characters) received by the port over the connection; only present in STOP records.
- `Acct-Output-Octets` - number of bytes (characters) sent by the port over the connection; only present in STOP records.
- `Acct-Session-Id` - unique Accounting identifier to make it easy to match START and STOP records in a log file.

- `Acct-Authentic` - indicates how the user was authenticated, whether by RADIUS, the RAS itself, or another remote authentication protocol:

  1 - RADIUS
  2 - Local
  3 - Remote

- `Acct-Session-Time` - elapsed time of connection in seconds; only present in STOP records.

- `Acct-Input-Packets` - number of packets received by the port over the connection; only present in STOP records.

- `Acct-Output-Packets` - number of packets sent by the port over the connection; only present in STOP records.

- `Acct-Termination-Cause` - a number that indicates how the session was terminated; only present in STOP records:

  1 - User Request
  2 - Lost Carrier
  3 - Lost Service
  4 - Idle Timeout
  5 - Session Timeout
  6 - Admin Reset
  7 - Admin Reboot
  8 - Port Error
  9 - NAS Error
  10 - NAS Request
  11 - NAS Reboot
  12 - Port Unneeded
  13 - Port Preempted
  14 - Port Suspended
  15 - Service Unavailable
  16 - Callback
  17 - User Error
  18 - Host Request

- `Acct-Multi-Session-Id` - unique accounting identifier to make it easy to link together multiple related sessions in a log file

- `Acct-Link-Count` - gives the count of links which are known to have been in a given multi-link session at the time the accounting record is generated.

Statistics Dialog

Steel-Belted Radius provides information on the status of the server. The Statistics dialog provides three tabs with statistics for all types of RADIUS activity on the currently selected server: Authentication, Accounting, and Proxy forwarding.

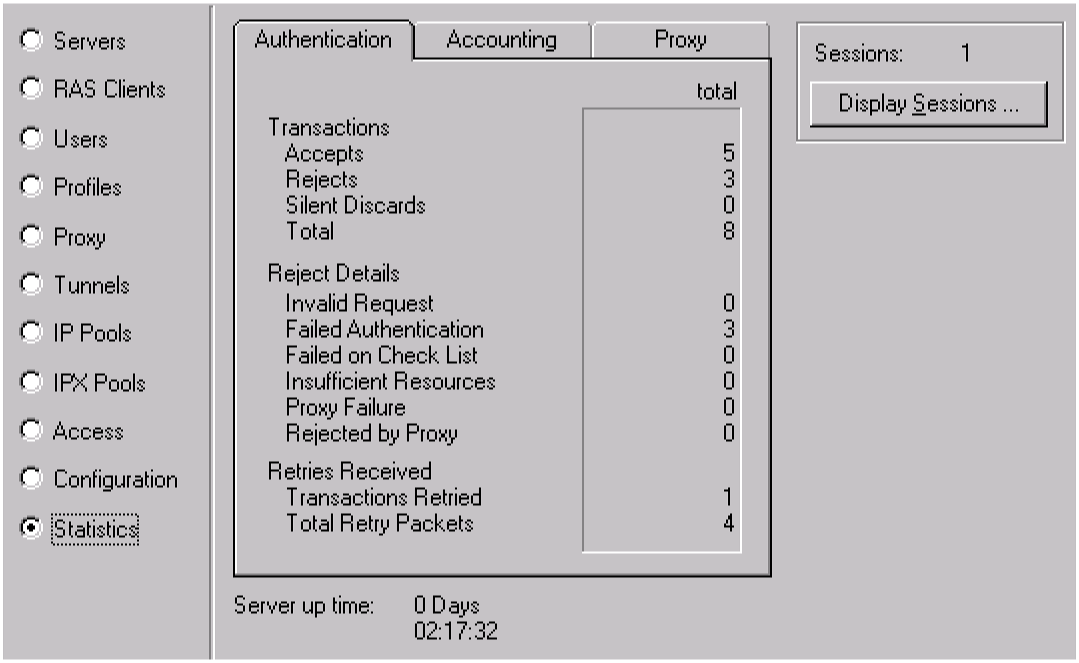
You can also:

- View the amount of time Steel-Belted Radius has been running.
- View an on-screen report of all users currently connected via a NAS or Tunnel, based on real-time RADIUS accounting information.

NOTE: Only the standard IETF RADIUS statistics are available from the Statistics dialog. To access Steel-Belted Radius extended statistics, you must use other utilities. See “Statistics Variables” on page 264.

Authentication Statistics

Authentication statistics provide information such as the number of accept and reject messages and the reasons for rejecting authentication.



Sessions: 1

	total
Transactions	
Accepts	5
Rejects	3
Silent Discards	0
Total	8
Reject Details	
Invalid Request	0
Failed Authentication	3
Failed on Check List	0
Insufficient Resources	0
Proxy Failure	0
Rejected by Proxy	0
Retries Received	
Transactions Retried	1
Total Retry Packets	4

Server up time: 0 Days
02:17:32

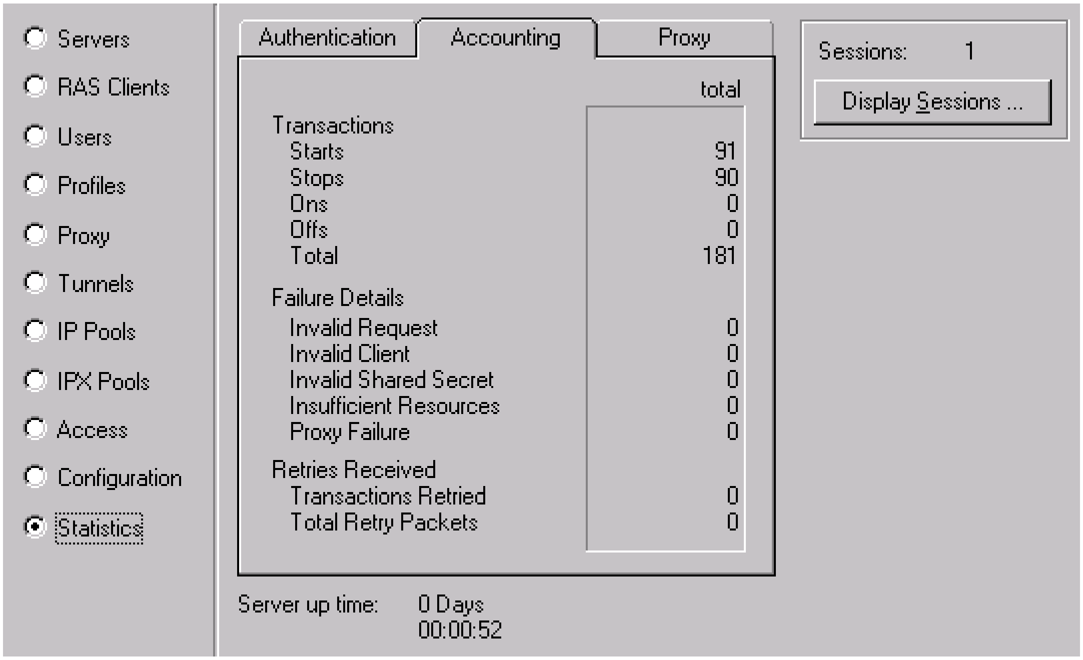
Statistics Dialog, Authentication Tab (Windows version)

The following table describes the authentication statistics, with possible interpretations in italics.

Authentication Statistic	Meaning
Transactions	
Accepts	The total number of RADIUS transactions that resulted in an accept response.
Rejects	The total number of RADIUS transactions that resulted in a reject response. These are broken out in Reject Details below.
Silent Discards	The total number of requests in which the client could not be identified. *A device may have been configured to use Steel-Belted Radius but no RAS Client entry has been created on the server with the name and/or IP address of the client; or the RAS Client entry has been configured with an incorrect name or IP address; or some rogue device is attempting to compromise RADIUS security*.
Total	The total of the three fields above.
Reject Details	
Invalid Request	The total number of invalid RADIUS requests made. *A device is sending incorrectly formed packets to Steel-Belted Radius; either there is a configuration error or the device does not conform to the RADIUS standard*.
Failed Authentication	The total number of failed authentication requests, where the failure is due to invalid username or password. *If all transactions are failing authentication, the problem may be that the shared secret entered into Steel-Belted Radius does not match the shared secret entered on the client device*.
Failed on Check List	The total number of requests that were authenticated but failed to meet the Check-List requirements.
Insufficient Resources	The total number of rejects due to a server resource problem.
Proxy Failure	The total number of rejects that had to be issued because Proxy forwarding to another RADIUS server failed.
Rejected by Proxy	The total number of rejects due to receiving a reject response from a Proxy RADIUS target server.
Retries Received	
Transactions Retried	The number of requests for which one or more duplicates was received.
Total Retry Packets	The total number of duplicate packets received.

Accounting Statistics

Accounting statistics provide information such as the number of transaction STARTs and STOPs and the reasons for rejecting attempted transactions. The START and STOP numbers will rarely match, as many transactions may be "in progress" at any given time.



Sessions: 1

```
                                   total
Transactions
  Starts                              91
  Stops                               90
  Ons                                  0
  Offs                                 0
  Total                              181
Failure Details
  Invalid Request                      0
  Invalid Client                       0
  Invalid Shared Secret                0
  Insufficient Resources               0
  Proxy Failure                        0
Retries Received
  Transactions Retried                 0
  Total Retry Packets                  0

Server up time:   0 Days
                  00:00:52
```

Statistics Dialog, Accounting Tab (Windows version)

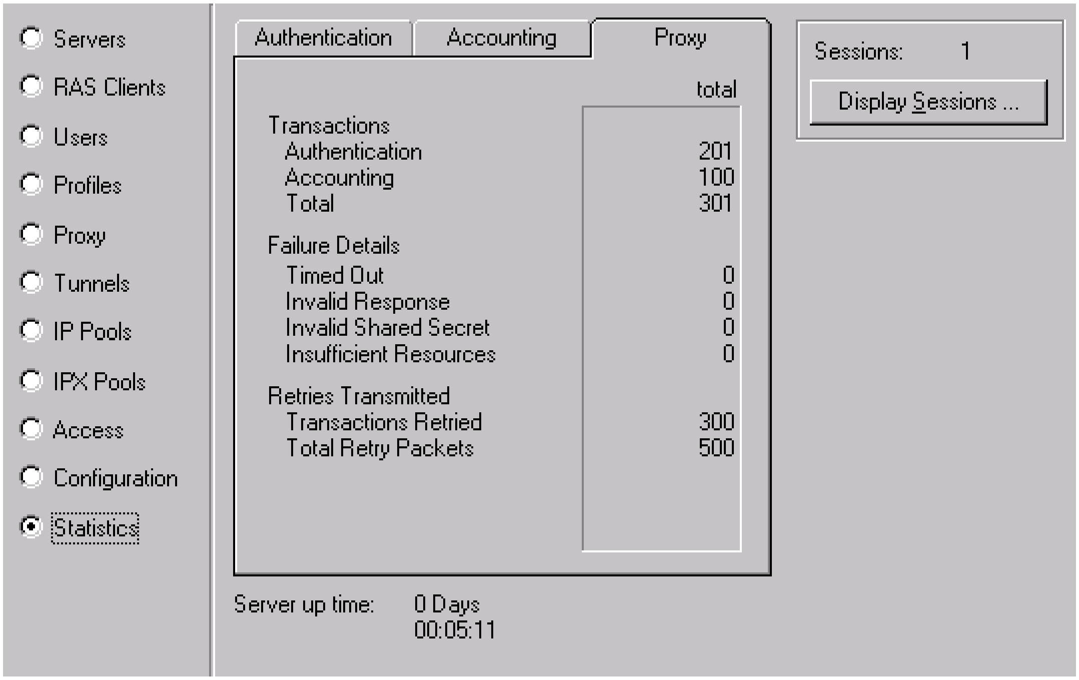
The following table describes the accounting statistics and suggested actions in italics (if appropriate).

Accounting Statistic	Meaning
Transactions	
Starts	The total number of transactions in which a dial-in connection was started following a successful authentication.
Stops	The total number of transactions in which a dial-in connection was terminated.
Ons	The total number of Accounting-On messages received, indicating that a RAS client has rebooted.
Offs	The total number of Accounting-Off messages received, indicating that a RAS client has shut down.

Accounting Statistic	Meaning
Total	The total of the four fields above.
Failure Details	
Invalid Request	The total number of invalid RADIUS requests made. *A device is sending incorrectly formed packets to Steel-Belted Radius; either there is a configuration error or the device does not conform to the RADIUS standard*.
Invalid Client	The total number of requests in which the RAS Client could not be identified. *A device may have been configured to use Steel-Belted Radius but no RAS Client entry has been created with the name and/or IP address of the client; or the RAS Client entry has been configured with an incorrect name or IP address; or some rogue device is attempting to compromise RADIUS security*.
Invalid Shared Secret	The total number of packets for which an incorrect digital signature was received. *The shared secret does not match between Steel-Belted Radius and the client device; or some rogue device is attempting to compromise RADIUS security*.
Insufficient Resources	The total number of rejects due to a server resource problem.
Proxy Failure	The total number of times that Proxy RADIUS forwarding failed.
Retries Received	
Transactions Retried	The number of requests for which one or more duplicates was received.
Total Retry Packets	The total number of duplicate packets received.

Proxy Statistics

Proxy statistics provide information such as the number of proxy authentication or accounting requests and the reasons for any transaction failures that may have occurred.



Sessions: 1

	total
Transactions	
Authentication	201
Accounting	100
Total	301
Failure Details	
Timed Out	0
Invalid Response	0
Invalid Shared Secret	0
Insufficient Resources	0
Retries Transmitted	
Transactions Retried	300
Total Retry Packets	500

Server up time: 0 Days 00:05:11

Statistics Dialog, Proxy Tab

The following table describes the proxy statistics, with possible interpretations in italics.

Proxy Statistic	Meaning
Transactions	
Authentication	The total number of authentication transactions between the proxy and target RADIUS servers.
Accounting	The total number of accounting transactions between the proxy and target RADIUS servers.
Total	The total of the two fields above.
Failure Details	
Timed Out	The total number of RADIUS transactions that timed out. This means that after all retry attempts were made, the transaction still timed out.

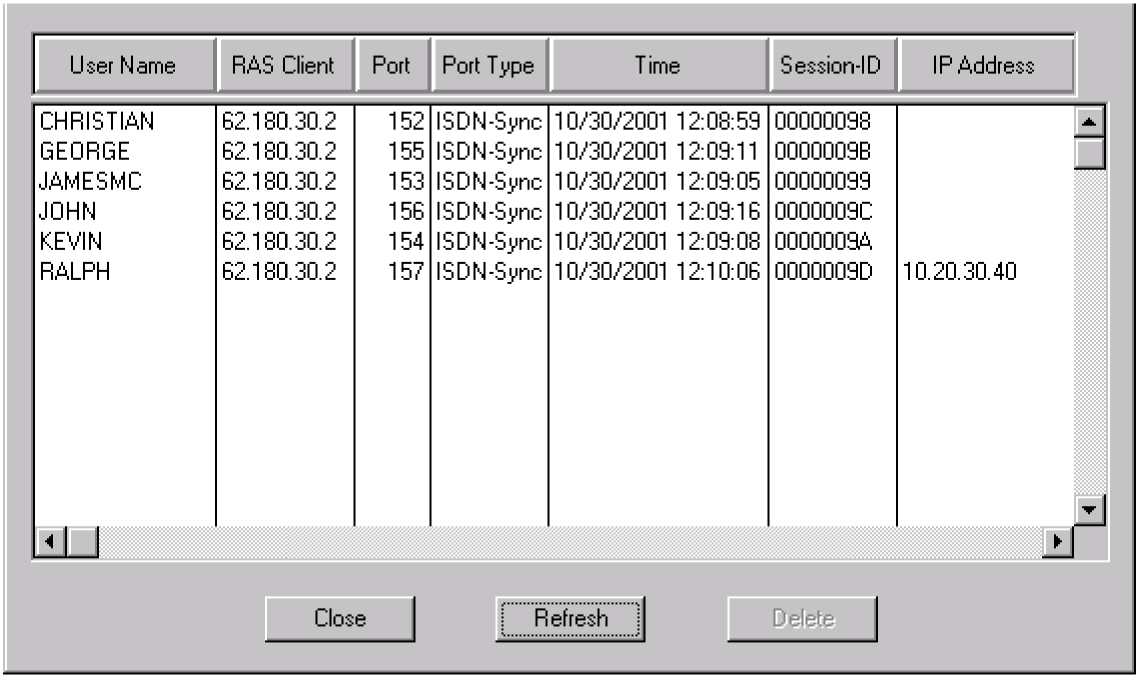
Proxy Statistic	Meaning
Invalid Response	The total number of invalid RADIUS responses received. *A target is sending incorrectly formed packets to Steel-Belted Radius; either there is a configuration error or the target RADIUS server does not conform to the RADIUS standard. Or, Steel-Belted Radius did not receive a proxy state echo in the received packet*.
Invalid Shared Secret	The total number of packets for which an incorrect digital signature was received. *The shared secret does not match between Steel-Belted Radius and the target; or some unauthorized rogue device is attempting to compromise RADIUS security.*
Insufficient Resources	The total number of rejects due to a server resource problem.
Retries Transmitted	
Transactions Retried	The number of requests for which one or more retried transmissions was performed.
Total Retry Packets	The total number of duplicate packets received.

