Juniper Networks
Steel-Belted Radius Appliance

Upgrade Guide

Release 5.4
July 2007

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: SBR-TD-AUPGR54 Revision 03

Revision History

Date	Description
17 May 2007	Initial draft of Steel-Belted Radius Appliance 5.4 x Upgrade Guide.
18 July 2007	Updated screenshots and edited text.

M07718

Table of Contents

About This Guide

This document describes how to upgrade a Steel-Belted Radius Appliance, which is a standalone RADIUS server in a rack-mountable device, to Release 5.4.*x* of the Steel-Belted Radius software.

Before You Begin

This manual assumes that you have installed the Steel-Belted Radius Appliance and have previously configured the Steel-Belted Radius software. For information on how to install the Steel-Belted Radius hardware, refer to the *Steel-Belted Radius Appliance Hardware Setup Guide*. For information on how to configure the Steel-Belted Radius software, refer to the *Steel-Belted Radius Appliance Configuration Setup Guide*.

Audience

This manual is intended for network administrators responsible for implementing and maintaining authentication, authorization, and accounting services. This manual assumes that you are familiar with the NEWS program, which is used to configure the Steel-Belted Radius Appliance hardware. This manual also assumes you are familiar with general RADIUS (Remote Authentication Dial In User Service) and networking concepts and the specific environment in which you are installing Steel-Belted Radius.

Related Documentation

The following documents supplement the information in this manual.

Steel-Belted Radius Documentation

Please review the Release Notes that accompanies your Steel-Belted Radius software for late-breaking information not available in this manual.

In addition to this manual, the Steel-Belted Radius documentation includes the following manuals:

- The *Steel-Belted Radius Administration Guide* describes how to configure and administer the Steel-Belted Radius server software.
- The *Steel-Belted Radius Reference Guide* describes the configuration files and settings used by Steel-Belted Radius.

Contacting Technical Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (in the United States) or 408-745-9500 (outside the United States).

Check our website (http://www.juniper.net) for additional information and technical notes. When you are running SBR Administrator, you can choose **Web > Steel-Belted Radius User Page** to access a special home page for Steel-Belted Radius users.

When you call technical support, please have the following information at hand:

- Your Steel-Belted Radius product edition and release number.
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- Question or description of the problem, with as much detail as possible.
- Any documentation that can help resolve the problem, such as error messages, memory dumps, compiler listings, and error logs.

Chapter 1

Preparing to Upgrade

This chapter consists of checklists and forms designed to help a network administrator gather the information required to upgrade a Steel-Belted Radius Appliance. If you use the following checklists and forms to gather configuration and network information before you start upgrading the Steel-Belted Radius Appliance, you should be able to complete the upgrade process smoothly in about an hour.

Equipment Checklist

Use the following checklist to document that you have the equipment required for the Steel-Belted Radius Appliance upgrade on hand.

- ☐ Administration PC (Windows laptop recommended)
- ☐ Hub and Cat 5 Ethernet cable (or crossover Ethernet cable)
- ☐ Power Cables
- ☐ Steel-Belted Radius installation CDs (may require access to CD-ROM writer and recordable CD-Rs if you download ISO images)
- ☐ Monitor, keyboard, and mouse for the Steel-Belted Radius Appliance.

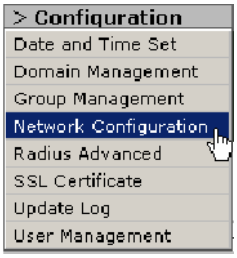
Gathering Network Information

Perform the following procedures to gather information about your network settings. Use Table 1 on page 2 to record the settings for your network.

Gathering IP Configuration Information

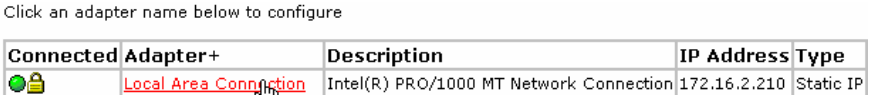
1. Run NEWS.
2. Choose **Configuration > Network Configuration** (Figure 1).

Figure 1: Displaying Network Configuration Information



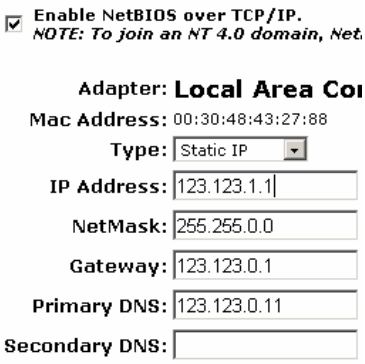
3. When the adapter list (Figure 2) appears, click an adapter name to display its settings.

Figure 2: Adapter List



4. Record the network settings displayed for Network Interface Card (NIC) 1 in Table 1.

Figure 3: Recording Network Configuration Information



5. Repeat steps 3–4 for Network Interface Card (NIC) 2.

Table 1: Network Information

Setting	Your Information
NIC 1 IP Address	
NIC 1 Net Mask	
NIC 1 Gateway	
NIC 1 Primary DNS	
NIC 1 Secondary DNS	
NIC 1 WINS	
NIC 1 NetBIOS setting	
NIC 2 IP Address	

Table 1: Network Information (continued)

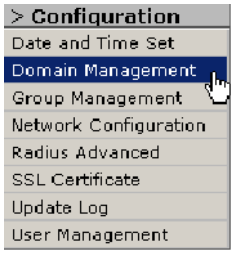
Setting	Your Information
NIC 2 Net Mask	
NIC 2 Gateway	
NIC 2 DNS (Primary)	
NIC 2 DNS (Secondary)	
NIC 2 WINS	
NIC 2 NetBIOS setting	
System Name	
Domain Name	
Domain Login	
Domain Password	

Gathering System Name Information

To gather system name information:

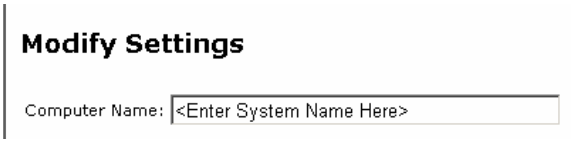
1. Run NEWS.
2. Choose **Configuration > Domain Management** (Figure 4).

Figure 4: Choosing Configuration > Domain Management



3. When the **Computer Name** field appears, record the name of your system in Table 2 on page 4.

Figure 5: Recording the Computer Name



Gathering Domain Information

1. Run NEWS.
2. Choose **Configuration > Domain Management** (Figure 4).
3. When the domain fields (Figure 6) appear, record your domain information in Table 2 on page 4.

Figure 6: Recording Domain Information

Record Your Network Settings

Use Table 2 to document the settings for your network.

Table 2: File Checklist

Setting	Your Information
Location of the *radiusbackup.cab* file	
Appropriate Certificates (if applicable)	
Computer Name	
Domain to Join	
Domain Administrator logon name	
Domain Administrator password	
Workgroup name	
Workgroup Administrator user name	
Workgroup Administrator password	
Local Administrator logon password	

Prepare Your Installation CDs

An ISO file contains the complete disk image of an ISO-9660 file system, including data files and filesystem files. If you download a Steel-Belted Radius ISO file from Juniper Networks, you must copy each ISO file to a recordable CD **as an image**, and then use the CDs to install the Steel-Belted Radius software on your Steel-Belted Radius Appliance or to re-image the device back to an unconfigured state.

NOTE: The application you use to create the installation CD must be capable of recording raw ISO images. If you copy the ISO image as a file to CD-R, the Steel-Belted Radius Appliance will not read the contents of the images.

To create your installation CD-ROM:

1. Download the ISO files appropriate for your Steel-Belted Radius Appliance from the Steel-Belted Radius User webpage (http://www.juniper.net/customers/support/products/aaa_802/sbr_user.jsp).

Table 3 identifies the ISO files you need to download for each model and edition of the Steel-Belted Radius Appliance. Use the MD5 hash value for each file to confirm that the file is complete and correct.

