Juniper Networks
Steel-Belted Radius

Getting Started Guide

Release 6.0
February 2007
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software copyright 1989, 1991, 1992 by Carnegie Mellon University Derived Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this software copyright 2001-2002, Networks Associates Technology, Inc All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA, OR PROFITS, OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are copyright © 2001-2002, Cambridge Broadband Ltd All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA, OR PROFITS, OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software copyright © 1995-2002 Jean-loup Gailly and Mark Adler This software is provided ‘as-is’, without any express or implied warranty. In no event will the author be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- This notice may not be removed or altered from any source distribution.

HTTPClient package Copyright © 1996-2001 Ronald Tschalar (ronald@innovation.ch).

This library is free software, you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.


This library is free software, you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
# Table of Contents

## About This Guide

- Audience ................................................................. vii
- What’s In This Manual .................................................. vii
- Typographical Conventions ........................................ viii
  - Editions/Usage In ...................................................... ix
  - Syntax ......................................................................... ix
- Related Documentation ................................................ x
  - Steel-Belted Radius Documentation ............................... x
  - Requests for Comments (RFCs) ...................................... x
  - Third-Party Products .................................................. xi
- Contacting Technical Support .......................................... xi

## Chapter 1  Overview

- Steel-Belted Radius Features ........................................ 1
- Release Highlights ..................................................... 2
  - Release 6.0 .................................................................. 2
  - Release 5.4 .................................................................. 3
  - Release 5.3 .................................................................. 4
- Licensing ........................................................................ 4

## Chapter 2  Preparing for Installation

- Review the Release Notes ............................................. 7
- Select a Server ........................................................... 7
- Verify System Requirements .......................................... 8
  - System Requirements – Windows ................................. 8
  - System Requirements – Solaris ..................................... 11
  - System Requirements – Linux ...................................... 13
- Verify Network Connectivity ......................................... 15
- Verify Host Name Resolution ......................................... 15
- Verify Administrator Account Access .............................. 15
- Obtain a Server License Number ................................. 16

## Chapter 3  Windows Installation

- Before You Begin ...................................................... 17
- Installing the Steel-Belted Radius Server Software .......... 17
- Upgrading from a 30-Day Trial Installation ..................... 20
- Upgrading from Steel-Belted Radius Version 4.x ............. 21
- Upgrading from Steel-Belted Radius Version 5.x ............. 23
- Upgrading from RSA RADIUS Server Version 6.1 ........... 25
  - Upgrading in a Replication Environment ....................... 25
<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Uninstalling Steel-Belted Radius</th>
<th>91</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Uninstalling on Windows</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the Steel-Belted Radius Server</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the SBR Administrator Files</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>Uninstalling on Solaris</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the Steel-Belted Radius Server</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the SBR Administrator Files</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Uninstalling on Linux</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the Steel-Belted Radius Server</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>Uninstalling the SBR Administrator Files</td>
<td>95</td>
</tr>
<tr>
<td>Appendix A</td>
<td>RIF2XML Conversion Utility</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Locating the RIF-to-XML Utility</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Before You Begin</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Using the RIF-to-XML Utility</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>After You Finish</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>105</td>
</tr>
</tbody>
</table>
About This Guide

The Steel-Belted Radius Getting Started Guide describes how to install or upgrade the Steel-Belted Radius software on a server running the Solaris operating system, the Linux operating system, or the Windows XP/Windows Vista/Windows Server 2003 operating system.

Audience

This manual is intended for network administrators who are responsible for implementing and maintaining authentication, authorization, and accounting services for an enterprise. This manual assumes that you are familiar with general RADIUS and networking concepts and the specific environment in which you are installing Steel-Belted Radius.

If you use Steel-Belted Radius with third-party products such as Oracle or RSA SecurID, you should be familiar with their installation, configuration, and use.

What’s In This Manual

This manual contains the following chapters and appendixes:

- Chapter 1, “Overview,” presents an overview of Steel-Belted Radius and describes installation and licensing requirements for Steel-Belted Radius.
- Chapter 2, “Preparing for Installation,” describes the tasks that you should complete before you install Steel-Belted Radius.
- Chapter 3, “Windows Installation,” describes how to install the Steel-Belted Radius server software and SBR Administrator on a Windows host.
- Chapter 4, “Solaris Installation,” describes how to install the Steel-Belted Radius server software and SBR Administrator on a Solaris host.
- Chapter 5, “Linux Installation,” describes how to install the Steel-Belted Radius server software and SBR Administrator on a Linux host.
- Chapter 6, “Verifying Native User Authentication,” describes how to configure basic settings and native users in Steel-Belted Radius and how to use the RadiusTest utility to verify that Steel-Belted Radius can authenticate a native user.
- Chapter 7, “Uninstalling Steel-Belted Radius,” describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows, Solaris, or Linux host.

- Appendix A, “RIF2XML Conversion Utility,” describes how to use the rif2xml utility to convert a database exported by an older version of Steel-Belted Radius in RADIUS Import Format (RIF) to the Extensible Markup Language (XML) format used by Steel-Belted Radius version 5.x and 6.0.

- The Glossary provides brief explanations for RADIUS terminology used in this and other Steel-Belted Radius manuals.

**Typographical Conventions**

Table 1 describes the text conventions used throughout this manual.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface</strong></td>
<td>Indicates buttons, field names, dialog names, and other user interface elements.</td>
<td>Use the <strong>Scheduling</strong> and <strong>Appointment</strong> tabs to schedule a meeting.</td>
</tr>
</tbody>
</table>
| **Plain sans serif typeface** | Represents:  
- Code, commands, and keywords  
- URLs, file names, and directories | Examples:  
- Code: `certAttr.OU = 'Retail Products Group'`  
- URL: Download the JRE application from [http://java.sun.com/j2se/](http://java.sun.com/j2se/) |
| **Italics**         | Identifies:  
- Terms defined in text  
- Variable elements  
- Book names | Examples:  
- Defined term: *An RDP client* is a Windows component that enables a connection between a Windows server and a user’s machine.  
- Variable element: Use settings in the **Users > Roles > Select Role > Terminal Services** page to create a terminal emulation session.  
- Book name: See the *Steel-Belted Radius Administration Guide*. |
Editions/Used In

Steel-Belted Radius is available in multiple editions to meet the requirements of different types of customers. This manual uses the following abbreviations to identify editions of Steel-Belted Radius:

- GEE: Global Enterprise Edition
- SPE: Service Provider Edition
- SPE + EAP: Service Provider Edition with optional EAP Extension Module
- SPE + MIM: Service Provider Edition with optional Mobile IP Module
- EE: Enterprise Edition

Syntax

- `radiusdir` represents the directory into which Steel-Belted Radius has been installed. By default, this is `C:\Program Files\Juniper Networks\Steel-Belted Radius` for Windows systems and `/opt/JNPRsbr/radius` on Linux and Solaris systems.

- Brackets `[ ]` enclose optional items in format and syntax descriptions. In the following example, the first `Attribute` argument is required; you can include an optional second `Attribute` argument by entering a comma and the second `Attribute` argument (but not the square brackets) on the same line.

  `<add | replace> = Attribute [,Attribute]`

In configuration files, brackets identify section headers:

  the [Processing] section of `proxy.ini`

In screen prompts, brackets indicate the default value. For example, if you press Enter without entering anything at the following prompt, the system uses the indicated default value (`/opt`).

  Enter install path [/opt]:

- Angle brackets `< >` enclose a list from which you must choose an item in format and syntax descriptions.

- A vertical bar (`|`) separates items in a list of choices. In the following example, you must specify `add` or `replace` (but not both):

  `<add | replace> = Attribute [,Attribute]`
Related Documentation

The following documents supplement the information in this manual.

**Steel-Belted Radius Documentation**

Please review the *ReleaseNotes.txt* file that accompanies your Steel-Belted Radius software. This file contains the latest information about features, changes, known problems, and resolved problems. If the information in the *ReleaseNotes.txt* file differs from the information found in the Steel-Belted Radius manuals, use the information in the *ReleaseNotes.txt* file.

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

- The *Steel-Belted Radius Reference Guide* describes the configuration files and settings used by Steel-Belted Radius.
- The *Steel-Belted Radius Administration Guide* describes how to configure and administer the Steel-Belted Radius software.
- The *LDAP Schema* diagram presents the LDAP schema information in a poster format.

**Requests for Comments (RFCs)**

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFCs) online at [http://www.ietf.org/rfc.html](http://www.ietf.org/rfc.html). Table 2 lists the RFCs that apply to this guide.

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>Title</th>
</tr>
</thead>
</table>
About This Guide

Third-Party Products

For more information about configuring your access servers and firewalls, consult the manufacturer's documentation that is provided with each device.

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 (for example, Global Enterprise Edition version 6.0).
- 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.
Thank you for selecting the Steel-Belted Radius® software. Steel-Belted Radius is a complete implementation of the RADIUS (Remote Authentication Dial In User Service) protocol that runs in your Windows, Solaris, or Linux environment. It interfaces with a wide variety of network access equipment, and authenticates remote and WLAN users against numerous back-end databases — enabling you to consolidate the administration of your remote and WLAN users, however they connect to your network. Steel-Belted Radius records usage statistics in an accounting database, so you can track and document user sessions for accounting and billing purposes.

### Steel-Belted Radius Features

- Centralized management of user access control and security.

- Flexible authentication options let you use your existing OS-based authentication database, token-based authentication systems, and external SQL/LDAP databases for remote and WLAN user authentication.

- Support for a wide variety of 802.1X-compliant network access devices ensures compatibility in your network environment.

- Flexible, powerful proxy RADIUS features let you easily distribute authentication and accounting requests to the appropriate RADIUS server for processing.

- High-performance operation guarantees speedy internet access, with no waiting by the customer.

- **GEE/SPE:** Advanced external authentication features let you authenticate against multiple, redundant SQL or Lightweight Directory Access Protocol (LDAP) databases according to configurable load balancing and retry strategies, ensuring the highest level of service delivery to your users.

- **GEE/SPE:** You can control the time periods during which each user is allowed access. An access request is granted only during a user’s allowed access hours; otherwise it is refused, even if the user presents valid credentials.

- **GEE/SPE:** You can define and apply administrative access levels to user or group accounts on the server machine. You can apply read, write, and read/write access selectively to different categories of configuration data.
- **GEE/SPE**: Auto-restart permits the Steel-Belted Radius server to restart itself automatically if it experiences a shutdown.

- **GEE/SPE**: Advanced proxy features let you easily authenticate users against RADIUS servers at other sites.
  - You have a choice of user name format, and you can configure routing based on user name decoration, dialed number identification service (DNIS), or specific attributes.
  - You can selectively modify attributes as proxy packets flow to and from Steel-Belted Radius.
  - You can specify groups of proxy target servers that handle proxy requests according to load-balancing or retry strategies — for the best performance and reliability.

- **GEE/SPE**: Directed authentication and accounting features simplify the hosting of RADIUS services by allowing Steel-Belted Radius to provide different services for each of your customers. Incoming requests can be directed to specific authentication or accounting methods based on user name decoration or DNIS.

- **GEE/SPE**: Your choice of interface lets you configure Steel-Belted Radius by means of a graphical SBR Administrator program or by means of LDAP (either programatically or at the command line prompt).

- **Solaris only**: SNMP support lets you centrally monitor Steel-Belted Radius from your SNMP console, in the same manner as you monitor other devices and services on your network. Steel-Belted Radius offers full SNMP support including SNMP traps and alarms.

- **Windows only**: Perfmon counter and Windows event support let you centrally monitor Steel-Belted Radius using platform tools, in the same manner as you monitor other services on your network.

---

### Release Highlights

#### Release 6.0

Release 6.0 of the Steel-Belted Radius software includes the following changes:

- **Web-delivered SBR Administrator**—The SBR Administrator configuration application is downloaded through a web browser from the Steel-Belted Radius server without requiring a permanent installation. You can download and run instances of SBR Administrator from multiple Steel-Belted Radius servers simultaneously.

- **Operating system changes**—Release 6.0 adds support for RedHat Linux ES/AS version 4.x, SuSE Linux version 10.x, and Windows Vista. Solaris 8 and Windows 2000 are no longer supported.
Oracle 10g—Release 6.0 adds support for Oracle 10g. Note that Steel-Belted Radius interoperates with Oracle 10g by means of the native OCI on Solaris, by means of JDBC on Linux and Solaris, and by means of ODBC on Windows.

Location-based profiles (GEE/SPE only)—Release 6.0 adds support for assigning profiles to users based on the network access device through which the user is accessing a network.

Location groups—Release 6.0 adds support for grouping of network access devices to simplify administration of location and profile rules.

Audit logs—Release 6.0 adds support for administration audit logs that identify administrator logins/logouts, changes made during an administration session, and results of replication attempts.

EAP configuration through SBR Administrator—Release 6.0 adds support for configuration of EAP methods and certificates through the SBR Administrator.

Filter configuration through SBR Administrator—Release 6.0 adds support for management of filters used by tunneled EAP methods and proxy/directed realms (GEE/SPE only) through the SBR Administrator.

Certificate confirmation—Release 6.0 allows an administrator to confirm that a certificate is associated with a user or host through the SBR Administrator.

Support for TLS and AD accounts—On Windows servers, EAP-TLS can verify the presence of a user’s certificate in Active Directory.

Realm scripting and attribute filtering (GEE/SPE only)—A separately licensed scripting module lets you provide scripts that select a realm for processing for a particular request and filter the attributes of a particular request. Scripts can independently query databases and LDAP directories.

CCM improvements—Release 6.0 adds support for replication of all features that do not track resources on the local server.

**Release 5.4**

Release 5.4 of the Steel-Belted Radius software includes changes to the following:

- File permissions for log files (Solaris/Linux)—You can specify user and group file permissions for Steel-Belted Radius log files to control who can read them.

- Address ranges for RADIUS clients—If you have a number of RADIUS clients with contiguous IP addresses, you can define a RADIUS client entry with a range of IP addresses. All clients with addresses in that range, including clients added later, can send RADIUS requests.

- Operating system changes—Steel-Belted Radius supports Solaris 10. Windows NT is no longer supported.

- Optional null terminator in reply attributes—A setting in the radius.ini file controls whether Steel-Belted Radius sends reply attributes of type string without a null terminator.
Simplified CCM upgrades—The procedure for upgrading servers in a Centralized Configuration Management realm is simplified, allowing your primary server to remain the primary throughout.

Master dictionary overrides—By default, inbound proxy responses use the master dictionary when filling in attributes. You can cause the RADIUS client’s dictionary to be used instead, by specifying the UseMasterDictionary parameter in \texttt{radius.ini} or in a \texttt{.pro} or \texttt{.dir} file.

High-resolution timestamps in logs—You can have higher-resolution time stamps in the RADIUS log if you specify \texttt{LogHighResolutionTime = yes} in the \texttt{[Configure]} section of \texttt{radius.ini}.

**Release 5.3**

Release 5.3 of the Steel-Belted Radius software includes the following changes:

- Centralized Configuration Management—Release 5.3 adds support for Centralized Configuration Management (CCM).
- EAP-EOTP and EAP-POTP support—Release 5.3 adds support for the Extensible Authentication Protocol-Extended One-Time Password (EAP-EOTP/EAP-15) and EAP-Protected One-Time Password (EAP-POTP/EAP-32) authentication with the SecurID authentication method.
- Package-based installation—Release 5.3 adds support for package-based installation of the Steel-Belted Radius software.

**Licensing**

If you want to install the Steel-Belted Radius server software for a 30-day evaluation, you do not need a license key.

If you want to install a permanent (non-evaluation) copy of the Steel-Belted Radius server software, you must have a single-seat software license key.

If you have more than one copy of the Steel-Belted Radius server software installed, you must have a site license key, or you must have a separate license key for each installation.

The SBR Administrator can be downloaded to as many workstations as you require. The SBR Administrator does not require a license key.

For details about licensing, please refer to the Steel-Belted Radius license agreement or contact Juniper Networks.

**NOTE:** (GEE/SPE) The Steel-Belted Radius license permits you to configure a total of 10 directed authentication and/or directed accounting methods. If you need additional methods, contact Juniper Networks to purchase blocks of additional licenses.
Chapter 2

Preparing for Installation

This chapter describes the tasks you should complete before you install Steel-Belted Radius.

Review the Release Notes

The Steel-Belted Radius release notes contain important late-breaking information, such as known software problems and documentation corrections. Please review the release notes that accompany your Steel-Belted Radius software before you install or upgrade Steel-Belted Radius to ensure you are informed about important information not found elsewhere.

Select a Server

Select an appropriate host to run the Steel-Belted Radius server software. An appropriate RADIUS server has the following properties:

- Secure physical location – Network security begins with physical security. Without a secure physical location, such as a locked server room, your authentication server’s security can be compromised, resulting in compromises to network security.

- Root access on the host limited to the system administrator – You should restrict logon access to the Steel-Belted Radius server to system administrators and others who need it. Ideally, the server should have no (or few) user accounts.

- Adequate memory and disk space – See “Verify System Requirements” on page 8 for information on hardware and software requirements.

- Administrative interface not accessible from outside your network – If your Steel-Belted Radius server has one network connection, limit access to the ports Steel-Belted Radius uses for configuration and administration.

If your Steel-Belted Radius server has more than one network connection, the network connection used to configure and administer Steel-Belted Radius should be on an administrative network that is physically separate from other networks.
Verify System Requirements

This section describes the hardware and software requirements for running Steel-Belted Radius on the Windows, Solaris, or Linux operating system.

System Requirements – Windows

The Steel-Belted Radius for Windows server software package includes the server software, various dictionary and database files to support authentication, and the SBR Administrator application, which provides an administration user interface.