Sessions List

Steel-Belted Radius tracks the status of the user connections that it authenticates. You can display this information by clicking the **Display Sessions** button at the upper right of the Statistics dialog. The **Sessions** list (also called the “Current Users display”) will appear.

The list is based on RADIUS accounting data. It will only be accurate if all of your NAS devices are configured to support RADIUS accounting.

NOTE: Steel-Belted Radius maintains the Current User list on disk. The information will not be lost if you unload and reload the server.



User Name	RAS Client	Port	Port Type	Time	Session-ID	IP Address
CHRISTIAN	62.180.30.2	152	ISDN-Sync	10/30/2001 12:08:59	00000098	
GEORGE	62.180.30.2	155	ISDN-Sync	10/30/2001 12:09:11	0000009B	
JAMESMC	62.180.30.2	153	ISDN-Sync	10/30/2001 12:09:05	00000099	
JOHN	62.180.30.2	156	ISDN-Sync	10/30/2001 12:09:16	0000009C	
KEVIN	62.180.30.2	154	ISDN-Sync	10/30/2001 12:09:08	0000009A	
RALPH	62.180.30.2	157	ISDN-Sync	10/30/2001 12:10:06	0000009D	10.20.30.40

Current Users Dialog (Windows version)

For every active dial-in session, the Sessions list displays a line containing the following fields:

- **User Name** shows the name of the authenticated user. If the user is:
  - Native, the field will show the username only, in the form username.
  - Non-native, the field will show the remote system name as well as the username, in the form `\\systemname\username`.
  - Associated with a specific tunnel, the field will show the tunnel name as well as the username, in the form `\\tunnelname\username`.
- **RAS Client** is the NAS's identifier, which will either be the name of the device or its IP address.
- **Port** is a unique port number on the NAS that has been assigned to the connection. To determine the actual physical port on the NAS, consult the NAS documentation.
- **Port Type** describes how the port is used or configured. Possibilities include Async, Sync, ISDN, and so forth.

- **Time** indicates the date and time at which the connection was started.
- **Session ID** contains the unique key for the session, a number generated by the NAS.
- **IP Address** shows the IP address that was assigned to the user from an IP address pool. (If an IP address was statically assigned, this field is blank.)

NOTE: For tunnel connections, if Steel-Belted Radius was used to authenticate both the user and the tunnel, then two entries are displayed in the Current Users window: one entry for the authenticated user, and one for the authenticated tunnel.

Modifying the Sessions List Columns

You can modify the order and size of the fields in the Sessions List easily with the mouse.

- To resize any field, move the mouse to the right edge of a field heading. When the resize cursor appears, click and drag the field width as you please.
- To move any field, click on any field heading and drag it left or right to the desired position.

  NOTE: This feature is supported only by Windows.

Sorting the Sessions List (Windows only)

The Sessions List is always maintained in sorted order, based on each column of the report starting from the first column at the left. Thus, to sort the report according to the values in any field, simply drag that field to the leftmost position.

Refreshing the Sessions List

The Sessions List shows a snapshot of the current connected users taken when you first open the dialog. To update the report with fresh information, click **Refresh**.

Deleting Entries from the Sessions List

Normally, the system will take care of maintaining the correct information in the Sessions list based on accounting information received from the NAS. However, it is sometimes possible that a user who has logged off will still be indicated as active in the Current User list. This may occur as a result of communication failures between the NAS and Steel-Belted Radius, or it could occur if either the NAS or Steel-Belted Radius is taken down for a period of time.

In most cases, Steel-Belted Radius can correct such anomalies itself. For example, if a new user dials in to the same port on the same NAS, Steel-Belted Radius infers that the prior user must have disconnected and will remove the entry.

You can also manually correct the Sessions list by highlighting any entry and clicking **Delete**. In addition to removing the user from the list, the user's connection count (if it is being tracked) will decrease by one, and any pooled IP or IPX address that had been assigned to that user will be returned to the appropriate pool.

Reporting Capabilities

The Report command lets you assemble any of the Steel-Belted Radius database information that is available through the Administrator program's dialogs into a report. For example, you can output to a report all the information you've set up about RAS Clients, Users, Proxies, and the like.

Windows only: The **Report** command outputs the information in rich text format to a filename of your choice (normally REPORT.RTF), then opens that report using the word processor of your choice (normally WORDPAD.EXE). From the word processor, you can apply further formatting to the report, save it to an archive, or print it.

Setting Report Options (Windows only)

Before creating your first report, make sure that the settings for the output filename and the word processor with which you will view the report are correct:

1 Run the Administrator program.

2 Select the **File Settings** command. The Settings dialog appears.

3 Make sure the Report viewer and Report filename settings are to your liking. Be sure that the word processor that you specify as Report viewer is capable of interpreting RTF (rich text format).

4 When you are satisfied with the settings, click **OK**.

Creating a Report

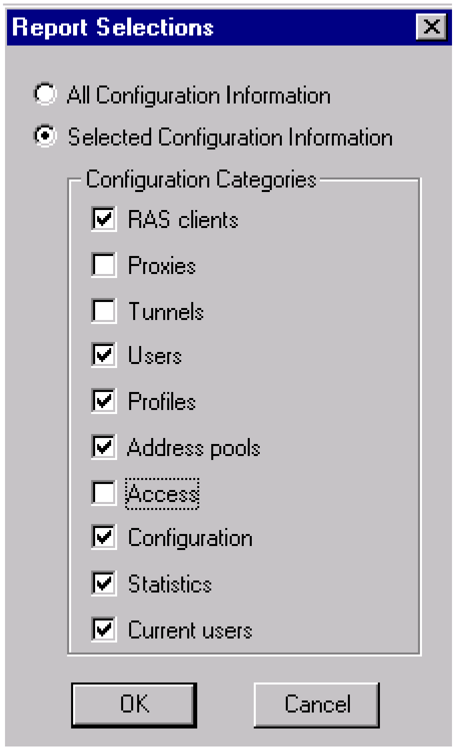
To create a report:

1 Run the Administrator program.

2 Depending on your platform:

- Under **Unix**: Click the **Report** button at the bottom of the Steel-Belted Radius Administrator display.
- Under **Windows**: Select the **File Report** command.

3 The Report Selections dialog appears.



Report Selections

○ All Configuration Information

● Selected Configuration Information

Configuration Categories

☑ RAS clients

□ Proxies

□ Tunnels

☑ Users

☑ Profiles

☑ Address pools

□ Access

☑ Configuration

☑ Statistics

☑ Current users

Report Selections Dialog (Unix version)

4 To generate a complete report on every aspect of the server, check **All configuration information**.

Otherwise, check **Selected configuration information**, and check the categories of information you'd like to include.

5 Click **OK**. Depending on your platform:

- Under **Unix**: A new instance of your browser pops up, displaying the resulting report. You can save this report to HTML format if desired.
- Under **Windows**: The report file will be created and will appear in your selected word processor.

Windows NT Performance Monitor

The Steel-Belted Radius service has information which can be viewed with the Performance Monitor on Windows NT/2000.

To view a graph of Steel-Belted Radius performance:

1 Start `perfmon.exe` on your administrative workstation.

NOTE: You may also start `perfmon.exe` *on a Steel-Belted Radius server machine.*

2 Select **Edit > Add to Chart**. Select the Steel-Belted Radius service from the list of Objects. If you are running multiple Steel-Belted Radius servers, you will be able to select the correct one by computer name.

3 Select the counters that you wish to graph. For each counter, choose **Color**, **Scale**, and other display options as desired. Then click **Add**.

Most perfmon counters relating to Steel-Belted Radius have self-explanatory names, such as `Acct Failures - Insufficient Resources` or `Acct Failures - Invalid Shared Secret`.

Of special interest is the `Failed Auths -` *n* counter. There are 16 such counters, where *n* is a number between 1 and 16. The `Failed Auths -` *n* perfmon counter tracks the total number of failed authentication requests that were encountered for all of the RADIUS clients that you've mapped to collection number *n*.

To set up the Failed Auths - n counter, see "radius.ini [FailedAuthOriginStats] Section (Windows only)" on page 142.

4 When you are finished adding counters, click **Done**.

The Performance Monitor window will display a graph of the counters you've selected. The graph will update itself at regular intervals until you close the Performance Monitor window.

5 You can start multiple versions of `perfmon.exe` to view more than one Steel-Belted Radius server at one time.

The following perfmon counters are available.

perfmon Counter	Meaning
Acct Failures - Insufficient Resources	The number of accounting requests that were discarded because the RADIUS server was unable to obtain sufficient system resources to process the request.
Acct Failures - Invalid Clients	The number of accounting requests that were discarded because the RADIUS client identified in the request was not defined in the RADIUS server database.

perfmon Counter	Meaning
Acct Failures - Invalid Requests	The number of accounting requests that were discarded because the request was malformed or contained invalid attributes.
Acct Failures - Invalid Shared Secret	The number of accounting requests that were discarded because the request contained an invalid digital signature. This is usually due to a mismatch in the shared secrets defined on the RADIUS client and the RADIUS server.
Acct Proxy Failures	The number of forwarded accounting requests for which failures were encountered.
Acct Requests Forwarded	The number of accounting requests that were forwarded to other RADIUS servers.
Acct Requests Retried	The number of unique accounting requests for which retries were received by the RADIUS server.
Acct Requests Retried/sec	The number of accounting requests per second for which one or more retries has been received by the RADIUS server.
Acct Retry Requests	The number of actual accounting request retries received by the RADIUS server.
Acct Retry Requests/sec	The number of accounting request retries per second received by the RADIUS server.
Acct Service Time	The number of seconds that elapsed from the time the last completed accounting request was received to the time the RADIUS server sent a response. Responses generated by proxies are not reflected in this statistic.
Acct Starts	The number of accounting start requests received by the RADIUS server. An accounting start signifies the granting of a connection to an end-user by the remote access server.
Acct Starts/sec	The number of accounting start requests received by the RADIUS server per second. An accounting start signifies the granting of a connection to an end-user by the remote access server.
Acct Stops	The number of accounting stop requests received by the RADIUS server. An accounting stop signifies that an end-user has disconnected from the remote access server.
Acct Stops/sec	The number of accounting stop requests received by the RADIUS server per second. An accounting stop signifies that an end-user has disconnected from the remote access server.
Auth Failure - Authentication Failures	Number of unique authentication requests to which the RADIUS server replied with a reject because no user specified in the database possessed a matching password. A mismatch in shared secrets would also cause this counter to be incremented.
Auth Failure - Checklist Mismatches	Number of unique authentication requests to which the RADIUS server replied with a reject because the request did not include required checklist information.

perfmon Counter	Meaning
Auth Failure - Insufficient Resources	Number of unique authentication requests to which the RADIUS server replied with a reject because the RADIUS server ran into a system resource limitation.
Auth Failure - Invalid Clients	Number of unique authentication requests to which the RADIUS server replied with a reject because the request was from a RADIUS client not identified in the RADIUS server's database.
Auth Failure - Invalid Requests	Number of unique authentication requests to which the RADIUS server replied with a reject because the request was malformed or contained invalid attributes.
Auth Proxy Failures	The number of forwarded authentication requests for which failures were encountered.
Auth Proxy Rejects	The number of forwarded authentication requests for which rejects were received from the target RADIUS server.
Auth Requests	The number of unique authentication requests that the RADIUS server has received.
Auth Requests Forwarded	The number of authentication requests that were forwarded to another RADIUS server.
Auth Requests Retried	The number of unique authentication requests for which retries were received by the RADIUS server.
Auth Requests Retried/sec	The number of authentication requests per second for which one or more retries has been received by the RADIUS server.
Auth Requests/sec	The number of unique authentication requests that the RADIUS server has received per second.
Auth Retry Requests	The number of actual authentication request retries received by the RADIUS server.
Auth Retry Requests/sec	The number of authentication request retries per second received by the RADIUS server.
Auth Service Time	The number of seconds that elapsed from the time the last completed authentication request was received to the time the RADIUS server sent an Accept response. Accept responses generated for tunnel requests or by proxies are not reflected in this statistic.
Auth SQL Disconnects	The number of times an existing connection to a SQL authentication database failed.
Auth SQL Failures	The number of times an attempt to connect to a SQL authentication database failed.
Auth SQL Records Not Found	The number of times no record was found in a SQL authentication database for the specified username.
Auth SQL Timeouts	The number of times a timeout occurred attempting to execute a SQL authentication request.
Auth Successes	The number of unique authentication requests to which the RADIUS server replied with an Accept.

perfmon Counter	Meaning
Auth Successes/sec	The number of unique authentication requests to which the RADIUS server replied with an accept per second.
Concurrency Auth Failures	The number of times an authentication request was forwarded to the concurrency server and the concurrency server returned a reject for reasons other than users being over their port limits.
Concurrency Auth Service Time	The number of seconds elapsed from the last time an authentication request was sent to the concurrency server and a response was received.
Concurrency Auth Timeouts	The number of times an authentication request was forwarded to the concurrency server and no response was received within the configured time for the proxy entry.
Concurrency Over Port Limit	The number of times an authentication request was forwarded to the concurrency server and the concurrency server returned a reject because users were over their port limits.
Failed Auths - 1	The number of failed authentication requests that were encountered for clients categorized in collection number 1. To set up this counter, see “radius.ini [FailedAuthOriginStats] Section (Windows only)” on page 142.
Failed Auths - 2	The number of failed authentication requests that were encountered for clients categorized in collection number 2.
Failed Auths - 3	The number of failed authentication requests that were encountered for clients categorized in collection number 3.
Failed Auths - 4	The number of failed authentication requests that were encountered for clients categorized in collection number 4.
Failed Auths - 5	The number of failed authentication requests that were encountered for clients categorized in collection number 5.
Failed Auths - 6	The number of failed authentication requests that were encountered for clients categorized in collection number 6.
Failed Auths - 7	The number of failed authentication requests that were encountered for clients categorized in collection number 7.
Failed Auths - 8	The number of failed authentication requests that were encountered for clients categorized in collection number 8.
Failed Auths - 9	The number of failed authentication requests that were encountered for clients categorized in collection number 9.
Failed Auths - 10	The number of failed authentication requests that were encountered for clients categorized in collection number 10.
Failed Auths - 11	The number of failed authentication requests that were encountered for clients categorized in collection number 11.
Failed Auths - 12	The number of failed authentication requests that were encountered for clients categorized in collection number 12.
Failed Auths - 13	The number of failed authentication requests that were encountered for clients categorized in collection number 13.