Table 3: Steel-Belted Radius ISO Files

Model Number	Software Edition	ISO Files	File Size (MB)	MD5 Hash
SYS-G-JNP500-000 SYS-G-JNP500-050	Enterprise Edition	SBR-EEE-542-CD_1.ISO	603	7c22d7aaf88bc25ffb966daa95750706
		SBR-EEE-542-CD_2.ISO	599	016efd1f9a835026880be2b6f3504ec3
		SBR-EEE-542-CD_3.ISO	413	cc8040c3c4cb1d046b9143ea57657384
SYS-G-JNP-500-500 , SYS-G-JNP500-550	Global Enterprise Edition	SBR-GEE-542-CD_1.ISO	603	8d75eb9b955932bd6e563f5bbdba1ad8
		SBR-GEE-542-CD_2.ISO	599	b9a5499ffc17378c02c78ea1521a99b0
		SBR-GEE-542-CD_3.ISO	413	057efb2f64a38eb1654c48ed5351bfc5
SYS-FNK400-000, SYS-FNK300-000	Enterprise Edition	SBR-EE-542-W2K-CD_1.ISO	603	4883833a3e20edae8cf3cf7af5a776cf
		SBR-EE-542-W2K-CD_2.ISO	508	ea1ef69ba439dce191c7533c2ba48ebb
SYS-FNK400-500, SYS-FNK300-500	Global Enterprise Edition	SBR-GE-542-W2K-CD_1.ISO	603	cc436c9016afa5bb50bb1e8c5030058f
		SBR-GE-542-W2K-CD_2.ISO	508	0c874dfc00ac126d38b5c42a445e75c4

2. Use any application capable of burning a raw ISO CD image, such as K3b, Nero Burning ROM, or Roxio Easy-CD Creator, to record the **.iso** file on a recordable CD.

   When you record a raw ISO image to a CD, the recording application interprets the ISO image as a complete CD image and extracts the directories and files in the image to the CD-R.

   For best results, you should record your installation CD at a low speed (4X or 8X).

3. Verify that your new installation CD-R was recorded correctly.

   Insert the CD-R into your computer and display its contents. If the CD-R was recorded correctly, you should not see the **.iso** file used to record the CD-R. Instead, you should see a list of files and directories.

File Replacement Checklists

Before you upgrade your Steel-Belted Radius Appliance, you must identify the Steel-Belted Radius configuration files. You can use the configuration files' modification dates to identify which files may have been customized. If you are not certain which files you need to archive, contact Juniper Networks Technical Support. For a complete explanation of these files, please refer to the *Steel-Belted Radius Reference Guide*.

Use the checklists that follow to identify which files you need to merge after upgrading.

General Configuration Files

The *.ini files configure operational settings in Steel-Belted Radius. Use the following checklist to identify the files that have been customized for your installation.

- ☐ access.ini
- ☐ account.ini
- ☐ admin.ini
- ☐ authReport.ini
- ☐ authReportAccept.ini
- ☐ authReportBadSharedSecret.ini
- ☐ authReportUnknownClient.ini
- ☐ authReportReject.ini
- ☐ authlog.ini
- ☐ blacklist.ini
- ☐ bounce.ini
- ☐ ccagw.ini
- ☐ classmap.ini
- ☐ dhcp.ini
- ☐ eap.ini
- ☐ events.ini
- ☐ filter.ini
- ☐ lockout.ini
- ☐ proxy.ini
- ☐ radius.ini
- ☐ redirect.ini
- ☐ securid.ini
- ☐ servtype.ini
- ☐ spi.ini
- ☐ tacplus.ini
- ☐ update.ini
- ☐ vendor.ini

Dictionary Files

The *.dct files configure how Steel-Belted Radius interoperates with a remote access server (RAS) or network access server (NAS).

Use the following checklist to identify the dictionary files that have been customized for your installation. If your .dct files have different names, use the lines to record the name of the files.

- ☐ Special1.dct _____
- ☐ Special2.dct _____
- ☐ Special3.dct _____

Authentication Files

The *.aut files configure how Steel-Belted Radius interoperates with a backend data store for the purpose of looking up user information.

Use the following checklist to identify the authentication files that have been customized for your installation. If your .aut file has a different name, use the line to record the name of the file. If you have other .aut files, list each one separately.

- ☐ Ldapauth.aut _____
- ☐ Sqlauth.aut _____
- ☐ Peapauth.aut _____
- ☐ Securidauth.aut _____
- ☐ Sidalt.aut _____
- ☐ Tlsauth.aut _____
- ☐ Ttlsauth.aut _____
- ☐ Uniport.aut _____
- ☐ Winauth.aut _____

Server Certificates Files

The *.pfx file stores your server certificate.

Use the following checklist to identify the certificate files that has been customized for your installation. If your .pfx file has a different name, use the line to record the name of the file.

- ☐ *Your_Corp*.pfx _____

Trusted CA Root Certificates

The *.der file stores your trusted CA root certificate.

Use the following checklist to identify the root certificate file that has been customized for your installation. If your .der file has a different name, use the line to record the name of the file. If you have other .der files, list each one separately.

- ☐ *Your_Corp*.der _____

EAP Configuration File

The *.eap file configures EAP helper information.

Use the following checklist to identify the EAP helper files that has been customized for your installation. If your .eap file has a different name, use the line to record the name of the file.

- ☐ Tlsauth.eap _____

SecurID Authentication Files

The sdconf.rec file configures how Steel-Belted Radius interoperates with RSA SecurID. You must archive the sdconf.rec file if you use RSA SecurID.

☐ Sdconf.rec

Directed Realm Configuration Files

The *.dir files store information used for directed authentication. These files should be listed in the proxy.ini file.

Use the following checklist to identify the directed realm configuration files that have been customized for your installation. If your .dir files have different names, use the lines to record the name of the file.

☐ *RealmName1*.dir _____

☐ *RealmName2*.dir _____

☐ *RealmName3*.dir _____

Proxy Realm Configuration Files

The *.pro files store information used for proxy realm authentication. These files should be listed in the proxy.ini file.

Use the following checklist to identify the proxy realm authentication configuration files that have been customized for your installation. If your .pro files have different names, use the lines to record the name of the files.

☐ *Realm1*.pro _____

☐ *Realm2*.pro _____

☐ *Realm3*.pro _____

DHCP Pool Configuration File

The *.dhc files store information used for Dynamic Host Configuration Protocol (DHCP) allocation of IP addresses.

Use the following checklist to identify the DHCP authentication configuration files that have been customized for your installation. If your .dhc file has a different name, use the line to record the name of the file.

☐ Pool.dhc _____

Attribute Pool Configuration File

The *.rr files store information used for attribute pool configuration.

Use the following checklist to identify the .rr files that have been customized for your installation. If your .rr file has a different name, use the line to record the name of the file.

☐ Acme.rr _____

Chapter 2

Upgrading the Appliance

Pre-Upgrade Checklist

Before you start upgrading the Steel-Belted Radius Appliance, verify that the follow tasks have been completed and that all required equipment and information is at hand.

- ☐ Required hardware is available: see “Equipment Checklist” on page 1
- ☐ Steel-Belted Radius CD-ROM is available: see “Prepare Your Installation CDs” on page 4
- ☐ Upgrade license information is available
- ☐ Device and network information has been recorded correctly
- ☐ Person performing the upgrade has the appropriate access permissions

The upgrade process for the Steel-Belted Radius Appliance should take 1–2 hours to complete.

Connecting the Administration PC

You must use a Windows PC or laptop as an administration workstation to configure the Steel-Belted Radius Appliance. The administration PC must meet the requirements listed in Table 4.

Table 4: Administration PC Requirements

Operating system	■ Windows 2000 ■ Windows 2003 ■ Windows XP
Networking	Standard Ethernet port
Browser	Internet Explorer version 6.0 or later

You will also need a standard Ethernet cable and a switch/hub (or an Ethernet crossover cable) to establish a network connection between the administration PC and the Steel-Belted Radius Appliance.

Connect the Ethernet port on the administration PC to the LAN 1 Ethernet port on the Steel-Belted Radius Appliance. You can use standard Ethernet cables and a hub/switch (or a crossover Ethernet cable) to connect to the two devices.

Configuring the Administration PC

You must configure the administration PC to communicate with the Steel-Belted Radius Appliance.

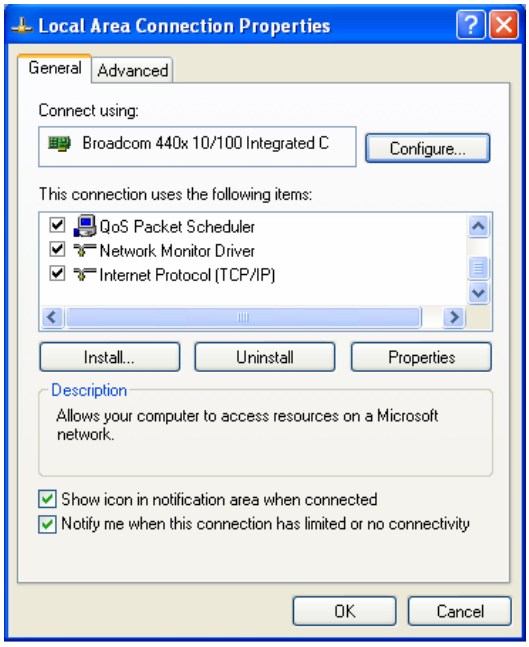
Configuring a Network Address

The following procedure, which describes how to configure a TCP/IP address on the administration PC, assumes that the administration PC is running the Windows 2000 operating system. If you are running another version of the Windows operating system, consult the user manual on configuring network TCP/IP settings. The interface for configuring TCP/IP properties is similar for all Windows operating systems.