Table 3: Windows Server – System Requirements

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Windows XP Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td></td>
<td>Windows Vista</td>
</tr>
</tbody>
</table>

Networking

TCP/IP must be configured.
Table 3: Windows Server – System Requirements (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>The Steel-Belted Radius server software requires a host with at least 256 megabytes of working memory (512 megabytes for servers with more than 10,000 RADIUS users.)&lt;br&gt;The SBR Administrator requires a host with at least 256 megabytes of memory.</td>
</tr>
<tr>
<td>Disk space</td>
<td>The Steel-Belted Radius server software requires approximately 40 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system’s product configuration.&lt;br&gt;The SBR Administrator requires approximately 60 megabytes of local disk space.</td>
</tr>
<tr>
<td>Monitor</td>
<td>The SBR Administrator requires a monitor that supports 256+ colors.</td>
</tr>
<tr>
<td>Web browser</td>
<td>SBR Administrator works with the following browsers:&lt;br&gt;■ Microsoft Internet Explorer 6.0, 6.1, or 7.0&lt;br&gt;■ Netscape Navigator 7.x or 8.1&lt;br&gt;■ Mozilla Firefox 1.5 or later&lt;br&gt;Your browser must be running the Java Runtime Environment (JRE) version 1.4.2 or later. You can download JRE software from <a href="http://java.sun.com">http://java.sun.com</a>.&lt;br&gt;Refer to your browser documentation for information on how to install and configure your web browser.</td>
</tr>
<tr>
<td>Database (optional)</td>
<td>The Windows version of Steel-Belted Radius supports any SQL database server that is Open Database Connectivity (ODBC) compliant for RADIUS authentication and accounting. Although Oracle versions 8.0.0, 9.0.0, and 10.0.0 are supported, versions 8.1.7 and 9.2.0 are recommended.&lt;br&gt;If your Steel-Belted Radius server runs on Windows and you use stored procedures, you should use the Oracle 9i client.</td>
</tr>
<tr>
<td>Adobe Reader (optional)</td>
<td>If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation. The free Adobe Reader software can be downloaded from <a href="http://www.adobe.com">http://www.adobe.com</a>. Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software.</td>
</tr>
</tbody>
</table>
Hardware or software firewalls, such as Microsoft Firewall, may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports:

- TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI)
- TCP 1812 – Steel-Belted Radius control port
- TCP 1813 – SBR Administrator port
- UDP 1645 – Legacy RADIUS authentication port
- UDP 1646 – Legacy RADIUS accounting port
- UDP 1812 – IETF RADIUS authentication port
- UDP 1813 – IETF RADIUS accounting port
- UDP port range – Proxy RADIUS source port range (specified in the http://www.juniper.net/customers/support/products/aaa_802/sbr_user.jsp file. Default is 1024–65535.)

To create port exceptions in Windows Firewall, choose Start > Control Panel > Windows Firewall. When the Windows Firewall window opens, click the Exceptions tab, click the Add Port button, and enter the name, port number, and port type for each port you want to include in the exception list.
System Requirements – Solaris

The Steel-Belted Radius for Solaris server software package includes the server
daemon, various dictionary and database files to support authentication, and the
SBR Administrator application, which provides an administration user interface.

Table 4: Solaris Server – System Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Sun UltraSPARC workstation or equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td></td>
</tr>
<tr>
<td>Sun Solaris 9 SPARC Platform Edition 8/03 (or later)</td>
<td></td>
</tr>
<tr>
<td>Sun Solaris 10 SPARC Platform Edition 3/05 (or later)</td>
<td></td>
</tr>
<tr>
<td>The following patches (or better) are required for Solaris 9:</td>
<td></td>
</tr>
<tr>
<td>112963-25 ld.so.1</td>
<td></td>
</tr>
<tr>
<td>111711-16 libc 32-bit</td>
<td></td>
</tr>
<tr>
<td>111712-16 libc 64-bit</td>
<td></td>
</tr>
<tr>
<td>117560-03 libmtsk</td>
<td></td>
</tr>
<tr>
<td>111722-05 libm</td>
<td></td>
</tr>
<tr>
<td>115697-02 mtmalloc</td>
<td></td>
</tr>
<tr>
<td>The following patches (or better) are recommended, but not required, for Solaris 9:</td>
<td></td>
</tr>
<tr>
<td>112785-56 X11 6.6.1: Xsun</td>
<td></td>
</tr>
<tr>
<td>113886-28 OpenGL 1.3 32-bit for J2SE</td>
<td></td>
</tr>
<tr>
<td>113887-28 OpenGL 1.3 64-bit for J2SE</td>
<td></td>
</tr>
<tr>
<td>113096-03 X11 6.6.1: OWconfig for J2SE</td>
<td></td>
</tr>
<tr>
<td>The following patches (or better) are required for Solaris 10:</td>
<td></td>
</tr>
<tr>
<td>120900-04 libzonecfg</td>
<td></td>
</tr>
<tr>
<td>121133-02 zoneadm</td>
<td></td>
</tr>
<tr>
<td>119254-28 patchadd</td>
<td></td>
</tr>
<tr>
<td>119578-22 FMA patch for J2SE</td>
<td></td>
</tr>
<tr>
<td>118822-30 kernel patch for J2SE</td>
<td></td>
</tr>
<tr>
<td>118833-24 kernel patch</td>
<td></td>
</tr>
<tr>
<td>120753-02 libmtsk</td>
<td></td>
</tr>
<tr>
<td>119963-07 libc</td>
<td></td>
</tr>
<tr>
<td>The following patches (or better) are recommended, but not required, for Solaris 10:</td>
<td></td>
</tr>
<tr>
<td>121620-02 MediaLib</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Desktop manager</th>
<th>Gnome2-metacity or CDE-dtwm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>At least 256 megabytes of working memory</td>
</tr>
<tr>
<td></td>
<td>(512 megabytes for servers with more than 10,000 RADIUS users.)</td>
</tr>
<tr>
<td></td>
<td>The SBR Administrator requires a host with at least 256 megabytes of memory.</td>
</tr>
<tr>
<td>Disk space</td>
<td>The Steel-Belted Radius server software requires 325–650 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system’s product configuration.</td>
</tr>
<tr>
<td></td>
<td>The Solaris version of SBR Administrator requires at least 81 megabytes of local disk space.</td>
</tr>
<tr>
<td>Monitor</td>
<td>The SBR Administrator requires a monitor that supports 256+ colors.</td>
</tr>
<tr>
<td>Networking</td>
<td>TCP/IP must be configured.</td>
</tr>
</tbody>
</table>
### Table 4: Solaris Server – System Requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perl</strong></td>
<td>Perl (version 5.8.3 is required if you want to use the auto-restart feature of Steel-Belted Radius. Earlier and later versions of Perl may cause problems. If you install version 5.8.3 of Perl on Solaris, you do not need to overwrite the Sun-supplied version at <code>/usr/bin/perl</code>. However, the first line of the <code>radiusd</code> script must specify the Perl executable that corresponds to version 5.8.3. For example, if Perl 5.8.3 is installed as <code>/usr/local/bin/perl</code>, then the first line of the <code>radiusd</code> script must specify <code>#!/usr/local/bin/perl</code>.</td>
</tr>
<tr>
<td><strong>Database (optional)</strong></td>
<td>The Solaris version of Steel-Belted Radius supports any SQL database server that is Open Database Connectivity (ODBC) compliant for RADIUS authentication and accounting. Although Oracle versions 8.0.0, 9.0.0, and 10.0.0 are supported, versions 8.1.7, 9.2.0 and 10.2.0 are recommended. Oracle 10 typically requires a patch for Oracle bug 4516865 to correct the installed Oracle file access modes. The JDBC plug-in has been tested with MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.</td>
</tr>
</tbody>
</table>
| **Web browser** | SBR Administrator works with the following browsers on all Solaris versions:  
- Mozilla Firefox 1.5–1.7 and 2.0  
- Netscape Navigator 6.00, 7.x, and 8.1  
Additionally, SBR Administrator works with the following browser on Solaris 10:  
- Mozilla 1.7  
Your browser must be running the Java Runtime Environment (JRE) version 1.4.2 or later. You can download JRE software from [http://java.sun.com](http://java.sun.com). Refer to your browser documentation for information on how to install and configure your web browser. |
| **Adobe Reader (optional)** | If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation and have an appropriate value specified in your PATH variable. The free Adobe Reader software can be downloaded from [www.adobe.com](http://www.adobe.com). Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software. |
| **Firewall (optional)** | Hardware or software firewalls may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports:  
- TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI)  
- TCP 1812 – Steel-Belted Radius control port  
- TCP 1813 – SBR Administrator port  
- UDP 1645 – Legacy RADIUS authentication port  
- UDP 1646 – Legacy RADIUS accounting port  
- UDP 1812 – IETF RADIUS authentication port  
- UDP 1813 – IETF RADIUS accounting port  
- UDP port range – Proxy RADIUS source port range (specified in the `radius.ini` file. Default is 1024–65535.) |
System Requirements – Linux

The Steel-Belted Radius for Linux server software package includes the server daemon, various dictionary and database files to support authentication, and the SBR Administrator application, which provides an administration user interface.

Table 5: Linux Server – System Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Intel X86 workstation or server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>SuSE Linux Enterprise Server 9.0 or 10</td>
</tr>
<tr>
<td></td>
<td>RedHat Enterprise Linux ES 3.0 or 4.0</td>
</tr>
<tr>
<td></td>
<td>RedHat Enterprise Linux AS 3.0 or 4.0</td>
</tr>
<tr>
<td></td>
<td>The server must run glibc 2.3.2 or 2.3.3, which is present by default in the supported versions of SuSE and RedHat Linux.</td>
</tr>
<tr>
<td>Memory</td>
<td>At least 256 megabytes of working memory</td>
</tr>
<tr>
<td></td>
<td>(512 megabytes for servers with more than 10,000 RADIUS users.)</td>
</tr>
<tr>
<td></td>
<td>The SBR Administrator requires a host with at least 256 megabytes of memory.</td>
</tr>
<tr>
<td>Disk space</td>
<td>The Steel-Belted Radius server software requires 235–470 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system’s product configuration.</td>
</tr>
<tr>
<td></td>
<td>The Linux version of SBR Administrator requires at least 88 megabytes of local disk space.</td>
</tr>
<tr>
<td>Monitor</td>
<td>The SBR Administrator requires a monitor that supports 256+ colors.</td>
</tr>
<tr>
<td>Networking</td>
<td>TCP/IP must be configured.</td>
</tr>
<tr>
<td>Perl</td>
<td>Perl (version 5.8.3) is required if you want to use the auto-restart feature of Steel-Belted Radius. Earlier and later versions of Perl may cause problems.</td>
</tr>
<tr>
<td></td>
<td>The first line of the \texttt{radiusd} script must specify the Perl executable that corresponds to version 5.8.3. For example, if Perl 5.8.3 is installed as \texttt{/usr/local/bin/perl}, then the first line of the \texttt{radiusd} script must specify: \texttt{#!/usr/local/bin/perl}.</td>
</tr>
<tr>
<td>Database (optional)</td>
<td>The server must not have a BTrieve server. Steel-Belted Radius installs its own BTrieve server, which is not accessible to other processes.</td>
</tr>
<tr>
<td></td>
<td>The JDBC plug-in has been tested with MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.</td>
</tr>
</tbody>
</table>
Table 5: Linux Server – System Requirements (continued)

<table>
<thead>
<tr>
<th>Web browser (optional)</th>
<th>SBR Administrator works with the following browsers on all Linux platforms:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Mozilla Firefox 1.5–1.7 and 2.0</td>
</tr>
<tr>
<td></td>
<td>■ Netscape Navigator 6.00, 7.x, and 8.1</td>
</tr>
<tr>
<td></td>
<td>Additionally, SBR Administrator works with the following browsers on the</td>
</tr>
<tr>
<td></td>
<td>indicated platforms:</td>
</tr>
<tr>
<td></td>
<td>■ Konqueror 3.4 (Red Hat Linux ES and AS 5)</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 1.0 (Red Hat Linux ES and AS 4)</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla 1.6 (SuSE Linux 9)</td>
</tr>
<tr>
<td></td>
<td>■ Mozilla Firefox 1.0 (SuSE 10)</td>
</tr>
<tr>
<td></td>
<td>■ Konqueror 3.4 (SuSE 10)</td>
</tr>
<tr>
<td></td>
<td>Your browser must be running the Java Runtime Environment (JRE)</td>
</tr>
<tr>
<td></td>
<td>version 1.4.2 or later. You can download JRE software from</td>
</tr>
<tr>
<td></td>
<td>Refer to your browser documentation for information on how to install</td>
</tr>
<tr>
<td></td>
<td>and configure your web browser.</td>
</tr>
</tbody>
</table>

| Adobe Reader (optional) | If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation and have an appropriate value specified in your PATH variable. The free Adobe Reader software can be downloaded from www.adobe.com. Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software. |

<table>
<thead>
<tr>
<th>Firewall (optional)</th>
<th>Hardware or software firewalls may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI)</td>
</tr>
<tr>
<td></td>
<td>■ TCP 1812 – Steel-Belted Radius control port</td>
</tr>
<tr>
<td></td>
<td>■ TCP 1813 – SBR Administrator port</td>
</tr>
<tr>
<td></td>
<td>■ UDP 1645 – Legacy RADIUS authentication port</td>
</tr>
<tr>
<td></td>
<td>■ UDP 1646 – Legacy RADIUS accounting port</td>
</tr>
<tr>
<td></td>
<td>■ UDP 1812 – IETF RADIUS authentication port</td>
</tr>
<tr>
<td></td>
<td>■ UDP 1813 – IETF RADIUS accounting port</td>
</tr>
<tr>
<td></td>
<td>■ UDP port range – Proxy RADIUS source port range (specified in the radius.ini file. Default is 1024–65535.)</td>
</tr>
</tbody>
</table>
Verify Network Connectivity

Use the ping command to verify that the server on which you are going to install Steel-Belted Radius can communicate with other devices, such as remote access servers, database servers, DHCP servers, DNS servers, and management workstations, on your network, over your TCP/IP network.

C:\> ping 192.168.12.54

Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255

If the ping command fails, verify that the IP address of the remote host is correct, that the remote host is operational, and that all routers between your server and the remote host are operational.

Verify Host Name Resolution

The server on which you are going to install Steel-Belted Radius must have a stable, accessible IP address that is mapped in /etc/hosts or the Domain Name System (DNS) server to a resolvable hostname.

To verify that the server has a resolvable hostname, use the ping command with the server’s hostname:

C:\> ping foo.juniper.net

Pinging foo.juniper.net [192.168.12.21] with 32 bytes of data:
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255

Verify Administrator Account Access

You must have administrator (Windows)/root (Solaris/Linux) access to the server on which you are going to install the Steel-Belted Radius server software.
Obtain a Server License Number

If you want to install the Steel-Belted Radius server software for a 30-day evaluation, you do not need a license number.

If you want to install a single permanent (non-evaluation) copy of Steel-Belted Radius, you must have a single-seat software license number.

If you have more than one copy of the Steel-Belted Radius software installed, you must have a site license number or you must have a separate license number for each installation.

The SBR Administrator can be installed on as many workstations as you require. The SBR Administrator does not require a license number.

For details about licensing, please refer to the Steel-Belted Radius license agreement or contact Juniper Networks.
Chapter 3

Windows Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software or the SBR Administrator configuration application on a Windows domain controller, server, or workstation.

Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see “System Requirements – Windows” on page 8.

- If you are upgrading an existing installation, back up your root and server certificates, and verify you know the password for your server certificate.

- Microsoft IAS (Internet Authentication Service) cannot be configured on the same server as Steel-Belted Radius. If Microsoft IAS is running on the server on which you are planning to install Steel-Belted Radius, disable it.

- The Steel-Belted Radius service should run under a local account. By default, Steel-Belted Radius runs as a local system account. If you change this, Windows domain authentication is disabled.

Installing the Steel-Belted Radius Server Software

To install the Steel-Belted Radius server software on a Windows server:

1. Log on to the Windows server as an administrator.

2. Specify whether you want to run the Steel-Belted Radius server software installation from a CD or from a network server.

   - CD-ROM installation – If you want to install the Steel-Belted Radius server software from a CD, insert the Steel-Belted Radius installation disk, choose Start > Run, and enter the drive letter and setup command:

     D:\setup

- Network installation – Locate and run the Steel-Belted Radius Windows Installer Package (Steel-Belted Radius.msi file) from a network server, or copy the file to your computer and run it locally.

3. When the Welcome window opens, click Next to continue.

4. When the Customer Information window opens, enter your customer information.
   - Enter your user name in the User Name field.
   - Enter the name of your company in the Organization field.
   - If you are installing a purchased copy of the Steel-Belted Radius server, enter the license number printed on your license agreement card in the Serial Number field.
   - If you are installing an evaluation copy of the Steel-Belted Radius server, leave the Serial Number field blank and check the Install 30-day trial checkbox.

   Click Next to continue.

5. If you checked the Install 30-day trial checkbox in 4., use the Select Server Type window to specify which edition of the Steel-Belted Radius server software you want to install.

   The Steel-Belted Radius server software is available in three editions:
   - Global Enterprise Edition (GEE)
   - Service Provider Edition (SPE)
   - Enterprise Edition (EE) (with optional LDAP Configuration Interface support)

   Click Next to continue.

6. When the License Agreement window opens, read the agreement, click the I accept the terms in the license agreement radio button, and click Next to continue.

7. When the Custom Setup window appears, specify whether you want to change the default settings for installing Steel-Belted Radius.

   By default, the Steel-Belted Radius software and documentation is installed in the C:\Program Files\Juniper Networks\Steel-Belted Radius\Service directory. If you want to install the Steel-Belted Radius server software to a directory other than the default, click the Change button and specify your custom installation settings.

   Click Next to continue.
If you are updating an existing Steel-Belted Radius installation, a window identifies the location where your current files will be archived. Click Next to continue.

8. When the Windows Account window opens, enter your Windows administrator account name in the Account field. Click Next to continue.

The Windows account information you enter is the default login account for SBR Administrator. You must use this account name the first time you log into SBR Administrator.

NOTE: Make sure the login account you specify has a password. If a user without a password is specified as the administrator, the user will not be able to log into the SBR Administrator application.

9. When the Select Server Edition window opens, specify whether you want to install a standalone server, a primary server, or a replica server.

- If you click the Install as Standalone SBR Server button, you do not need to specify replication information.

- If you click the Install as Primary SBR Server button and click Next, you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter the replication secret in the Primary Server Secret and Re-enter Secret fields and click Next to continue.

- If you click the Install as Replica SBR Server button and click Next, you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
  - If you want to browse for a replication package on your computer or network, click the Browse for replica package button, click the Browse button, and navigate to the directory containing the replica.ccmpkg file.
  - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), click the Provide Primary Server data button, and specify the name, IP address(es), and replication secret of the primary server.

Click Next to continue.

10. When the Start Services window opens, check the Yes, start the Steel-Belted Radius service checkbox if you want the Steel-Belted Radius service to start immediately. Click Next to continue.
11. If you want to register the Steel-Belted Radius server as an Agent Host with an RSA SecurID server, check the Yes, I’d like to register checkbox, click the Browse button, and navigate to the directory containing the sdconf.rec, radius.cer, server.cer, server.key, and failover.dat files.

**NOTE:** When you register your Steel-Belted Radius master or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

12. When the Ready to Install window opens, click Install to begin the installation.

As the installation proceeds, the Installation Status window displays your progress.

13. When the Setup Complete window opens, check the Show the readme file checkbox if you want to review the release notes for the Steel-Belted Radius server software.

Click Finish.

You must now finish configuring the new Steel-Belted Radius server to suit your network’s authentication and accounting needs. For example, you can edit the [Addresses] section of the radius.ini file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the Steel-Belted Radius Reference Guide for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS service. Refer to “Starting the Steel-Belted Radius Service” on page 29 for information on starting the RADIUS service. Refer to the Steel-Belted Radius Administration Guide for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

### Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Juniper Networks website. If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator program and connect to your Steel-Belted Radius server.

3. Choose File > License.
4. When the Add a License for Server window opens, enter your license number and click **OK**.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.