perfmon Counter	Meaning
Failed Auths - 14	The number of failed authentication requests that were encountered for clients categorized in collection number 14.
Failed Auths - 15	The number of failed authentication requests that were encountered for clients categorized in collection number 15.
Failed Auths - 16	The number of failed authentication requests that were encountered for clients categorized in collection number 16.
Forwarded Requests Retried	The number of unique forwarded accounting and authentication requests for which retries were transmitted by the RADIUS server.
Forwarded Requests Retried/sec	The number of unique forwarded accounting and authentication requests for which retries were transmitted per second by the RADIUS server.
Forwarded Retry Requests	The number of actual retransmissions of forwarded accounting and authentication request performed by the RADIUS server.
Forwarded Retry Requests/sec	The number of actual retransmissions of forwarded accounting and authentication request per second performed by the RADIUS server.
Proxy Failures - Insufficient Resources	The number of authentication and accounting requests that were forwarded to other RADIUS servers for which the RADIUS server was unable to obtain sufficient system resources to process the request.
Proxy Failures - Invalid Response	The number of authentication and accounting requests that were forwarded to other RADIUS servers for which malformed or invalid responses were received.
Proxy Failures - Invalid Shared Secret	The number of authentication and accounting requests that were forwarded to other RADIUS servers for which responses were discarded because the response contained an invalid digital signature. This is usually due to a mismatch in the shared secrets defined on the RADIUS client and RADIUS server.
Proxy Failures - Time Out	The number of authentication and accounting requests that were forwarded to other RADIUS servers for which no response was received after the specified number of retries.
Seconds since started	Number of seconds Steel-Belted Radius has been running.
Sessions Online	The number of sessions currently active in the RADIUS server's Sessions list.
Static Acct Service Time	The number of seconds elapsed from the last time an accounting request was sent to the static accounting proxy server and a response was received.
Total Acct Failures	The total number of unique accounting requests to which the RADIUS server did not reply. Reasons for the failures are identified in other statistics.

perfmon Counter	Meaning
Total Acct Failures/sec	The total number of unique accounting requests to which the Radius server did not reply per second because of an error. Reasons for the failures are identified in other statistics.
Total Acct Offs	The number of accounting off requests received by the RADIUS server. An accounting off signifies that the accounting support in the RADIUS client has been disabled. This request is most often issued when a RADIUS client in being shut down.
Total Acct Offs/sec	The number of accounting off requests received by the RADIUS server per second.
Total Acct Ons	The number of accounting on requests received by the RADIUS server. An accounting on signifies that the accounting support in the RADIUS client has been enabled. This request is most often issued when a RADIUS client is powered on.
Total Acct Ons/sec	The number of accounting on requests received by the RADIUS server per second.
Total Auth Challenges	The number of authentication requests that resulted in a RADIUS challenge response.
Total Auth Failures	The total number of unique authentication requests to which the RADIUS server replied with a reject. Reasons for the failures are identified in other statistics.
Total Auth Failures/ sec	The total number of unique authentication requests to which the RADIUS server replied with a reject, per second. Reasons for the failures are identified in other statistics.
Total Forwarded Request Failures	The total number of forwarded authentication and accounting requests that encountered failures.
Total Forwarded Request Failures/sec	The total number of forwarded authentication and accounting requests that encountered failures, per second.
Total Forwarded Requests	The total number of authentication and accounting requests that were forwarded to other RADIUS servers.
Total Forwarded Requests/sec	The total number of authentication and accounting requests per second that were forwarded to other RADIUS servers.
Users Online	The number of unique user names represented in the RADIUS server's Sessions List.

Windows NT Events

Steel-Belted Radius generates a variety of Windows NT events. Regardless of severity, each event is attributed to one of the following three Windows NT services:

the “core” Steel-Belted Radius service, the authentication service, or the accounting service. Service identifiers are as follows.

ID	Symbolic Name	Text
1	`RADCAT_CORE`	Core
2	`RADCAT_AUTH`	Authentication
3	`RADCAT_ACCT`	Accounting

The following three topics group Steel-Belted Radius events according to their severity: Informational, Warning, and Error.

Informational Events

The following events are for informational purposes only. They do not require intervention by an operator.

NOTE: Some informational events serve to “clear” a previous warning event.

ID	Informational Event	Meaning
100	The Steel-Belted Radius service was started.	—
101	The Steel-Belted Radius service was stopped.	—
102	Count of available threads has risen to acceptable threshold of *nnnn*.	The low thread available condition has subsided. You can configure the value *nnnn* using the [Thresholds] section of the `events.ini` configuration file.
103	Amount of free file system space has risen to acceptable threshold. Free byte count is *nnnnnnnn*.	The low file system space condition has subsided. You can configure the value *nnnnnnnn* using the [Thresholds] section of `events.ini`.
104	Steel-Belted Radius has reconnected to the Concurrency Server after a ConcurrencyFailure.	—
105	Steel-Belted Radius has reconnected to the SQL database after a SQLConnectFail.	—
106	Steel-Belted Radius has reconnected to the LDAP database after an LDAPConnectFail.	—
107	A user's account has been locked due to excessive authentication attempts within a defined period of time.	—

ID	Informational Event	Meaning
108	A user account, previously locked due to an excessive amount of rejected authentication attempts, becomes unlocked.	—
109	The target server for proxy spooling reconnected.	—

Warning Events

Warning events may require intervention as indicated in the following table.

The text `This event represents nnnn failures` reflects a setting in the [EventDilutions] section of the events.ini file. You can set this value to a higher number so that the event is reported less frequently.

ID	Warning Event	Meaning
5001	Count of available threads has dropped to minimum threshold of *nnnn*.	A low thread count available condition has been detected. This event can be issued in the authentication or accounting category to indicate a shortage of authentication or accounting threads. You can configure the value *nnnn* using the [Thresholds] section of the events.ini configuration file.
5002	Concurrency server returned failure indication. This event represents *nnnn* failures.	A reject was returned from the concurrency server in response to a proxied authentication request. The reject was for a reason other than exceeded port limit. You can configure the value *nnnn* using the [EventDilutions] section of events.ini.
5003	Timed out in proxy attempt to concurrency server. This event represents *nnnn* requests timing out.	A timeout was encountered when proxy-forwarding an authentication request to the concurrency server. You can configure the value *nnnn* using the [EventDilutions] section of events.ini.
5004	Local failure encountered in attempt to proxy to concurrency server. This event represents *nnnn* requests timing out.	A local processing failure was encountered when trying to proxy-forward an authentication request to the concurrency server. You can configure the value *nnnn* using the [EventDilutions] section of events.ini.
5005	Timed out in static accounting proxy attempts. This event represents *nnnn* failures.	A timeout was encountered when proxy-forwarding an accounting request to the concurrency server. You can configure the value *nnnn* using the [EventDilutions] section of events.ini.

ID	Warning Event	Meaning
5006	Local failure encountered in attempt to proxy for static accounting. This event represents *nnnn* requests timing out.	A local processing failure was encountered when trying to proxy-forward an accounting request to the concurrency server. You can configure the value nnnn using the [EventDilutions] section of `events.ini`.
5007	Amount of free file system space has dropped below minimum threshold. Free byte count is *nnnnnnnn*.	A low available file system space condition has been detected. You can configure the value *nnnnnnnn* using the [Thresholds] section of `events.ini`.
5008	*nnnn* attempts to connect to SQL server failed.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5009	*nnnn* disconnects from SQL server due to error.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5010	*nnnn* timeouts on SQL requests.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5011	Access to accounting server database has timed out. This event represents *nnnn* timeouts.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5012	Access to accounting server database has failed. This event represents *nnnn* failures.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5013	Verification Server has timed out. This event represents *nnnn* Verification Server timeouts.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5014	Verification Server requests have failed. This event represents *nnnn* Verification Server failures.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5015	The connection to an LDAP server has failed.	—
5016	Communication with an LDAP server has failed. This event represents *nnnn* connection failures.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5017	The LDAP server has disconnected. This event represents *nnnn* connection failures.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.
5018	A request to the LDAP server has timed out. This event represents *nnnn* request timeouts.	You can configure the value *nnnn* using the [EventDilutions] section of `events.ini`.

ID	Warning Event	Meaning
5019	The LDAP server has disconnected	—
5020	A request to the LDAP server has timed out.	—
5021	The target server of proxy spooling fails to respond (non-dilutable).	—
5022	The target server of proxy spooling fails to respond (dilutable).	—

Error Events

Error events usually require some form of intervention by the operator.

Most Steel-Belted Radius error events are generated at startup, as the service initializes each of its components. If any component fails at startup, the “service start” operation is aborted and the system generates an error event. The text of the error will generally indicate what Steel-Belted Radius was trying to do when it failed.

In some cases, the operator may be able to take direct action in response to an error event. For example, if the system is unable to open a log file, perhaps the system disk is full, leaving no room to create additional files. You can easily check and remedy this condition.

If a solution does not emerge right away, the event text will at least pinpoint the problem area in the software. You should escalate the problem to your next level of support. When you do, be sure to indicate the ID, name, and text of the event.

ID	Error Event
10000	StartServiceCtrlDispatcher failed with error *nnnn*.
10001	SetServiceStatus failed with error *nnnn*.
10002	Invalid private directory 'directory' specified.
10003	Unable to create thread.
10004	Unable to create mutex.
10005	Unable to initialize signal handling.
10006	Unable to configure event processing.
10007	Unable to create or open log file.
10008	Unable to initialize LDAP administration interface.
10009	Unable to initialize RPC administration interface.

ID	Error Event
10010	Unable to initialize base IP interface.
10011	Unable to initialize current user list processing.
10012	Unable to initialize challenge continuation cache.
10013	Unable to initialize RAS activity monitor.
10014	Unable to initialize dictionary processing.
10015	Unable to process vendor.ini file.
10016	Unable to initialize Btrieve|Raima database.
10018	Unable to initialize admin user rights component.
10019	Unable to open Btrieve|Raima database.
10020	Unable to initialize tunnel DNIS lookup component.
10021	Unable to initialize configuration caching component.
10022	Unable to initialize database caching component.
10023	Unable to initialize license processing.
10024	Unable to initialize NDS trustee processing.
10025	Unable to initialize NetWare host lookup processing.
10026	Unable to initialize IP/IPX pool resource management.
10027	Unable to initialize user login count tracking.
10028	Unable to create persistent store for Sessions list.
10029	Unable to initialize persistent store for Sessions list.
10030	Unable to initialize performance monitor interface component.
10031	Unable to initialize admin locking component.
10032	Unable to initialize plug-in support component.
10033	Unable to initialize duplicate request cache.
10034	Unable to initialize name mangling support.
10035	Unable to initialize name stripping support.
10036	Error *nnnn* returned from call to GetDiskFreeSpaceEx. File system space checking disabled.
10037	Unable to initialize name validation support. Service start aborted.
10038	Unable to initialize system resource checking. Service start aborted.
10039	Unable to initialize statistic collection. Service start aborted.
10040	Attempt to connect to SQL server *xxxxxxxx* failed.
10041	Disconnect from SQL server *xxxxxxxx* due to error.
10042	Timeout on SQL request.
10043	Unable to allocate reserved memory specified by ReserveMemoryKB. You can set the ReserveMemoryKB value in the [Thresholds] section of the events.ini configuration file.

ID	Error Event
10044	Memory allocation failure encountered. Reserved memory released as last resort.
10045	*nnnn* memory allocation failures have occurred. You can configure the value nnnn using the [EventDilutions] section of `events.ini`.
10046	The connection to the Accounting Server has failed.
10047	The connection to the Verification Server has failed.
10050	The initialization of common IP services at server startup has failed.

Server Configuration

6

Server Configuration Files

This chapter describes files that control the behavior of the Steel-Belted Radius server. While you will need to learn about these files in order to customize the operation of the server for advanced operation, the default settings will allow you to run a generic configuration of the server immediately after installation without requiring you to alter these files.

Server configuration files include:

- Initialization files, which enable, disable, and configure various features of the server. These files are loaded at startup time, and reside in the Steel-Belted Radius server directory:

  account.ini
  eap.ini
  events.ini
  filter.ini
  radius.ini
  tacplus.ini
  vendor.ini

- Dictionary files, which specify RADIUS attributes. Like initialization files, these files are loaded at startup time, and reside in the Steel-Belted Radius server directory:

  *.dct
  *.dci
  dictiona.dcm

- Automatic EAP Helper configuration files, which specify options for automatic EAP helper methods.These files are loaded at startup time and reside in the Steel-Belted Radius server directory:

  *.eap

- The services file, which assigns default UDP ports for RADIUS communications to and from the Steel-Belted Radius server. The location of the file is:

  - (Under **Unix**) /etc/
  - (Under **Windows**) C:\winnt\system32\drivers\etc\

Other files are described at length in later chapters. These files control the server's interactions with "outside parties," including:

- External databases, for authentication and accounting respectively:

  *.aut
  *.acc

Syntax

The pound (‘#’) character comments out a line, as long as the ‘#’ is the first non-space character in the line. The semicolon (‘;’) may be used as a comment character in the same way.

account.ini File

The account.ini initialization file contains information that controls how RADIUS accounting attributes will be logged by Steel-Belted Radius.

account.ini [Alias/*name*] Sections

The [Alias/*name*] sections of account.ini are used to associate attributes of different names, but identical meaning. For example, one NAS vendor may call an attribute `Acct-Octet-Pkt` and another may call it `Acct-Oct-Packets`, yet the two attributes mean the same thing.

Each [Alias/*name*] section permits you to map one RADIUS accounting attribute that is already being logged by Steel-Belted Radius to any number of other attributes. You may provide as many [Alias/*name*] sections as you wish, using the following syntax for each section:

```
[Alias/name]
VendorSpecificAttribute=
VendorSpecificAttribute=
.
.
.
```

Field	Meaning
name	The preferred attribute name. The name attribute must be one that you are currently logging to a column in the Steel-Belted Radius accounting log file (.ACT). Therefore, it must be listed in the [Attributes] section of account.ini.
VendorSpecificAttribute	Each entry is given on one line. An equal sign (‘=’) must immediately follow each VSA name, without any intervening space. Otherwise, the entry will be considered invalid.

Each *`VendorSpecificAttribute`* in the list will be logged to the *`name`* column in the accounting log file. Because you’re listing these attributes in an [Alias/*name*] section, you’ll probably want to make sure they are not listed in the [Attributes] section, or in addition to the *name* column, they will be logged separately to their own columns as well.

All of the attribute names that you reference in an [Alias/*name*] section must be defined in a dictionary file that is already installed on the Steel-Belted Radius server. This includes *name* and each *VendorSpecificAttribute* entry.

In the following example, the standard RADIUS attribute Acct-Octet-Packets is mapped to the vendor-specific attributes Acct-Octet-Pkt and Acct-Oct-Packets. Values encountered for all three attributes will be logged in the Acct-Octet-Packets column in the accounting log file:

```
[Alias/Acct-Octet-Packets]
Acct-Octet-Pkt=
Acct-Oct-Packets=
```

account.ini [Attributes] Section

The [Attributes] section of account.ini lists all the attributes that will be logged in the accounting log file. When you first install Steel-Belted Radius, the account.ini file is set up so that all standard RADIUS attributes and all supported vendors' accounting attributes are listed.

You can configure what is logged to the accounting log file by rearranging the order of attributes in the [Attributes] section. You can delete or comment out any attributes that are not of interest to your billing system or which do not apply to the equipment that you are using. This will allow you to design the content and column order of any spreadsheets that you plan to create based upon the accounting log file.

The syntax is as follows:

```
[Attributes]
AttributeName=
AttributeName=
.
.
.
```

For example:

```
[Attributes]
User-Name=
NAS-Port=
Framed-IP-Address=
Acct-Status-Type=
Acct-Delay-Time=
Acct-Session-Id=
```

The [Attributes] section lists one `AttributeName` on each line. You must ensure that an equal sign ('=') immediately follows each `AttributeName`, with no spaces in between. Otherwise, the entry will be considered invalid.

Each `AttributeName` in the [Attributes] section must already be defined in a dictionary file (.dct) that is already installed on the Steel-Belted Radius server. This dictionary may be standard RADIUS or vendor-specific.

NOTE: The first six attributes in each log file entry (Date, Time, RAS-Client, Record-Type, Full-Name, and Auth-Type) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the account.ini *file [Attributes] section.*

account.ini [Configuration] Section

account.ini [Configuration] field	Meaning
LogDir	If this setting is present, it will override the default system location (the private directory). You may need to add this section and field if it does not exist in your account.ini file. *NOTE: With directed realms, you can still maintain multiple accounting log locations*.

account.ini [Settings] Section

Steel-Belted Radius writes all accounting data to the current accounting log file (.ACT) until that log file is closed; then upon closing the file Steel-Belted Radius opens a new one and begins writing accounting data to it.

You can configure how often this "rollover" of the accounting log file occurs.

The naming conventions of the accounting log files support the fact that there may be more than one file per day. The formats are as follows. In the examples below, *y*=year digit, *m*=month digit, *d*=day digit, and *h*=hour digit. The extra sequence number _*nnnnn* starts at _00000 each day.