1. From the Start menu, choose **Settings > Network and Dialup Connections**.
2. Right-click the **Local Area Connection** icon and select **Properties**.

   The Local Area Connection Properties dialog (Figure 7) opens.

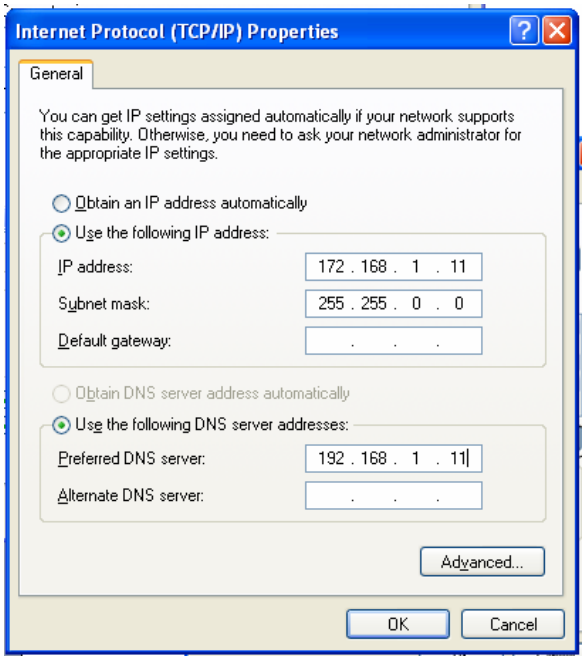
Figure 7: Local Area Connection Properties Dialog



3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties**.

The TCP/IP Properties window (Figure 8) opens.

Figure 8: TCP/IP Properties Dialog



5. Click the **Use the following IP address** radio button.

6. Enter 192.168.1.*n* in the **IP address** field.

   Substitute a number in the range 1–254 (other than 10, which is the default host address for the Steel-Belted Radius Appliance) for *n* in the IP address you enter.

7. Enter 255.255.255.0 in the **Subnet mask** field.

8. Enter the IP address you used in step 6. above in the **Preferred DNS server** field.

9. Do not enter anything in the **Default gateway** field.

10. Click **OK** to close the TCP/IP Properties dialog.

11. Click **OK** to close the Local Area Connection Properties window.

12. If you are running Windows 2000 with Service Pack 4.0 + , proceed to the "Initial Steel-Belted Radius Appliance Connection" on page 19.

    If the administration PC is using an operating system other than Windows 2000 with Service Pack 4.0 + , reboot the computer to put the configured IP address into effect.

Deleting or Moving Logging and Accounting Files

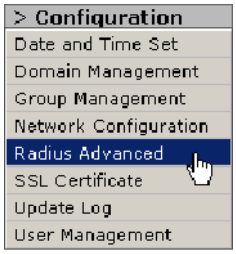
If you don't need your logging (*yyyymmdd*.log) and accounting (*yyyymmdd*.act) files for auditing or other purposes, you should delete them before backing up your Steel-Belted Radius directory to make the backup faster and the resulting file smaller.

NOTE: If you have many .log/.act files, you can configure Steel-Belted Radius to delete the files for you automatically. Refer to "Tips and Tricks" on page 32 for information on how to remove a large number of files during an overnight rollover:

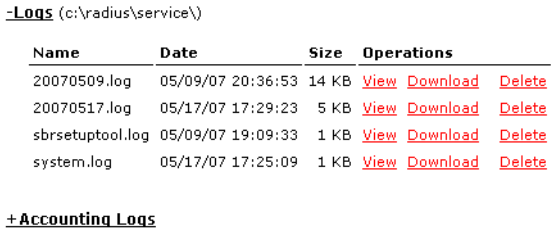
NOTE: Older versions of NEWS may not support the Delete function. If this applies to you, skip this procedure.

To remove Log and Accounting files:

1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Select **Configuration > Radius Advanced**.



3. When the Advanced Radius Configuration window appears, click the **Logs** and **Accounting Logs** entries to display the system log and accounting log files.



4. Click the **Delete** link for each log file you want to delete.

After you stop Steel-Belted Radius, you should archive and delete (or just delete) any .log and .act files that you do not need to minimize the size of the archive file.

Backing Up the Steel-Belted Radius Directory

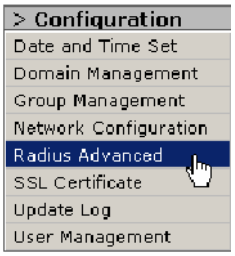
This section describes how to back up the directory containing your Steel-Belted Radius files to a .cab archive file before you upgrade the Steel-Belted Radius Appliance.

NOTE: Before you back up your Steel-Belted Radius directory, verify that pop-ups are enabled in your web browser. Refer to your web browser help or documentation for information on how to enable pop-ups.

To back up your Steel-Belted Radius directory to an archive (.cab) file:

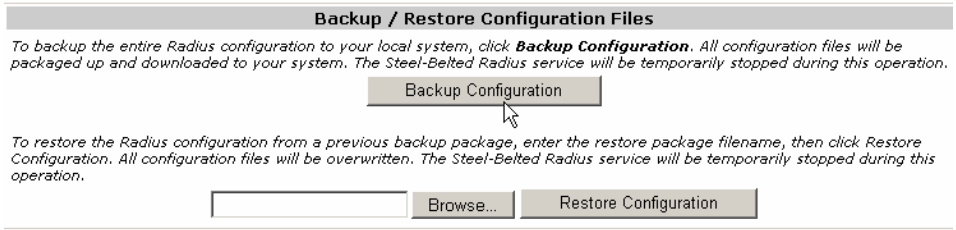
1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Choose **Configuration > Radius Advanced** (Figure 9).

Figure 9: Choosing Configuration > Radius Advanced



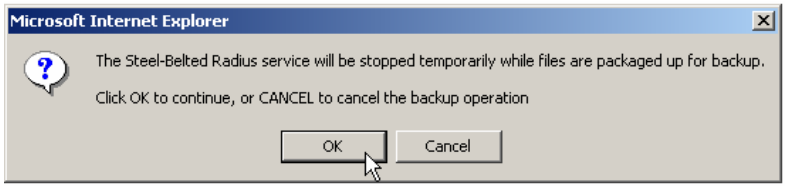
3. Click the **Backup Configuration** button (Figure 10).

Figure 10: Clicking the Backup Configuration Button



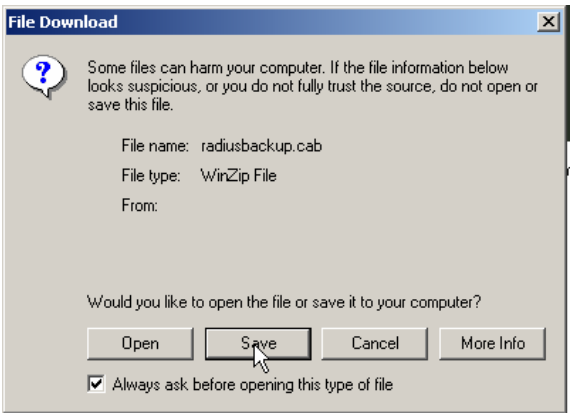
4. When you are prompted to stop the Steel-Belted Radius service (Figure 11), click **OK**.

Figure 11: Stopping the Steel-Belted Radius Service



5. When the File Download window (Figure 12) opens, click **Save**.

Figure 12: Saving the radiusbackup.cab File



6. Specify the directory in which you want to save the radiusbackup.cab file and click **OK**.

After you save the radiusbackup.cab file, you are ready to export your Steel-Belted Radius database.

Exporting Your Steel-Belted Radius Database

You use the SBR Administrator to export your Steel-Belted Radius database to an archive file.

- If your Steel-Belted Radius Appliance is running software version 4.*x*, you will export your Steel-Belted Radius database to a RADIUS Interchange Format (.rif) file, which you must convert to XML before importing into your upgraded Appliance.
- If your Steel-Belted Radius Appliance is running software version 5.*x*, you will export your Steel-Belted Radius database to an XML file.