5. Click **OK** to close the confirmation window.

6. Restart your Steel-Belted Radius server.

   The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number.

Refer to the *Steel-Belted Radius Administration Guide* for information on using SBR Administrator.

---

### Upgrading from Steel-Belted Radius Version 4.x

Upgrading Steel-Belted Radius requires that you back up your Steel-Belted Radius files, install the new Steel-Belted Radius server software, and then merge your old configuration files (such as *.ini and *.aut) with the new configuration files.

When you install the new Steel-Belted Radius server software, your database configuration is preserved for use with the upgraded server software. The installer moves your current configuration files from the C:\Radius\Service directory to a backup subdirectory.

Perform the following steps to upgrade your Steel-Belted Radius software from version 4.x to version 6.0:

1. Export everything in your Steel-Belted Radius (version 4.x) database to a RADIUS Import Format (.rif) file.

   Refer to the *Steel-Belted Radius Administration Guide (version 4.x)* for information on how to export your Steel-Belted Radius database to a .rif file.

   **NOTE:** Before you can import your database information from a .rif file into Steel-Belted Radius (version 5.x and 6.0), you must run the rif2xml.exe utility to convert your .rif file to .xml format. For information on the rif2xml.exe utility, see Appendix A, “RIF2XML Conversion Utility.”

2. Back up your \radiusdir directory and the exported .rif file to an archive location.

3. Verify that you have your Steel-Belted Radius version 6.0 license number.

4. Close all applications running on your Steel-Belted Radius server.
5. Uninstall the Steel-Belted Radius version 4.x software.
   a. Choose Start > Control Panel > Add or Remove Programs.
   b. When the Add or Remove Programs window opens, select Steel-Belted Radius.
   c. Click Remove.
   d. When a window asking you to confirm you want to remove Steel-Belted Radius opens, click Yes.
   e. After the control panel indicates the Steel-Belted Radius server software has been uninstalled, archive or delete files remaining in the C:\Radius\Service directory.

6. Install the Steel-Belted Radius version 6.0 server software on your server.
   When the Start Services window in the installer opens, uncheck the Yes, start the Steel-Belted Radius service checkbox to indicate you do not want the Steel-Belted Radius service to start. Click Next to continue.
   For more information, see “Installing the Steel-Belted Radius Server Software” on page 17.

   **NOTE:** Do not cancel the Steel-Belted Radius installer after you start running it. Doing so may result in a loss of data.

7. Export your Steel-Belted Radius (version 6.0) database to an Extensible Markup Language (.xml) file.
   Refer to the Steel-Belted Radius Administration Guide (version 6.0) for information on how to export your Steel-Belted Radius database to a .xml file.

8. Back up your \radiusdir directory and the exported .xml file to an archive location.
   This step ensures that you have a clean copy of the Steel-Belted Radius (version 6.0) configuration files in the event you need them.

9. Copy your backed-up configuration files (*.ini, *.aut, *.dir, *.pro, *.rr, *.eap) to C:\Program Files\Juniper Networks\Steel-Belted Radius\Service or merge the settings from your backed-up configuration files into the new Steel-Belted Radius configuration files.
   The configuration files installed as part of Steel-Belted Radius version 6.0 include settings that were not present in earlier versions.
   - If you want to preserve your previous settings (and if you want to use the default values for settings introduced in previous versions of Steel-Belted Radius), you can copy your archived configuration files to C:\Program Files\Juniper Networks\Steel-Belted Radius\Service, replacing the newly installed versions of those files.
If you want to use non-default settings for features introduced in previous versions of Steel-Belted Radius, you must merge the settings from your archived configuration files with the settings in the new configuration files.

**NOTE:** Do not merge the settings from the archived version of the eap.ini file to the newly installed default eap.ini file. Use SBR Administrator to apply the EAP settings you were using before the upgrade.

Refer to the Steel-Belted Radius Reference Guide for information on the settings contained in each configuration file.

10. Copy your \certs directory, which contains your server certificate files, from the backup directory to the C:\Program Files\Juniper Networks\Steel-Belted Radius\Service directory.

11. If you added your own dictionaries or modified the default Steel-Belted Radius dictionaries, re-add your custom dictionaries or modify the dictionaries installed with the Steel-Belted Radius version 6.0 software as appropriate.

12. Restart the Steel-Belted Radius service.

    Choose Start > Control Panel > Administrative Tools > Services. Choose the Steel-Belted Radius entry. Click Restart the service.

13. Run SBR Administrator and verify your configuration settings are complete and correct.

---

**Upgrading from Steel-Belted Radius Version 5.x**

Upgrading Steel-Belted Radius requires that you back up your Steel-Belted Radius files, install the new Steel-Belted Radius server software, and then merge your old configuration files (*.ini, *.aut, *.dir, *.pro, *.rr, *.eap) with the new configuration files.

When you install the new Steel-Belted Radius server software, your database configuration is preserved for use with the upgraded server software. The installer moves your current configuration files from the \Radius\Service directory to a backup subdirectory.

Perform the following steps to upgrade your Steel-Belted Radius software from version 5.3 or 5.4 to version 6.0:

1. Export your Steel-Belted Radius database to an Extensible Markup Language (.xml) file.

    Refer to the Steel-Belted Radius Administration Guide for information on how to export your Steel-Belted Radius database to a .xml file.

2. Back up your \radiusdir directory and the exported .xml file to an archive location.
The Steel-Belted Radius installer backs up your files and database when it runs. The file archive created in this step ensures that your configuration is preserved in the event the installer fails before it finishes running.

3. Verify that you have your Steel-Belted Radius version 6.0 license number.

4. Close all applications running on your Steel-Belted Radius server.

   You do not need to stop the Steel-Belted Radius service when you upgrade the Steel-Belted Radius server software.

5. Install the Steel-Belted Radius version 6.0 server software on your server.

   When the Start Services window in the installer opens, uncheck the **Yes, start the Steel-Belted Radius service** checkbox to indicate you do not want the Steel-Belted Radius service to start. Click **Next** to continue.

   After the Steel-Belted Radius installer finishes running, the configuration and dictionary files that were in `\Radius\Service` are backed up in a new `C:\Program Files\Juniper Networks\Steel-Belted Radius\Service_Date_IDnumber` directory.

   For more information, see “Installing the Steel-Belted Radius Server Software” on page 17.

---

**NOTE:** Do not cancel the Steel-Belted Radius installer after you start running it. Doing so may result in a loss of data.


   This step ensures that you have a clean copy of the Steel-Belted Radius database files (version 6.0) in the event you need them.

   Refer to the *Steel-Belted Radius Administration Guide* for information on how to export your Steel-Belted Radius database to a .xml file.

7. Back up your `\radiusdir` directory and the exported .xml file to an archive location.

   This step ensures that you have a clean copy of the Steel-Belted Radius configuration files (version 6.0) in the event you need them.

8. Copy your backed-up configuration files (*.ini, *.aut, *.dir, *.pro, *.rr, *.eap) to `C:\Program Files\Juniper Networks\Steel-Belted Radius\Service` or merge the settings from your backed-up configuration files into the new Steel-Belted Radius configuration files.

   The configuration files installed as part of Steel-Belted Radius version 6.0 include settings that were not present in earlier versions.
If you want to preserve your previous settings (and if you want to use the default values for settings introduced in version 6.0 of Steel-Belted Radius), you can copy your archived configuration files to `C:\Program Files\Juniper Networks\Steel-Belted Radius\Service`, replacing the newly installed versions of those files.

If you want to use non-default settings for features of Steel-Belted Radius, you must merge the settings from your archived configuration files with the settings in the new configuration files.

**NOTE:** Do not merge the settings from the archived version of the `eap.ini` file to the newly installed default `eap.ini` file. Use SBR Administrator to apply the EAP settings you were using before the upgrade.

Refer to the Steel-Belted Radius Reference Guide for information on the settings contained in each configuration file.

9. If you added your own dictionaries or modified the default Steel-Belted Radius dictionaries, re-add your custom dictionaries or modify the dictionaries installed with the Steel-Belted Radius version 6.0 software as appropriate.

10. Restart the Steel-Belted Radius service.

    Choose **Start > Control Panel > Administrative Tools > Services**. Choose the **Steel-Belted Radius** entry. Click **Restart the service**.

11. Run SBR Administrator and verify that your configuration settings are complete and correct.

---

**Upgrading from RSA RADIUS Server Version 6.1**

This section describes how to upgrade servers running RSA RADIUS Server version 6.1 in a replication environment and how to upgrade a standalone server running RSA RADIUS Server version 6.1.

**Upgrading in a Replication Environment**

In environments that use replication (primary and replica servers), you must upgrade your replica servers, install SBR Administrator, and then upgrade your former primary server.

**Upgrade Your Replica Servers**

You must install and configure your replica RADIUS servers before you install and configure your primary server. Perform the following steps for each replica RADIUS server in your replication realm.

1. Use the Services Control Panel to stop the RSA RADIUS Server service on the replica server.
To open the Services Control Panel, choose **Start > Control Panel > Administrative Tools > Services**. Select the **RSA RADIUS Server** entry and click **Stop the service**.

2. Install the Steel-Belted Radius server software on your replica RADIUS server.

When you run the installer, click the **Install as Replica SBR Server** button and specify how the replica server can locate the replica package containing the replica server’s Steel-Belted Radius replication settings. When prompted, confirm that you are upgrading from an existing replica.

See “Installing the Steel-Belted Radius Server Software” on page 17 for information on how to install the Steel-Belted Radius server software.

---

**NOTE:** When the installer prompts you for a license number, enter your Steel-Belted Radius version 6.0 license number. You cannot use an evaluation license to upgrade from RSA RADIUS Server to Steel-Belted Radius.

---

When you run the installer, your RSA RADIUS Server configuration files are copied to an archive directory. The default location for the archive directory is **C:\Program Files\RSA Security**.

3. Merge the settings from your archived configuration files with the settings in the newly-installed default configuration files on your replica server.

The default location for server files is **C:\Program Files\Juniper Networks\Steel-Belted Radius\Service**.

Do not replace the new configuration files with your old ones, since your new files may include settings for functions that were not available in the RSA RADIUS Server software.

---

**NOTE:** Do not merge the settings from the archived version of the **eap.ini** file to the newly installed default **eap.ini** file. The **eap.ini** is updated by replication and should be configured with SBR Administrator only on the primary server.

---

4. Use a text editor to configure the **Enable=1** setting for the **.aut** file, associated with each authentication method you want to use.

Refer to the **Steel-Belted Radius Administration Guide** for information about authentication methods.

5. Use the Services Control Panel to start the RSA RADIUS Server service on the replica server.

To open the Services Control Panel, choose **Start > Control Panel > Administrative Tools > Services**. Select the **RSA RADIUS Server** entry and click **Start the service**.
6. Publish a new configuration package from the primary RADIUS server to the modified replica.

Publishing a configuration package after you upgrade each replica RADIUS server ensures that the modified replica has the appropriate configuration settings.

Repeat Steps 1–6 for each replica server before upgrading your primary server.

**Upgrade Your Primary Server**

You must install and configure your replica RADIUS servers before you install and configure your primary server. Perform the following steps to upgrade your primary RADIUS server.

1. Use the Services Control Panel to stop the RSA RADIUS Server service on the primary server.

   To open the Services Control Panel, choose Start > Control Panel > Administrative Tools > Services. Select the RSA RADIUS Server entry and click Stop the service.

2. Install the Steel-Belted Radius server software on your primary RADIUS server.

   When you run the installer, click the Install as Primary SBR Server button and specify how the primary server can locate the package containing the Steel-Belted Radius replication settings. When prompted, confirm that you are upgrading from an existing primary server.

   See “Installing the Steel-Belted Radius Server Software” on page 17 for information on how to install the Steel-Belted Radius server software.

   **NOTE:** When the installer prompts you for a license number, enter your Steel-Belted Radius version 6.0 license number. You cannot use an evaluation license to upgrade from RSA RADIUS Server to Steel-Belted Radius.

   When you run the installer, your RSA RADIUS Server configuration files are copied to an archive directory. The default location for the archive directory is C:\Program Files\RSA Security\service_yymmdd_hhmmss.

3. Merge the settings from your archived configuration files with the settings in the newly-installed default configuration files on your primary server.

   The default location for server files is C:\Program Files\Juniper Networks\Steel-Belted Radius\Service.

   Do not replace the new configuration files with your old ones, since your new files may include settings for functions that were not available in the RSA RADIUS Server software.

   **NOTE:** Do not merge the settings from the archived version of the eap.ini file to the newly installed default eap.ini file. The eap.ini is updated by replication and should be configured with SBR Administrator only on the primary server.
4. Use a text editor to configure the `Enable=1` setting for the `.aut` file associated with each authentication method you want to use. Refer to the Steel-Belted Radius Administration Guide for information about authentication methods.

5. Use the Services Control Panel to restart the Steel-Belted Radius service on the replica server.

6. Publish a new configuration package from the upgraded primary RADIUS server. Publishing a configuration package ensures that all replica servers have the appropriate configuration settings.

---

### Restoring a Previous Configuration

When you install the Steel-Belted Radius server software, the installation script saves your existing configuration to a backup directory to preserve your configuration settings. If you are re-installing the same version and edition of Steel-Belted Radius on a server, you can copy the configuration files from the backup directory to the Steel-Belted Radius server directory to restore your previous configuration.

If you are upgrading your Steel-Belted Radius software from an older version, do not copy your configuration files to the Steel-Belted Radius server directory. For more information, see “Upgrading from Steel-Belted Radius Version 4.x” on page 21 or “Upgrading from Steel-Belted Radius Version 5.x” on page 23, as appropriate.

---

### Stopping the Steel-Belted Radius Service

After the Steel-Belted Radius service is installed on a Windows server, it stops and starts automatically each time you shut down or restart the server. You can stop the Steel-Belted Radius service at any time by performing the following steps:

1. Choose **Start > Control Panel > Administrative Tools > Services**.

2. When the Services window opens, click the **Steel-Belted Radius** entry.

3. Click the **Stop the service** button.
Starting the Steel-Belted Radius Service

You must restart the Steel-Belted Radius service after you modify configuration files. To start the Steel-Belted Radius server after it has been stopped:

1. Choose **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. When the Services window opens, click the **Steel-Belted Radius** entry.
3. Click the **Start the service** button.

To restart the Steel-Belted Radius server without stopping it:

1. Choose **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. When the Services window opens, click the **Steel-Belted Radius** entry.
3. Click the **Restart the service** button.
Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see “System Requirements – Solaris” on page 11.

- Make sure that you are (or have access to) a system administrator and someone who understands your RADIUS authentication and accounting requirements.

- If you are installing the optional SNMP module, stop all SNMP agents running on your server.

---

**NOTE:** If your server runs SNMP agents other than the one supplied with Steel-Belted Radius, you must coordinate the port numbers used by your SNMP agents to avoid port contention.
Upgrade Files

The install, configure, and uninstall scripts for Steel-Belted Radius version 6.0 automatically archive your Steel-Belted Radius files to the `/radius/install/backups` directory. To facilitate future software upgrades, the install, configure, and uninstall scripts create a number of `.dat` files in the `/radius/install` directory. These files store information used for future upgrades. You should not move, rename, or otherwise modify these files.

Table 6: Upgrade Files and Directories

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/radius/install/package.dat</code></td>
<td>Contains a unique package identifier.</td>
</tr>
<tr>
<td><code>/radius/install/preinstall.dat</code></td>
<td>Contains the absolute pathname of the backup directory for your old Steel-Belted Radius software and configuration files (pre-installation backup).</td>
</tr>
<tr>
<td><code>/radius/install/install.dat</code></td>
<td>Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.0 software and configuration files, as shipped without modification (post-installation backup).</td>
</tr>
<tr>
<td><code>/radius/install/upgrade.dat</code></td>
<td>Contains the absolute pathname of the Steel-Belted Radius version 6.0 upgrade source (if any).</td>
</tr>
<tr>
<td><code>/radius/install/configure.dat</code></td>
<td>Contains configuration state data.</td>
</tr>
<tr>
<td><code>/radius/install/uninstall.dat</code></td>
<td>Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.0 software and working configuration files (pre-uninstall backup).</td>
</tr>
<tr>
<td><code>/radius/install/backups/</code></td>
<td>Contains the backups referenced by the .dat files.</td>
</tr>
</tbody>
</table>

Package Management Commands

Table 7 lists useful Solaris package management commands.

Table 7: Useful Package Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkginfo -x</td>
<td>egrep &quot;FUNK</td>
</tr>
<tr>
<td>pkginfo -l JNPRsbrge</td>
<td>Report high level description for specified package</td>
</tr>
<tr>
<td>pkginfo -r JNPRsbrge</td>
<td>Show installed directory</td>
</tr>
<tr>
<td>pkgadd -d /path/to/JNPRsbrge.sol.pkg [-a none] JNPRsbrge.sol.pkg</td>
<td>Install [at specified /path]</td>
</tr>
<tr>
<td>pkgrm JNPRsbrge</td>
<td>Uninstall Steel-Belted Radius.</td>
</tr>
</tbody>
</table>
Installing the Steel-Belted Radius Server Software

The installer for the Solaris version of the Steel-Belted Radius server software uses **pkgadd** files, which have filenames that include the edition and version of the server software.

This section assumes that you are installing Steel-Belted Radius on your Solaris server for the first time or that you are installing Steel-Belted Radius in a directory other than the one used by previous installations (clean installation). If you are upgrading an existing Steel-Belted Radius installation to version 6.0, refer to “Upgrading from Steel-Belted Radius Version 4.x” on page 40 or “Upgrading from Steel-Belted Radius Version 5.x” on page 41 for information on upgrade options and considerations.

To install the Steel-Belted Radius server software on a Solaris server:

1. Log into the Solaris server as root.

2. Copy the Steel-Belted Radius installation files to the Solaris server.

   Copy the files from the `/solaris` directory on the installation CD-ROM to a local or remote hard disk partition that is readable by root.