File Generation Method	File Naming Convention
Default (24 hours)	*yyyymmdd*.ACT
Non-24-hour rollover	*yyyymmdd_hhmm*.ACT
Rollover due to size	*yyyymmdd_nnnnn*.ACT

File Generation Method	File Naming Convention
Rollover due to size or startup when non-24-hour time in effect	*yyyymmdd_hhmm_nnnnn*.ACT

The following fields have been provided for use in the [Settings] section of account.ini. These fields control which entries will be written to the accounting log file, and ensure the compatibility of these entries with a variety of database systems. The following "rollover" fields may be present in the [Settings] section.

account.ini [Settings] field	**Meaning**
BufferSize	The size of the buffer used in the accounting logging process, in bytes. The default is 32768.
Carryover	If set to 1 (the default), each time a new accounting log file is created, a summary of the Sessions List is written to the file. If 0, the list is not written.
Enable	If set to 1 (the default), the accounting log feature is enabled. If 0, no .ACT files will be created on this server. Accounting servers should have Enable set to 1; for efficiency, non-accounting servers should have Enable set to 0.
LineSize	The maximum size of a single accounting log line. The default is 4096. The allowable range is 1024 to 32768.
MaxSize	The maximum size of an accounting log file, in bytes. Once the accounting log file reaches this limit, it will be closed and a new file started. A value of 0 (the default) means unlimited size.
QuoteBinary	If set to 1 (the default), binary values written to the accounting log file will be enclosed in quotes; if 0, quotes will not be used. You should set this value according to the format expected by the accounting application that will eventually receive the entries.
QuoteInteger	If set to 1 (the default), integer values written to the accounting log file will be enclosed in quotes. If 0, quotes will not be used. You should set this value according to the format expected by the accounting application that will eventually receive the entries.
QuoteIPAddress	If set to 1 (the default), IP addresses written to the accounting log file will be enclosed in quotes; if 0, quotes will not be used. You should set this value according to the format expected by the accounting application that will eventually receive the entries.
QuoteText	If set to 1 (the default), text strings written to the accounting log file will be enclosed in quotes; if 0, quotes will not be used. You should set this value according to the format expected by the accounting application that will eventually receive the entries.

account.ini [Settings] field	Meaning
QuoteTime	If set to 1 (the default), time and date values written to the accounting log file will be enclosed in quotes; if 0, quotes will not be used. You should set this value according to the format expected by the accounting application that will eventually receive the entries.
Rollover	How often the current accounting log file will be closed and a new file opened (a rollover), up to one rollover per minute. Non-zero values indicate the number of minutes until the next rollover. A value of 0 (the default) will cause a rollover once every 24 hours, at midnight local time.
RolloverOnStartup	If set to 1, each time Steel-Belted Radius is started up, it will close the current accounting log file and open a new one. A sequence number *_nnnnn* is appended to the log file name, just as when MaxSize is reached. If 0 (the default), each time Steel-Belted Radius is started up, it will continue to append entries to the previously open accounting log file.
Titles	If set to 1 (the default), each time a new accounting log file is created, the title line (containing column headings) is written to the file. If 0, the line is not written.
UTC	If set to 1, time and date values will be provided according to universal time coordinates (UTC, formerly known as Greenwich mean time or GMT). If 0 (the default), time and date values will reflect local time.

account.ini [TypeNames] Section

Each entry in the [TypeNames] section of account.ini maps a possible value of the Acct-Status-Type attribute to a string. The syntax is as follows:

```
[TypeNames]
TypeID = TypeName
TypeID = TypeName
.
.
.
```

where the fields have meaning as follows:

account.ini [TypeNames] Field	
TypeID	Each *TypeID* is a numeric value that corresponds to a possible value of the Acct-Status-Type attribute. This attribute appears in every incoming RADIUS accounting packet to identify the types of data it is likely to contain.

account.ini [TypeNames] Field	
TypeName	Each *TypeName* value is a string. This string will be written to the accounting log to identify the type of packet.

The standard Acct-Status-Type values 1, 2, 3, 7, and 8 are already listed in the [TypeNames] section of account.ini as follows:

```
[TypeNames]
1=Start
2=Stop
3=Interim
7=On
8=Off
```

You can edit the [TypeNames] section to add vendor-specific packet types to this list. This will make your accounting log files easier to read and use. For example:

```
[TypeNames]
1=Start
2=Stop
3=Interim
7=On
8=Off
639=AscendType
28=3ComType
```

If no string is given for a particular Acct-Status-Type, Steel-Belted Radius will use the numeric value of the incoming Acct-Status-Type attribute, formatted as a string.

events.ini File

The events.ini configuration file controls dilutions and thresholds for Steel-Belted Radius events which are used to communicate failures, warnings, and other information. Events are handled by the Windows NT Events mechanism.

See “Windows NT Events” on page 117 for a list of valid event values. Look for the number in the left-most column in the tables listing Informational, Warning, and Error events. Note that only some of these events support thresholds or are dilutable.

events.ini [EventDilutions] Section

The [EventDilutions] section of events.ini controls how often a Steel-Belted Radius event is actually generated, in relation to how often the event is detected by the system. This feature allows certain events (those being issued too frequently to make it practical to report each one of them) to be logged on a more infrequent basis.

The correct syntax is as follows:

```
[EventDilutions]
EventName=DilutionCount
```

where *EventName* identifies a Steel-Belted Radius event and *DilutionCount* specifies how many times this event must occur before it will be recorded in the Windows NT event log or to the SNMP manager program.

The following example configures warning event number 5008:

```
[EventDilutions]
SQLConnectFailure=5
```

This example assumes Steel-Belted Radius is configured to authenticate against a SQL database; and after configuring the radsql.aut file and restarting the server, some SQL error condition exists, preventing Steel-Belted Radius from successfully connecting to the database. Steel-Belted Radius will continue to attempt the connection and will report these attempts in the *date*.log file. However, Steel-Belted Radius will not trigger warning event 5008 until the fifth connection attempt fails.

events.ini [Suppress] Section

The [Suppress] section of events.ini allows you to suppress Steel-Belted Radius events. For example:

```
[Suppress]
5010
5020
```

events.ini [Thresholds] Section

The [Thresholds] section of events.ini allows you to specify thresholds that will trigger specific events. These settings can involve more than one event type.

This section allows for fine tuning of Steel-Belted Radius event generation in regards to crucial items such as system memory, thread count, and file system space, and can differ for each computer depending on resources, configuration, and other applications.

This table lists the event names for both Windows and Unix, in that order.

The following fields may be present:

events.ini [Thresholds] Field	**Meaning**
ThreadAvailWarningIssue=*x*	When the number of available threads reaches *x*, issue the warning event RADMSG_THREADS_LOW or funkSbrTrapLowThreads (5001).
ThreadAvailWarningClear=*y*	When the number of available threads reaches *y* at some later point, issue the informational event RADMSG_THREADS_NORMAL or funkSbrTrapThreadsNormal (102).
FileSystemFreeKBWarningIssue=*x*	When the number of kilobytes of available system disk space reaches *x*, issue the warning event RADMSG_FILE_SYSTEM_LOW or funkSbrTrapLowFSSpace (5007).
FileSystemFreeKBWarningClear=*y*	When the number of kilobytes of available system disk space reaches *y* at some later point, issue the informational event RADMSG_FILE_SYSTEM_NORMAL or funkSbrTrapFSNormal (103).
ReserveMemoryKB=*x*	Reserve this amount of memory (in kilobytes) for cases of overload.
PoolPctAddressAvailWarningIssue=*x*	When the number of available IP addresses in any IP Address Pool drops below, *x*%, issue a funkSbrTrapIPAddrPoolLow warning.
PoolPctAddressAvailWarningClear=*y*	If the number of available IP addresses in any IP Address Pool has fallen below *x*% but have returned to above *y*%, issue an informational message.

For example:

```
[Thresholds]
ThreadAvailWarningIssue=10
ThreadAvailWarningClear=20
```

Using this example, a warning event (5001) will be issued when the number of available accounting or authentication threads fall below 10 percent, and an informational event (102) will be issued when it rises above 20 percent.

filter.ini File

The `filter.ini` configuration file allows you to set up rules for filtering attributes into and out of RADIUS packets.

Filter Rules

Each filter in the `filter.ini` file consists of the filter name in square brackets ([*name*]) followed by the rules for that filter.

Each rule takes one of the following three forms:

```
keyword  attribute  value
keyword  attribute
keyword
```

The complete set of valid syntax combinations is as follows:

filter.ini Rule Syntax	Meaning
ALLOW	This keyword by itself specifies that all attributes, regardless of value, are to be allowed in the packet.
ALLOW *attribute*	This rule specifies that this attribute will be allowed in the packet, regardless of its value.
ALLOW *attribute value*	The rule lists a specific attribute/value pair to allow in the packet.
EXCLUDE	The keyword by itself specifies that all attributes, regardless of value, are to be excluded from the packet.
EXCLUDE *attribute*	The rule specifies that this attribute will be excluded from the packet, regardless of its value.
EXCLUDE *attribute value*	The rule specifies an attribute/value pair to exclude from the packet.
ADD *attribute value*	The rule lists a specific attribute/value pair to add to the packet. The attribute will be added after all other rules are processed.
REPLACE *attr1* WITH *attr2*	The rule specifies that any occurrence of *attr1* will be replaced by *attr2*, which will keep *attr1*'s value.
REPLACE *attr1* WITH *attr2 v2*	The rule specifies that any occurrence of *attr1* (regardless of value) will be replaced by *attr2* whose value will be set to *v2*.
REPLACE *attr1 v1* WITH *attr2*	The rule specifies that any occurrence of *attr1* whose value is *v1* will be replaced by *attr2* (which keeps value *v1*).
REPLACE *attr1 v1* WITH *attr2 v2*	The rule specifies that any occurrence of *attr1* whose value is *v1* will be replaced by *attr2* having a value *v2*.

An attribute will be `ADD`ed to a packet only if it is legal to do so. Some attributes may only appear once in a RADIUS packet; others may appear multiple times. Thus, if an attribute that is the subject of an `ADD` rule is already present in the packet (after processing `ALLOW` and `EXCLUDE` rules) and may only appear once, it will not be added.

The Steel-Belted Radius dictionary file `radius.dct` provides string aliases for certain integer values defined in the RADIUS standard. You are free to use these strings in attribute filter rules.

WARNING: You can set up filter rules in any way you wish. While this provides you with tremendous flexibility, it also means that Steel-Belted Radius does not prevent you from creating an invalid RADIUS packet. Some attributes are not appropriate for certain types of requests. For example, adding a pooled `Framed-Ip-Address` *to an accounting request could cause a loss of available ip addresses*.

Order of Filter Rules

The order of rules is important. General default rules that take no parameters, such as `ALLOW` (allow all attributes unless otherwise specified) or `EXCLUDE` (exclude all attributes unless otherwise specified) must appear as the first rule in the filter. Later rules may supersede earlier rules; the last applicable rule “wins.” `ADD` rules are applied after the `ALLOW` and `EXCLUDE` rules.

More specific rules with more parameters (`ADD` ***`attribute value`***) act as exceptions to less specific rules with fewer parameters (`ALLOW` ***`attribute`***, `EXCLUDE`). For example, you might want to `ALLOW` a certain attribute and `EXCLUDE` one or more specific values for that attribute. Or you might `EXCLUDE` all attributes, `ALLOW` specific attributes, and `ADD` specific attribute/value pairs.

There are two basic approaches to designing a filter:

- Start the rule list with a default `EXCLUDE` rule (no parameters) and add `ALLOW` rules for any attributes or attribute/value pairs that you want to insert into the packet. `ADD` and REPLACE rules may also be used.
- Start the rule list with a default `ALLOW` rule (no parameters) and add `EXCLUDE` rules for any attributes or attribute/value pairs that you want to remove from the packet. `ADD` and REPLACE rules may also be used.

Values in Filter Rules

The value of an attribute is interpreted based on the type of the attribute.

Attribute Type	Meaning
hexadecimal	A hexadecimal value is specified just as a string. Special characters may be included using escape codes.
int1, int2, int4, integer	1-, 2- or 4-byte decimal number (integer is equivalent to int4). *NOTE: The Steel-Belted Radius dictionary file* `radius.dct` *provides string aliases for certain integer values defined in the RADIUS standard. You are free to use these strings in attribute filter rules*.
ipaddr, ipaddr-pool	An IP address in dotted notation; for example: `EXCLUDE NAS-IP-Address 127.0.0.1`

Attribute Type	Meaning
ipxaddr-pool	A sequence of hex digits; for example: `ALLOW Framed-IPX-Network 0042A36B`

string	String attribute (includes null terminator). A string is specified as text. The text may be enclosed in double-quotes (“”). The text is interpreted as a regular expression. Backslash (‘\’) is the escape character. Escape codes are interpreted as follows:
	Code **Meaning**
	\a 7
	\b 8
	\f 12
	\n 10
	\r 13
	\t 9
	\v 11
	nnn *nnn* is a decimal value between 0 and 255
	\x*nn* *nn* is a hexadecimal value between 00 and FF
	c *c* is a single character, interpreted literally
	A literal backslash (‘\’) within a string as well as double-quotes (") within quoted strings should be prefixed with an escape character. For example:
	`ADD Reply-Message Session limit is one hour`
	`ADD Reply-Message "Session limit is one hour"`
	`ADD Reply-Message "Your user name is \"George\""`

time	A time value is specified with a string indicating date and time: *yyyy/mm/dd hh:mm:ss* The date portion is mandatory; the time portion may be specified to whatever degree of precision is required, or may be omitted entirely. For example: 1999/10/3 14:00:00 and 1999/10/3 14 both refer to October 10, 1999 at 2:00 p.m. For example: `ADD Ascend-PW-Expiration 2001/1/1`

Referencing Attribute Filters

Steel-Belted Radius attribute filtering offers total flexibility. You can use the same filter for all packets in all realms. You can apply filtering to some realms, and not others (to disable filtering for a realm, omit filtering parameters from the ttlsauth.aut file). Often, you will use filtering only for packets that are routed “out” to realms (the FilterOut parameter).

In order to reference the filtering rules defined in the filter.ini file, you must use the FilterOut and FilterIn parameters in the [Auth] and [Acct] sections of a RADIUS realm configuration file.

The full syntax used is:

```
[Auth]
FilterIn=name1
FilterOut=name2

[Acct]
FilterIn=name3
FilterOut=name4
```

where *name1*, *name2*, and so forth provide the names of filters, sections in the filter.ini file called [*name1*], [*name2*], and so forth. The *name* values in this syntax are completely independent of each other. They may be all the same, all different, or some combination of same and different.

WARNING: If a [name] section is not found in the filter.ini file, it will be equivalent to assigning a filter that EXCLUDEs all attributes. In other words, assigning a filter name that cannot be found causes the final packet to be emptied of all attributes.

WARNING: In accounting filters, you should not allocate IP addresses from Steel-Belted Radius IP address pools, as these addresses will never be released.

radius.ini File

The radius.ini initialization file is the main configuration file that determines the operation of the Steel-Belted Radius server. It contains information that controls a variety of server functions, primarily authentication.

WARNING: Use caution when editing radius.ini*, so that values pertaining to one feature are not overwritten or lost while you configure another feature. It is a good idea to make a backup copy of* radius.ini *before you start editing it.*

radius.ini [Addresses] Section

If you are using a server that has more than one network interface (a multi-homed server), you may need to guarantee which interfaces are bound and which are ignored by naming them explicitly. In order to do this, you will need to add an [Addresses] section to the radius.ini file.

You will have to choose whether you want all of your proxy traffic routed through one interface, or if you want to dedicate interfaces to particular realms.

See "proxy.ini [Interfaces] Section" on page 172 if you wish to configure your system to route proxy realms through specific interfaces.

To route all of your proxy traffic through a single interface, set the value for `ProxySource` (in the [Configuration] section of radius.ini) to the appropriate IP address(es) (which must have been listed in the [Addresses] section).

