# Pulse Secure Steel-Belted Radius

## Installation and Upgrade Guide

## Release 6.27


| | |
|---|---|
| Release | **6.27** |
| Published Date | **October 2019** |

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 authors 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 Tschalär (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.

Strut Layout Java AWT layout manager Copyright © 1998 Matthew Phillips (mpp@ozemail.com.au).

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.

M0817.

The original tac_plus code (which this software and considerable parts of the documentation are based on) is distributed under the following license:

Copyright (c) 1995-1998 by Cisco systems, Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies of the software and supporting documentation, the name of Cisco Systems, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that modification, copying and distribution is by permission of Cisco Systems, Inc.

Cisco Systems, Inc. makes no representations about the suitability of this software for any purpose. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The code written by Marc Huber is distributed under the following license: Copyright (C) 1999-2015 Marc

Huber (<Marc.Huber@web.de>).

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 end-user documentation included with the redistribution, if any, must include the following acknowledgment:

  This product includes software developed by Marc Huber (<Marc.Huber@web.de>).

  Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED 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 ITS AUTHOR 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.

apache/httpclient, that is used in SBR-E software is of license type "Apache License 2.0" and refer the following URL for more information:
https://github.com/apache/httpcomponents-client/blob/4.5.x/LICENSE.txt.

bcgit/bc-java, that is used in SBR-E software is of license type "MIT" and refer the following URL for more information:
https://github.com/bcgit/bc-java/blob/r1rv60/LICENSE.html.

google/gwt, that is used in SBR-E software is of license type "Apache License 2.0" and refer the following URL for more information:
http://www.gwtproject.org/terms.html.

gwtbootstrap3/gwtbootstrap3, that is used in SBR-E software is of license type "Apache License 2.0" and refer the following URL for more information:
https://github.com/gwtbootstrap3/gwtbootstrap3/blob/0.9.3/LICENSE.

kohsuke/WinSW, that is used in SBR-E software is of license type "MIT" and refer the following URL for more information:
https://github.com/kohsuke/winsw/blob/winsw-v2.2.0/LICENSE.txt.

laaglu/lib-gwt-file, that is used in SBR-E software is of license type "GNU Lesser General Public License v3" and refer the following URL for more information:
http://www.gnu.org/licenses/lgpl.html .

# Revision History

The following table lists the revision history for this document.

| Revision | Date | Description |
|---|---|---|
| 6.27 | October 2019 | 6.27-R1 Updates |
| 6.26 | May 2019 | 6.26-R1 Updates |

# Contents

Revision History ..... 6
Requesting Technical Support ..... 11
About This Guide ..... 12
Audience ..... 12
What's in This Manual? ..... 12
Typographical Conventions ..... 13
Editions/Used In ..... 13
Related Documentation ..... 13
Requests for Comments (RFCs) ..... 14
Contacting Technical Support ..... 15
Chapter 1 ..... 16
Overview ..... 16
Steel-Belted Radius Features ..... 16
Chapter 2 ..... 18
Preparing for Installation ..... 18
Review the Release Notes ..... 18
Select a Server ..... 18
Verify System Requirements ..... 19
Verify Network Connectivity ..... 20
Verify Host Name Resolution ..... 21
Verify Administrator Account Access ..... 21
Obtain a Server License Number ..... 21
Chapter 3 ..... 22
Windows Installation ..... 22
Before You Begin ..... 22
Prerequisites for Java Web Server in Windows ..... 22
Fresh Installation ..... 22
Backup of Existing Configuration/User Data ..... 22
Installing the Steel-Belted Radius Server Software ..... 23

Start the Steel-Belted Radius....30
Launch the Steel-Belted Radius Administrator....30
Configure Steel-Belted Radius Server....30
Restoration of Backed-Up Data....31
Upgrading the Steel-Belted Radius....31
Backup of Existing Configuration/User Data....31
Installation of Steel-Belted Radius – Upgrade....32
Start the Steel-Belted Radius Service....34
Launch the Steel-Belted Radius Administrator/WebGUI....34
Restoration of Previous Configuration....35
Manual Migration of Configuration Files....35
Manual Migration of XML Configuration....35
Manual Migration of Java scripts....35
Manual Migration of Certificates....35
Manual Migration of Dictionaries....36
Manual Migration of Third-Party Plugins and other Binaries....36
Inclusion of Newly Added/Deleted Parameters....36
Stopping the Steel-Belted Radius Service....36
Starting the Steel-Belted Radius Service....36
Upgrading from a 30-Day Trial Installation....37
Chapter 4....38
Linux Installation....38
Before You Begin....38
Fresh Installation....38
Installing the RPM in SUSE Platform....38
Installing the RPM in SUSE 15 Platform....42
Installing the RPM in RHEL Platform....43
Configuring the Radius Application....44
Start the Application....48
Launch the SBR Administrator....48
Upgrade....48
Back up of Existing Radius Directory....49
Installing the RPM in SUSE Platform....49