To export your Steel-Belted Radius database:

1. Run SBR Administrator and connect to your Steel-Belted Radius server (Figure 13).

Figure 13: Connecting to Your Steel-Belted Radius Server (Version 4.*x*)

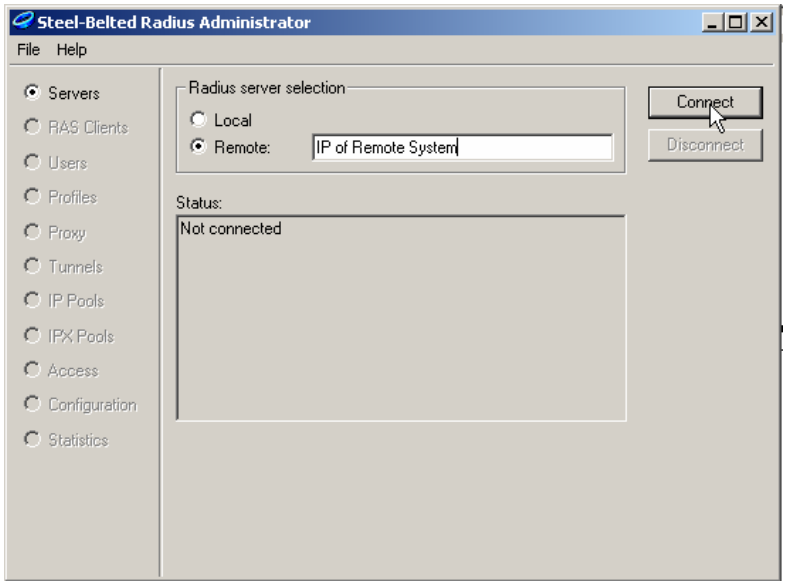
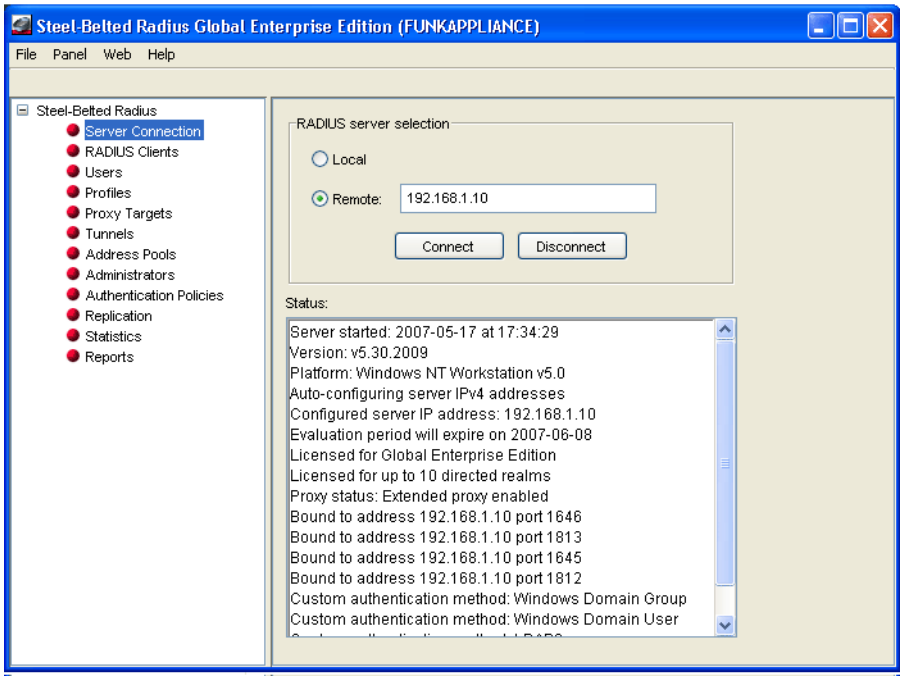


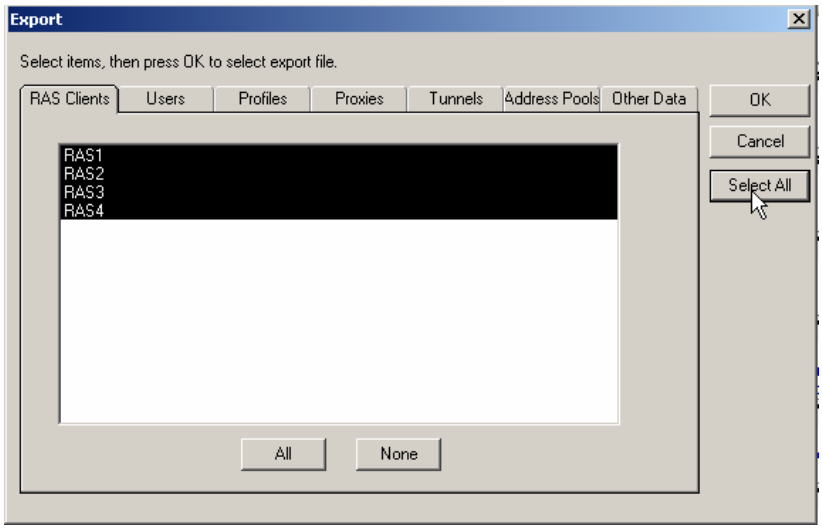
Figure 14: Connecting to Your Steel-Belted Radius Server (Version 5.*x*)



2. Choose **File > Export**.

3. Click **Select All** (Figure 15).

Figure 15: Clicking the Select All Button

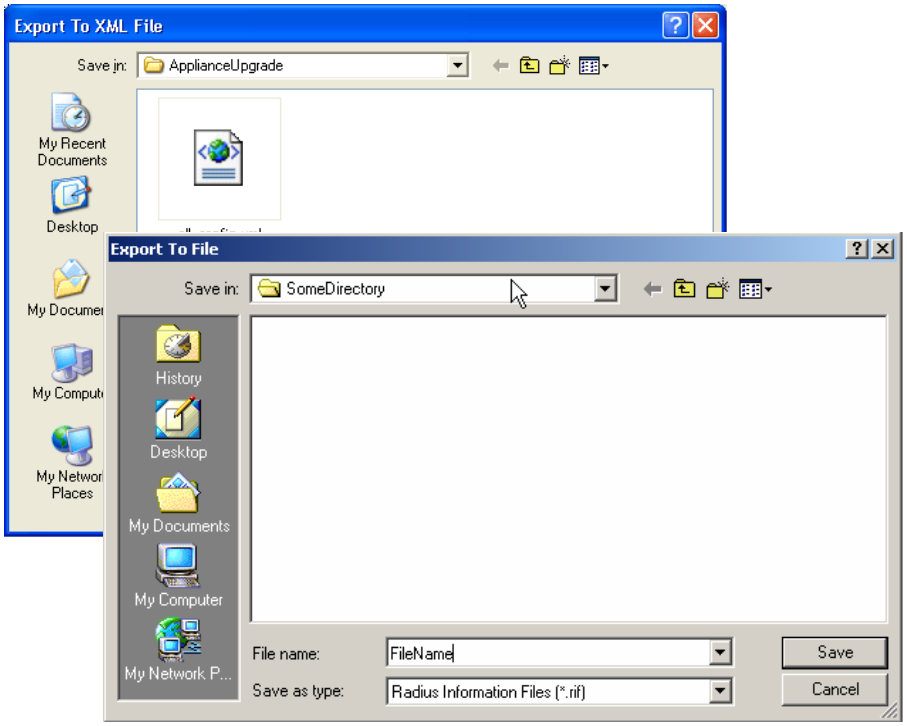


4. Click **OK**.

5. Specify the directory in which you want to save the .rif or .xml backup file (Figure 16).

   Record the path to the backup file. After you upgrade your Steel-Belted Radius software, you will convert the .rif file to an XML file format.

Figure 16: Specifying a Backup Directory (v4 and v5 Versions)



Upgrading Steel-Belted Radius

After you have backed up your Steel-Belted Radius directory to a .cab file and exported your Steel-Belted Radius database to a .rif or .xml file, you are ready to upgrade the Steel-Belted Radius Appliance.

You will need Administrative privileges for the network and a monitor, keyboard, and mouse for this step in the upgrade process.

CAUTION: The upgrade process for the Steel-Belted Radius Appliance cannot be reversed. After you complete these steps, you cannot recover information from the Steel-Belted Radius Appliance. Make sure your archive files have been created and are stored in a safe location before proceeding.

1. Connect the monitor, keyboard, and mouse to the Steel-Belted Radius Appliance.

   You may have to uncap the monitor port on the back of the Appliance by removing a plate with two screws before you can connect the monitor.

2. Insert CD #1 into the CD-ROM drive on the Steel-Belted Radius Appliance.

3. Reboot the Steel-Belted Radius Appliance.

   a. In the NEWS interface, choose **Shutdown > Shutdown or Reboot**.

   b. When the Power Controls window opens, enter your administrator password in the **Password** field.

   c. Click the **Reboot** button.

   d. When you are prompted to confirm you want to reboot the Steel-Belted Radius Appliance, click **OK**.