For example:

```
[Addresses]
192.10.20.30
192.10.20.31

[Configuration]
ProxySource = 192.10.20.30
```

WARNING: Setting the ProxySource value will override proxy routing on a realm-by-realm basis.

radius.ini [Configuration] Section

The [Configuration] section of radius.ini contains parameters that control the most basic behavior of the Steel-Belted Radius server. The following fields may be present:

radius.ini [Configuration] Field	
Allow-Unmasked-Password	If set to `Yes`, it will be possible through the Administrator program to view previously entered passwords (provided they are not strongly encrypted). If set to `No` (the default), it will be possible to unmask passwords as you enter them, but not to view passwords that have already been entered.
Allow-Unmasked-Secret	If set to `Yes`, it will be possible through the Administrator program to view previously entered shared secrets. If set to `No` (the default), it will be possible to unmask shared secrets as you enter them, but not to view shared secrets that have already been entered.
Apply-Login-Limits	If set to `Yes` (the default), then the maximum number of concurrent connections for each user will be enforced, and connection attempts above the limit will be rejected. If set to No, then connections above the limit will be allowed, but an event will be noted in the authentication log file.

radius.ini [Configuration] Field	
AuthenticateOnly	If set to 1, no response attributes will be included in the response packet to an AuthenticateOnly (Service-Type 8) request. If set to 0, the normal response attributes will be included in the response. The default is 1.
CheckMessageAuthenticator	If set to 1, the validation of received Message-Authenticator attributes is enabled. The default is 0. The validation of Message-Authenticator can occur either on receipt of an Access-Request from a NAS device or on receipt of an Access-Request, Access-Reject, or Access-Challenge from a proxy (extended proxy only). *NOTE: validation does not occur for ordinary proxy*.
FramedIPAddressHint	If set to `Yes`, the attribute Framed-IP-Address will be treated as a hint. If this attribute appears in the Access-Request and the user's return list is configured to allocate Framed-IP-Address from a pool, the IP address in the Access-Request is returned instead of a newly-allocated IP Address. See “Hints” on page 44.
LogDir	Sets the destination directory where authentication log files will be stored. The default is the RADIUS database private directory.
LogLevel	Sets the rate at which Steel-Belted Radius will write entries to the activity log file (.LOG). The LogLevel may be the number 0, 1, or 2 -- where 0 is the production logging level, 1 is the informational logging level, and 2 is the debug logging level.
LogAccept	Specifies whether or not messages associated with Accepts that meet the current LogLevel should be recorded in the log file. It is set to 1 (on) by default.
LogReject	Specifies whether or not messages associated with Rejects that meet the current LogLevel should be recorded in the log file. It is set to 1 (on) by default.
PhantomTimeout	The maximum number of seconds that a phantom accounting record will remain active. As soon as the corresponding start packet is received, a phantom record will be discarded. If a phantom record still exists at the end of its timeout period, it will be discarded then. See “Phantom Records” on page 48.

radius.ini [Configuration] Field	
PrivateDir	Name of the location of the Steel-Belted Radius server directory; the server directory contains the database and dictionary files (if not specified, defaults to the same directory where the Steel-Belted Radius service/daemon resides).
ProxySource	The IP address listed in the [Addresses] section corresponding to the interface through which all outgoing proxy traffic will be routed.
ProxyStripRealm	This setting controls whether the proxy realm decoration is stripped before sending the request downstream. If set to 0, no realm name stripping will be performed. The default is 1.
TraceLevel	The RADIUS packet tracing level between 0 and 2, where 0 indicates the default action of no packet tracing, 1 indicates that the parsed contents of packets is to be logged and 2 indicates that the raw contents of the packet is to be logged. Packet traces are written to the log file and can be a useful tool for troubleshooting interoperability problems.
TreatAddressPoolsAsDisjoint	If set to 1, then Steel-Belted Radius treats each IP address pool as though it operates off its own disjoint address space. Thus, this disables the normal checks to ensure that an IP address is only allocated to a single address pool. The default is 0, so that a single IP address can only be allocated to a single session and a single IP address pool. *NOTE: Due to the requirements of resource management, Steel-Belted Radius uses the Class attribute to track IP addresses. This attribute contains the IP pool name and IP address.*
UseNewAttributeMerge	If set to 1, the new profile and user attribute merging calculation is performed. If set to 0, the older calculation technique is used. *See “Resolving Profile and User Attributes” on page 38 for explanation of new attribute merge*. Default is 1 (enabled).

radius.ini [CurrentSessions] Section

The [CurrentSessions] section of radius.ini controls the Current Sessions List. The following field may be present:

radius.ini[CurrentSessions] Field	Meaning
CaseSensitiveUsernameCompare	If set to 1 (the default), when the server searches its Current Sessions List for sessions that have the same username, it will use case-sensitive look-ups. If 0, it will ignore case.

radius.ini [Debug] Section

The [Debug] section of radius.ini enables you to troubleshoot RADIUS problems in which the log files must be immediately written to disk instead of cached. The following field may be present:

radius.ini[Debug] Field	Meaning
Log-Flush-Time	Specified in milliseconds, at 500ms increments. If set to 0, log messages are written to disk immediately; otherwise, they are cached at least until a background worker thread takes control. For example, if set to 1000, log messages will be cached for at most 1 second. The default value is 4000ms (4 seconds).

WARNING: Do not change the settings in this file unless you are working with technical support on debugging a problem with your server. Changing debug status will have serious repercussions on the operation of your server, and you should restore debug settings to normal as soon as possible.

radius.ini [FailedAuthOriginStats] Section (Windows only)

The [FailedAuthOriginStats] section of radius.ini enables you to identify when a specific NAS is associated with certain Windows NT Performance Monitor (perfmon) counters. This in turn helps you to identify a specific region of your network that may be having difficulties. The syntax is as follows:

```
[FailedAuthOriginStats]
RADIUSclient=IDnumber
RADIUSclient=IDnumber
.
.
.
```

Where *RADIUSclient* is the name of a NAS or other client device as defined in the RAS Clients dialog, and *IDnumber* is a number in the range 1 to 16. These numbers map to the following Steel-Belted Radius perfmon counters:

```
Failed Auths - 1
Failed Auths - 2
.
.
.
Failed Auths - 16
```

For example, if you map a NAS named herman to the number 3:

```
[FailedAuthOriginStats]
herman=3
```

Then the perfmon counter Failed Auths - 3 will tell you the number of failed authentication requests that have originated from NAS herman.

See "Windows NT Performance Monitor" on page 112.

radius.ini [IPPoolSuffixes] Section

The [IPPoolSuffixes] section of radius.ini allows you to define suffixes that can be used to split the NAS-Specific IP Address Pools into smaller subcategories.

See "NAS-Specific IP Address Pools" on page 78.

The syntax is as follows:

```
[IPPoolSuffixes]
Suffix1
Suffix2
...
```

For example, to create three categories that append -Bronze, -Silver, and -Gold to IP Address Pool names, this section would be defined as follows:

```
[IPPoolSuffixes]
-Bronze
-Silver
-Gold
```

radius.ini [Ports] Section

The [Ports] section of radius.ini provides an alternative method for setting the UDP ports used by Steel-Belted Radius. The following fields may be present:

radius.ini [Ports] Field	Meaning
UDPAuthPort	The UDP port(s) used for authentication (one line per port assignment).
UDPAcctPort	The UDP port(s) used for accounting (one line per port assignment).

For example:

```
[Ports]
UDPAuthPort = 1645
UDPAuthPort = 1812
UDPAcctPort = 1646
UDPAcctPort = 1813
```

WARNING: Be careful when configuring these settings and consider the impact on the /services *file.*

See “services File” on page 158.

Listening on Multiple UDP Ports

The following explains how the server determines which ports to listen on for incoming authentication requests (the logic for accounting requests works in the same manner):

1 If one or more UDPAuthPort settings are present in the [Ports] section of the radius.ini, the collection of unique port numbers specified in this section represents the sum total of the ports the server will listen on for authentication requests.

A limit is imposed on the maximum number of ports that can be specified: the number of ports to listen on multiplied by the number of interfaces on the local host cannot exceed an operating-system-specific number. The total number of ports available on **Windows** computers is 64 and on **Unix** computers is 4096, but some of these ports will already be in use by other services before Steel-Belted Radius begins. If this limit is exceeded, the RADIUS authentication subcomponent will fail to initialize.

2 If no UDPAuthPort settings are present in the [Ports] section, the server will attempt to read the port number associated with the `radius` service specified in /etc/services. If present, the server will listen on this port number.

Only a single port can be specified in the services file. If multiple ports are required, they will need to be specified in the radius.ini file.

3 If no UDPAuthPort settings are present in the [Ports] section and no `radius` service is listed in the `/etc/services` file, the server will listen for authentication requests on the default UDP ports 1645 and 1812.

The UDPAcctPort setting performs the same purposes for purposes of accounting, and the above information is relevant in the same way. The name of the service to look for in `/etc/services` is `radacct` and the fallback UDP ports are 1646 and 1813.

NOTE: Any failure to bind to one of the selected UDP ports will also cause the affected subcomponent (authentication or accounting) to fail to initialize.

radius.ini [Self] Section

The [Self] section of radius.ini lists all the realm names that indicate this Steel-Belted Radius server. The syntax is as follows:

```
[Self]
RealmName
RealmName
.
.
.
```

You can use the [Self] section to map a realm name to the Steel-Belted Radius server. This way, if you acquire a batch of new user accounts, users don’t have to change anything about the way they enter usernames. They can enter the name *`User<Delimiter>RealmName`* or *`RealmName<Delimiter>User`* as usual.

When a username comes into Steel-Belted Radius, if the [Self] section lists *`RealmName`*, Steel-Belted Radius will understand that it is the target, and will handle the request locally, rather than directing the request somewhere else.

radius.ini [Strip] Section

The [Strip] section specifies if, and how, User-Name stripping is to occur. That is, these sections configure Steel-Belted Radius to manipulate the username by stripping the incoming `User-Name` attribute value of realm names and other “decorations.”

The [Strip] section (and accompanying [StripPrefix] and [StripSuffix] sections) look like the following:

```
[Strip]
Authentication=Yes
Accounting=No
```

```
StripPrefixCharacters=@#%
StripSuffixCharacters="! "

[StripPrefix]
PrefixStringToStrip1
PrefixStringToStrip2
.
.
.
[StripSuffix]
SuffixStringToStrip1
SuffixStringToStrip2
.
.
.
```

The meaning of the [Strip] fields are as follows:

radius.ini **[Strip] fields**	**Meaning**
Authentication	If set to YES, then the [StripPrefix] and [StripSuffix] rules are used to strip the username before further processing of an authentication request. The default is NO.
Accounting	If set to YES, then the [StripPrefix] and [StripSuffix] rules are used to strip the username before further processing of an accounting request. The default is NO.
Proxy	Reserved for future use.
StripPrefixCharacters	A list of ASCII characters to strip from the prefix. If a space character appears in the list, the entire list must be surrounded by quotation marks.
StripSuffixCharacters	A list of ASCII characters to strip from the suffix. If a space character appears in the list, the entire list must be surrounded by quotation marks.

Strip Characters (Example)

Take the following [Strip] section as an example:

```
[Strip]
Authentication=yes
Accounting=yes
Proxy=no
StripPrefixCharacters = @#%
StripSuffixCharacters = " !"
```

If the incoming username is "`@@@testuser   !`", then the string is processed and converted to "`testuser`".

Strip Prefix and Suffix

The [StripPrefix] section should give a list of any prefixes that should be removed from the beginning of usernames, including the delimiter.

The [StripSuffix] section should give a list of any prefixes that should be removed from the beginning of usernames, including the delimiter.

For example:

```
[Strip]
Authentication=yes
Accounting=yes
Proxy=no

[StripPrefix]
(isp.com\)
(att.net])

[StripSuffix]
(@myrealm.com)
(@yahoo.com)
```

In this example, any usernames containing the prefixes `isp.com\` or `att.net]` in authentication and accounting requests will have them stripped off. Similarly, any usernames containing the suffixes `@myrealm.com` or `@yahoo.com` in authentication or accounting requests will have them stripped off.

NOTE: The [Strip] name processing does not apply to the LDAP plug-in.

radius.ini [ValidateAuth] and [ValidateAcct] Sections

The [Validate] sections in radius.ini allow username validation to occur. These sections enable Steel-Belted Radius to examine the User-Name attribute in the incoming packet to determine whether it employs a valid character set, and to act accordingly. The following [Validate] sections are available:

```
[ValidateAuth]
User-Name = RegularExpression

[ValidateAcct]
User-Name = RegularExpression
```

The following fields may be present:

radius.ini [Validate] Field	Meaning
[ValidateAuth]	This section applies only to authentication servers.
[ValidateAcct]	This section applies only to accounting servers.
User-Name	Names the regular expression against which the User-Name attribute will be validated. If the User-Name entry is absent from the section or the regular expression is blank, no validation occurs.
RegularExpression	The regular expression lists each valid character or range of characters. A dash (‘-’) indicates a range of alphanumeric characters. For example, A-Z indicates every uppercase alphabetic character. A backslash (‘\’) followed by a non-alphanumeric character indicates that character literally, for example \? indicates the question mark. ‘\’ is also used as an escape character, as follows: \a bell (7) \b backspace (8) \t tab (0x09) \n newline (10) \v vertical tab (11) \f formfeed (12) \r return (13) \x*nn* hex value, where *nn* are 2 hex digits *nnn* decimal value, where *nnn* are 3 decimal digits

The following example indicates a string composed only of upper- and lower-case characters, digits, periods and commas:

```
User-Name = A-Za-z0-9.,
```

The following example permits upper- and lower-case characters only:

```
User-Name = A-Za-z0-9
```

vendor.ini File

The vendor.ini initialization file contains information that allows Steel-Belted Radius to work with the products of other vendors.

vendor.ini [Vendor-Product Identification] Section

The [Vendor-Product Identification] section of vendor.ini identifies and provides information about the network access servers that can be used with Steel-Belted Radius. For each make/model of vendor product, the following fields may be present:

vendor.ini [Vendor-Product Identification] Field	Meaning
Vendor-Product	This required field specifies the name of the product. A product name must be unique, cannot include blanks and must consist of 31 or fewer characters. These product names are used only in the **Make/model** pull-down list in the RAS Clients dialog. This list is used when adding a new client or when selecting a vendor-specific attribute.
Dictionary	This required field specifies the dictionary file to use for this product. The dictionary file must be located in the same directory as the Steel-Belted Radius daemon or service (usually C:\RADIUS\service). You do not need to specify a extension on the dictionary name; Steel-Belted Radius automatically attaches an extension of .DCT to the dictionary names listed in this field. *See "Dictionary Files" on page 151*..
Send-Class-Attribute	If set to No, the Class attribute will not be sent to the client on Access-Accept. (This feature is designed to accommodate devices that don't handle this attribute properly.) The default is Yes.
Ignore-Acct-Ss	If set to Yes, the digital signature of accounting packets based on the shared secret is ignored. This is to accommodate devices that don't properly sign accounting packages. The default is No.
Send-Session-Timeout-on-Challenge	If set to Yes, the Session-Timeout attribute will be sent to the client on Access-Challenge responses that include EAP messages. This attribute advises a NAS on how long it should wait for a user response to the challenge. The default is No.
Ignore-Ports	This field determines whether Steel-Belted Radius may infer that one user has logged off if the port that was in use is now being used by another user. If set to No, then such an inference will be made and the previous user will be removed from the Active Users list. If set to Yes, then no such inference will be made and both users will be deemed active. The default is No.

vendor.ini [Vendor-Product Identification] Field	Meaning
Discard-After	Used for inbound Proxy RADIUS servers that send username information in a “decorated” format. For example, if a Proxy RADIUS server sends usernames of the form `username@company`, then specifying ‘@’ will result in all text after the @ delimiter character being discarded for authentication purposes; the string `username` will be used.
Discard-Before	Same as discard-after, except the name is on the right of the delimiter character and discardable information is on the left.
Max-EAP-Fragment	You can specify the size of the maximum EAP-Message in the ttlsauth.aut and tlsauth.eap files. The maximum fragment length defaults to 1020. This is inefficient, however, as the fragment length will need to be set to a number low enough to work with all of a customer's Access Points. This setting allows specifying a maximum EAP fragment length on a make/model basis. The maximum EAP fragment length emitted by TLS or TTLS will be the lesser of the maximum specified in their .eap/.aut files and this setting.

vendor.ini Product-Scan Settings

After you define a Vendor-Product entry in vendor.ini, the name of this entry can be selected in the RAS Clients dialog as a possible value for the Make/model field. The Product-Scan-Auth and Product-Scan-Acct settings can be used within a Vendor-Product entry to permit dynamic make/model selection to occur. That is, these settings enable Steel-Belted Radius to examine the incoming packet to determine the make/model of the NAS device that originated the packet.