   The following example copies the files to the `/opt/JNPRsbr/temp` directory.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/solaris/* /opt/JNPRsbr/temp
   ```

3. Uncompress the Steel-Belted Radius installation package.

   ```
   # gunzip -dc JNPRsbrXX.sol.pkg.tgz | tar xf -
   ```

   where **XX** specifies the version of Steel-Belted Radius you want to install:

   - **ge** – Steel-Belted Radius/Global Enterprise Edition (JNPRsbrge)
   - **sp** – Steel-Belted Radius/Service Provider Edition (JNPRsbrsp)
   - **ee** – Steel-Belted Radius/Enterprise Edition (JNPRsbree)

   **NOTE:** If extraneous error messages similar to the following appear in your console window when you insert the installation CD-ROM, you should ignore them:

   ```
   rigel does not conform to the ISO-9660 specification:
   rigel hsfs: file len greater than max allowed
   rigel hsfs: Due to this error, the file system may not be correctly interpreted.
   rigel hsfs: Other such errors in this file system will be silently ignored.
   ```
4. Run the installer package.

   ```bash
   # pkgadd -d directory -a none JNPRsbrXX.sol.pkg
   ```

   where `directory` specifies the directory where you placed the installation package and `XX` specifies the version of Steel-Belted Radius you want to install.

   ```bash
   # pkgadd -d /export/home/carter/sbr -a none JNPRsbrge.sol.pkg
   ```

   Processing package instance `<JNPRsbrge.sol.pkg>` from
   ```bash
   /export/home/carter/sbr
   ```

   JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)
   (sparc) 6.0.0000
   (C) Copyright 1996-2007 Juniper Networks, Inc. See license.txt

5. Specify the base directory in which you want to install the Steel-Belted Radius files.

   By default, the installation package puts the Steel-Belted Radius files in the `/opt/JNPRsbr/` base directory.

   Enter path to package base directory [?,q] `/opt/JNPRsbr`

   The selected base directory `/opt/JNPRsbr` must exist before installation is attempted.
   Do you want this directory created now [y,n,?,q] y
   Using `/opt/JNPRsbr` as the package base directory.
   ## Processing package information.
   ## Processing system information.
   ## Verifying disk space requirements.
   ## Checking for conflicts with packages already installed.
   ## Checking for setuid/setgid programs.

6. When you are prompted to confirm you want to install the package, enter y.

   This package contains scripts which will be executed with super-user permission during the process of installing this package.
   Do you want to continue with the installation of `<JNPRsbrge>` [y,n,?] y

   Installing JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition) as `<JNPRsbrge>`

   ## Executing preinstall script.
   ## Installing part 1 of 1.
   :.
   ## Executing postinstall script.

   Newly installed server directory will be backed up as:
   `/opt/JNPRsbr/radius/install/backups/2006:12:15-06:39:56`
   Installation of `<JNPRsbrge>` was successful.

7. Navigate to the directory where you installed Steel-Belted Radius.

   ```bash
   # cd /opt/JNPRsbr/radius/install
   ```
8. Execute the following command to run the configuration script for the Steel-Belted Radius server software:

```
# ./configure
```

9. Review the Steel-Belted Radius license agreement.

Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter y

```
Do you accept the terms in the license agreement? [n] y
```

10. Indicate whether you have a license for your Steel-Belted Radius software.

You can enter a license string or use a one-time 30 day trial license.

Would you like to enter a license string? [n]

Installed a 30 day evaluation license.

- If you purchased Steel-Belted Radius, type y and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

- If you do not have a license number, type n and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product’s full feature set for a limited period.

11. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

```
Do you wish to enable LCI? [n]
License does not have LCI support.
```

12. Specify whether you are upgrading an existing Steel-Belted Radius installation or configuring a new installation.

- Enter n if you are performing a new installation.

- Enter the directory path to the Steel-Belted Radius files if you are upgrading an existing Steel-Belted Radius installation and you know the name of the current Steel-Belted Radius directory.

- Enter s if you are upgrading an existing Steel-Belted Radius installation and you want to search for the Steel-Belted Radius directory.

```
Please enter backup or radius directory from which to upgrade.
Enter n for new configuration, s to search, or q to quit.
[n] n
```
13. Specify that you do not want to remove older versions of Steel-Belted Radius.

    WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.

    Manually remove pre-existing software now? [y]: n

14. Specify the login name of the initial Steel-Belted Radius administrator.

    The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

    Enter initial admin user (account must have an associated password) [root]:

    **NOTE:** Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

15. Specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

    Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: sa

    - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

      If appropriate, enter y when you are asked whether you are upgrading a primary server. Doing so tells the installer to preserve the server’s replication realm information.

    - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica.ccmpkg configuration package containing your Steel-Belted Radius replication settings.

      - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.

      - If you want to specify the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address, and replication secret of the primary server.

      If appropriate, enter y when you are asked whether you are upgrading a replica server. Doing so tells the installer to preserve the replica server’s replication settings.

    - If you enter sa (standalone RADIUS server), you do not need to specify replication information.
16. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

- If you do not want to configure Steel-Belted Radius for use with an external LDAP data service, press Enter.
- If you want to configure Steel-Belted Radius for use with an external LDAP data service, type y and press Enter. You are prompted to enter the path for the LDAP library files:

  Do you want to configure LDAP? [n]: y
  Enter path for LDAP library files [/usr/lib]:

  To accept the default path (/usr/lib), press Enter.

17. Specify whether you want to configure Steel-Belted Radius for use with an Oracle database.

   Configuring for use with generic database
   Do you want to configure for use with Oracle? [n]:

   If no, press Enter.
   If yes, type y and press Enter. You are prompted to version and path information for the Oracle library files.

   Configuring for use with Oracle.
   Supported Oracle version: 8, 9, 10
   What version of Oracle will be used? [9] 10
   Configuring for use with Oracle 10
   Setting the environment variable ORACLE_HOME.
   Enter ORACLE_HOME [:] /opt/10g/app/oracle/product/10.1.0
   Setting the environment variable LD_LIBRARY PATH.
   Enter path for Oracle shared libraries
   [/opt/10g/app/oracle/product/10.1.0/lib32]:
   Setting the environment variable TNS_ADMIN.
   Enter TNS_ADMIN [/opt/10g/app/oracle/product/10.1.0/network/admin]:

   NOTE: Steel-Belted Radius requires that you use the Oracle 10 32-bit executables, which are stored in the /lib32 directory. Steel-Belted Radius is not compatible with the Oracle 10 64-bit executables stored in the /lib directory.

18. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can to monitor your Steel-Belted Radius server from an SNMP management station.

   Do you want to configure SNMP? [n]:

   If no, press Enter to proceed to the next prompt.
   If yes, type Y and press Enter. The installer prompts you for the information it needs to configure the funksnmpd.conf and startsnmp.sh files.
a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

   **Choose a community string:** public

b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

   Specify the range of IPv4 addresses that may query this agent, such as 1.2.3.0/24.

   Address range: **192.168.70.0/24**

c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the SNMP subagent on the Steel-Belted Radius server.

   SNMPv2 trap sink: **192.168.70.86**

   Configuration of SNMP complete.

---

### NOTE:
Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

---

19. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

   Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

   **NOTE:** When you register your Steel-Belted Radius master or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

---

20. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

   Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: **e**

   Steel-Belted Radius stores its autoboot settings in the local `\radiusdir\radius\sbrd` file.

   - If you enter `e` (enable), the configure script copies the settings in the `sbrd` file to the `/etc/init.d` boot script and deletes old Steel-Belted Radius autoboot settings, thereby enabling autobooting for Steel-Belted Radius v6.0.

   - If you enter `d` (disable), the configure script does not copy the settings in the `sbrd` file to the `/etc/init.d` boot script and deletes old Steel-Belted Radius autoboot settings, thereby disabling autobooting for all versions of Steel-Belted Radius.
If you enter `p` (preserve), the configure script does not copy the settings in the `sbrd` file to the `/etc/init.d` boot script or delete old Steel-Belted Radius autoboot settings, thereby leaving your previous autoboot settings unchanged.

**Next Steps**

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

The SBR Administrator can be launched using the following URL:

```
http://<servername>:1812
```

Configuration complete

You must now finish configuring the new Steel-Belted Radius server to suit your network’s authentication and accounting needs. For example, you can edit the `[Addresses]` section of the `radius.ini` file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS process. Refer to “Starting the RADIUS Server” on page 55 for information on starting the RADIUS process. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

---

**Upgrading from a 30-Day Trial Installation**

You can download an evaluation version of Steel-Belted Radius from the Juniper Networks website (http://www.juniper.net/products_and_services/). If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator and connect to your Steel-Belted Radius server.

   Refer to the *Steel-Belted Radius Administration Guide* for information on using the SBR Administrator.

3. Choose File > License.

4. When the Add a License for Server window opens, enter your license number and click OK.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.
5. Click **OK** to close the confirmation window.

6. Restart your Steel-Belted Radius server.

   The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number. Refer to “Starting the RADIUS Server” on page 55 for information on how to restart your Steel-Belted Radius server.

---

### Upgrading from Steel-Belted Radius Version 4.x

Upgrading your Steel-Belted Radius software from version 4.x to version 6.0 involves archiving your Steel-Belted Radius configuration files and database, unconfiguring and uninstalling your old software, installing and configuring your new software, and merging any settings you customized in your old Steel-Belted Radius configuration files to the configuration files in the `radiusdir` directory.

Perform the following steps to upgrade your Steel-Belted Radius software from version 4.x to version 6.0:

1. Export your Steel-Belted Radius (version 4.x) database to a RADIUS Import Format (.rif) file.

   Refer to the *Steel-Belted Radius Administration Guide* (version 4.x) for information on how to export your Steel-Belted Radius database to a .rif file.

2. Back up your `/radiusdir` directory and the .rif file to a newly-created archive directory.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup. This backup directory is needed for data migration tasks that are associated with future upgrades.

   Note that you must use the dictionary files (`dict*`, `*.dct`, and `*.dci` files) used by Steel-Belted Radius version 4.x after you upgrade to version 6.0 so that checklist/return list processing uses consistent information.

   ```
   # cd /opt/funk
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xBp - )
   ```

3. Stop the Steel-Belted Radius daemon by issuing the following commands:

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

4. Uninstall the Steel-Belted Radius version 4.x software by issuing the following commands:

   ```
   sh install.sh -unconfig
   sh install.sh -uninstall
   ```

5. Install the Steel-Belted Radius version 6.0 server software on your server.
For more information, see “Installing the Steel-Belted Radius Server Software” on page 33.

6. Run the rif2xml utility to convert the .rif file containing your Steel-Belted Radius database to an XML database structure.

Refer to “RIF2XML Conversion Utility” on page 97 for information on running the rif2xml utility.

7. Copy the dictionary files (dictionary.dcm, *.dct, and *.dci files) you backed up in 2. to the \radiusdir directory on the Steel-Belted Radius server.

8. Run the SBR Administrator.

Refer to the Steel-Belted Radius Administration Guide for information on how to use the SBR Administrator.

9. Choose File > Import to import the converted XML database generated by the rif2xml utility into Steel-Belted Radius.

Refer to the Steel-Belted Radius Administration Guide for information on how to import information into Steel Belted Radius.

10. Merge any settings you customized in your old Steel-Belted Radius configuration files (*.ini, *.aut, *.dir, *.pro, *.rr) to the configuration files in the \radiusdir directory.

Do not replace the new Steel-Belted Radius configuration files with your old ones, or you may disable Steel-Belted Radius features and functions that require settings in the new files that do not exist in your old files.

NOTE: Do not merge the settings from the archived versions of your eap.ini, *.aut, or filter.ini files to the newly installed configuration files. Use the SBR Administrator to enter the EAP and filter settings you were using before the upgrade.

11. Restart Steel-Belted Radius.

Upgrading from Steel-Belted Radius Version 5.x

The procedure for upgrading your Steel-Belted Radius software has changed from previous (5.x) releases. Previously, you backed up and uninstalled your old Steel-Belted Radius software before installing new software. Steel-Belted Radius version 6.0 allows you to install your new software before deleting your old software. Steel-Belted Radius version 6.0 also helps you migrate your configuration and data files during the upgrade process.

Before You Begin

Before you upgrade your Steel-Belted Radius software from version 5.x to version 6.0, you should answer the following questions:
Do you want to relocate your Steel-Belted Radius files?
The Steel-Belted Radius v5.x software was typically installed in the /opt/funk directory. By default, the Steel-Belted Radius v6.0 software is installed in the /opt/JNPRsbr directory.

Do you want to retain your current Steel-Belted Radius configuration settings?
When you upgrade your Steel-Belted Radius software to version 6.0, you can start with the default Steel-Belted Radius configuration files, or you can choose to retain your current configuration files (data migration). The Steel-Belted Radius installer can create the following backups:

- Pre-installation backup—If you install Steel-Belted Radius v6.0 over a 5.x version, the installer copies your old software and configuration settings to a backup directory (basedir/radius/install/backups/YYYY:MM:DD:HH:MM:SS). The name of this pre-installation backup is recorded in the preinstall.dat file (described on page 32). The installer displays a message identifying the name of the pre-installation backup (“Existing server directory will be backed up as....”)

- Post-installation backup—The installer always copies the default Steel-Belted Radius version 6.0 software and configuration settings to a backup directory (basedir/radius/install/backups/YYYY:MM:DD:HH:MM:SS). The name of this post-installation backup is recorded in the install.dat file (described on page 32). The installer displays a message identifying the name of the post-installation backup (“Newly installed server directory will be backed up as....”)

If you want to preserve your previous (version 5.x) configuration settings, you can tell the configure script to migrate your settings from the pre-installation directory (or from another backup directory) to the working (/radius) directory. You would then copy parameters from the default configuration files in the post-installation backup to your configuration files to set up new Steel-Belted Radius features.

If you want to start with the default Steel-Belted Radius v6.0 settings, you can tell the configure script to skip the data migration and install the default configuration files. You could then merge settings from the archive files in the pre-installation backup directory to the default files to re-create your current configuration.

NOTE: Do not modify the backup directories or the .dat files that identify them. If you do, you may have difficulty upgrading your Steel-Belted Radius software in the future.

If you specify that you want to retain your current Steel-Belted Radius configuration settings when you run the installation script, the installer puts the default Steel-Belted Radius version 6.0 configuration files in the /radiusdir/install directory.

Do you want to retain your old (version 5.x) Steel-Belted Radius software?
During the configuration process, you will be asked whether you want to uninstall your old Steel-Belted Radius software. If you indicate that you do, the configure script will terminate so you can uninstall your old software manually. After you have uninstalled your old Steel-Belted Radius software, you can restart the configuration script to resume the installation/configuration process.
Figure 1 presents a decision tree that summarizes the choices you make and tasks you perform when upgrading from Steel-Belted Radius v5.x to Steel-Belted Radius v6.0.

Note the following:

- The diagram assumes that your Steel-Belted Radius v5.x software is currently installed in the /opt/funk directory (called olddir in the diagram). If your current software is installed in a different directory, substitute the path to that directory.

- The diagram assumes that your Steel-Belted Radius v6.0 software will be installed in the /opt/JNPRsbr directory (called newdir in the diagram). If your software will installed in a different directory, substitute the path to that directory.

- If you choose to overwrite your current software with the Steel-Belted Radius v6.0 software, then olddir and newdir represent the same directory.

- The configuration process consists of three phases:

  - In Stage 1, you specify whether you want to use your current data files to configure Steel-Belted Radius (data migration). After Stage 1 is complete, you will be asked whether you want to delete your old Steel-Belted Radius software.

  - In Stage 2, you specify a default administrator and a centralized configuration management (CCM) role (stand-alone, primary server, or replica server).

  - In Stage 3, you specify configuration information for LDAP, external databases, SNMP, autoboot (sbrd script), and whether you want your server to function as an Agent Host with RSA Authentication Manager. If you re-run the configure script in the future, it will automatically start at Stage 3.
Figure 1: Decision Tree for Steel-Belted Radius Upgrades (Solaris version)

```
packages
/var/spool/pkg/JNPRsbrXX.xol.pkg

olddir=/opt/Funk
# parent of existing RADIUS server directory

newdir=/opt/JNPRsbr
# parent of target RADIUS server directory

Start

Overwrite existing installation?

No

Remove old installation(s)?

Yes

Copy existing configuration?

No

CONFIGURE STAGE 1

cd /newdir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Specify migration from olddir

Yes

CONFIGURE STAGE 1

cd /newdir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Specify new configuration

CONFIGURE STAGE 1

cd /newdir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Accept migration from olddir

Exit configuration
Remove old installations
Run configuration again

cd /newdir/radius/install
./configure

MANUAL CONFIGURATION

# Edit configuration files
# Run ./configure again to change Stage 3 settings

START STEEL-BELTED RADIUS

newdir/radius/sbrd start

RUN SBR ADMINISTRATOR

http://servername:1812
```
Figure 2 presents this decision process as a set of upgrade scenarios:

- Scenario 1 illustrates a non-relocating software upgrade (meaning that the version 6.0 software is installed in the old /opt/funk directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default configuration files are copied to the /opt/funk/radius/install/backups/YYYY:MM-DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 2 illustrates a non-destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that retains the existing configuration information. The default configuration files are copied to the /opt/JNPRsbr/radius/install/backups/YYYY:MM-DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 3 illustrates a destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that retains the existing configuration information. The default configuration files are copied to the /opt/JNPRsbr/radius/install/backups/YYYY:MM-DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 4 illustrates a non-relocating software upgrade (meaning that the version 6.0 software is installed in the old /opt/funk directory) that installs clean (default) configuration files. The old software and configuration settings are archived in the /opt/funk/radius/install/backups/YYYY:MM-DD-HH:MM:SS directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- Scenario 5 illustrates a non-destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that installs clean (default) configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- Scenario 6 illustrates a destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that installs clean (default) configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.
Figure 2: Upgrade Scenarios

Upgrade Procedure

Perform the following steps to upgrade your Steel-Belted Radius software from version 5.x to version 6.0 on a Solaris server.

1. Log into the Solaris server as root.

2. Back up your /radiusdir directory to an archive location.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup. This backup directory is needed for data migration tasks that are associated with future upgrades.

   ```
   # cd /opt/funk
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xfBp - )
   ```

3. Back up your root and server certificates, and verify you know the password for your server certificate.

   You will install your server certificate for Steel-Belted Radius v6.0 by running the SBR Administrator configuration application.

4. Stop the RADIUS process currently running on your server.

   ```
   # /opt/funk/radius/sbrd stop
   ```

5. If you installed the 969531-01 or 969541-01 security patch for Steel-Belted Radius v5.3 or 5.4, uninstall the security patch.

   You must uninstall the security patch manually, using the appropriate package removal command (pkgrm).

Copy the files from the `/solaris` directory on the installation CD-ROM to a local or remote hard disk partition that is readable by `root`. The following example copies the files to the `/opt/JNPRsbr/temp` directory.

```
# cd /
# mkdir -p /opt/JNPRsbr/temp
# cp -pR /cdrom/sbr/solaris/* /opt/JNPRsbr/temp
```

7. Run the installer package.

```
# pkgadd -d directory -a none JNPRsbrXX.sol.pkg
```

where `directory` specifies the directory where you placed the installation package and `XX` specifies the version of Steel-Belted Radius you want to install.

```
# pkgadd -d /opt/JNPRsbr/temp -a none JNPRsbrge.sol.pkg
```

Processing package instance `<JNPRsbrge.sol.pkg>` from

`<opt/JNPRsbr/temp>`

`JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)`

`sparc 6.0.0000`

`(C) Copyright 1996-2007 Juniper Networks, Inc. See license.txt`

8. Specify the base directory in which you want to install the Steel-Belted Radius files.

By default, the installation package puts the Steel-Belted Radius files in the `/opt/JNPRsbr/` base directory.

Enter path to package base directory `?` `/opt/JNPRsbr`

The selected base directory `<opt/JNPRsbr>` must exist before installation is attempted.

Do you want this directory created now `[y,n,?]` `y`

Using `<opt/JNPRsbr>` as the package base directory.