Installing the RPM in SUSE15 platform ....52
Installing the RPM RHEL Platform ....53
Configuring the Radius Application ....54
Inclusion of Newly Added/Deleted Parameters ....57
Start the Application ....58
Launch the SBR Administrator ....58
Starting the RADIUS Server ....58
Stopping the RADIUS Server ....58
Displaying RADIUS Status Information ....58
Unconfiguring the RADIUS Server ....59
Upgrading from a 30-Day Trial Installation ....59
Chapter 5 ....61
Migrating Steel-Belted Radius from Solaris to Linux ....61
Steps to Migrate Steel-Belted Radius from Solaris to Linux ....61
Back-up the Solaris Steel-Belted Radius 6.17 ....61
Fresh Installation of Steel-Belted Radius in Linux ....61
Manual Restoration of Steel-Belted Radius Files ....62
Manual Migration of Configuration files ....62
Manual Migration of JRE extensions ....63
Manual Migration of SNMP Configuration ....63
Manual Migration of Dictionaries ....63
Manual Configuration of JavaScript files ....63
Manual Migration of Third-party plugins and other Binaries ....63
Inclusion of newly added/deleted parameters ....63
Starting Steel-Belted Radius Application ....64
Launch the Steel-Belted Radius Administrator/WebGUI ....64
Manual Migration of Licenses ....64
Migrating Configuration Data in SBR Administrator ....64
Manual Migration of ROOT Certificates ....65
Chapter 6 ....66
Uninstalling Steel-Belted Radius ....66
Uninstalling Steel-Belted Radius on Windows ....66
Uninstalling the Steel-Belted Radius Server ....66
Uninstalling the Legacy SBR Administrator Files ....66
Uninstalling Steel-Belted Radius on Linux ....66
Uninstalling the Steel-Belted Radius Server ....67
Uninstalling the Legacy SBR Administrator Files ....67

Glossary ..... 68
Index ..... 73

# Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—For product warranty information, visit **https://www.pulsesecure.net**
- Find product documentation: **https://www.pulsesecure.net/techpubs/**
- Find solutions and answer questions using our Knowledge Base: **https://www.pulsesecure.net/support**

### Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://www.pulsesecure.net/support.**
- Call Phone: 1-844-751-7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see **https://www.pulsesecure.net/support**

# About This Guide

The Steel-Belted Radius Installation and Upgrade Guide describes how to install or upgrade the Steel-Belted Radius software on a server running the Linux operating system or the Windows 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 or upgrade the Steel-Belted Radius server software on a Windows host.
- Chapter 4, "Linux Installation" describes how to install or upgrade the Steel-Belted Radius server software on a Linux host.
- Chapter 5, "Migrating Steel-Belted Radius from Solaris to Linux" describes how to migrate the Steel-Belted Radius from Solaris to Linux.
- Chapter 6, "Uninstalling Steel-Belted Radius" describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows or Linux host.
- 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 1: Typographical Conventions**

| Convention | Description | Examples |
|---|---|---|
| Bold typeface | Indicates buttons, field names, dialog names, and other user interface elements. | Use the Scheduling and Appointment tabs to schedule a meeting. |
| *Italics* | Identifies Book names | See the *Steel-Belted Radius Administration guide* |
| Brackets [ ] | To enclose optional items in format and syntax descriptions. | For example, the first Attribute argument is required; the syntax indicates you can include an optional second Attribute argument by entering a comma and the second Attribute argument (without the square brackets) on the same line.<br><br><add \| replace> = Attribute [,Attribute] |
| Angle brackets < > | To enclose a list from which you must choose an item in format and syntax descriptions. | Use < > brackets to select an item.<br><br><add \| replace> = Attribute [,Attribute] |
| Vertical bar ( \| ) | It separates items in a list of choices. | Use the \| bar to separate item<br><br><add \| replace> = Attribute [,Attribute] |

## 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
- EE: Enterprise Edition

## Related Documentation

Table 2 lists and describes the Steel-Belted Radius document set:

**Table 2: Steel-Belted Radius Documentation**

| Document | Description |
|---|---|
| Steel-Belted Radius Installation and Upgrade Guide | Describes how to install or upgrade the Steel-Belted Radius software on the server and SBR Administrator applications on a client workstation |
| Steel-Belted Radius Administration and Configuration Guide | Describes how to configure and operate the Steel-Belted Radius and its separately licensed modules |
| Steel-Belted Radius Reference Guide | Describes the settings and valid values of the Steel-Belted Radius Configuration files |
| Steel-Belted Radius Release Notes | Contains the latest information about features, changes, known problems and resolved problems |

| Document | Description |
|---|---|
| Steel-Belted Radius LDAP Scripting Guide | Describes how to use scripts written in JavaScript programming language to enhance the search capabilities of the Steel-Belted Radius LDAP Authentication module |

Note: If the information in the Release Notes differs from the information in any guide, follow the Release Notes.

## Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFCs) online at **https://www.ietf.org/rfc.html.** Table 3 lists the RFCs that apply to this guide.

**Table 3: Related RFCs**

| RFC Number | Title |
|---|---|
| RFC 1155 | *Structure and Identification of Management Information for TCP/IP-based Internets. M. Rose, K. McCloghrie*, May 1990. |
| RFC 1213 | *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II. K. McCloghrie, M. Rose*, March 1991. |
| RFC 2271 | *An Architecture for Describing SNMP Management Frameworks. D. Harrington, R. Presuhn, B. Wijnen,* January 1998. |
| RFC 2284 | *PPP Extensible Authentication Protocol (EAP). L. Blunk, J. Volbrecht,* March 1998. |
| RFC 2433 | *Microsoft PPP CHAP Extensions. G. Zorn, S. Cobb*, October 1998. |
| RFC 2548 | *Microsoft Vendor-specific RADIUS Attributes. G. Zorn.* March 1999. |
| RFC 2607 | *Proxy Chaining and Policy Implementation in Roaming. B. Aboba, J. Vollbrecht*, June 1999. |
| RFC 2618 | *RADIUS Authentication Client MIB. B. Aboba, G. Zorn*. June 1999. |
| RFC 2619 | *RADIUS Authentication Server MIB. G. Zorn, B. Aboba*. June 1999. |
| RFC 2620 | *RADIUS Accounting Client MIB. B. Aboba, G. Zorn*. June 1999. |
| RFC 2621 | *RADIUS Accounting Server MIB. G. Zorn, B. Aboba*. June 1999. |
| RFC 2622 | *PPP EAP TLS Authentication Protocol. B. Aboba, D. Simon,* October 1999. |
| RFC 2809 | *Implementation of L2TP Compulsory Tunneling via RADIUS. B. Aboba, G. Zorn.* April 2000. |
| RFC 2865 | *Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson.* June 2000. |
| RFC 2866 | *RADIUS Accounting. C. Rigney*. June 2000. |
| RFC 2867 | *RADIUS Accounting Modifications for Tunnel Protocol Support. G. Zorn, B. Aboba, D. Mitton.* June 2000. |
| RFC 2868 | *RADIUS Attributes for Tunnel Protocol Support. G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret.* June 2000. |
| RFC 2869 | *RADIUS Extensions. C. Rigney, W. Willats, P. Calhoun*. June 2000. |
| RFC 2882 | *Network Access Servers Requirements: Extended RADIUS Practices. D. Mitton.* July 2000. |
| RFC 3162 | *RADIUS and IPv6. B. Aboba, G. Zorn, D. Mitton.* August 2001. |
| RFC 3575 | *Internet Assigned Numbers Authority (IANA) considerations for Remote Authentication Dial In User Service (RADIUS). B. Aboba,* July 2003. |
| RFC 3579 | *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).*<br>*B. Aboba, P. Calhoun,* September 2003. |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.* |

## Contacting Technical Support

For technical support, open a support case using the Case Manager link at:

**https://www.pulsesecure.net/support/**

Check our website (**https://www.pulsesecure.net/support/)** for additional information and technical notes. When you are running Legacy SBR Administrator, you can choose **Web** > **Steel-Belted Radius User page** to access a special home page for Steel-Belted Radius users. When you are running WebGUI, you can choose **Help** > **Home Page** > **Steel-Belted Radius Home 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 6.1).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- Question or description of the problem, with as much detail as possible.
- Any documentation that can help resolve the problem, such as error messages, memory dumps, compiler listings, and error logs.

# Chapter 1

# Overview

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, 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: 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: 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: 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: Auto-restart permits the Steel-Belted Radius server to restart itself automatically if it experiences a shutdown.
- GEE: 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: 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: Your choice of interface lets you configure Steel-Belted Radius by means of a graphical SBR Administrator program or by means of LDAP (either programmatically or at the command line prompt).
- Linux 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.