A dynamic Vendor-Product entry might appear as follows:

```
Vendor-Product = DeviceNameInRASClientsList
Product-Scan-Auth = MakeModelSelect
Product-Scan-Acct = MakeModelForAccounting

[MakeModelForAuthentication]
Product = String
Product = String
.
.
.
Product =

[MakeModelForAccounting]
Product = String
Product = String
.
.
.
Product =
```

The meaning of these fields is as follows:

vendor.ini **Product-Scan Field**	**Meaning**
Vendor-Product	This setting creates a label which will appear as a selection in the Steel-Belted Radius Administrator program, RAS Clients dialog, **Make/model** drop-down list.

Dictionary Files

For each product listed in the vendor.ini file, Steel-Belted Radius provides a dictionary file (.dct). Dictionary files enable Steel-Belted Radius to exchange attributes with RADIUS clients of that product type. A dictionary file provides the information that the server needs:

- When receiving RADIUS requests, to know which attributes it should expect to receive from devices of a certain product type.
- When composing a RADIUS response, to include the specific reply attributes required by devices of that product type.

Windows

Dictionary files must be placed in the same directory as the Steel-Belted Radius service (usually C:\RADIUS\Service). While starting up, Steel-Belted Radius scans its home directory for all files with an extension of .dct (regular dictionary files) or .dci (import dictionary files) and concatenates them into a single dictionary.

Unix

Dictionary files must be placed in the same directory as the Steel-Belted Radius daemon. During initialization, Steel-Belted Radius reads the file dictiona.dcm in the server directory to get a list of files with an extension of .dct (regular dictionary files) or .dci (import dictionary files) and concatenates them into a single dictionary.

Dictionary File Records

Records in a dictionary file must begin with one of the following keywords. Each keyword is described in detail below.

Keyword	Meaning
@	Include the referenced file
ATTRIBUTE	Define a new attribute
VALUE	Define a named integer value for an attribute
MACRO	Define a macro used to simplify repetitive definitions
OPTIONS	Define options beyond the scope of attribute definitions
#	Ignore this text (comment)

Editing Dictionary Files

The product-specific files shipped with Steel-Belted Radius already reflect specific vendors' implementations of RADIUS clients. Therefore, you will not usually need to modify the dictionary files shipped with Steel-Belted Radius. However, if you are in communication with your NAS vendor about a new product, a new attribute, or a new value for an attribute, you can add this information to your existing Steel-Belted Radius configuration by editing dictionary files - with care, and using the instructions in this section.

In either case, whether you edit an existing dictionary file or create a new one, you must do the following before your changes will be fully integrated into Steel-Belted Radius:

1 Add a new vendor-product entry to vendor.ini so that you can reference the new dictionary while configuring Steel-Belted Radius.

See "vendor.ini File" on page 148.

2 Place your dictionary file in the same directory as the Steel-Belted Radius service (usually `C:\RADIUS\Service`) or daemon.

3 Edit the `dictiona.dcm` file so that it includes your new dictionary file, and stop and restart the server.

4 Stop and restart the server.

Include Records

Records in a dictionary file that begin with the '@' character are treated as special include records. The string that immediately follows the '@' character identifies the name of a dictionary file whose contents are to be included. For example, the entry `@vendorA.dct` would include all of the entries in the file vendorA.dct.

Include records are only honored one level deep. If, for example, file vendorA.dct specifies an inclusion of file radbase.dct that, in turn, includes radacct.dct, vendorA.dct will be considered to include all records in radbase.dct, but not those in radacct.dct.

Master Dictionary File

The master dictionary dictiona.dcm consists of include records that reference the various vendor-specific dictionaries. The order in which the vendor-specific dictionaries are included in the master dictionary has significance only if there are two vendor-specific dictionaries that contain conflicting definitions for the same attribute or attribute value.

As with standard dictionary file processing, the earlier definition of the attribute or attribute value takes precedence over any later definitions of the same attribute or attribute value. For example:

```
@vendorA.dct
@vendorB.dct
@vendorC.dct
@vendorD.dct
```

One limitation of standard dictionary files (that the `attrib_id` of all the attribute records must be unique) is waived for the master dictionary file. Multiple vendors may well define different attribute names for the same attribute identifier (assuming the attribute identifier is not already used in the base RADIUS specification). Since attributes in the Steel-Belted Radius database are stored by name (rather than by `attrib_id`), the waiver of this rule introduces no ambiguity into the database.

Import Dictionary Files

Import dictionary files (.dci) are special dictionary files that are only used when importing user data from the users text file supported by UNIX implementations of RADIUS.

See “Importing from Other File Formats” on page 93.

The purpose of the import dictionary files is to map the names of attributes commonly used in these implementations to those that are in use in Steel-Belted Radius.

When the Administrator program is used to import user data from an external text file, the pull-down that requests information about the type of the text file contains the list of all import dictionary files for which a standard dictionary file by the same name is present. Importing the user data from the text file causes the import dictionary to be used to translate the attribute names to attribute IDs and the standard dictionary to convert the attribute IDs back to attribute names.

The expected format of records in the import dictionary files is identical to that of records in standard dictionaries.

ATTRIBUTE Records

Attribute records define new attributes and conform to the following syntax:

```
ATTRIBUTE  attrib_name  attrib_id  syntax_type  flags
```

where the parameters have meaning as follows:

Parameter	Meaning
attrib_name	Name of the attribute (up to 31 characters with no embedded blanks)
attrib_id	Integer in the range 0 to 255 identifying the attribute's encoded identifier
syntax_type	Syntax type of the attribute.
flags	Defines whether an attribute appears in the Check-List, the Return-List (or both), whether it is multi-valued and whether it is orderable.

The following example illustrates a typical attribute record:

```
ATTRIBUTE    Framed-IP-Netmask     9     ipaddr    Cr
```

This attribute record specifies all of the following:

- An attribute named Framed-IP-Netmask is supported.
- Its encoded identifier is 9.
- It must use the syntax of an IP address.
- It can appear multiple times in a Check-List and at most one time in a Return-List for User or Profile entries in the Steel-Belted Radius database.

Attribute Name and Identifier

No two attribute records in a single dictionary file should have the same `attrib_name` or `attrib_id`. If a duplicate `attrib_name` or `attrib_id` is encountered, the later definition of the attribute is ignored in favor of the earlier one (the earlier one is considered to be an override).

Syntax Type Identifier

The supported standard `syntax_type` identifiers are:

Syntax Type	Meaning
hexadecimal	Hexadecimal string
hex1, hex2, hex4	1-, 2- or 4-byte hexadecimal number
int1, int2, int4, integer	1-, 2- or 4-byte decimal number (integer is equivalent to int4)
ipaddr	IP address or IP netmask attribute
ipaddr-pool	IP address selected from an IP address pool
ipxaddr-pool	IPX network number selected from an IPX address pool
string	String attribute (includes null terminator)
stringnz	String attribute (without null terminator)
time	Time attribute (number of seconds since 00:00:00 GMT, 1/1/1970)

Compound Syntax Types

In addition to the standard `syntax_type` identifiers listed above, the dictionary can accommodate compound syntax types for use in defining vendor-specific attributes. Instead of a single `syntax_type` identifier, one or more of the following options can be combined inside square brackets to form a compound syntax type:

Option	Meaning
vid=*nnn*	The device manufacturer's SMI Network Management Private Enterprise code (assigned by ISO) in decimal form.
type*N*=*nnn*	Type field for vendor-specific attribute as defined in the RADIUS specification; *N* specifies the length of the field (in bytes), *nnn* specifies the decimal value of the field.
len*N*=*nnn*	Length field for vendor-specific attribute as defined in the RADIUS specification; *N* specifies the length of the field (in bytes), *nnn* specifies the decimal value of the field (a plus sign prior to the value indicates that the length of the data portion is to be added to *nnn* to obtain the actual length).
data=*syntax_type*	The actual data to be included in the attribute; the syntax can be any of the standard syntax types.
tag=*nnn*	Tunnel attributes include a tag field, which may be used to group attributes in the same packet which refer to the same tunnel. Since some vendors' equipment does not support tags, this syntax type is optional and must be present in order for the attribute to include a tag field. A value of 0 indicates that the field should be present but ignored.

An example of a vendor-specific attribute definition follows:

```
ATTRIBUTE vsa-xxx 26 [vid=1234 type1=1 len1=+2 data=string] R
```

Flag Characters

The `flags` field consists of the concatenation of one or more characters from the following list:

Flag Character	Meaning
b *or* B	Indicates that an attribute may be bundled in a single Vendor-Specific-Attribute for a particular vendor id. That is, it may be included as one of a series of subattributes within a single VSA.
c	Attribute can appear a single time within a User or Profile Check-List.
C	Attribute can appear multiple times within a User or Profile Check-List.
r	Attribute can appear a single time within a User or Profile Return-List.
R	Attribute can appear multiple times within a User or Profile Return-List.
t	Attribute can appear a single time within a Tunnel attribute list.
T	Attribute can appear multiple times within a Tunnel attribute list.
o *or* O	Attribute is orderable; the administrator can control the order in which such attributes are stored in the Steel-Belted Radius database (this flag only makes sense for multi-valued attributes).

VALUE Records

Value records are used to define names for specific integer values of previously defined integer attributes. Value records are never required, but are appropriate where specific meaning can be attached to an integer value of an attribute. The value record must conform to the following syntax:

```
VALUE  attrib_name  value_name  integer_value
```

where the parameters have meaning as follows:

Parameter	Meaning
attrib_name	Name of the attribute (up to 31 characters with no embedded blanks)
value_name	Name of the attribute value (up to 31 characters with no embedded blanks)
integer_value	Integer value associated with the attribute value

No two value records in a dictionary file should have the same `attrib_name` and `value_name` or the same `attrib_name` and `integer_value`. If a duplicate is encountered, the later definition of the attribute value is ignored in favor of the earlier one (the earlier one is considered to be an override).

The following example illustrates the use of the VALUE record to define more user-friendly attribute values for the Framed-Protocol attribute:

```
ATTRIBUTE  Framed-Protocol     7     integer     Cr
VALUE      Framed-Protocol     PPP           1
VALUE      Framed-Protocol     SLIP          2
```

Using these dictionary records, the administrator need not remember that the integer value 1 means PPP and the integer value 2 means SLIP when used in conjunction with the Framed-Protocol attribute. Instead, the Steel-Belted Radius Administrator program will allow you to choose from a list of attribute values including PPP and SLIP.

MACRO Records

Macro records are used to streamline the creation of multiple vendor-specific attributes that include many common parameters. A macro record can be used to encapsulate the common parts of the record. The macro record must conform to the following syntax:

MACRO *macro_name*(*macro_vars*) *subst_string*

where the parameters have meaning as follows:

Parameter	Meaning
macro_name	Name of the macro
macro_vars	One or more comma-delimited macro variable names
subst_string	String into which macro variables are to be substituted; any sequence of characters conforming to the format %*x*% for which a macro variable called *x* has been defined will undergo the substitution process

The following example illustrates the use of a macro that simplifies the specification of multiple vendor-specific attributes:

```
MACRO Cisco-VSA(t, s) 26 [vid=9 type1=%t% len1=+2 data=%s%]
ATTRIBUTE   Cisco-xxx   Cisco-VSA(1, string)    R
ATTRIBUTE   Cisco-yyy   Cisco-VSA(4, int4)      C
ATTRIBUTE   Cisco-zzz   Cisco-VSA(9, ipaddr)    r
```

Using the macro preprocessor built into the Steel-Belted Radius dictionary processing, the records in the example above would be translated to the following records before being further processed.

```
ATTRIBUTE Cisco-xxx 26 [vid=9 type1=1 len1=+2 data=string] R
ATTRIBUTE Cisco-yyy 26 [vid=9 type1=4 len1=+2 data=int4]   C
ATTRIBUTE Cisco-zzz 26 [vid=9 type1=9 len1=+2 data=ipaddr] r
```

OPTION Records

By default, each vendor-specific attribute is encoded in a single VSA record. The format of a VSA record is as follows:

Bits	Field
0 - 7	Type: contains the value 26.
8 - 16	Length of data in bytes.
17 - 47	Vendor ID
48 - on	Vendor data

If you provide a parameter to the OPTION setting, however, multiple vendor-specific attributes can be present in the vendor-data portion of a single VSA record.

The OPTION record must conform to the following format:

```
OPTION bundle-vendor-id = vid
```

IMPORTANT: You must also set the B flag in order for attribute bundling to happen. That is, in order for a particular vendor-specific attribute to be bundled, you must both set the OPTION record for the vendor's vendor-ID and set the B (or b) flag for the specific attribute.

The Nortel Rapport dictionary supports this option, for example. If you want to combine Nortel's vendor-specific attributes in a single VSA, you would provide the entry:

```
OPTION bundle-vendor-id=562
```

This is because 562 is Nortel's Vendor ID, as set in the MACRO record. The Nortel Rapport vendor-specific attributes now would be concatenated within the vendor-data portion of a RADIUS VSA attribute (up to 249 octets).

services File

Steel-Belted Radius reads the services file at startup. Among the items of information in the services file are the port assignments for RADIUS authentication and accounting services. The location of the file depends on your operating system:

- Under **Unix**: `/etc/` (may also be mapped using NIS or NIS+)
- Under **Windows**: C:\winnt\system32\drivers\etc\

The Steel-Belted Radius server uses the following default UDP ports:

- 1645 for RADIUS authentication

- 1646 for RADIUS accounting

The Steel-Belted Radius server can be configured to use any available UDP ports for authentication and accounting. You can configure new default assignments for these ports as follows:

1. Open the services file using any text editor.
2. To set the port for authentication, set the value of the `radius` parameter.
3. To set the port for accounting, set the value of the `radacct` parameter. For example:

```
radius   1812/udp  # entry for radius authentication
radacct  1813/udp  # entry for radius accounting
```

If there is no entry in the services file for `radius` or `radacct`, the Steel-Belted Radius server will use the default values (1645 and 1646, and 1812 and 1813).

NOTE: Any assignments made in the radius.ini file override the assignments made in this file.

See "radius.ini [Ports] Section" on page 144 and "RADIUS Ports" on page 25.

You can determine the ports that Steel-Belted Radius is using at any time by examining the Authentication log files *yyyymmdd*.LOG or the Accounting log files *yyyymmdd*.ACT for that time period.

Extensible Authentication Protocol

7

Concepts

Steel-Belted Radius supports Extensible Authentication Protocol (EAP), a standard for communication between clients, Access Points, NASs, and servers that provides for the future extensibility of authentication protocols.

EAP allows specialized knowledge about authentication protocols to be taken out of a NAS or Access Point so that it is merely a carrier of information between authentication server and client. This means that new types of authentication can be supported by adding the appropriate functionality to server and client, without needing to make any changes to PPP or NAS devices. When the authentication process is complete, the RADIUS server simply informs the NAS or Access Point of the result.

For technical details about EAP, see RFCs 2284 and 2869.

Support for EAP in Steel-Belted Radius has been designed to anticipate other innovative authentication types appearing on the horizon.

For a full listing of the EAP types currently supported by Steel-Belted Radius, refer to the Funk Software website.

Handling EAP Requests

The flow of RADIUS packets in an EAP scenario is quite different from the transactions using standard user credentials (e.g. PAP, CHAP). Standard user credentials involve the transmission of a RADIUS request from the NAS (or Access Point) to Steel-Belted Radius and a response (either an Accept or Reject) from the server back to the NAS (or Access Point).

With EAP, the first packet sent from the NAS (or Access Point) to Steel-Belted Radius will contain an `EAP-Message` attribute containing an EAP Identity Response. This is a signal sent by the system being authenticated that it wishes to be authenticated via EAP. It is now up to Steel-Belted Radius to select the EAP protocol with which it is to authenticate the end-user.

The contents of the `User-Name` attribute is the only guideline available to Steel-Belted Radius in selecting the appropriate EAP protocol. Should Steel-Belted Radius select an EAP protocol that is not supported by the client, the client will have the opportunity to send an EAP-NAK and to request a specific alternate protocol.

NOTE: Given this general flow, a RADIUS request with EAP credentials will have to incur a minimum of two network roundtrips between the NAS (or Access Point) and the Steel-Belted Radius before reaching a successful conclusion.

Automatic EAP Helpers

Automatic EAP helpers serve as intermediaries between EAP and traditional authentication methods. These helper modules may be configured (using an associated .eap file) to work with existing authentication methods to shield the authentication methods from the particulars of the selected EAP protocol.