```
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
```

9. When you are prompted to confirm you want to install the package, enter `y`.

This package contains scripts which will be executed with super-user permission during the process of installing this package.

Do you want to continue with the installation of `<JNPRsbrge>` `[y,n,?]` `y`

Installing `JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)` as `<JNPRsbrge>`

```
## Executing preinstall script.
## Installing part 1 of 1.
```
## Executing postinstall script.

Newly installed server directory will be backed up as:
/opt/JNPRsbr/radius/install/backups/2006:12:15-06:39:56
Installation of <JNPRsbrge> was successful.

10. Navigate to the directory where you installed Steel-Belted Radius.

```
# cd /opt/JNPRsbr/radius/install
```

11. Navigate to the directory where you installed Steel-Belted Radius and run the configuration script for Steel-Belted Radius.

```
# cd /opt/JNPRsbr/radius/install
# ./configure
```

12. Review the Steel-Belted Radius license agreement.

Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter y.

```
Do you accept the terms in the license agreement? [n] y
```

13. Indicate whether you have a license number.

You can enter a license string or use a one-time 30 day trial license.
Would you like to enter a license string? [n]

- If you purchased Steel-Belted Radius, type y and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

- If you do not have a license number, type n at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product’s full feature set for a limited period.

14. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

```
Do you wish to enable LCI? [n]
License does not have LCI support.
Installed a 30 day evaluation license.
```
15. Specify whether you want to migrate your current Steel-Belted Radius configuration files.

- If you are performing a non-relocating update (or if you are performing a relocating update and you want to migrate your configuration files), specify the directory path to your current Steel-Belted Radius files. If you are performing a non-relocating update, the default is the pre-installation backup of your current settings.

Please enter backup or radius directory from which to upgrade. Enter n for new configuration, s to search, or q to quit.

[/radiusdir/radius/install/backups/timestamp]

Press Enter to accept the default value, or enter a different path if you want to use a different set of configuration files. You can enter s if you want to search for the directory path for your Steel-Belted Radius files.

- If you are performing a relocating update (and you do not want to migrate your configuration files), enter n to specify that you want to use the default configuration files.

Please enter backup or radius directory from which to upgrade. Enter n for new configuration, s to search, or q to quit.

[n] n

16. Specify whether you want to remove your old Steel-Belted Radius software.

If you want to remove your old Steel-Belted Radius software, enter y at the Manually remove pre-existing software now? prompt, uninstall the old software, and then run the configuration script again. When you restart the configuration script, the script returns you to this step.

WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.

Manually remove pre-existing software now? [y]: y
Please execute configure again when you are finished

Administrator deletes old Steel-Belted Radius files:

Steel-Belted Radius version 5.0.x: install.sh -uninstall
Steel-Belted Radius version 5.3/5.4: pkgrm FUNKsbrXX

Administrator then restarted the configure script:

# cd /opt/JNPRsbr/radius/install
#.configure
17. Specify the login name of the initial Steel-Belted Radius administrator.

The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

Enter initial admin user (account must have an associated password) [root]:

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

18. If you are not migrating your old configuration data (that is, if you answered \textit{n} in Step 15, specify whether you want to install the Steel-Belted Radius server as a primary server (\textit{p}), a replica server (\textit{r}), or a standalone RADIUS server (\textit{sa}).

Configure SBR server as primary (\textit{p}), replica (\textit{r}), or stand alone (\textit{sa}) [\textit{sa}]: \textit{r}

- If you enter \textit{p} (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

- If you enter \textit{r} (replica server), you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
  - If the replication package is present on your computer or network, you are prompted to specify the path to the \textit{replica.ccmpkg} file.
  - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address(es), and replication secret of the primary server.

- If you enter \textit{sa} (standalone RADIUS server), you do not need to specify replication information.

19. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

Do you want to configure LDAP? [\textit{n}]:

- If no, press Enter.

- If yes, type \textit{y} and press Enter. You are prompted to enter the path for the LDAP library files:

Enter path for LDAP library files [/usr/lib]:

To accept the default path (/usr/lib), press Enter.
20. Specify whether you want to configure Steel-Belted Radius for use with an Oracle database.

    Configuring for use with generic database
    Do you want to configure for use with Oracle? [n]:

If no, press Enter.

If yes, type `y` and press Enter. You are prompted to version and path information for the Oracle library files.

    Configuring for use with Oracle.
    Supported Oracle version: 8, 9, 10
    What version of Oracle will be used? [9] 9
    Setting the environment variable ORACLE_HOME.
    Enter ORACLE_HOME [:] /opt/10g/app/oracle/product/9.2.0
    Setting the environment variable LD_LIBRARY_PATH.
    Enter path for Oracle shared libraries:
    /opt/10g/app/oracle/product/9.2.0/lib
    Setting the environment variable TNS_ADMIN.
    Enter TNS_ADMIN: /opt/10g/app/oracle/product/9.2.0/network/admin

21. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can monitor your Steel-Belted Radius server from an SNMP management station.

    Do you want to configure SNMP? [n]:

If no, press Enter to proceed to the next prompt.

If yes, type `y` and press Enter. The configure script prompts you for the information it needs to configure the `jnprsnmpd.conf` and `startsnmp.sh` files.

a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

    Choose a community string: public

b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by `/32`. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by `/24`.

    Specify the range of IPv4 addresses that may query this agent, such as `1.2.3.0/24`.
    Address range: 192.168.70.0/24
c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

SNMPv2 trap sink: **192.168.70.86**
Configuration of SNMP complete.

**NOTE:** Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

22. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

**NOTE:** When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

23. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: **e**

- If you enter **e**, the configure script saves the **sbrd** script and copies it to the /etc/init.d boot script.
- If you enter **d**, the configure script discards changes made to the **sbrd** script.
- If you enter **p**, the configure script saves the **sbrd** script but does not copy it to the /etc/init.d boot script.

**Next Steps**

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete

You must now finish configuring the new Steel-Belted Radius server to suit your network’s authentication and accounting needs. For example, you can edit the [Addresses] section of the radius.ini file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.
After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the radius process. Refer to “Stopping the RADIUS Server” on page 56 for information on starting the RADIUS process. Refer to the Steel-Belted Radius Administration Guide for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

Upgrading from RSA RADIUS Server Version 6.1

This section describes how to upgrade servers running RSA RADIUS Server version 6.1 in a replication environment and how to upgrade a standalone server running RSA RADIUS Server version 6.1.

Upgrading in a Replication Environment

In environments that use replication (primary and replica servers), you must upgrade your replica servers before you upgrade your primary server. Perform the following procedure for each server in your replication realm, making sure that you upgrade your primary server last.

1. Back up the directory containing your RSA RADIUS Server configuration files.

   The default location for RSA RADIUS Server files is /opt/rsa/radius.

2. Execute the following command to remove the Steel-Belted Radius replication package.

   \[ \text{pkgrm RSARadius} \]

3. Install version 6.0 of the Steel-Belted Radius software on the server.

   See “Installing the Steel-Belted Radius Server Software” on page 33 for information on how to install the Steel-Belted Radius server software.

4. Execute the following command to run the Steel-Belted Radius configuration script:

   \[ \text{/opt/JNPRsbr/radius/install/configure} \]

5. When the configuration script prompts you for a license number, enter your Steel-Belted Radius version 6.0 license number.

   \[ \text{NOTE: Do not run the uninstall_rsa.sh script that is installed as part of RSA RADIUS Server. Running the uninstall_rsa.sh script will delete your entire install directory.} \]

   \[ \text{NOTE: You cannot use an evaluation license to upgrade from RSA RADIUS Server to Steel-Belted Radius.} \]
6. When the configuration script prompts you to specify what type of server (primary, replica, or standalone) you are configuring, enter r to indicate a replica server or p to indicate a primary server.

7. If prompted, specify the location of the replica.ccmpkg package generated by the primary RADIUS server (or specify the name/IP address/replication secret of the primary RADIUS server).

8. If you want to register the server as an Agent Host with RSA Authentication Manager v6.1 or later, specify the location of the RSA configuration files. Registering as an Agent Host creates a new node secret, which is required for communication between the Steel-Belted Radius server and the RSA SecurID server.

The default location for the RSA configuration files is /opt/rsa/radius.

9. Merge any modified configuration (.ini) files except eap.ini from the archive directory created in 1.

10. Copy all database files (radiusdata.*, vista.taf, and sbr_id.xml) from the RSA RADIUS Server archive directory (default is opt/rsa/radius/install/backups/timestamp).

11. Use a text editor to configure the Enable=1 setting for the .aut file associated with each authentication method you want to use.

Refer to the Steel-Belted Radius Administration Guide for information about authentication methods.

12. Copy all database files (radiusdata.*, vista.taf, and sbr_id.xml) from the RSA RADIUS Server archive directory.

13. Use the ./sbrd start commands to restart the Steel-Belted Radius server.

When the replica server restarts, it automatically downloads and installs its configuration package.

---

**Configuring a Standalone Server**

To configure a standalone server to interact with RSA Authentication Manager:

1. Execute the following command to run the Steel-Belted Radius configuration script.

   /opt/JNPRsbr/radius/install/configure

2. Merge any settings you customized in your RSA RADIUS Server configuration files (*.ini, *.aut, *.dir, *.pro, *.rr) to the configuration files in the \radiusdir directory.
Do not replace the new configuration files with your old ones, or you may disable Steel-Belted Radius features and functions that require settings in the new files that do not exist in your old files.

**NOTE:** Do not merge the settings from the archived version of the `eap.ini` file to the newly installed default `eap.ini` file. Use the SBR Administrator to apply the EAP settings you were using before the upgrade.

3. Copy all database files (`radiusdata.*`, `vista.taf`, and `sbr_id.xml`) from the RSA RADIUS Server archive directory (default is `opt/rsa/radius/install/backups/timestamp`).

4. Restart Steel-Belted Radius.

---

**Restoring a Previous Configuration**

When you install the Steel-Belted Radius server software, the installation script saves your existing configuration to a backup directory to preserve your configuration settings. If you are re-installing the same version and edition of Steel-Belted Radius on a server, you can copy the configuration files from the backup directory to the Steel-Belted Radius server directory to restore your previous configuration.

If you are upgrading your Steel-Belted Radius software from an older version, do not copy your configuration files to the Steel-Belted Radius server directory. For more information, see “Upgrading from Steel-Belted Radius Version 4.x” on page 40 or “Upgrading from Steel-Belted Radius Version 5.x” on page 41, as appropriate.

---

**Starting the RADIUS Server**

Use the following command to start the RADIUS server manually.

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

When you execute the `sbrd start` command, Steel-Belted Radius starts the `mkded` (btrieve) process to allow database access, and then starts the `radius` process.

If you change configuration settings for your Steel-Belted Radius server, you may need to restart Steel-Belted Radius to make the changes effective. As an alternative to issuing an `sbrd stop` command immediately followed by an `sbrd start` command, you can use the `sbrd restart` command to restart Steel-Belted Radius. When you issue the `sbrd restart` command, Steel-Belted Radius shuts down and then immediately starts the `mkded` (btrieve) and `radius` processes.

```
   cd server-directory
   ./sbrd restart
```
Stopping the RADIUS Server

Use the following commands to stop the RADIUS server:

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

When you execute the `sbrd stop` command, Steel-Belted Radius allows its subsystems to complete outstanding work and release resources, and then stops the `mkded` (btrieve) and `radius` processes gracefully.

If Steel-Belted Radius fails to stop after you issue the `sbrd stop` command, you can use the optional `force` argument to terminate all subsystems immediately.

```
cd server-directory
./sbrd stop force
```

Resetting the RADIUS Database

If Steel-Belted Radius fails, the RADIUS database may remain running. If this happens, the Steel-Belted Radius process may refuse to run. To resolve this problem, execute the following command to stop the `mkded` (btrieve) process.

```
cd server-directory
./sbrd stop force
```

After the `mkded` (btrieve) process is stopped, you can start the `radius` process and the database by executing the following command:

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

Displaying RADIUS Status Information

You can use the `sbrd status` command to display status information for the RADIUS process.

```
cd server-directory
./sbrd status
```

Figure 3 illustrates the output of the `sbrd status` command.
Figure 3: Output of sbrd status Command

```plaintext
> sbrd status
ecarte 25927 .mkded start
btrieve processes are active

— Shared Memory Segments —
key shmid owner perms bytes nattch status
0x42545256 891968 ecarte 600 8000000 2

— Semaphore Arrays —
key semid owner perms nsems
0x42545256 167116 ecarte 660 250

btrieve shared IPC objects exist
btrieve state is running
btrieve status 1101

ecarte 2066 radius sbr.xml
radius processes are running
radius state is running
radius status 1101

Aggregate state is running
```
Chapter 5
Linux Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software and the SBR Administrator configuration application on a Linux server. This chapter also describes how to install the optional SNMP software for use with the GEE and SPE editions of Steel-Belted Radius.

Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see “System Requirements – Linux” on page 13.

- Make sure that you are (or have access to) a system administrator and someone who understands your RADIUS authentication and accounting requirements.

- If you are installing Steel-Belted Radius on a server running SuSE Linux, review the `/etc/hosts` file on the server. Comment out entries with addresses in the range 127.0.0.2-254, Do not comment out the `/etc/hosts` entry with the address 127.0.0.1.

- If you are installing the optional SNMP module, stop all SNMP agents running on your server.

---

**NOTE:** If your server runs SNMP agents other than the one supplied with Steel-Belted Radius, you must coordinate the port numbers used by your SNMP agents to avoid port contention.
Upgrade Files

The install, configure, and uninstall scripts for Steel-Belted Radius version 6.0 automatically archive your Steel-Belted Radius files to the `/radius/install/backups` directory. To facilitate future software upgrades, the install, configure, and uninstall scripts create a number of `.dat` files in the `/radius/install` directory. These files store information used for future upgrades. You should not move, rename, or otherwise modify these files.

Table 8: Upgrade Files and Directories

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius/install/package.dat</code></td>
<td>Contains a unique package identifier.</td>
</tr>
<tr>
<td><code>radius/install/preinstall.dat</code></td>
<td>Contains the absolute pathname of the backup directory for your old Steel-Belted Radius software and configuration files (pre-installation backup).</td>
</tr>
<tr>
<td><code>radius/install/upgrade.dat</code></td>
<td>Contains the absolute pathname of the Steel-Belted Radius version 6.0 upgrade source (if any).</td>
</tr>
<tr>
<td><code>radius/install/configure.dat</code></td>
<td>Contains configuration state data.</td>
</tr>
<tr>
<td><code>radius/install/uninstall.dat</code></td>
<td>Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.0 software and working configuration files (pre-uninstall backup).</td>
</tr>
<tr>
<td><code>radius/install/backups/</code></td>
<td>Contains the backups referenced by the .dat files.</td>
</tr>
</tbody>
</table>

Package Management Commands

Table 9 lists useful Linux package management commands.

Table 9: Useful Package Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>`rpm -q -a</td>
<td>egrep &quot;FUNK</td>
</tr>
<tr>
<td><code>rpm -q -i sbr-gee-6.0.0-0</code></td>
<td>Report high level description for specified package</td>
</tr>
<tr>
<td><code>rpm -q --queryformat &quot;%{INSTALLPREFIX}&quot; sbr-gee-6.0.0-0</code></td>
<td>Show installed directory</td>
</tr>
<tr>
<td><code>rpm -i [-prefix /path] sbr-gee.6.0.0-0.i386.lin.rpm</code></td>
<td>Install Steel-Belted Radius [at the specified /path]</td>
</tr>
<tr>
<td><code>rpm -U [-prefix /path] sbr-gee.6.0.0-0.i386.lin.rpm</code></td>
<td>Upgrade an existing Steel-Belted Radius installation [in the specified /path]</td>
</tr>
<tr>
<td><code>rpm -e sbr-gee-6.0.0-0</code></td>
<td>Uninstall Steel-Belted Radius.</td>
</tr>
</tbody>
</table>
Installing the Steel-Belted Radius Server Software

The installer for the Linux version of the Steel-Belted Radius server software uses RPM (Red Hat Package Manager) files, which have filenames that include the edition and version of the server software.

This section assumes that you are installing Steel-Belted Radius on your Linux server for the first time or that you are installing Steel-Belted Radius in a directory other than the one used by previous installations (clean installation). If you are upgrading an existing Steel-Belted Radius installation to version 6.0, refer to “Upgrading from Steel-Belted Radius Version 5.x” on page 66 for information on upgrade options and considerations.

To install the Steel-Belted Radius server software on a Linux server or workstation:

1. Log into the Linux server as root.

2. Copy the Steel-Belted Radius installation files to the Linux server.

   Copy the files from the /linux directory on the installation CD-ROM to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/JNPRsbr/temp directory.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/linux/* /opt/JNPRsbr/temp
   ```

3. Run the installer.

   ```
   # rpm -i sbr-XXX-version.i386.lin.rpm
   ```

   where XXX specifies the version of Steel-Belted Radius you want to install:

   - gee—Steel-Belted Radius/Global Enterprise Edition
   - spe—Steel-Belted Radius/Service Provider Edition
   - ent—Steel-Belted Radius/Enterprise Edition

   and version specifies the software version you want to install. For example, to run the RPM package used to install the GEE version of Steel-Belted Radius v6.0 to /opt/JNPRsbr, you would enter the following:

   ```
   # rpm -i /path/sbr-gee-6.0.0-0.i386.lin.rpm
   ```

   By default, the RPM package installs the Steel-Belted Radius files in the /opt/JNPRsbr directory. If you want to install Steel-Belted Radius in a directory other than /opt/JNPRsbr, you can use the --prefix option:

   ```
   # rpm -i --prefix installdir /path/sbr-edition-version.i386.lin.rpm
   ```
4. Navigate to the directory where you installed Steel-Belted Radius.

   `# cd /opt/JNPRsbr/radius/install`

5. Execute the following command to run the configuration script for Steel-Belted Radius:

   `# ./configure`

6. Review the Steel-Belted Radius license agreement.

   Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter `y`.

   Do you accept the terms in the license agreement? [n] y

7. Indicate whether you have a license number.

   You can enter a license string or use a one-time 30 day trial license. Would you like to enter a license string? [n]

   - If you purchased Steel-Belted Radius, type `y` and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

   - If you do not have a license number, type `n` at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product’s full feature set for a limited period.

8. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI)

   Do you wish to enable LCI? [n]

   License does not have LCI support.

9. Specify whether you are upgrading an existing Steel-Belted Radius installation or configuring a new installation.

   - Enter `n` if you are performing a new installation.

   - Enter the directory path to the Steel-Belted Radius files if you are upgrading an existing Steel-Belted Radius installation and you know the name of the current Steel-Belted Radius directory.

   - Enter `s` if you are upgrading an existing Steel-Belted Radius installation and you want to search for the Steel-Belted Radius directory.