   Depending on what software version you are running on the Steel-Belted Radius appliance, a time indicating how long the reboot will take may appear.

4. When the Steel-Belted Radius Appliance reboots, press the Delete key on the keyboard connected to the device to enter the System BIOS.

5. Navigate to the BOOT menu in the System BIOS and verify that the first boot device listed is CD-ROM.

6. Navigate to the **Advanced > Advanced Chipset Control** panel in the System BIOS and change the **SATA Mode** setting from **RAID** to **IDE**.

NOTE: If you do not change the SATA mode setting from RAID to IDE, the Steel-Belted Radius will fail to restart properly.

7. Navigate to **Exit** and press Enter for **Save & Exit Setup**.

8. When you are prompted to confirm that you want to **SAVE to CMOS and EXIT,** enter Y and press Enter to continue.

9. When you receive a WARNING window, press any key to start the Ghost re-imaging process.

   The Ghost re-imaging process restores the Steel-Belted Radius Appliance to a non-configured state and then installs the new Steel-Belted Radius image.

10. When system instructs you to do so, insert CD #2 (and for ROHS systems, CD #3) into the CD-ROM drive.

The Steel-Belted Radius Appliance reboots itself when the Ghost Re-imaging Process finishes running. After the Steel-Belted Radius Appliance reboots itself, the SysPrep process applies new settings, installs the NEWS system, and hardens the Steel-Belted Radius Appliance operating system. The Steel-Belted Radius Appliance may reboot itself several times while the SysPrep process is running.

Initial Steel-Belted Radius Appliance Connection

1. If necessary, turn on the Steel-Belted Radius Appliance.

   The power button is located behind the bezel on the front of the Steel-Belted Radius Appliance. Pull the bezel forward, tilt down and remove the packing foam inside the bezel. The power button is the last button on the right.

2. Confirm the connection (link) lights next to the network ports on the Steel-Belted Radius Appliance are lit.

3. Launch Internet Explorer v6.0+ on the administration PC.

   Disregard any error message that indicates the browser is not connected to the Internet.

4. Enter https://192.168.1.10:3886 in the **Address** field of the browser to connect to the Steel-Belted Radius Appliance.

   You must use https instead of http to specify this is a secure connection.

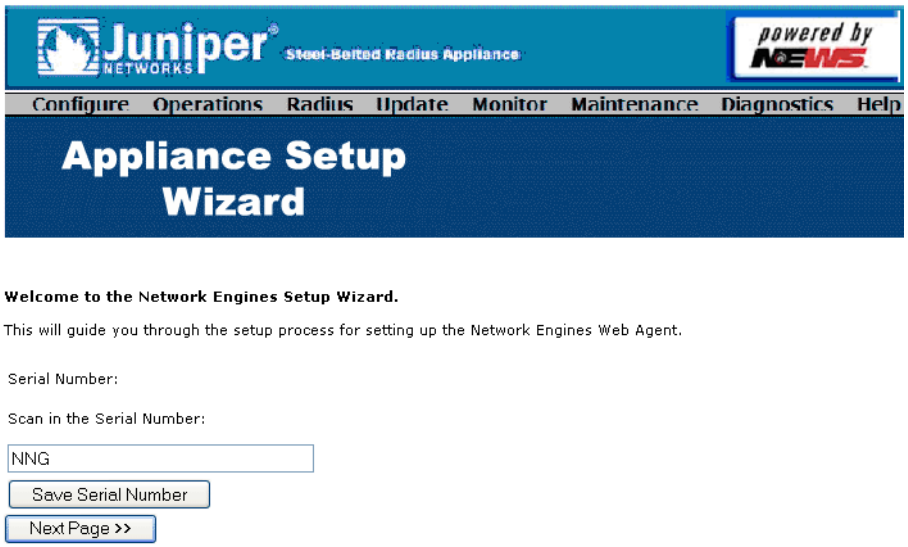
5. When the Security Alert dialog (Figure 17) opens, click **Yes**.

   Figure 17: Security Alert Dialog

6. When the Appliance Setup Wizard window (Figure 18) opens, enter the serial number for your Steel-Belted Radius Appliance (which is a number that starts with NNG on the back of the Appliance) in the **Scan in the Serial Number** field, click **Save Serial Number**, and then click **Next Page**.

Figure 18: Entering the Appliance Serial Number



7. When the Setup Wizard - Password window (Figure 19) opens, enter the administrator password for the device in the **New Password** field, and enter the identical password in the **Confirm new password** field.

   Passwords must be at least eight characters in length and must contain a mix of uppercase and lowercase letters, digits, and non-alphanumeric characters.

Figure 19: Specifying a Device Password

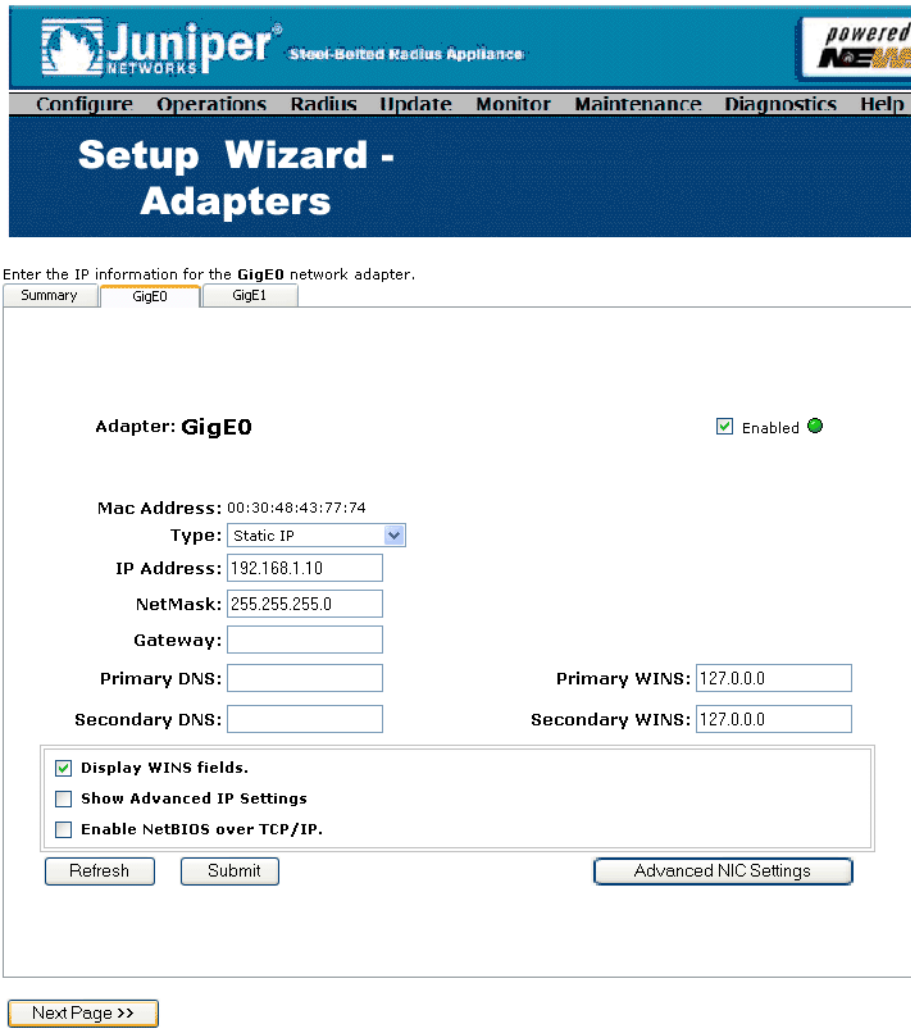
8. After you have entered the device password twice, click **Next Page**.

9. When the Setup Wizard - Adapters window (Figure 20) opens, enter IP address information for the management NIC.

   You should retrieve this information from the records you made in Table 1 on page 2.

NOTE: After you configure IP address information for the management NIC on the Steel-Belted Radius Appliance, you will need to modify the settings on your administration PC to use the same TCP/IP subnet to re-connect to the Steel-Belted Radius Appliance. Refer to "Configuring the Administration PC" on page 10 for information on how to specify TCP/IP settings on your administration PC.