The following table reveals whether each EAP type is implemented as an EAP helper or stand-alone module in Steel-Belted Radius:

EAP-Type	Implemented As
EAP-TTLS	Authentication Method Module
LEAP	Automatic EAP helper for MS-CHAP-v1
EAP Generic-Token	Authentication Method Module (SecurID)
EAP MD5-Challenge	Automatic EAP helper for CHAP

Whether or not an automatic EAP helper can be used in conjunction with a specific authentication method depends on what types of credentials the authentication method supports.

The automatic EAP helper that implements EAP MD5-Challenge generates CHAP credentials, while the helper that implements LEAP generates MS-CHAP-v1 credentials. As such, EAP MD5-Challenge can only be used with authentication methods that support CHAP, and LEAP with authentication methods that support MS-CHAP-v1.

The following table summarizes the support for MS-CHAP-v1 and CHAP in the Steel-Belted Radius authentication methods:

Auth. Method	MS-CHAP-V1	CHAP
Native	Yes	Yes
Proxy RADIUS	Yes	Yes

Authentication Request Routing

The order in which authentication methods and automatic EAP helpers are called to handle an authentication request is dependent on two factors:

1. The ordered list of enabled authentication methods (viewable in the Configuration panel of the Steel-Belted Radius administration GUI)
2. The EAP-related configuration for each of the enabled authentication methods (found in the eap.ini file).

When Steel-Belted Radius receives an authentication request that does not contain EAP credentials, it passes the request to each enabled authentication method until one of the methods claims the request.

The EAP settings in the `eap.ini` file only come into play when a request with EAP credentials is received. An authentication request contains EAP credentials if it includes one or more `EAP-Message` attributes and contains no other form of user credentials (e.g., `User-Password`).

The EAP-Only Setting

When an authentication method's `EAP-Only` setting is 1, Steel-Belted Radius will prevent the authentication method from being called for any request that does not contain EAP credentials. Under this setting, the authentication method will also be bypassed if an authentication request specifically requests an EAP protocol that is not listed in the authentication method's `EAP-Type` list in the `eap.ini` file.

The First-Handle-Via-Auto-EAP Setting

If your configuration involves clients that will be using more than one EAP protocol, the Steel-Belted Radius server must select an initial EAP protocol with which to proceed when receiving an authentication request with EAP credentials.

Selecting the incorrect EAP protocol is not fatal; the client will simply send an EAP NAK in response to the server's selected protocol and will suggest an alternate one. After one additional network roundtrip, the correct EAP protocol will then be active.

Depending on the capabilities of the authentication methods that are being used, you may, however, be able to cut out this additional network roundtrip that will affect a portion of your EAP-based authentication requests.

If an authentication method is capable of checking for the existence of a user and of retrieving the user's password information with only the use of the information available in the authentication request (e.g., the username), it is said to be *prefetch-capable*. A prefetch-capable authentication method could be consulted first to see if a user exists in its database before committing to a specific EAP protocol.

If your authentication method is prefetch-capable, you would set `First-Handle-Via-Auto-EAP` to 0, indicating that the authentication method should have the first chance to handle the request. You would also set `First-Handle-Via-Auto-EAP` to 0 if the authentication method is capable of handling EAP credentials all on its own (clearly, it would not expect an automatic helper EAP method to do work on its behalf in this case).

By configuring the authentication method to be called first, Steel-Belted Radius can delay selection of an EAP protocol until it has ascertained whether or not the user exists in a particular authentication method's database. This is a useful technique when you plan to use more than one EAP protocol, but you don't know which one the client will want. Even in this scenario, automatic EAP helpers may still end up performing the EAP protocol processing; it's just that they will take over after the authentication method has retrieved a user's password information, rather than before.

The goal of an automatic EAP helper is to generate credentials against which traditional authentication methods (ones that do not understand EAP) can operate. Once an automatic EAP helper has generated these credentials, the authentication method that triggered the use of the helper will be checked first for a password/credential match. Should this match not be present, the same traditional credentials will be passed to all remaining enabled authentication method in the master list (in the order in which they appear in the list).

Auth. Method	Prefetch Capable?
Native User	Yes

EAP-NAK Notifications

If you are supporting only one type of client or only one EAP protocol, Steel-Belted Radius will select that EAP protocol for all EAP-based authentication requests it receives. If you are planning to support multiple EAP protocols and don't intend to maintain databases that track the appropriate EAP protocol on a user-by-user basis, Steel-Belted Radius will automatically select the appropriate EAP protocol for you.

When multiple EAP protocols are in play, you should configure each authentication method you plan to use with all the EAP protocols that may be used with it. In this configuration, when Steel-Belted Radius receives an authentication request containing EAP information, it will choose the first EAP protocol listed for the first authentication method that claims the request. Should the client require a different EAP protocol, it will send back an EAP-NAK that specifies the EAP protocol it would prefer to use.

Upon receiving an EAP-NAK, Steel-Belted Radius will perform a scan of the authentication methods, in search of the first authentication method that has the requested EAP protocol listed (the authentication method may support this EAP protocol directly or with the help of an automatic EAP helper).

If the requested EAP protocol does not appear in any of the authentication methods' lists of supported EAP protocols, Steel-Belted Radius will reject the authentication request.

Reauthenticating Connections

Most Access Points understand only a limited number of attributes that may be included in a RADIUS response to signal that the user has been accepted. The `Session-Timeout` attribute is of particular significance in a WLAN realm as it instructs the Access Point how long to allow the user to remain connected to a WLAN before having to re-authenticate to the Steel-Belted Radius server.

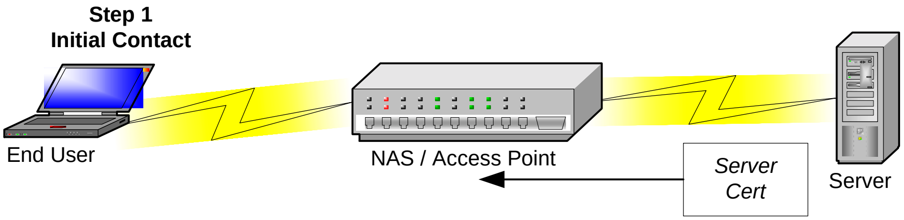
You can configure your choice of `Session-Timeout` settings using standard Steel-Belted Radius reply-list items on a user-by-user basis. If you are using EAP-TTLS to authenticate users, you can also have these modules automatically generate `Session-Timeout` attributes based on policies set in their configuration files. This level of control is necessary for EAP-TTLS as these modules also support *session resumption*, a quicker method of re-authenticating users. The value in the `Session-Timeout` attribute may need to be dynamically calculated in these cases.

NOTE: Not all Access Points support the Session-Timeout attribute. You should check your Access Points' specifications to determine whether this configuration must be performed in a fixed manner on the Access Point or if the Access Point should defer to the server.

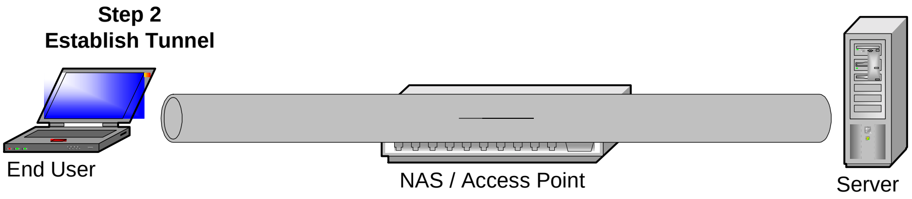
EAP Types

EAP-TTLS

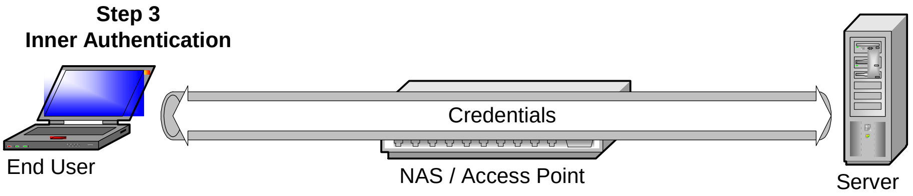
EAP-TTLS is a protocol devised by Funk Software and Certicom. It does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password; but the password credentials are transported in a securely encrypted "tunnel" established based upon the server certificates. This process is illustrated in the diagram below:



After the authentication server determines that the user has made an authentication request, it sends its certificate to the user's system.



The authentication server's certificate is used to establish a tunnel between the user and the server.



Once the tunnel is established, credentials can be exchanged safely between the server and the user since tunnels encrypt all data in a secure fashion. This stage is called *inner authentication*.

With EAP-TTLS, it is not necessary to create a new infrastructure of user certificates. User authentication is performed against the same security database that is already in use on the corporate LAN.

The routing of the inner authentication request can be handled either via standard Steel-Belted Radius authentication request routing or a directed realm. If your EAP-TTLS tunnel ends at a dedicated server and all the inner authentication requests are to be performed by other servers, you will want to use standard request routing so the proxy realm target can be determined in a standard fashion (i.e., the decoration of the username revealed by inner authentication). If your EAP-TTLS tunnel and inner authentication are handled by the same server, you can use a directed realm to specify which authentication method(s) will handle the inner authentication.

LEAP

LEAP is an EAP protocol devised by Cisco that allows a client and server to mutually authenticate each other. Each party does this by confirming that the other has the MD4 hash of the user's password.

LEAP also supports the generation of keying material for use in link layer encryption via protocols such as WEP.

EAP Generic-Token

EAP Generic-Token is an EAP protocol that is defined as part of the base EAP specification. It allows for an open-ended exchange between the owner of a security token (e.g., SecurID) and an authentication server.

EAP MD5-Challenge

EAP MD5-Challenge is an EAP protocol that is defined as part of the base EAP specification. It has security characteristics similar to those provided by CHAP credentials, except that in the case of EAP MD5-Challenge, a RADIUS server rather than a NAS generates the challenge bytes.

eap.ini File

The `eap.ini` configuration file allows you to configure what EAP authentication types will be attempted for authenticating users against the different Steel-Belted Radius authentication methods.

Each authentication method that you wish EAP authentication to be performed against must be configured within this `eap.ini` file.

This file must contain one section for each authentication method that you use. The name of the section must be the same as the filename of the authentication method's configuration file, without the `.aut` extension. Each section contains the following fields:

<Authent-Method> field	Meaning
EAP-Only	If set to 0, the authentication method will accept all types of user credentials. This field should be set to 1 if the authentication method will only be given EAP credentials or only act as a back-end server to an automatic EAP protocol method. The default is 0.

<Authent-Method> field	Meaning
EAP-Type	A comma-separated list of all the EAP protocols to support for this authentication method. The first protocol in the list is the primary protocol. Protocols that appear later in the list will only be used with this authentication method if the client responds with an EAP NAK and specifies such a protocol or if another authentication method triggers the use of the protocol but cannot complete the request. Valid values include the following: TTLS, LEAP, Generic-Token, MD5-Challenge Leave this list empty to disable EAP for this authentication method.
First-Handle-Via-Auto-EAP	If set to 1 and the user credentials are EAP, an appropriate automatic EAP helper method is called before the authentication method. The purpose of calling the automatic EAP helper method is to convert the user's EAP credentials into a format acceptable to the authentication method. If set to 0, the authentication method itself will handle the request directly, before any automatic helper methods. The default is 1.

Example:

```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
EAP-Type = TTLS, LEAP, MD5-Challenge
```

NOTE: Steel-Belted Radius comes configured with an eap.ini file that should work for all but the most complex or unusual environments. We suggest that you use this default configuration unless you find that it does not meet your needs.

Configuring For EAP-TTLS

The EAP-TTLS protocol is supported in Steel-Belted Radius via a plug-in called ttlsauth. EAP-TTLS is an authentication method and, as such, appears in the administrative GUI much as a normal authentication method would. The ttlsauth plug-in must be configured with a server certificate and the accompanying private key.

The inner authentication forwarded by the plug-in will be processed by an attribute filter that can be used to embellish the list of forwarded attributes. Any Access-Accept response may be processed by another attribute filter that can decide which attributes are forwarded on the final RADIUS Access-Accept for the EAP-TTLS exchange.

In order for EAP-TTLS to operate correctly, the [ttlsauth] section of the `eap.ini` file should set `EAP-Type` to `TTLS` and `First-Handle-Via-Auto-EAP` to 0.

ttlsauth.aut File

The EAP-TTLS plug-in is configured via the `ttlsauth.aut` file, which has three sections.

Server_Settings Section

The [Server_Settings] section allows you to configure the basic operation of the EAP-TTLS plug-in. It consists of the following fields:

ttlsauth.aut **[Server_Settings] field**	**Meaning**
Server_Certificate_Info_File	The full path of the file that will contain information about the server's certificate. This is not the location of the PKCS#12 file that contains the certificate, but rather the file that contains information about it.
TLS_Message_Fragment_Length	Set to the maximum size TLS message length that may be generated during each iteration of the TLS exchange. Anecdotal evidence suggests that some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). The default value (1020) will prevent the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame and is likely to be the safest setting. Setting a smaller value will affect the number of RADIUS challenge/response roundtrips required to conclude the TLS exchange. While a value of 1400 may result in 6 roundtrips, a value of 500 may result in 15 roundtrips. The minimum value is 500.

ttlsauth.aut [Server_Settings] field	Meaning
Return_MPPE_Keys	Setting this attribute to 1 will cause the EAP-TTLS module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is only authenticating end-users and WEP is not being used, this attribute may be set to 0. The default value is 1.
DH_Prime_Bits	Use this attribute to select the size prime that the EAP-TTLS module will use for Diffie-Hellman modular exponentiation. The larger the prime, the less susceptible the system is to certain types of attacks. The smaller the prime, the cheaper (in CPU terms) the Diffie-Hellman key agreement operation. Supported values are 768, 1024, 1536, 2048, 3072 and 4096. The default value is 1024.

Request Filters Section

Request filters affect the attributes of inner authentication requests. This section consists of the following fields:

ttlsauth.aut [Request_Filters] field	Meaning
Transfer_Outer_Attribs_to_ New	This filter only affects a new inner authentication request (rather than continuations of previous requests). If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request. If this filter is not specified, no attributes from the outer request are transferred to the inner request.
Transfer_Outer_Attribs_to_ Continue	This filter only affects a continued inner authentication request (rather than the first inner authentication request). If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request. If this filter is not specified, no attributes from the outer request are transferred to the inner request.
Edit_New	This filter only affects a new inner authentication request (rather than continuations of previous requests). If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_New above) and attributes included in the inner authentication request sent through the tunnel by the client. If this filter is not specified, the request remains unaltered.
Edit_Continue	This filter only affects a continued inner authentication request (rather than a new inner authentication request). If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_Continue above) and attributes included in the inner authentication request sent through the tunnel by the client. If this filter is not specified, the request remains unaltered.

IMPORTANT: All of the filters named in these settings must be defined in the filter.ini file.

Response Filters Section

Response filters affect the attributes in the responses returned to authentication requests. This section consists of the following fields:

ttlsauth.aut [Response_Filters] field	Meaning
Transfer_Inner_Attribs_To_Accept	This filter only affects an outer Access-Accept response that is sent back to a NAS or AP. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.
Transfer_Inner_Attribs_To_Reject	This filter only affects an outer Access-Reject response that is sent back to a NAS or AP. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.

IMPORTANT: All of the filters named in these settings must be defined in the filter.ini file.

Session _Resumption Settings

The [Session_Resumption] section allows you specify whether session resumption will be allowed and under what conditions it will be performed. It consists of the following fields:

ttlsauth.aut [Session_Resumption] field	Meaning
Session_Timeout	Set this attribute to the maximum number of seconds you want the client to remain connected to the NAS or Access Point before having to re-authenticate. If not set to 0, the lesser of this value and the remaining resumption limit (see description below) will be sent in a Session-Limit attribute to the NAS or AP on the RADIUS Access Accept response. If set to 0, no Session-Limit attribute will be generated by the plug-in. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute. The default value is 0. Setting of a value such as 600 (10 minutes) does not necessarily cause a full re-authentication to occur every 10 minutes. The resumption limit can be configured to make most re-authentications very fast and very (computationally) cheap.
Termination_Action	Set this attribute to the integer value that you want returned in a Termination-Action attribute. This is a standard attribute supported by most Access Points and determines what will happen when the session timeout has been reached. If you do not specify a value for this attribute, the plug-in will not generate such an attribute. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute. The default is not to send this attribute.
Resumption_Limit	Set this attribute to the maximum number of seconds you want the client to be able to re-authenticate using the TLS session resumption feature. This type of re-authentication is very fast and very (computationally) cheap. It does, however, depend on previous authentications and may not be considered as secure as a complete (computationally expensive) authentication. Specifying a value of 0 disables the session resumption feature. The default value is 0.