   Please enter backup or radius directory from which to upgrade. Enter n for new configuration, s to search, or q to quit.

   [n] n
10. Specify that you do not want to remove older versions of Steel-Belted Radius.

   WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.

   Manually remove pre-existing software now? [y]: n

11. Specify the login name of the initial Steel-Belted Radius administrator.

   The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

   Configuring for RedHat4
   Enter initial admin user (account must have an associated password) [root]:

   NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

12. Specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

   Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: sa

   - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

   If appropriate, enter y when you are asked whether you are upgrading a primary server. Doing so tells the installer to preserve the server’s replication realm information.

   - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica.ccmpkg configuration package containing your Steel-Belted Radius replication settings.

     - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.

     - If you want to specify the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address, and replication secret of the primary server.

   - If you enter sa (standalone RADIUS server), you do not need to specify replication information.
13. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

- If you do not want to configure Steel-Belted Radius for use with an external LDAP data service, press Enter.

- If you want to configure Steel-Belted Radius for use with an external LDAP data service, type y and press Enter. You are prompted to enter the path for the LDAP library files:

  Do you want to configure LDAP? [n]: y
  Enter path for LDAP library files [/usr/lib]:

  To accept the default path (/usr/lib), press Enter.

14. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can monitor your Steel-Belted Radius server from an SNMP management station.

  Do you want to configure SNMP? [n]:

If you do not want to install the optional SNMP module, press Enter to proceed to the next prompt.

If you want to install the optional SNMP module, type y and press Enter. The configure script prompts you for the information it needs to configure the jnprsnmpd.conf and startsnmp.sh files.

  a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

  Choose a community string: public

  b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

  Specify the range of IPv4 addresses that may query this agent, such as 1.2.3.0/24.
  Address range: 192.168.70.0/24

  c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

  SNMPv2 trap sink: 192.168.70.86
  Configuration of SNMP complete.

---

**NOTE:** Refer to the Steel-Belted Radius Administration Guide for information on configuring the SNMP agent.
15. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

**NOTE:** When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

16. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: e

Steel-Belted Radius stores its autoboot settings in the local \radiusdir\radius\sbrd file.

- If you enter e (enable), the configure script copies the settings in the sbrd file to the /etc/init.d boot script and deletes old Steel-Belted Radius autoboot settings, thereby enabling autobooting for Steel-Belted Radius v6.0.
- If you enter d (disable), the configure script does not copy the settings in the sbrd file to the /etc/init.d boot script and deletes old Steel-Belted Radius autoboot settings, thereby disabling autobooting for all versions of Steel-Belted Radius.
- If you enter p (preserve), the configure script does not copy the settings in the sbrd file to the /etc/init.d boot script or delete old Steel-Belted Radius autoboot settings, thereby leaving your previous autoboot settings unchanged.

**Next Steps**

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

The SBR Administrator can be launched using the following URL:
http://<servername>:1812

Configuration complete

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the radius.ini file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the Steel-Belted Radius Reference Guide for information on how to edit the configuration files used by Steel-Belted Radius.
After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS process. Refer to “Starting the RADIUS Server” on page 80 for information on starting the RADIUS process. Refer to the Steel-Belted Radius Administration Guide for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Juniper website (http://www.juniper.net/products_and_services/). If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator and connect to your Steel-Belted Radius server.

   Refer to the Steel-Belted Radius Administration Guide for information on using the SBR Administrator.

3. Choose File > License.

4. When the Add a License for Server window opens, enter your license number and click OK.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.

5. Click OK to close the confirmation window.

6. Restart your Steel-Belted Radius server.

   The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number. Refer to “Starting the RADIUS Server” on page 80 for information on how to restart your Steel-Belted Radius server.

Upgrading from Steel-Belted Radius Version 5.x

The procedure for upgrading your Steel-Belted Radius software has changed from previous (5.x) releases. Previously, you backed up and uninstalled your old Steel-Belted Radius software before installing new software. Steel-Belted Radius version 6.0 allows you to install your new software before deleting your old software. Steel-Belted Radius version 6.0 also helps you migrate your configuration and data files during the upgrade process.
Before You Begin

Before you upgrade your Steel-Belted Radius software from version 5.x (5.0, 5.3, or 5.4) to version 6.0 on a server, you should answer the following questions:

Where do you want to install your Steel-Belted Radius v6.0 software?

The Steel-Belted Radius v5.x software was typically installed in the /opt/funk directory. By default, the Steel-Belted Radius v6.0 software is installed in the /opt/JNPRsbr directory. You can use the rpm --prefix basedir command to specify the target directory for Steel-Belted Radius installation.

Do you want to retain your current Steel-Belted Radius configuration settings?

When you upgrade your Steel-Belted Radius software to version 6.0, you can start with the default Steel-Belted Radius configuration files, or you can choose to retain your current configuration files (data migration). The Steel-Belted Radius installer can create the following backups:

- Pre-installation backup—If you install Steel-Belted Radius v6.0 over a 5.x version, the installer copies your old software and configuration settings to a backup directory (basedir/radius/install/backups/YYYY:MM:DD:HH:MM:SS). The name of this pre-installation backup is recorded in the preinstall.dat file (described on page 60). The installer displays a message identifying the name of the pre-installation backup (“Existing server directory will be backed up as....”)

- Post-installation backup—The installer always copies the default Steel-Belted Radius version 6.0 software and configuration settings to a backup directory (basedir/radius/install/backups/YYYY:MM:DD:HH:MM:SS). The name of this post-installation backup is recorded in the install.dat file (described on page 60). The installer displays a message identifying the name of the post-installation backup (“Newly installed server directory will be backed up as....”)

If you want to preserve your previous (version 5.x) configuration settings, you can tell the configure script to migrate your settings from the pre-installation directory (or from another backup directory) to the working (/radius) directory. You would then copy parameters from the default version 6.0 configuration files in the post-installation backup to your configuration files to set up new Steel-Belted Radius features.

If you want to start with the default Steel-Belted Radius v6.0 settings, you can tell the configure script to skip the data migration and install the default version 6.0 configuration files. You could then merge settings from the archive files in the pre-installation backup directory to the default files to re-create your current configuration.

**NOTE:** Do not modify the backup directories or the .dat files that identify them. If you do, you may have difficulty upgrading your Steel-Belted Radius software in the future.
Do you want to retain your old (v5.x) Steel-Belted Radius software on your server?

During the configuration process, you will be asked whether you want to uninstall your old Steel-Belted Radius software. If you indicate that you do, the configure script will terminate so you can uninstall your old software manually. After you have uninstalled your old Steel-Belted Radius software, you can restart the configuration script to resume the installation/configuration process.

Figure 4 presents a decision tree that summarizes the choices you make and tasks you perform when upgrading from Steel-Belted Radius v5.x to Steel-Belted Radius v6.0.

Note the following:

- The diagram assumes that your Steel-Belted Radius v5.x software is currently installed in the /opt/funk directory (called olddir in the diagram). If your current software is installed in a different directory, substitute the path to that directory.

- The diagram assumes that your Steel-Belted Radius v6.0 software will be installed in the /opt/JNPRsbr directory (called newdir in the diagram). If your software will be installed in a different directory, substitute the path to that directory.

- If you choose to overwrite your current software with the Steel-Belted Radius v6.0 software, then olddir and newdir represent the same directory.

- The configuration process consists of three phases:
  - In Stage 1, you specify whether you want to use your current data files to configure Steel-Belted Radius (data migration). After Stage 1 is complete, you will be asked whether you want to delete your old Steel-Belted Radius software.
  - In Stage 2, you specify a default administrator and a centralized configuration management (CCM) role (stand-alone, primary server, or replica server).
  - In Stage 3, you specify configuration information for LDAP, external databases, SNMP, autoboot (sbrd script), and whether you want your server to function as an Agent Host with RSA Authentication Manager. If you re-run the configure script in the future, it will automatically start at Stage 3.
Figure 4: Decision Tree for Steel-Belted Radius Upgrades (Linux version)

```
packages
/cdrom/linux/rpm-sbr-XXX.6.0.0-0.i386.lin.rpm

olddir/opt/funk
# parent of existing RADIUS server directory

newdir/opt/JNPRsbr
# parent of target RADIUS server directory

Start

Overwrite existing installation?

No

Copy existing configuration?  Yes

No

Copy existing configuration?  No

Yes

CONFIGURE STAGE 1

cd /olddir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Specify migration from olddir

CONFIGURE STAGE 1

cd /olddir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Specify new configuration

CONFIGURE STAGE 1

cd /olddir/radius/install
./configure
# Accept license agreement
# Enter evaluation or license key
# Accept migration from olddir

Remove old installation(s)?

Yes

Exit configuration
Remove old installations
Run configuration again

cd /newdir/radius/install
./configure

No

CONFIGURE STAGE 2

# Configure OS, admin, CCM

CONFIGURE STAGE 3

# Configure LDAP, external database, SNMP, RSA, autoboot

MANUAL CONFIGURATION
# Edit configuration files
# Run ./configure again to change Stage 3 settings

START STEEL-BELTED RADIUS
newdir/radius/sbrd start

RUN SBR ADMINISTRATOR
http://servername:1812
```

IMPORTANT: Do not use the rpm -U command on servers running SuSE Linux.
Figure 5 presents this decision process as a set of upgrade scenarios:

- **Scenario 1** illustrates a non-relocating software upgrade (meaning that the version 6.0 software is installed in the old /opt/funk directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default version 6.0 configuration files are copied to the /opt/funk/radius/install/backups/YYYY:MM:DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- **Scenario 2** illustrates a non-destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that retains the existing configuration information. The default version 6.0 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/YYYY:MM:DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- **Scenario 3** illustrates a destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that retains the existing configuration information. The default version 6.0 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/YYYY:MM:DD-HH:MM:SS directory; you can use these files to merge new settings into your configuration files manually.

- **Scenario 4** illustrates a non-relocating software upgrade (meaning that the version 6.0 software is installed in the old /opt/funk directory) that installs clean (default) version 6.0 configuration files. The old software and configuration settings are archived in the /opt/funk/radius/install/backups/YYYY:MM:DD-HH:MM:SS directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- **Scenario 5** illustrates a non-destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the old /opt/funk directory is preserved) that installs clean (default) version 6.0 configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- **Scenario 6** illustrates a destructive relocating software upgrade (meaning that the version 6.0 software is installed in the /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that installs clean (default) version 6.0 configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.
Figure 5: Upgrade Scenarios

<table>
<thead>
<tr>
<th>Steel-Belted Radius Software</th>
<th>/opt/funk</th>
<th>/opt/funk</th>
<th>/opt/JNPRsbr</th>
<th>/opt/JNPRsbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Old Data (Upgrade)</td>
<td>Scenario 1: Non-relocating software upgrade; retain existing configuration; overwrite old software</td>
<td>Scenario 2: Relocating software upgrade; retain existing configuration; preserve old software</td>
<td>Scenario 3: Relocating software upgrade; retain existing configuration; delete old software</td>
<td></td>
</tr>
<tr>
<td>Use New Data (Clean Install)</td>
<td>Scenario 4: Non-relocating software upgrade; use default (clean) configuration; overwrite old software</td>
<td>Scenario 5: Relocating software upgrade; use default (clean) configuration; preserve old software</td>
<td>Scenario 6: Relocating software upgrade; use default (clean) configuration; delete old software</td>
<td></td>
</tr>
</tbody>
</table>

**Upgrade Procedure (RedHat Linux)**

Perform the following steps to upgrade your Steel-Belted Radius software from version 5.x to version 6.0 on a server running RedHat Linux:

1. Log into the Linux server as **root**.

2. Stop the RADIUS process currently running on your server.
   
   ```
   # /opt/funk/radius/sbrd stop
   ```

3. Back up your `/radiusdir` directory to an archive location.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup. This backup directory is needed for data migration tasks that are associated with future upgrades.

   ```
   # cd /opt/funk
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xBp - )
   ```

4. Back up your root and server certificates, and verify you know the password for your server certificate.

   You will install your server certificate for Steel-Belted Radius v6.0 by running the SBR Administrator configuration application.

5. Copy the Steel-Belted Radius installation files to the Linux server.

   Copy the files from the `/linux` directory on the installation CD-ROM to a local or remote hard disk partition that is readable by **root**. The following example copies the files to the `/opt/JNPRsbr/temp` directory; you can use any directory you choose.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/linux/* /opt/JNPRsbr/temp
   ```
6. If you installed the 969531-01 or 969541-01 security patch for Steel-Belted Radius v5.3 or 5.4, uninstall the security patch.

You must uninstall the security patch manually, using the appropriate package removal command (`rpm -e`).

7. Run the installer for the Steel-Belted Radius v6.0 server software.

7A. Non-relocating installation: If you want to install your Steel-Belted Radius v6.0 software in the directory that contains your Steel-Belted Radius version 5.x software (overwriting your current Steel-Belted Radius software with the version 6.0 software), execute the following command:

```
rpm -U --prefix /opt/funk sbr-XXX-version.i386.lin.rpm
```

where **XXX** specifies the edition of Steel-Belted Radius you want to install:

- **gee**—Steel-Belted Radius/Global Enterprise Edition
- **spe**—Steel-Belted Radius/Service Provider Edition
- **ent**—Steel-Belted Radius/Enterprise Edition

and **version** specifies the software version you want to install. For example:

```
rpm -U --prefix /opt/funk sbr-gee-6.0.0.i386.lin.rpm
```

7B. Relocating installation: If you want to install your Steel-Belted Radius v6.0 software in a directory other than the one containing your Steel-Belted Radius version 5.x software, execute the following command:

```
rpm -i [--prefix installdir] sbr-XXX-version.i386.lin.rpm
```

8. Navigate to the directory where you installed Steel-Belted Radius and run the configuration script for Steel-Belted Radius.

```
# cd /opt/JNPRsbr/radius/install
# ./configure
```

9. Review the Steel-Belted Radius license agreement.

Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter `y`.

```
Do you accept the terms in the license agreement? [n] y
```

10. Indicate whether you have a license number.