Figure 20: Specifying Configuration Settings for the GigE0 Adapter



10. Use the **Type** list to select the type of address (Static IP) you want the Steel-Belted Radius Appliance to use.

11. Enter the IP address for the Steel-Belted Radius Appliance in the **IP Address** field.

12. Enter the subnet mask for your network in the **NetMask** field.

13. Enter the gateway (router) IP address in the **Gateway** field.

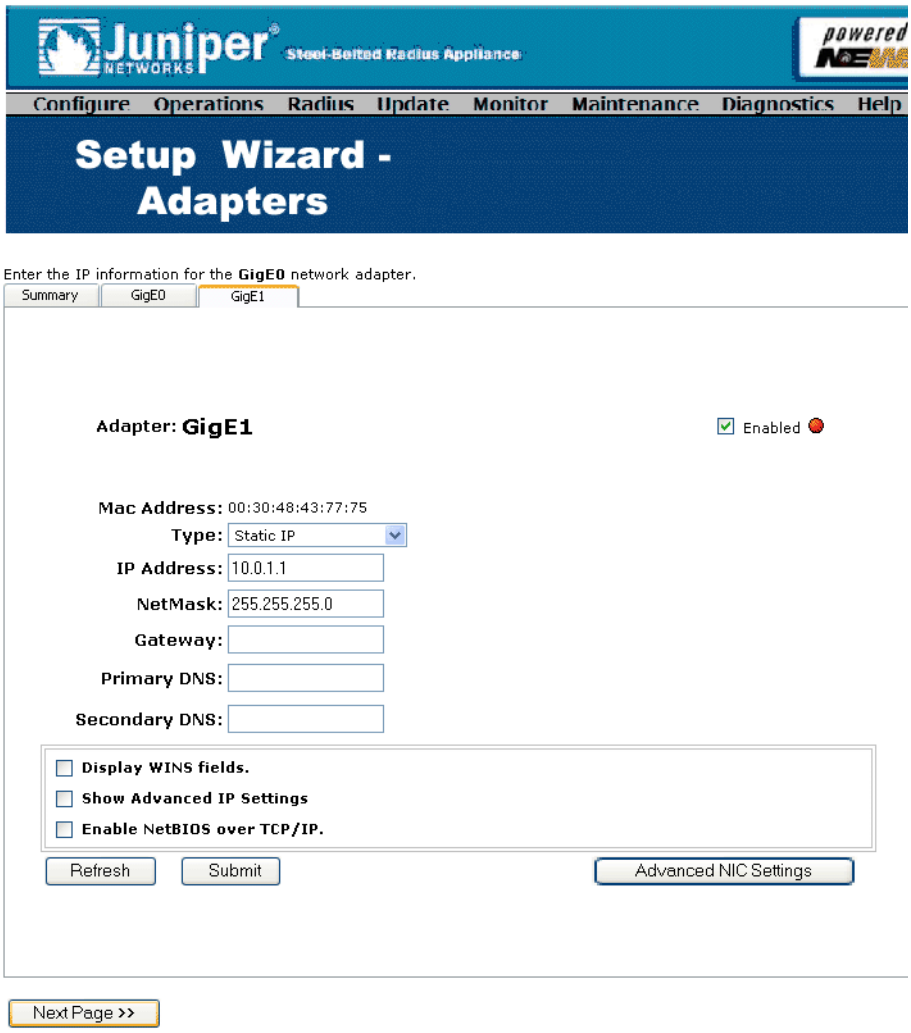
14. Enter the IP addresses for your primary and secondary DNS nameservers in the **Primary DNS** and **Secondary DNS** fields.

15. If your network is running the Windows Internet Naming Service (WINS), enter the IP addresses for your primary and secondary WINS servers in the **Primary WINS** and **Secondary WINS** fields.

16. Click **Next Page**.

17. If you want to configure the GigE1 port, enter the appropriate settings in the GigE1 tab on the Setup Wizard - Adapters window (Figure 21).

Figure 21: Specifying Configuration Settings for the GigE1 Adapter



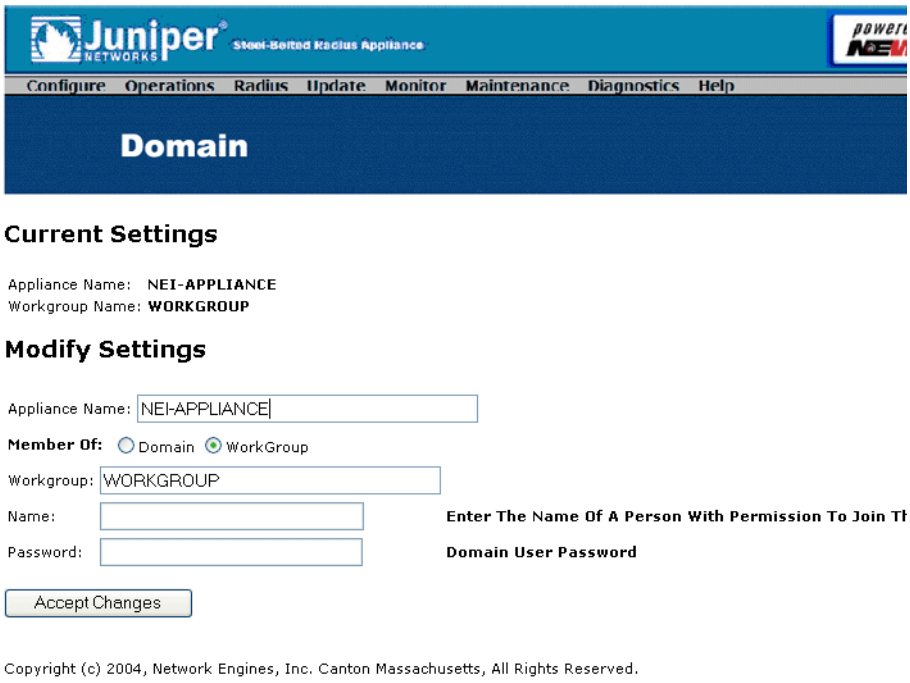
Configuring Hostname and Domain Settings

In typical situations, you must configure a hostname and a domain for a Steel-Belted Radius Appliance. In some situations, you must configure a hostname and a workgroup membership. Note that you cannot configure the Steel-Belted Radius Appliance to belong to both a domain and a workgroup.

To configure hostname and domain information:

1. Run the NEWS interface.
2. Choose **Configure > Network Domain**.
1. When the Domain window (Figure 22) opens, enter a system name that conforms to your network environment in the **Appliance Name** field.

Figure 22: Domain Window



2. Specify a domain or workgroup for the Steel-Belted Radius Appliance.
   - If you want to join the Steel-Belted Radius Appliance to a domain:
     a. Click the **Domain** radio button.
     b. Enter the appropriate domain name in the **Domain** field.
     c. Enter the user name for the domain administrator in the **Name** field.
     d. Enter the password for the domain administrator in the **Password** field.

- If you want to specify a workgroup membership for the Steel-Belted Radius Appliance:

  a. Click the **Workgroup** radio button.

  b. Enter the appropriate workgroup in the **Workgroup** field.

  c. Enter the user name for the workgroup administrator in the **Name** field.

  d. Enter the password for the workgroup administrator in the **Password** field.

3. Click **Accept Changes**.

4. Reboot the Steel-Belted Radius Appliance.

   a. In the NEWS interface, choose **Shutdown > Shutdown or Reboot**.

   b. When the Power Controls window opens, enter your administrator password in the **Password** field.

   c. Click the **Reboot** button.

   d. When you are prompted to confirm you want to reboot the Steel-Belted Radius Appliance, click **OK**.

   Depending on what software version you are running on the Steel-Belted Radius appliance, a time indicating how long the reboot will take may appear.

RIF to XML Conversion

NOTE: If your Steel-Belted Radius Appliance is running software version 5.*x*, you can ignore this section.

If your Steel-Belted Radius Appliance is running software version 4.x, you will need to convert the .rif archive file created when you export the Steel-Belted Radius database (described in "Exporting Your Steel-Belted Radius Database" on page 14). To convert the .rif file, you must run the rif2xml.exe tool, which is installed in the C:\Radius|Admin directory on the administration PC when you install the SBR Administrator application. The rif2xml.exe tool converts archive files stored in RADIUS Interchange Format (*.rif), which is used by Steel-Belted Radius v4.*x*, to XML format, which is used by Steel-Belted Radius v5.*x*.

To convert your .rif files, copy rif2xml.exe to the directory in which you saved your exported .rif file and then run the rif2xml.exe tool:

1. Choose **Start > Run**.

2. Enter CMD and press ENTER.

3. Navigate to the directory that holds your .rif file and the rif2xml.exe tool.

4. Execute the following command to run the rif2xml.exe tool.

   rif2xml.exe *rif_file*.rif *output*.xml

   where *rif_file*.rif is the name of your .rif archive file and *output*.xml is the name of the converted XML file you want to save.