Sample ttlsauth.aut File

```
[Bootstrap]
LibraryName=ttlsauth.dll
Enable=1
InitializationString=EAP-TTLS

[Server_Settings]
; The location of a file containing information about the server's
; certificate and private key
Server_Certificate_Info_File=c:\radius\service\certInfo.ini

; Maximum TLS Message fragment length EAP-TLS will handle.
TLS_Message_Fragment_Length = 1020

; Indicates whether the EAP-TLS module should return the
; MS-MPPE-Send-Key and MS-MPPE-Recv-Key attribute upon successful
; authentication of user.
Return_MPPE_Keys = 1

; Size of the prime to use for DH modular exponentiation.
DH_Prime_Bits = 1536

[Request_Filters]
Transfer_Outer_Attribs_to_New = My_Xfer_Out_New_Filter
Transfer_Outer_Attribs_to_Continue = My_Xfer_Out_Con_Filter
Edit_New = My_Edit_New_Filter
Edit_Continue = My_Continue_Filter

[Response_Filters]
Transfer_Inner_Attribs_To_Accept = My_Xfer_Acc_Filter
Transfer_Inner_Attribs_To_Reject = My_Xfer_Rej_Filter

[Session_Resumption]
; Maximum length of time (in seconds) the NAS/AP will allow
; the session to persist before the client is asked
; to re-authenticate.
Session_Timeout = 600

; Value to return for the Termination-Action attribute sent
; sent in an accepted client.
Termination_Action = 0

; Maximum length of time (in seconds) during which an authentication
; request that seeks to resume a previous TLS session will be
; considered acceptable.
Resumption_Limit = 3600
```

In order for this to work, you must also provide the following settings in the [ttlsauth] section of the eap.ini file:

```
    First-Handle-Via-Auto-EAP = 0
    EAP-Type = TTLS
```

Server Certificate Info File

The the `Server_Certificate_Info_File` field in the `ttlsauth.aut` file provides the filepath for the server certificate information file. This is an ASCII file with a single section, [Certificate_Info]. This separate file is meant to allow the administrator to isolate it in a portion of the file system that would be accessible to the Steel-Belted Radius server process but not to general users or operators of the system.

Server Certificate Info file [Certificate_Info] field	Meaning
Certificate_And_Private_Key_File	Identifies the PKCS#12 file containing the server's certificate (chain) and private key. This should be specified as a complete file system path (though on Solaris relative paths will work as well) in order to remove any ambiguity regarding the file that is being used.
Password	Specifies the password that is necessary to retrieve the server's private key that was included in the PKCS#12 file.

Example

```
[Certificate_Info]
; Location of the PKCS#12 file containing the certificate
; and private key of the server and all certificates necessary to
; establish a chain to the Certificate Authority that issued
; the certificate.
Certificate_And_Private_Key_File = c:\radius\service\test_server.pfx

; Password with which the private key contained in the PKCS#12
; file mentioned above was encrypted.
Password = tryme
```

Technical Bulletins

8

CCA Support for 3COM

Steel-Belted Radius can support the generation of 3Com CCA tunnel attributes.

Configuration

To enable the return of the required CCA tunnel attributes, the ccagw.ini file must be modified.

The ccagw.ini file contains information about gateways, which are stored in the [*gateway*] sections. A [*gateway*] section must be present for each gateway supported.

The following table describes each field:

ccagw.ini [gateway] Field	Meaning
Address	The address of the gateway.
TunnelRefresh	The number of seconds before the tunnel will refresh. The default value is 0.
Description	A text string describing the gateway.
Secret	The shared secret between Steel-Belted Radius and this gateway device.

For example:

```
[Jupiter-Gateway]
Address = 200.47.98.142
TunnelRefresh = 3600
Description = Jersey City facility, East Coast subscribers
Secret = Holland Tunnel
```

Setting User and Profile Attributes

To enable this functionality for a particular user, the return list for the user must contain the following attributes:

```
Tunnel-Authentication
VPN-Gateway
```

Both of these attributes are defined as strings. The value of each attribute must be set to the name of the gateway used in the ccagw.ini file. For example, the return list of a user would have to include:

```
Tunnel-Authentication = Jupiter-Gateway
VPN-Gateway = Jupiter-Gateway
```

It is important to make sure that both attributes name the correct gateway. If an unknown gateway is named, the request will be rejected.

NOTE: Steel-Belted Radius is capable of returning multiple pairs of attributes for different gateways. For each gateway named in one of the attributes, a different random session key is generated.

NOTE: Please see your 3Com documentation for further details.

Ascend Filter Translation

Ascend defines two attributes — `Ascend-Data-Filter` (242) and `Ascend-Call-Filter` (243) — that contain structured binary data representing a filter to be applied to the NAS device.

Instead of entering hexadecimal strings to configure these attributes, users can configure these attributes as text strings. Steel-Belted Radius will automatically convert the text strings to the proper binary representation. The original filter attributes are still supported, and these attributes still may be configured as hexadecimal strings.

The following attributes allow configuration as text:

```
Ascend-Data-Filter-String
Ascend-Call-Filter-String
```

When Steel-Belted Radius formats a response packet, it translates the string version of the attribute to the appropriate binary value, and returns the attribute in the Access-Accept message.

Configuration

These attributes may be entered as text strings through the Administrator. The attributes may also be returned from an LDAP or SQL database during authentication.

No syntax validation is performed when the attribute is configured. The validation of syntax only occurs when the response packet is formatted. If the syntax is invalid, a reject response will be issued and an error will be logged.

NOTE: These attributes should be tested before configured on a production server.

Two types of filter are supported: “ip” and “generic”. “ipx” filters are not supported.

Syntax

In the syntax descriptions below, brackets ‘[’ ‘]’ indicate that the items enclosed are optional.

```
ip [direction] [action] [srcip address[/mask]] [dstip
address[/mask]] protocol [srcport operator port] [dstport
operator port]
```

Parameter	Values
direction	May be "in" or "out". The default is "out".
action	May be "forward" or "drop". The default is "drop".
address	An IP address in decimal dotted notation.
mask	The number of bits (decimal) in the network portion, from 0 through 32. The default is based on class of network.
protocol	The protocol number (decimal); e.g., 6 for TCP, 17 for UDP. In addition, the following protocol names will be translated to the proper number: icmp(1), tcp(6), udp(17), ospf(89).
operator	May be "=", "!=", "<", or ">".
port	The port number (decimal). In addition, the following service names will be translated to the proper port number: ftp-data(20), ftp(21), telnet(23), smpt(25), nameserver(42), domain(53), tftp(69), gopher(70), finger(79), www(80), kerberos(88), hostname(101), nntp(119), ntp(123), exec(512), login(513), cmd(514), talk(517).

Example:

```
ip out forward srcip 10.1.1.0/24 6 dstport = 80 srcport < 1023
```

NOTE: Please see your Ascend documentation for specific details about the syntax for these attributes.

Quick Reference

9

When to Stop and Restart the Server

The **least** drastic action that will cause this change to take effect is indicated by **Yes** in this table:

Item changes:	Save the dialog or file	Stop/restart the server
Access dialog or object	**Yes**	(Also works)
account.ini file	No	**Yes**
Configuration dialog or object	**Yes**	(Also works)
*.dct files	No	**Yes**
*.eap files	No	**Yes**
eap.ini file	No	**Yes**
events.ini file	No	**Yes**
Import *.rif or users file	**Yes**	(Also works)
IP Pools dialog or object	**Yes**	(Also works)
IPX Pools dialog or object	**Yes**	(Also works)
Log levels (in radius.ini file)	No	(Also works)
Profiles dialog or object	**Yes**	(Also works)
Proxy dialog or object	**Yes**	(Also works)
radius.dct file (see Notes below)	No	**Yes**
radius.ini file	No	**Yes**
RAS Clients dialog or object	**Yes**	(Also works)
Servers dialog or object	**Yes**	(Also works)
services file	No	**Yes**
TTLS	No	(Also works)
Trace levels	No	(Also works)
Tunnels dialog or object	**Yes**	(Also works)
Users dialog or object	**Yes**	(Also works)
vendor.ini file	No	**Yes**

Configuration Files by Feature

Note that some of the files listed below are specific to one operating system. These are marked with either ‘(Unix)’ if they only exist under Unix versions of the package or ‘(Windows)’ if they only exist under Windows versions of the package.

Feature	Configuration File	File Purpose	Page
Accounting	account.ini	General configuration	127
	yyyymmdd.ACT	Log file with daily rollover at midnight	97
	yyyymmdd_hhmm_nnnn.ACT	Log file with configured rollover times	129
Administrator (Unix)	default.htm	Launch the Administrator applet from your browser	52
	index.htm	Alternative means of launching the Administrator applet from your browser	52
Administrator (Windows only)	radadnt.exe	Administrator program executable file	52
Attribute editing	filter.ini	Configure attribute editing	134
Dictionaries	vendor.ini	Map vendor-specific dictionary files to identifiers used in the server’s administrative database	148
	dictiona.dcm	Keep master list of dictionary files	151
	*.dct	Vendor-specific dictionary files for various NAS devices	151
	radius.dct	Standard RADIUS dictionary file	151
Documentation	readme.txt	Provide late-breaking information not found in the manual	3
EAP	eap.ini	Configure operation of EAP	168
EAP-TTLS	ttlsauth.aut	Configure operation of TTLS authentication	170
Events and counters	perfmon.exe (Windows)	Performance Monitor executable file	112
	events.ini	General configuration	132
Import / Export	*.dci	Dictionaries for importing users files that include vendor-specific attributes *NOTE: This type of file is not created by Steel-Belted Radius, but the data contained within a users file may be imported from another RADIUS server.*	151
	annex.dci	Dictionary for importing users files that include Annex vendor-specific attributes	93
	ascend.dci	Dictionary for importing users files that include Ascend vendor-specific attributes	93

Feature	Configuration File	File Purpose	Page
	portsmstr.dci	Dictionary for importing users files that include Portmaster vendor-specific attributes	93
	*.rif	RADIUS Information file *NOTE: This is the format that Steel-Belted Radius uses when exporting user data to a file, and the default file format that it uses when importing user data from another RADIUS server.*	91
	users	A specially formated text file, usually provided by RADIUS implementations based on source code from Livingston and Ascend, which contains user data *NOTE: This type of file is not created by Steel-Belted Radius, but the data contained within a users file may be imported from another RADIUS server.*	93
Installation (Unix only)	install.sh	Server installation and configuration	8
	filter.ini	Configure attribute editing	134
RADIUS	rfc2865.txt	Documentation of official authentication standards	21
	rfc2866.txt	Documentation of official accounting standards *NOTE: These RADIUS standard documents are RFC 2865 and 2866.*	21
RADIUS server (Unix only)	default.htm	Launch the Administrator applet from your browser	52
	index.htm	Alternate means of launching the Administrator applet from your browser	52
	install.sh	Server installation and configuration	8
RADIUS server	*yyyymmdd*.LOG	Server activity log file with daily rollover at midnight	96
	radadnt.exe (Windows)	Administrator program	52
	radius (Unix)	Server daemon	12
	radius.exe (Windows)	Server executable	15
	radius.ini	General configuration	138
	resetpwd (Unix)	Reset a forgotten server password	84
	services	UDP port settings *NOTE: This file may be found in Unix under /*etc/services *and in Windows under* C:\winnt\system32\drivers\etc\services	158

Feature	Configuration File	File Purpose	Page
Reporting (Windows)	REPORT.RTF	Default output filename and file type (Rich Text Format)	110
Vendor-specific attributes	vendor.ini	Map vendor-specific dictionary files to identifiers used in the server's administrative database	148
	dictiona.dcm	Keep master list of dictionary files	153
	*.dct	Vendor-specific dictionary files for various NAS devices	151
	radius.dct	RADIUS standard dictionary file	32

Configuration Files by Name and Extension

Note that some of the files listed below are specific to one operating system specific. These are marked with either '(Unix)' if they only exist under Unix versions of the package or '(Windows)' if they only exist under Windows versions of the package.

Configuration File	Feature	File Purpose	Page
account.ini	Accounting	General configuration	127
yyyymmdd.ACT	Accounting	Log file with daily rollover at midnight	97
yyyymmdd_hhmm_nnnn.ACT	Accounting	Log file with configured rollover times	129
annex.dci	Import / Export	Dictionary for importing users files that include Annex vendor-specific attributes	93
ascend.dci	Import / Export	Dictionary for importing users files that include Ascend vendor-specific attributes	93
*.dci	Import / Export	Dictionaries for importing users files that include vendor-specific attributes *NOTE: This type of file is not created by Steel-Belted Radius, but the data contained within a users file may be imported from another RADIUS server.*	93
*.dcm	Dictionaries	Keep master list of dictionary files	151
*.dct	Dictionaries	Vendor-specific dictionary files for various NAS devices	151
default.htm (Unix)	RADIUS server	Launch the Administrator applet from your browser	52

Configuration File	Feature	File Purpose	Page
dictiona.dcm	Dictionaries	Keep master list of dictionary files	151
eap.ini	EAP	Configure operation of EAP	168
events.ini	Events and counters	General configuration	132
*.exe (Windows)	(Various)	Executable files for: NT Performance monitor (perfmon.exe) Administrator program (radadnt.exe) Server (radius.exe)	 112 52 15
filter.ini	Proxy RADIUS	Configure attribute editing	134
*.htm, *html (Unix)	(Various)	Launch the Administrator applet from your browser	52
index.html	RADIUS server	Launch the Administrator applet from your browser	52
*.ini	(Various)	Initialization files for various purposes: accounting attributes (account.ini), dictionary integration (vendor.ini), events and counters (events.ini), RADIUS server configuration (radius.ini), and TACACS+ authentication (tacplus.ini)	126
install.sh (Unix)	RADIUS server	Server installation and configuration	8
yyyymmdd.LOG	RADIUS server	Server activity log file with daily rollover at midnight	96
perfmon.exe (Windows)	Events and counters	Performance Monitor executable file	112
portmstr.dci	Import / Export	Dictionary for importing users files that include Portmaster vendor-specific attributes	93
radadnt.exe (Windows)	RADIUS server	Administrator program executable file	52
radius (Unix)	RADIUS server	Server daemon	12
radius.dct	Dictionaries	Standard RADIUS dictionary file	151
radius.exe (Windows)	RADIUS server	Server executable	15
radius.ini	RADIUS server	General configuration	138
readme.txt	Documentation	Provide late-breaking information not found in the manual	3
REPORT.RTF (Windows)	Reporting	Default output filename and file type (Rich Text Format)	110
resetpwd (Unix)	RADIUS server	Reset a forgotten server password	84

Configuration File	Feature	File Purpose	Page
rfc2865.txt	RADIUS	Authentication standard	21
rfc2866.txt	RADIUS	Accounting standard	21
*.rif	Import / Export	RADIUS Information File *NOTE: This is the format that Steel-Belted Radius uses when exporting user data to a file, and the default file format that it uses when importing user data from another RADIUS server.*	91
*.rtf (Windows)	Reporting	Default output filename and file type (Rich Text Format)	110
services	RADIUS server	UDP port settings *NOTE: This file is in the directory* /etc/services *(Unix) or* C:\winnt\system32\driver *(Windows).*	158
*.txt	(Various)	Documentation in text format for various purposes, for example late-breaking information about the Steel-Belted Radius product (readme.txt)	3
		*NOTE: The RADIUS standard documents for authentication (*rfc2865.txt*) and for accounting (*rfc2866.txt*) may be found on the web at:* http://www.ietf.org/rfc/rfc2865.txt *and* http://www.ietf.org/rfc/rfc2866.txt	
users	Import / Export	A specially formatted text file, usually provided by RADIUS implementations based on source code from Livingston and Ascend, which contains user data. *NOTE: This type of file is not created by Steel-Belted Radius, but the data contained within a users file may be imported from another RADIUS server.*	93
vendor.ini	Dictionaries	Map vendor-specific dictionary files to identifiers used in the server's administrative database.	148