```
You can enter a license string or use a one-time 30 day trial license. Would you like to enter a license string? [n]
```
If you purchased Steel-Belted Radius, type y and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

If you do not have a license number, type n at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product's full feature set for a limited period.

11. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

   Do you wish to enable LCI? [n]
   License does not have LCI support.
   Installed a 30 day evaluation license.

12. Specify whether you want to migrate your current Steel-Belted Radius configuration files.

   If you are performing a non-relocating update (or if you are performing a relocating update and you want to migrate your configuration files), specify the directory path to your current Steel-Belted Radius files. If you are performing a non-relocating update, the default is the pre-installation backup of your current settings.

   Please enter backup or radius directory from which to upgrade.
Enter n for new configuration, s to search, or q to quit.
[/radiusdir/radius/install/backups/timestamp]

   Press Enter to accept the default value, or enter a different path if you want to use a different set of configuration files. You can enter s if you want to search for the directory path for your Steel-Belted Radius files.

   If you do not want to migrate your configuration files, enter n to specify that you want to use the default configuration files.

   Please enter backup or radius directory from which to upgrade.
Enter n for new configuration, s to search, or q to quit.
[n] n

13. Specify whether you want to remove your old Steel-Belted Radius software.

   If you want to remove your old Steel-Belted Radius software, enter y at the Manually remove pre-existing software now? prompt, uninstall the old software, and then run the configuration script again. When you restart the configuration script, the script returns you to this step.

   WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.
   Manually remove pre-existing software now? [y]: y
   Please execute configure again when you are finished
14. Specify the login name of the initial Steel-Belted Radius administrator.

The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

Enter initial admin user (account must have an associated password) [root]:

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

15. If you are not migrating your old configuration data (that is, if you answered n in Step 12.), specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: r

- If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

- If you enter r (replica server), you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.

  - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.

  - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address(es), and replication secret of the primary server.

- If you enter sa (standalone RADIUS server), you do not need to specify replication information.

16. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

Do you want to configure LDAP? [n]:

- If no, press Enter.

- If yes, type y and press Enter. You are prompted to enter the path for the LDAP library files:

Enter path for LDAP library files [~/usr/lib]:

[Administrator deletes old Steel-Belted Radius files by using the rpm -e command.]

# cd /opt/JNPRsbr/radius/install
# ./configure
To accept the default path (/usr/lib), press Enter.

17. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can monitor your Steel-Belted Radius server from an SNMP management station.

   Do you want to configure SNMP? [n]:

If no, press Enter to proceed to the next prompt.

If yes, type y and press Enter. The configure script prompts you for the information it needs to configure the jnpsnmpd.conf and startsnmp.sh files.

a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

   Choose a community string: public

b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

   Specify the range of IPv4 addresses that may query this agent, such as 1.2.3.0/24.
   Address range: 192.168.70.0/24

c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

   SNMPv2 trap sink: 192.168.70.86
   Configuration of SNMP complete.

   **NOTE:** Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

18. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

   Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

   **NOTE:** When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.
19. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: e

- If you enter e, the configure script saves the sbrd script and copies it to the /etc/init.d boot script.
- If you enter d, the configure script discards changes made to the sbrd script.
- If you enter p, the configure script saves the sbrd script and but does not copy it to the /etc/init.d boot script.

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete

You must now finish configuring the new Steel-Belted Radius server to suit your network’s authentication and accounting needs. For example, you can edit the [Addresses] section of the radius.ini file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the Steel-Belted Radius Reference Guide for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the radius process. Refer to “Starting the RADIUS Server” on page 80 for information on starting the RADIUS process. Refer to the Steel-Belted Radius Administration Guide for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

Upgrade Procedure (SuSE Linux)

Because the rpm -U command is not supported on SuSE Linux, upgrading the Steel-Belted Radius software on a server running SuSE Linux requires that you back up and uninstall your old Steel-Belted Radius software and configuration files, and then install and configure your new software. Note that, during configuration, you can migrate your Steel-Belted Radius settings from your backup directory.

For information on uninstalling your old Steel-Belted Radius software, see “Uninstalling on Linux” on page 94. Note that if you are uninstalling a 5.x version of Steel-Belted Radius, you may need to use /opt/funk instead of /opt/JNPRsbr in the command examples in this section.

NOTE: If you installed the 969531-01 or 969541-01 security patch for Steel-Belted Radius v5.3 or 5.4, uninstall the security patch before you uninstall your Steel-Belted Radius 5.x software. You must uninstall the security patch manually, using the appropriate package removal command (rpm -e).
For information on installing your new software, see “Installing the Steel-Belted Radius Server Software” on page 61.

Upgrading from RSA RADIUS Server Version 6.1

This section describes how to upgrade servers running RSA RADIUS Server v6.1 in a replication environment and how to upgrade a standalone server running RSA RADIUS Server v6.1.

Upgrading in a Replication Environment

In environments that use replication (primary and replica servers), you must upgrade your replica servers, install SBR Administrator, promote a replica server to be your new primary server, and then upgrade your former primary server.

Upgrade Your Replica Servers

You must install and configure your replica RADIUS servers before you install and configure your primary server. Perform the following steps for each replica RADIUS server in your replication realm.

1. Export your RSA RADIUS Server database to an XML (.xml) file.

   Refer to the RSA RADIUS Server Administration Guide for information on how to export your database to an XML file.

2. Back up the directory containing your RSA RADIUS Server configuration files.

   The default location for RSA RADIUS Server files is /opt/rsa/radius.

3. Execute the following command to remove the Steel-Belted Radius replication package.

   rpm -e sbr-rsa-1.0-1

   Do not run the uninstall_rsa.sh script that is installed as part of RSA RADIUS Server. Running the uninstall_rsa.sh script will delete your entire install directory.

4. Install version 6.0 of the Steel-Belted Radius software on each server.

   See “Installing the Steel-Belted Radius Server Software” on page 61 for information on how to install the Steel-Belted Radius server software on a primary server or replica server.

5. Execute the following command to run the Steel-Belted Radius configuration script:

   /opt/JNPRsbr/radius/install/configure
6. When the configuration script prompts you for a license number, enter your Steel-Belted Radius v6.0 license number.

**NOTE:** You cannot use an evaluation license to upgrade from RSA RADIUS Server to Steel-Belted Radius.

7. When the configuration script prompts you to specify what type of server (primary, replica, or standalone) you are configuring, enter r to indicate a replica server.

8. Specify the location of the `replica.ccmpkg` package generated by the primary RADIUS server (or specify the name/IP address/replication secret of the primary RADIUS server).

9. If you want to register the replica server as an Agent Host with RSA Authentication Manager v6.1 or later, specify the location of the RSA configuration files.

    Registering as an Agent Host creates a new node secret, which is required for communication between the Steel-Belted Radius server and the RSA SecurID server.

    The default location for the RSA configuration files is `/opt/rsa/radius`.

10. Merge any modified configuration (.ini) files except `eap.ini` from the Steel-Belted Radius archive directory.

    The default location for the Steel-Belted Radius archive directory is `/opt/JNPRsbr/radius/install/backups/timestamp`.

    **NOTE:** The `eap.ini` is updated by replication and should be configured only on the primary server.

11. Use a text editor to configure the `Enable=1` setting for the `.aut` file associated with each authentication method you want to use.

    Refer to the Steel-Belted Radius Administration Guide for information about authentication methods.

12. Use the `.sbrd start` command to restart the replica Steel-Belted Radius server.

    When the replica server restarts, it automatically downloads and installs its configuration package.

**Upgrade Your Primary Server**

You must install and configure your replica RADIUS servers before you install and configure your primary server. Perform the following steps to upgrade the primary RADIUS server in your replication realm.

1. Export your RSA RADIUS Server database to an XML (.xml) file.
Refer to the *RSA RADIUS Server Administration Guide* for information on how to export your database to an XML file.

2. Back up the directory containing your RSA RADIUS Server configuration files. The default location for RSA RADIUS Server files is `/opt/rsa/radius`.

3. Execute the following command to remove the Steel-Belted Radius replication package.

   ```
   rpm -e sbr-rsa-1.0-1
   ```

   Do not run the `uninstall_rsa.sh` script that is installed as part of RSA RADIUS Server. Running the `uninstall_rsa.sh` script will delete your entire install directory.

4. Install version 6.0 of the Steel-Belted Radius software on the primary server.

   See “Installing the Steel-Belted Radius Server Software” on page 61 for information on how to install the Steel-Belted Radius server software on a primary server.

5. Execute the following command to run the Steel-Belted Radius configuration script:

   ```
   /opt/JNPRsbr/radius/install/configure
   ```

6. When the configuration script prompts you for a license number, enter your Steel-Belted Radius v6.0 license number.

   **NOTE:** You cannot use an evaluation license to upgrade from RSA RADIUS Server to Steel-Belted Radius.

   7. When the configuration script prompts you to specify what type of server (primary, replica, or standalone) you are configuring, enter `p` to indicate a primary server.

   8. If you want to register the primary server as an Agent Host with RSA Authentication Manager v6.1 or later, specify the location of the RSA configuration files.

      Registering as an Agent Host creates a new node secret, which is required for communication between the Steel-Belted Radius server and the RSA SecurID server.

      The default location for the RSA configuration files is `/opt/rsa/radius`.

   9. Merge any modified configuration `.ini` files except `eap.ini` from the Steel-Belted Radius archive directory.
The default location for the Steel-Belted Radius archive directory is
/opt/JNPRsbr/radius/install/backups/timestamp.

**NOTE:** The eap.ini is updated by replication and should be configured only on the primary server.

10. Use a text editor to configure the `Enable=1` setting for the `.aut` file. associated with each authentication method you want to use.

Refer to the *Steel-Belted Radius Administration Guide* for information about authentication methods.

11. Use the `./sbrd start` command to restart the replica Steel-Belted Radius server.

When the replica server restarts, it automatically downloads and installs its configuration package.

**Configuring a Standalone Server**

To configure a standalone server to interact with RSA Authentication Manager:

1. Run the `/opt/JNPRsbr/radius/install/configure` configuration script.

2. Merge the settings from your archived configuration files with the settings in the newly-installed default configuration files.

Do not replace the new configuration files with your old ones, since your new files may include settings for functions that were not available in the RSA RADIUS Server software.

**NOTE:** Do not merge the settings from the archived version of the eap.ini file to the newly installed default eap.ini file. Use the SBR Administrator to apply the EAP settings you were using before the upgrade.

3. Copy the RADIUS database files (`radclnt.dat`, `radads.dat`, and `sbr_id.xml`) from the RSA RADIUS Server archive directory.

The default path for the archive directory is `opt/rsa/radius/install/backups/timestamp`.

4. Restart Steel-Belted Radius.

**Starting the RADIUS Server**

Use the following command to start the RADIUS server manually.

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

When you execute the sbrd start command, Steel-Belted Radius starts the mkded (btrieve) process to allow database access, and then starts the radius process.
If you change configuration settings for your Steel-Belted Radius server, you may need to restart Steel-Belted Radius to make the changes effective. As an alternative to issuing an `sbrd stop` command immediately followed by an `sbrd start` command, you can use the `sbrd restart` command to restart Steel-Belted Radius. When you issue the `sbrd restart` command, Steel-Belted Radius shuts down and then immediately starts the `mkded` (btrieve) and `radius` processes.

```
  cd server-directory
  ./sbrd restart
```

**Stopping the RADIUS Server**

Use the following commands to stop the RADIUS server:

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

When you execute the `sbrd stop` command, Steel-Belted Radius allows its subsystems to complete outstanding work and release resources, and then stops the `mkded` (btrieve) and `radius` processes gracefully.

If Steel-Belted Radius fails to stop after you issue the `sbrd stop` command, you can use the optional `force` argument to terminate all subsystems immediately.

```
  cd server-directory
  ./sbrd stop force
```

**Resetting the RADIUS Database**

If Steel-Belted Radius fails, the RADIUS database may remain running. If this happens, the Steel-Belted Radius process may refuse to run. To resolve this problem, execute the following command to stop the `mkded` (btrieve) process.

```
  cd server-directory
  ./sbrd stop force
```

After the `mkded` (btrieve) process is stopped, you can start the `radius` process and the database by executing the following command:

```
  cd server-directory
  ./sbrd start
```
Displaying RADIUS Status Information

You can use the `sbrd status` command to display status information for the RADIUS process.

```
   cd server-directory
   ./sbrd status
```

Figure 6 illustrates the output of the `sbrd status` command.

**Figure 6: Output of sbrd status Command**

```
> sbrd status
ecarter 25927 .mkded start
btrieve processes are active

    ——— Shared Memory Segments ———
    key    shmid       owner  perms   bytes    nattch status
    0x42545256   891968  ecarter     600   8000000     2

    ——— Semaphore Arrays ———
    key    semid       owner  perms  nsems
    0x42545256   167116  ecarter     660     250

btrieve shared IPC objects exist
btrieve state is running
btrieve status 1101

ecarte 2066 radius sbr.xml
radius processes are running
radius state is running
radius status 1101

Aggregate state is running
```
Chapter 6
Verifying Native User Authentication

This chapter describes how to verify that Steel-Belted Radius is configured to support native user authentication. Verifying native user authentication is the first step in troubleshooting other authentication problems.

You should complete the steps in this chapter, even if you do not anticipate using native user authentication, so that you can verify Steel-Belted Radius is installed and configured correctly.

Before You Begin

- Verify that you have installed the Steel-Belted Radius server software and SBR Administrator on a Windows, Solaris, or Linux host.
- Review the Steel-Belted Radius documentation.

Configuring the Server

After you have installed the Steel-Belted Radius software on your computer and have added the appropriate license numbers, you must configure the software. The specific steps you must perform depend on your network’s authentication and accounting needs.

A summary of the steps for configuring Steel-Belted Radius is as follows.

1. Configure each of your RADIUS client devices to communicate with your Steel-Belted Radius server. To do this, you must log into each device and run its configuration interface.

2. Run the SBR Administrator program.

   You start the SBR Administrator by running a browser and opening a connection to the Steel-Belted Radius server you want to configure.

   To open a connection on a local host listening on port 1812, use the following URL:
http://localhost:1812/sbr/index.html

To open a connection on a remote host listening on port 1812, use the following URL, where `ipaddress` is the IP address or DNS name of the remote server:


When the Steel-Belted Radius Administrator page opens, click the **Launch** link to download and start the SBR Administrator. You are then prompted to log in by entering your user credentials.

3. Use the RADIUS Clients panel to configure the server to communicate with each RADIUS client.

4. Use the Users panel to identify the users or groups of users who are permitted to access the RADIUS clients.

   Specify user attributes by selecting them in the Users panel or by creating user profiles in the Profiles dialog.

For more information, refer to the *Steel-Belted Radius Administration Guide*.

---

**Verifying Native User Authentication**

To verify native user authentication, you will need to download, install, and configure the RadiusTest utility.

**Downloading the RadiusTest Utility**

To download the RadiusTest utility:

1. Use a browser to point to the Steel-Belted Radius Technical Notes page ([http://www.juniper.net/customers/support/products/aaa_802/sbr_kb.html](http://www.juniper.net/customers/support/products/aaa_802/sbr_kb.html)).

2. Click the **Search** link.

3. When the Full Text Search window opens, enter **RD562** in the **Search** field and click the **Search** button.

4. Click the link for **Tech Note RD562** to open the “How to test SBR in Stand alone mode” technical note.

5. Scroll to the bottom of the technical note and click the **newtestr.zip** link.

6. When the File Download window opens, click **Save** and specify where to save the **newtestr.zip** file.
Installing the RadiusTest Utility

To install the RadiusTest utility:

1. Create a directory called /radiustest in the /Program Files/Juniper Networks/Steel-Belted Radius directory on your computer.
2. Navigate to where you installed the newtestr.zip file on your hard disk.
3. Double-click the newtestr.zip file icon to open the file archive.
4. Copy the four files in the file archive to the /Program Files/Juniper Networks/Steel-Belted Radius/radiustest/ directory.

Configuring Steel-Belted Radius

To configure Steel-Belted Radius to work with the RadiusTest utility:

1. Run the SBR Administrator.
2. Log into the SBR Administrator using your username and password.
3. Click the RADIUS Clients button to open the RADIUS Clients panel (Figure 7).

Figure 7: RADIUS Clients Panel
4. Click the **Add** button to open the Add RADIUS Client window (Figure 8).

**Figure 8: Add RADIUS Client Window**

5. Configure your computer as a RADIUS client entry by entering the name of your computer in the **Name** field and the IP address of your computer in the **IP Address** field. Enter `radius` in the **Shared Secret** field. Click **OK**.

6. Click the **Users > Native** button to open the Native Users panel (Figure 9).

**Figure 9: Native Users Panel**
7. Click the **Add** button to open the Add Native User window (Figure 10).

**Figure 10: Add Native User Window**

8. Configure a test user by entering a name (**testuser**) and a password (**testpw**). Click **OK**.

**Configuring the RadiusTest Utility**

To configure the RadiusTest utility:

1. Run the `radiustest.exe` application.

   The RadiusTest window (Figure 11) opens.
2. Enter the settings for your test user in the **User Info** fields.
   a. Enter the user name to be sent in the RADIUS authentication request (TESTUSER) in the **Name** field.
   b. Enter the user password (testpw) in the **Password** field.
   c. Specify an authentication type.
      
      **If you select PAP**, the user password is sent in a decodable format.
      
      **If you select CHAP**, the user password is hashed before being sent to the Steel-Belted Radius server.

3. Enter the settings for the Steel-Belted Radius server running on your computer in the **Server Info** fields.
   a. Enter the name or IP address of your computer in the **Name** field.
   b. Leave the **Dictionary** list set to radius.dct.
   c. Enter the shared secret (radius) in the **Shared Secret** field. This must be the same value you configured when you set up the RADIUS client.

4. Optionally, use the **Authentication** controls to specify whether you want to send an authentication request for the specified user to the Steel-Belted Radius server and to specify how long you want the RadiusTest utility to delay before sending the request.

   The information sent in the authentication request can be customized by modifying the [Auth-Attribs] section of the radtest.ini file.
5. Optionally, use the **Accounting Start** and **Accounting Stop** controls to specify whether you want to send accounting start and stop requests for the specified user to the Steel-Belted Radius server and how long you want the RadiusTest utility to delay before sending the request.

The information sent in the accounting request can be customized by modifying the [Acct-Start-Attribs] and [Acct-stop-Attribs] sections of the radtest.ini file.

6. Click the **Execute** button.

If native user authentication is configured properly, the **Authorization** and **Accounting** counters reflect successful authentication and accounting start messages.

If you click the **Details** button, the RadiusTest Details window displays the results of the most recent transaction:

```
RadTest Initialized - Socket bound

SessionStarting

Fixup attribute 5 = 0x8

>>> Authentication...

------- Packet: AUTH REQUEST   Length: 62 -------
User-Name = TESTUSER
User-Password = Encrypted 16 bytes:
<80> <E8> <77> <D3> <2E> <DA> <7D> <F5> <CF> <CE> <4C> <63> <EB> <2B> <6A> <A4>
NAS-IP-Address = 1.2.3.4
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002

-----------------------------------

>>> Sending Request id = 12 NAS = NAS DEFAULT
<<< Response Received for id = 12 NAS = NAS DEFAULT

------- Packet: AUTH ACCEPT   Length: 74 -------
Class = SBR

-----------------------------------

Fixup attribute 5 = 0x8

>>> Accounting Start...

------- Packet: ACCT REQUEST   Length: 119 -------
User-Name = TESTUSER
NAS-IP-Address = 1.2.3.4
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002
Acct-Status-Type = 0x00000001
Acct-Delay-Time = 0x00000064
Acct-Session-Id = 1234567
Class = SBR

-----------------------------------

>>> Sending Request id = 13 NAS = NAS DEFAULT
<<< Response Received for id = 13 NAS = NAS DEFAULT

------- Packet: ACCT RESPONSE   Length: 20 -------

-----------------------------------

Fixup attribute 5 = 0x8

>>> Accounting Stop...

------- Packet: ACCT REQUEST   Length: 119 -------
User-Name = TESTUSER
NAS-IP-Address = 1.2.3.4
```
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002
Acct-Status-Type = 0x00000002
Acct-Delay-Time = 0x0000000064
Acct-Session-Id = 1234567
Class = SBR

-----------------------------------
>>> Sending Request id = 14 NAS = NAS DEFAULT
<<< Response Received for id = 14 NAS = NAS DEFAULT
------ Packet: ACCT RESPONSE Length: 20 ------
-----------------------------------
Auth Time = 0 ms Acct Start Time = 0 ms Acct Stop Time = 0
|||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...||...|
Chapter 7
Uninstalling Steel-Belted Radius

This chapter describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows, Solaris, or Linux host.

Uninstalling on Windows

Use the Windows Add or Remove Programs control panel to uninstall the Steel-Belted Radius server software and SBR Administrator.

**Uninstalling the Steel-Belted Radius Server**

To uninstall the Steel-Belted Radius server software from a Windows host:

1. Choose **Start > Control Panel > Add or Remove Programs**.
2. When the Add or Remove Programs window opens, select **Steel-Belted Radius**.
3. Click **Remove**.
4. When a window asking you to confirm you want to remove Steel-Belted Radius opens, click **Yes**.
5. After the control panel indicates the Steel-Belted Radius server software has been uninstalled, archive or delete files remaining in the **C:\Program Files\Juniper Networks\Steel-Belted Radius\Service** directory.

**Uninstalling the SBR Administrator Files**

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Windows host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.
2. Open the directory where your SBR Administrator files are stored.

By default, this is **C:\Documents and Settings\username\Application Data\Juniper Networks**.
3. Delete the `WebDeployer` directory.

When you run the SBR Administrator application after you delete the `WebDeployer` directory, it automatically downloads the files it needs from the appropriate Steel-Belted Radius server.

---

**Uninstalling on Solaris**

This section describes how to uninstall the SNMP agent, Steel-Belted Radius server software, and SBR Administrator configuration application on a Solaris host.

**NOTE:** You should not uninstall Steel-Belted Radius if you intend to install a later version of the Steel-Belted Radius software on the same server. Doing so will make it impossible to migrate your current data and configuration information.

---

### Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from its default location `/opt/JNPRsbr`:

1. Log into the Solaris server as `root`.

2. Stop the `radius` process by issuing the following commands:

   ```
   # cd /opt/JNPRsbr/radius
   # ./sbrd stop
   ```

3. Back up your Steel-Belted Radius server directory.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup.

   ```
   # cd /opt/JNPRsbr
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xfBp - )
   ```

4. Display the list of Steel-Belted Radius software packages installed on your server by typing the following command:

   ```
   # cd /opt/JNPRsbr/radius
   # pkginfo -x | egrep "JNPR|sbr"
   JNPRsbrge JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)
   ```

5. Unconfigure the Steel-Belted Radius software by issuing the following command:

   ```
   # cd /opt/JNPRsbr/radius/install
   # ./unconfigure
   ```
6. Initiate the software uninstall by typing the `pkgrm <Edition>` command

   where `xx` represents the edition of Steel-Belted Radius you want to uninstall (`ge`, `sp`, or `ee`).

   When you are prompted to confirm you want to remove the package, enter `y`.

   ```
   # pkgrm JNPRsbrge
   
   The following package is currently installed:
   JNPRsbrge  JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition) (sparc) 6.0.0000
   
   Do you want to remove this package? y
   ## Removing installed package instance <JNPRsbrge>
   
   This package contains scripts which will be executed with super-user permission during the process of removing this package.