5. When you see a message similar to the following, close the DOS window.

   end of input RIF file

Configuring License Key Information

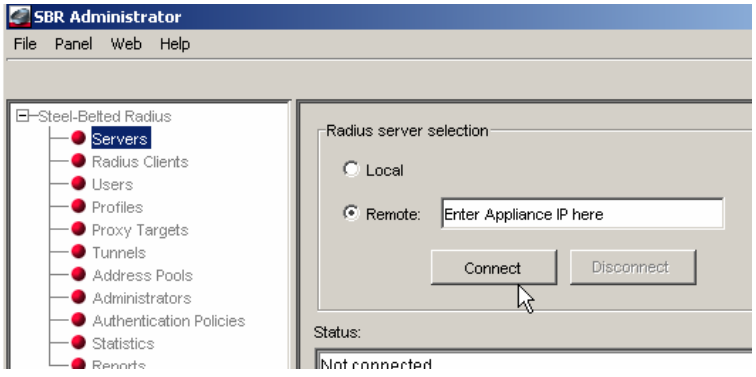
This section describes how to add one or more license keys to the Steel-Belted Radius server software running on the Steel-Belted Radius Appliance.

1. Run SBR Administrator.

2. Log into the Steel-Belted Radius Appliance.

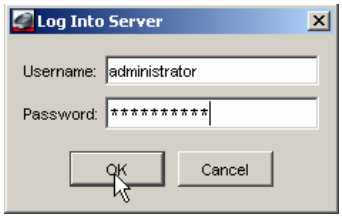
   Select the **Remote** button (Figure 23) and enter the IP address of the Steel-Belted Radius Appliance in the **Remote** field.

   Figure 23: Logging Into the Steel-Belted Radius Appliance



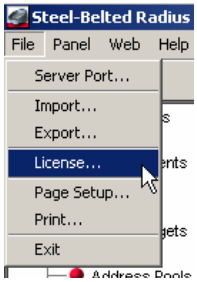
3. When a login dialog appears, enter your username in the **Username** field and your password in the **Password** field (Figure 24).

Figure 24: Entering Access Information



4. Choose **File > License** (Figure 25).

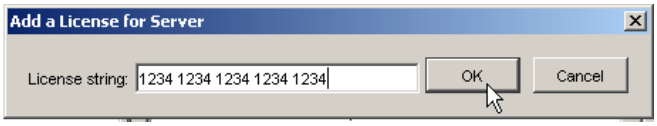
Figure 25: Choosing File > License



5. When the Add a License for Server dialog opens, enter your existing Steel-Belted Radius version 4.*x* license key and your version 5.*x* upgrade license key in the **License String** field (Figure 26).

   Click **OK** when you are finished.

Figure 26: Choosing File > License



6. Restart Steel-Belted Radius.

   See "Restarting Steel-Belted Radius" on page 30 for information on how to restart Steel-Belted Radius.

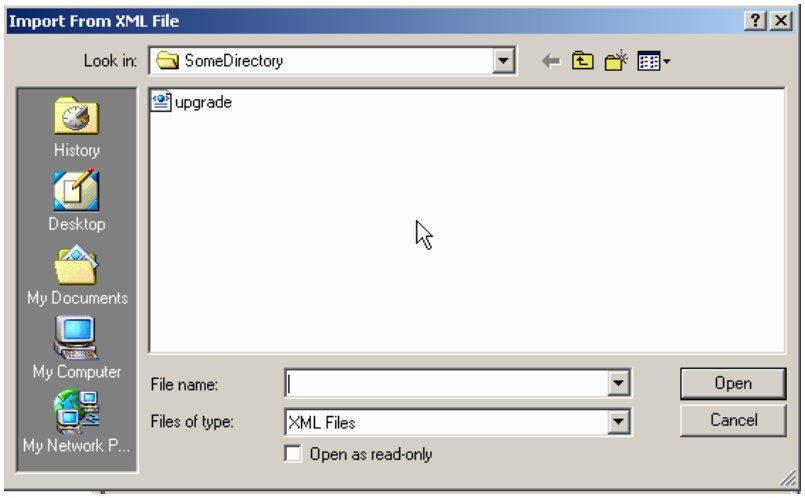
Importing Your Configuration Information

After you have added your Steel-Belted Radius version 5.x license, you are ready to import the Steel-Belted Radius database information you exported previously.

1. Run SBR Administrator.
2. Log into the Steel-Belted Radius Appliance.
3. Choose **File > Import**.

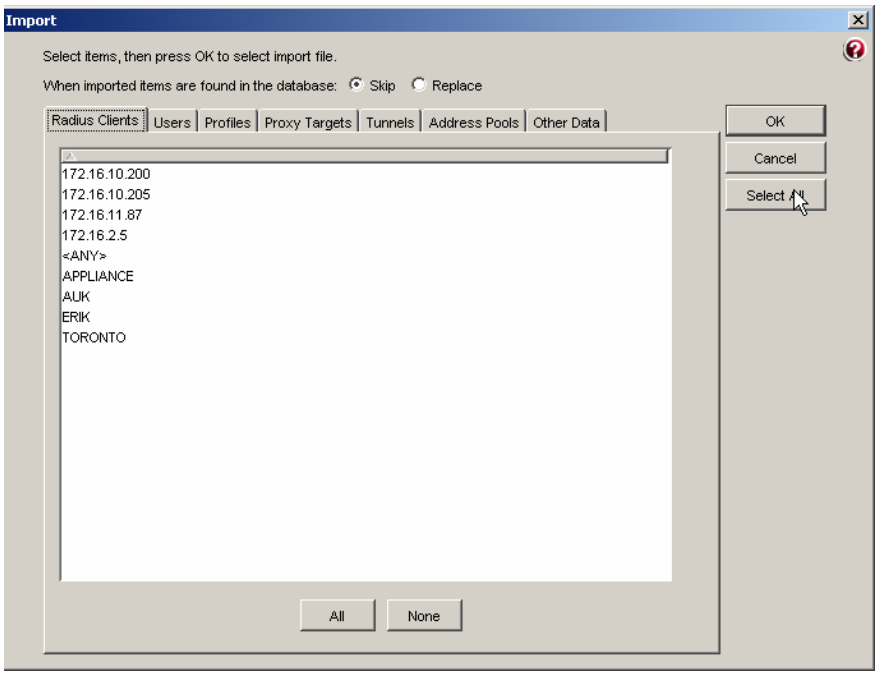
4. When the Import from XML File dialog (Figure 27) opens, select your configuration file and click **Open**.

Figure 27: Import from XML File Dialog



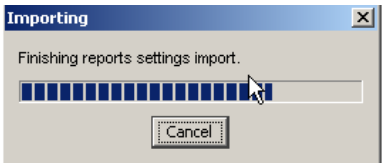
5. When the Import window (Figure 28) opens, click the **Select All** button to indicate you want to import all the settings you exported previously.

Figure 28: Import Dialog



6. Use the **Skip** and **Replace** radio buttons to specify whether you want Steel-Belted Radius to skip or replace an item if a duplicate entry is found during import.

7. Click **OK** to import the Steel-Belted Radius configuration settings from the XML file.



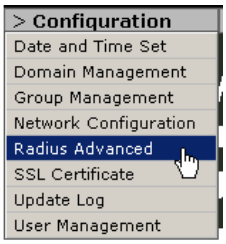
Importing Your Configuration Files

After you have imported your Steel-Belted Radius configuration settings, you must import your customized configuration files. Refer to “File Replacement Checklists” on page 6 to see which files you need to import.

To upload configuration files:

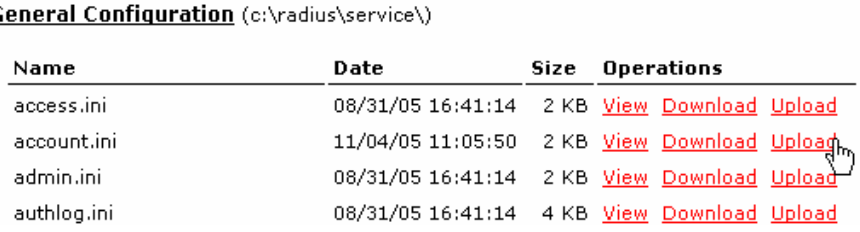
1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Choose **Configuration > Radius Advanced** (Figure 29).