   Do you want to continue with the removal of this package [y,n,?,q] y
   
   After you confirm you want to continue, the uninstaller displays the name of each file it removes. The uninstall is complete when you see the following:

   Removal of <JNPRsbrge> was successful.
   ```

7. Optionally, remove the Steel-Belted Radius backup directories.

   ```
   # cd /
   # rm -rf /opt/JNPRsbr
   ```

**Uninstalling the SBR Administrator Files**

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Solaris host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.

2. Issue the following command:

   ```
   rm -rf $HOME/.junipernetworks/WebDeployer
   ```

   If you run the SBR Administrator after you delete the `/WebDeployer` directory, your browser automatically downloads the files it needs to run SBR Administrator from the target Steel-Belted Radius server.
Uninstalling on Linux

This section describes how to uninstall the Steel-Belted Radius server software and SBR Administrator configuration application on a Linux host.

NOTE: If your server is running a Red Hat version of Linux, you should not uninstall Steel-Belted Radius if you intend to install a later version of the Steel-Belted Radius software on the same server. Doing so will make it impossible to migrate your current data and configuration information.

Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from its default location (/opt/JNPRsbr):

1. Log into the Solaris server as root.

2. Stop the radius process by issuing the following commands:

   ```
   # cd /opt/JNPRsbr/radius
   # ./sbrd stop
   ```

3. Back up your Steel-Belted Radius server directory.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup.

   ```
   # cd /opt/JNPRsbr
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xBp - )
   ```

4. If you are uninstalling the SNMP module, stop all SNMP agents currently running on your server.

5. Unconfigure the Steel-Belted Radius software by issuing the following commands:

   ```
   # cd /opt/JNPRsbr/radius/install
   # ./unconfigure
   ```

6. Execute the following command to uninstall the Steel-Belted Radius server software:

   ```
   # rpm -e sbr-edition-6.0.0-0
   ```

   where edition specifies the version of Steel-Belted Radius (Global Enterprise Edition (gee); Service Provider Edition (spe); Enterprise Edition (ee)) and version specifies the software version you want to install. For example, to run the RPM package used to uninstall the GEE version of Steel-Belted Radius version 6.0, you would enter the following:

   ```
   # rpm -e sbr-gee-6.0.0-0
   ```
The uninstall script archives all current configuration files, database files, and data files to the /install/backups/timestamp directory and deletes Steel-Belted Radius from your server.

7. Optionally, remove the Steel-Belted Radius backup directories.

```
# cd /
# rm -rf /opt/JNPRsbr
```

**Uninstalling the SBR Administrator Files**

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Linux host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.

2. Issue the following command:

```
rm -r -f $HOME/.junipernetworks/WebDeployer
```

If you run the SBR Administrator after you delete the /WebDeployer directory, your browser automatically downloads the files it needs to run SBR Administrator from the target Steel-Belted Radius server.
Uninstalling on Linux
Appendix A

RIF2XML Conversion Utility

The rif2xml conversion utility is designed to simplify the process of upgrading from older versions of Steel-Belted Radius. The rif2xml conversion utility converts a RADIUS Import Format (.rif) database exported from a pre-5.0 version of Steel-Belted Radius to an XML database structure compatible with Steel-Belted Radius version 6.0.

To upgrade from older releases of Steel-Belted Radius to version 6.0, you must export your Steel-Belted Radius database to a .rif file, run the rif2xml utility to convert the .rif file to an XML database, and then import the converted XML database into a current version of Steel-Belted Radius.

**NOTE:** The exported .rif database contains the settings for users, RADIUS clients, proxies, and tunnels in Steel-Belted Radius, but does not include settings stored in external files, such as .ini files or dictionaries. The exported .rif database does not include EAP information; you can retain your eap.ini settings by reusing your configuration files.

Locating the RIF-to-XML Utility

By default, the rif2xml utility is installed in `radiusdir/services` when you install Steel-Belted Radius. You do not need to install any additional software to use the utility.

Before You Begin

1. Run Steel-Belted Radius (version 4.x or earlier) and choose **File > Export** to export some or all of your current database to a .rif file.

2. Copy the dictionary files used by Steel-Belted Radius version 4.x to a temporary directory or to a server running a current version of Steel-Belted Radius.

   The dictionary files (dictiona.dcm, *.dct, and *.dci files) used on the server from which the RIF is exported must be used on the server to which the converted XML is imported.
Using the RIF-to-XML Utility

To use the RIF-to-XML utility:

1. Copy the exported .rif file to a directory on a server running version 6.0 of the Steel-Belted Radius server software.

2. Run the RIF-to-XML utility by issuing the following command:

\[ \text{rif2xml } \text{RIF\_filename } \text{XML\_filename} \]

where:

- \text{RIF\_filename} identifies the .rif file you want to convert
- \text{XML\_filename} identifies the output XML file containing the converted information

For example, issuing the following command causes the utility to read the 7sept2005.rif file, convert the data to XML format, and write the results to the 7sept2005.xml file.

\[ \text{rif2xml } \text{7sept2005.rif } \text{7sept2005.xml} \]

You must enter filenames relative to the location of the \text{rif2xml} utility.

\[ \text{NOTE: If the file you specify for } \text{XML\_filename} \text{ exists, the RIF-to-XML utility prompts you to confirm you want to overwrite the existing file.} \]

After You Finish

1. If you have not done so, copy the dictionary files (\text{dictiona.dcm} file, *.dct files, and *.dci files) used on the server from which the RIF file was exported to the server to which the converted XML will be imported.

2. Run the SBR Administrator and log into a Steel-Belted Radius server running software version 6.0.

3. Choose \text{File} > \text{Import} to import the converted XML database and settings to your Steel-Belted Radius server.
Glossary

802.1X  The IEEE 802.1X standard defines a mechanism that allows a supplicant (client) to connect to a wireless access point or wired switch (authenticator) so that the supplicant can provide authentication credentials that can be verified by an authentication server.

AAA    Authentication, authorization, and accounting.

accounting  The process of recording and aggregating resource use statistics and log files for a user, connection session, or function for billing, system diagnosis, and usage planning.

agent   SNMP module on a managed device that responds to requests from a management station and sends traps to one or more recipients (trap sinks) to inform administrators of potential problems.

AP     Access Point. A device that serves as a communication hub to connect 802.1X wireless clients to a wired network.

attribute  RADIUS attributes carry the specific authentication, authorization, and accounting.

authentication  The process of verifying the identity of a person or file system and whether the person is allowed on a protected network.

authentication server  A back-end database server that verifies, from the credentials provided by an access client, whether the access client is authorized to use network resources.

authorization  The process of controlling the access settings, such as privileges and time limits, that the user can exercise on a protected network.

AVP    Attribute-value pair. An attribute and its corresponding value; for example, User-Name=admin.

blacklist  A profile of checklist attributes that cause Steel-Belted Radius to reject an authentication request. For example, a blacklist profile might specify calling station phone numbers or IP addresses that are blocked by Steel-Belted Radius.

CA     Certificate authority. A trusted entity that registers the digital identity of a site or individual and issues a digital certificate that guarantees the binding between the identity and the data items in a certificate.

CCM    Centralized configuration management. The process by which information is shared between a primary RADIUS server and one or more replica RADIUS servers in a multi-server environment.

certificate  A digital file signed by a CA that guarantees the binding between an identity and the contents of the certificate.

CHAP   Challenge Handshake Authentication Protocol. An authentication protocol where a server sends a challenge to a requestor after a link has been established. The requestor responds with a value obtained by executing a hash function. The server
verifies the response by calculating its own hash value: if the two hash values match, the authentication is acknowledged.

**checklist**

A list of attributes that must accompany a request for connection before the connection request can be authenticated.

**CIDR**

Classless Inter-Domain Routing. In CIDR notation, an IP address is represented as A.B.C.D/n, where /n identifies the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.168.1.22/18 means “use the first 18 bits to represent the network and the remaining 14 bits to identify hosts.” Common prefixes are /8 (Class A network), /16 (Class B network), /24 (Class C network), and /32.

<table>
<thead>
<tr>
<th>CIDR Format</th>
<th>First Address</th>
<th>Last Address</th>
<th>Number of Usable IP Addresses</th>
<th>Comparable IP Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>10.0.0.0</td>
<td>10.255.255.255</td>
<td>16,777,214</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>10.0.0.0</td>
<td>10.255.255.255</td>
<td>65,534</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>192.168.0/24</td>
<td>192.168.0.0</td>
<td>192.168.0.255</td>
<td>254</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>192.168.0/25</td>
<td>192.168.0.0</td>
<td>192.168.0.127</td>
<td>126</td>
<td>255.255.255.128</td>
</tr>
<tr>
<td>192.168.0/26</td>
<td>192.168.0.0</td>
<td>192.168.0.63</td>
<td>62</td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>192.168.0/27</td>
<td>192.168.0.0</td>
<td>192.168.0.31</td>
<td>30</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>192.168.0/28</td>
<td>192.168.0.0</td>
<td>192.168.0.15</td>
<td>14</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>192.168.0/29</td>
<td>192.168.0.0</td>
<td>192.168.0.7</td>
<td>6</td>
<td>255.255.255.248</td>
</tr>
<tr>
<td>192.168.0/30</td>
<td>192.168.0.8</td>
<td>192.168.0.15</td>
<td>6</td>
<td>255.255.255.248</td>
</tr>
<tr>
<td>192.168.0/31</td>
<td>192.168.0.8</td>
<td>192.168.0.11</td>
<td>2</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>192.168.0/32</td>
<td>192.168.0.10</td>
<td>192.168.0.10</td>
<td>0</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>192.168.0/32</td>
<td>192.168.0.10</td>
<td>192.168.0.10</td>
<td>1</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

*a. Excludes the first address (network address) and last address (broadcast address) in an address range.*

**community**

An SNMP community is a group of devices and management stations running SNMP. An SNMP device or agent may belong to more than one SNMP community.

**community string**

Character string included in SNMP messages to identify valid sources for SNMP requests and to limit access to authorized devices.

- The read community string allows an SNMP management station to issue Get and GetNext messages.
- The write community string allows an SNMP management station to issue Set messages.

**credentials**

Data that is verified when presented to an authenticator, such as a password or a digital certificate.

**CRL**

Certificate Revocation List. A data structure that identifies the digital certificates that have been invalidated by the certificates’ issuing CA prior to their expiration date.

**daemon**

See process.

**dictionary**

Text file that maps the attribute/value pairs supported by third-party RADIUS vendors.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol. Protocol by which a server automatically assigns (leases) a network address and other configuration settings to a client temporarily or permanently.</td>
</tr>
<tr>
<td>DNIS</td>
<td>Dialed number identification service. A telephone service that identifies what number was dialed by a caller.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service. Internet protocol for mapping host names, domain names, and aliases to IP addresses.</td>
</tr>
<tr>
<td>EAP-32</td>
<td>See POTP.</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>Authentication method that uses EAP (Extensible Authentication Protocol) and FAST (Flexible Authentication via Secure Tunneling).</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Authentication method that uses EAP (Extensible Authentication Protocol) and TLS (Transport Layer Security).</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>Authentication method that uses EAP (Extensible Authentication Protocol) and TTLS (Tunneled Transport Layer Security).</td>
</tr>
<tr>
<td>GTC</td>
<td>Generic Token Card.</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers.</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force. Technical subdivision of the Internet Architecture Board that coordinates the development of Internet standards.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Implementation of the TCP/IP suite that uses a 32-bit addressing structure.</td>
</tr>
<tr>
<td>IPv6</td>
<td>Implementation of the TCP/IP suite that uses a 128-bit addressing structure.</td>
</tr>
<tr>
<td>Java</td>
<td>Programming language designed for use in distributed environments such as the Internet.</td>
</tr>
<tr>
<td>JDBC</td>
<td>Java Database Connectivity. Application programming interface for accessing a database from programs written in Java.</td>
</tr>
<tr>
<td>LDIF</td>
<td>LDAP Data Interchange Format. The format used to represent directory server entries in text form.</td>
</tr>
<tr>
<td>LEAP</td>
<td>Lightweight Extensible Authentication Protocol.</td>
</tr>
</tbody>
</table>
| MAC | (1) Message Authentication Code. A MAC function takes a variable-length input and a key to produce a fixed-length output to carry authentication and integrity protection of data.  
(2) Media Access Control. The unique hardware address associated with a computer network interface. |
| managed device | A device that runs an SNMP agent. |
| management station | Host that monitors and controls managed devices running SNMP agents. |
| MIB | Management Information Base. A database of objects, such as alarm status or statistics counters, that can be monitored or overwritten by an SNMP management station. |
MS-CHAP
Microsoft CHAP. Proprietary version of CHAP.

NAD
Network Access Device. Any device that accepts connection requests from remote users, authenticates users through RADIUS, and routes user onto the network. Identical in meaning to remote access server (RAS) and network access server (NAS).

NAT
Network Address Translation. Technique that allows an intranet to use IP addresses that are different from what the outside Internet thinks.

native user
A user authenticated by Steel-Belted Radius using its internal authentication database.

ODBC
Open Database Connectivity. Standard (open) application programming interface for accessing a database.

OTP token
One-time password token. Hardware or software module that generates one-time passwords that can be used to authenticate a user.

PAC
Protected Access Credential. A high-entropy secret that is known to both the RADIUS client and the RADIUS server to secure the TLS handshake in EAP-FAST authentication.

PAP
Password Authentication Protocol. An authentication protocol where a requestor sends an identifier and password to a server after a link has been established. If the identifier and password match an entry in the server’s database, the authentication is acknowledged.

PEAP
Protected Extensible Authentication Protocol. A two-phase authentication protocol where (1) an authentication server is authenticated to a supplicant using a digital certificate and a secure channel is established; and (2) the supplicant is authenticated to the authentication server through the secure channel.

POTP
Protected One-Time Password. EAP method that uses one-time password tokens for unilateral or mutual authentication.

process
A program on a Solaris or Linux host that runs continuously to handle service requests. Sometimes referred to as a daemon.

proxy RADIUS
Process of authenticating users whose profiles are on other RADIUS servers by forwarding access-request packets received from a RADIUS client to a remote RADIUS server (the proxy target), and then forwarding the response from the remote server back to the RADIUS client.

proxy target
The remote RADIUS server that actually performs authentication in a proxy RADIUS sequence.

RADIUS
Remote Authentication Dial In User Service. A client/server security administration standard that functions as an information clearinghouse, storing authentication information about users and administering multiple security systems across complex networks.

RAS
Remote Access Server. See network access device.

return list
A list of attributes that Steel-Belted Radius must return to a RADIUS client after authentication of a user succeeds. The return list usually provides additional parameters that the RADIUS client needs to complete the connection.

roaming
The ability to move from one Access Point coverage area to another without interruption of service or loss of connectivity.

RSA SecurID
Security token system that allows remote-access users to generate a pseudorandom value they can forward as part of an authentication sequence.

session ID
Session Identifier. A string of characters uniquely identifying the session.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1</td>
<td>Secure Hash Algorithm-1. A one-way cryptographic function that takes a message of any length and produces a 160-bit message digest.</td>
</tr>
<tr>
<td>shared secret</td>
<td>An encryption key known only to the sender and receiver of data.</td>
</tr>
<tr>
<td>silent discard</td>
<td>The process of discarding a packet without further processing and without notification to the sender.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer. Program layer that manages the security of messages on a network.</td>
</tr>
<tr>
<td>supplicant</td>
<td>The client in an 802.1X-authenticated network.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System (with enhancements). An authentication protocol that allows a RAS to communicate with an authentication server to determine if a user should have access to a protected network.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security.</td>
</tr>
<tr>
<td>trap</td>
<td>An SNMP message that reports a significant event, such as a problem, error, or change in state, that occurred within a managed device.</td>
</tr>
<tr>
<td>trap sink</td>
<td>The destination for trap messages sent by an SNMP agent on a managed device.</td>
</tr>
<tr>
<td>TTLS</td>
<td>Tunneled Transport Layer Security.</td>
</tr>
<tr>
<td>user database</td>
<td>A database where a RADIUS server keeps information about users, such as authentication information and network access permissions.</td>
</tr>
<tr>
<td>user profile</td>
<td>A record in the user database that describes how a particular user or class of users should be configured during authentication and authorization.</td>
</tr>
<tr>
<td>VSA</td>
<td>Vendor Specific Attributes.</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy. An encryption method designed to encrypt traffic between a WLAN client and an access point.</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network.</td>
</tr>
</tbody>
</table>
# Index

## Numerics

<table>
<thead>
<tr>
<th>Numeral</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>1</td>
</tr>
<tr>
<td>sbrd</td>
<td>92, 94</td>
</tr>
<tr>
<td>sbrd</td>
<td>55, 81</td>
</tr>
<tr>
<td>sbrd</td>
<td>55, 80</td>
</tr>
<tr>
<td>sbrd</td>
<td>56, 82</td>
</tr>
<tr>
<td>sbrd</td>
<td>56, 81</td>
</tr>
<tr>
<td>sbrd</td>
<td>56, 81</td>
</tr>
<tr>
<td>sbrd</td>
<td>2, 31, 59</td>
</tr>
<tr>
<td>SQL</td>
<td>1</td>
</tr>
<tr>
<td>SQL</td>
<td>9, 12</td>
</tr>
<tr>
<td>stop</td>
<td>56, 81</td>
</tr>
</tbody>
</table>

## A

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a License for Server window</td>
<td>21, 39, 66</td>
</tr>
<tr>
<td>auto-restart</td>
<td>12, 13</td>
</tr>
</tbody>
</table>

## D

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>directed authentication</td>
<td>2</td>
</tr>
<tr>
<td>DNIS</td>
<td>2</td>
</tr>
</tbody>
</table>

## F

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>56, 81</td>
</tr>
</tbody>
</table>

## I

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAS</td>
<td>17</td>
</tr>
<tr>
<td>Internet Authentication Service</td>
<td>IAS</td>
</tr>
</tbody>
</table>

## L

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>1</td>
</tr>
<tr>
<td>license number</td>
<td>20, 35, 39, 48, 62, 66, 72</td>
</tr>
</tbody>
</table>

## M

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>9, 11, 13</td>
</tr>
<tr>
<td>Microsoft IAS</td>
<td>17</td>
</tr>
</tbody>
</table>

## O

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODBC compliant</td>
<td>9, 12</td>
</tr>
<tr>
<td>Open Database Connectivity</td>
<td>9, 12</td>
</tr>
<tr>
<td>Oracle</td>
<td>9, 12</td>
</tr>
</tbody>
</table>

## P

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfmon</td>
<td>2</td>
</tr>
<tr>
<td>Perl</td>
<td>12, 13</td>
</tr>
<tr>
<td>process, RADIUS</td>
<td>46, 71</td>
</tr>
<tr>
<td>proxy RADIUS</td>
<td>1</td>
</tr>
</tbody>
</table>

## R

<table>
<thead>
<tr>
<th>Item</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS daemon</td>
<td>46, 71</td>
</tr>
<tr>
<td>radiusdir</td>
<td>ix</td>
</tr>
<tr>
<td>radtest.ini</td>
<td>88</td>
</tr>
<tr>
<td>rif file</td>
<td>97</td>
</tr>
<tr>
<td>rif2xml conversion utility</td>
<td>97</td>
</tr>
</tbody>
</table>