Figure 29: Choosing Configuration > Radius Advanced



3. Click the **Upload** link for each file you want to upload (Figure 30).

Figure 30: Uploading Configuration Files to the Appliance

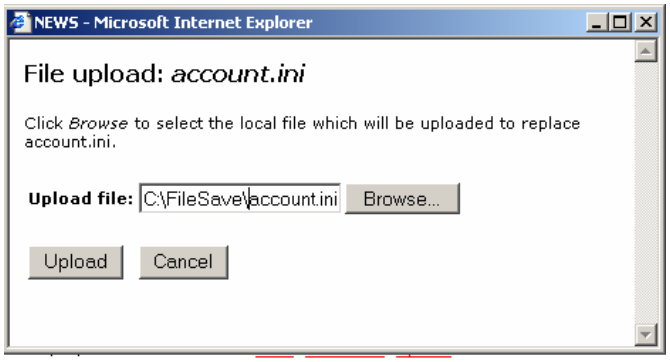


CAUTION: Take care to upload the right files to Steel-Belted Radius. Uploading (overwriting) the wrong file can cause Steel-Belted Radius to stop functioning. If you require more information, contact Juniper Technical Support.

4. When a popup window (Figure 31) prompts you to browse for the file you want to upload, navigate to the file you want to upload.

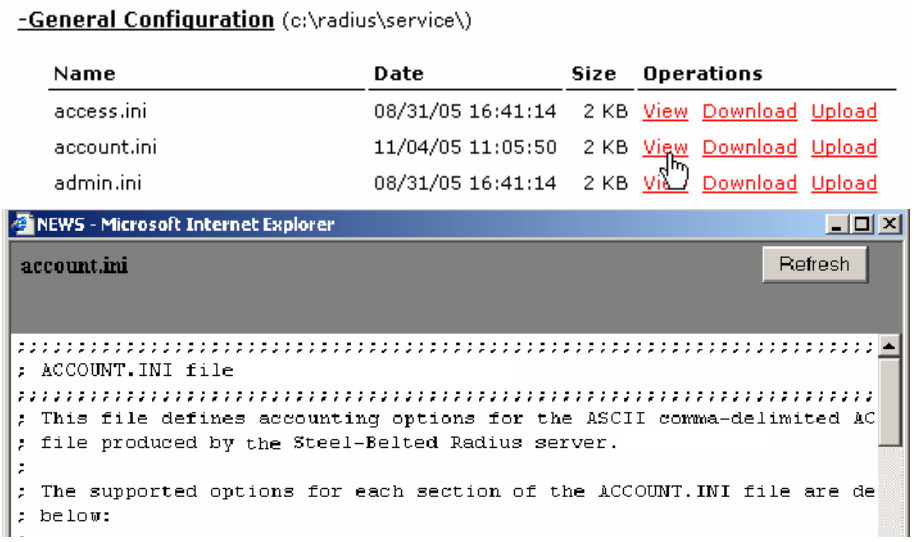
   For example, if you modified the account.ini file to record only RADIUS attributes specific to your environment, you would upload your copy of account.ini (overwriting the default version of the file) by clicking the **Upload** link and navigating to the directory in which you stored your customized copy.

Figure 31: File Upload Dialog



5. After you upload a file, click the **View** link for that file (Figure 32) and verify the correct file was uploaded.

Figure 32: Verifying an Uploaded Configuration File



6. When you finish uploading customized configuration files, restart Steel-Belted Radius.

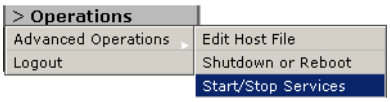
   For more information, see “Restarting Steel-Belted Radius” on page 30.

Restarting Steel-Belted Radius

To restart Steel-Belted Radius, you must stop the service and then start it.

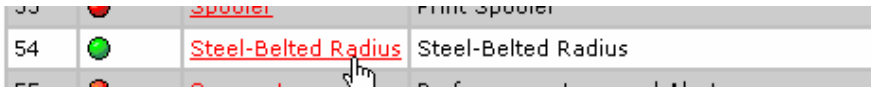
Stopping the Steel-Belted Radius Service

1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Choose **Operations > Advanced Operations > Start and Stop Services**.



3. When the list of services appears, click the **Steel-Belted Radius** link (Figure 33).

Figure 33: Choosing Services > Start and Stop Services

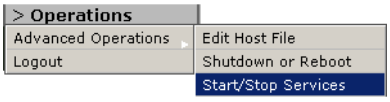


4. When the Steel-Belted Radius page opens, click the **Stop Service** button.

   After you click the **Stop Service** button, the Status icon turns black.

Starting the Steel-Belted Radius Service

1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Choose **Operations > Advanced Operations > Start and Stop Services**.



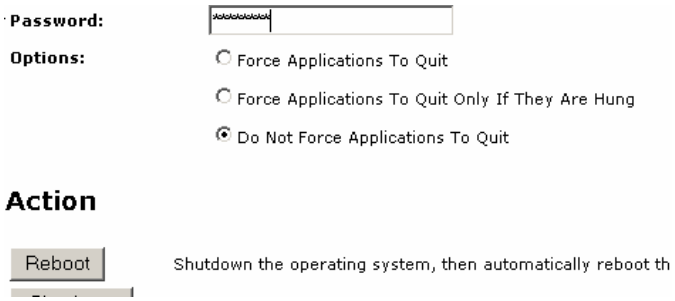
3. When the list of services appears, click the **Steel-Belted Radius** link.
4. When the Steel-Belted Radius page opens, click the **Start Service** button.

   After you click the **Start Service** button, Steel-Belted Radius restarts and reads its configuration files.

Shutting Down the Steel-Belted Radius Appliance

1. Use NEWS to connect to the Steel-Belted Radius Appliance.
2. Choose **Shutdown > Shutdown or Reboot**.
3. Enter the administrator password in the **Password** field and specify the shutdown option you want to use (Figure 34). Click **Reboot** to reboot the Appliance.

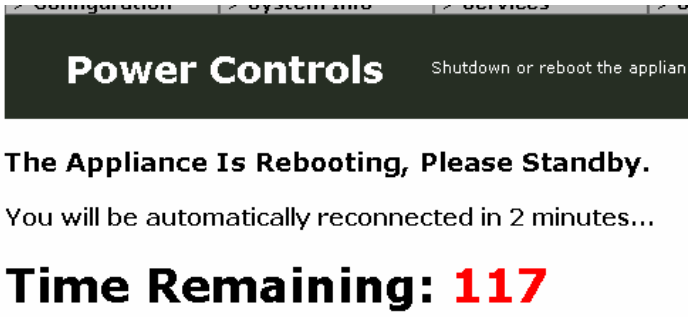
Figure 34: Shutting Down the Steel-Belted Radius Appliance



4. When you are prompted to confirm you want to reboot the Appliance, click **OK**.

   The Power Controls window (Figure 35) counts down the time until the server is rebooted.

Figure 35: Counting Down to Shutdown



At this point, the upgrade for your Steel-Belted Radius Appliance should be complete.

NOTE: If you modified the number of days Steel-Belted Radius retains logging and accounting files to purge old files, you should restore its previous value after the upgrade is complete.

Tips and Tricks

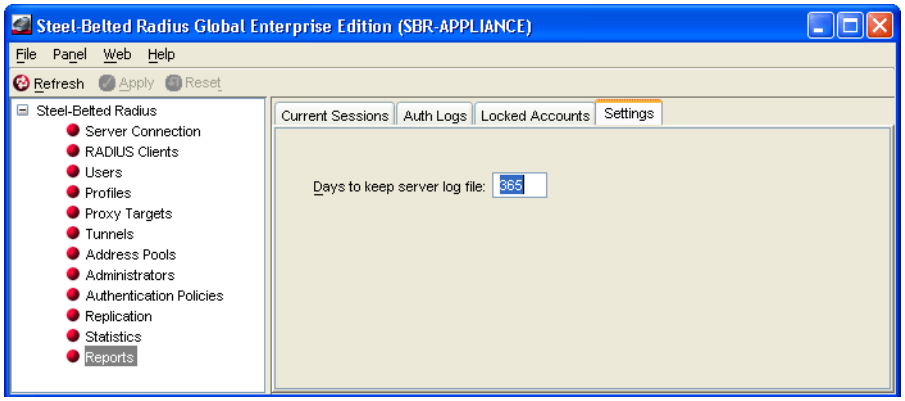
Deleting Multiple Log Files

If you have a large number of .log or .act log files that you do not want, perform the following procedure two days before your scheduled upgrade.

1. Run SBR Administrator and log into your Steel-Belted Radius Appliance.
2. Click **Reports** in the Sidebar, and click the **Settings** tab.

   The Settings panel (Figure 36) appears.

Figure 36: Configuration Panel



3. Enter a value of 1 in the **Days to keep server log file** field.

   This will automatically remove any .log or .act file older than one day.