# 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 7 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.
- Server does not run public network services such as FTP or HTTP—Running public network services or applications unrelated to user authentication on the Steel-Belted Radius server may adversely affect the performance of Steel-Belted Radius, since it must compete with other services and applications for the server's CPU resources. Moreover, running public network services on the authentication server potentially opens the server to malicious attacks.
- Server uses secure shared secret—The shared secret configured for Steel-Belted Radius protects all communications to and from the server, including session keys for wireless data encryption. You should configure shared secrets that are long enough and random enough to resist attack, and you should avoid using the same shared secret throughout your network.
- File permissions are set appropriately—If your Steel-Belted Radius software is running on a Linux server, you should set file permissions to limit access to configuration, accounting, and log files used by Steel- Belted Radius. You can configure default file permissions for Steel-Belted Radius files in the sbrd.conf file. Optionally, you can override the default file permissions specified in the sbrd.conf file for individual log files.

For information on setting permissions for Steel-Belted Radius files, refer to the *Steel-Belted Radius Administration Guide.*

## Verify System Requirements

This section describes the hardware and software requirements for running Steel-Belted Radius on the Windows, 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 administrative user interface.

**Table 4: Windows Server – System Requirements**

| Windows Server | System Requirements |
|---|---|
| Operating system | For the qualified and supported Operating Systems, refer section "System Requirements" in Steel-Belted Radius. |
| Networking | TCP/IP must be configured. |
| Memory | 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.)<br><br>The SBR Administrator requires a host with at least 256 megabytes of memory. |
| Disk space | The Steel-Belted Radius server software requires approximately 200 - 400 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system's product configuration.<br><br>The SBR Administrator requires approximately 80 megabytes of local disk space. |
| Monitor | The SBR Administrator requires a monitor that supports 256+ colors. |
| Web browser | For the qualified and supported Web browser, refer section "System Requirements" in **Steel-Belted Radius Release Notes**. |
| Database (optional) | For the qualified and supported SQL Database server, refer section "System Requirements" in *Steel-Belted Radius Release Notes*. |
| 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.<br><br>The free Adobe Reader software can be downloaded from **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, 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:<br>• TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI)<br>• TCP 1812 – Steel-Belted Radius control port<br>• TCP 1813 – SBR Administrator port<br>• UDP 1645 – Legacy RADIUS authentication port<br>• UDP 1646 – Legacy RADIUS accounting port<br>• UDP 1812 – IETF RADIUS authentication port<br>• UDP 1813 – IETF RADIUS accounting port<br>• UDP port range – Proxy RADIUS source port range (specified in the **https://www.pulsesecure.net/support** file. Default is 1024–65535.)<br>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 – 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**

| Linux Server | System Requirements |
|---|---|
| Hardware | Intel X86 workstation or server |
| Operating system | For the qualified and supported Operating System, refer section "System Requirements" in *Steel-Belted Radius Release Notes.* |
| Memory | At least 256 megabytes of working memory (512 megabytes for servers with more than 10,000 RADIUS users.)<br>The SBR Administrator requires a host with at least 256 megabytes of memory. |
| Disk space | 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.<br>The Linux version of SBR Administrator requires at least 88 megabytes of local disk space. |
| Monitor | The SBR Administrator requires a monitor that supports 256+ colors. |
| Networking | TCP/IP must be configured. |
| Perl | Perl is required if you want to use the auto-restart feature of Steel-Belted Radius. The first line of the radius script must specify the Perl executable path. For example, if Perl is installed as /usr/local/bin/perl, then the first line of the radius script must specify:<br>#!/usr/local/bin/perl. |
| Database (optional) | For the qualified and supported SQL Database server, refer section "System Requirements" in *Steel-Belted Radius Release Notes.* |
| Web browser (optional) | For the qualified and supported Web browser, refer section "System Requirements" in *Steel-Belted Radius Release Notes.* |
| 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. |
| 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:<br>• TCP 667 – LDAP Configuration Interface (LCI) port (required ifyou use the LCI)<br>• TCP 1812 – Steel-Belted Radius control port<br>• TCP 1813 – SBR Administrator port<br>• UDP 1645 – Legacy RADIUS authentication port<br>• UDP 1646 – Legacy RADIUS accounting port<br>• UDP 1812 – IETF RADIUS authentication port<br>• UDP 1813 – IETF RADIUS accounting port<br>• UDP port range – Proxy RADIUS source port range (specified in the radius.ini file. Default is 1024–65535.) |

## 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.pulsesecure.net

Pinging foo.pulsesecure.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 (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 either a separate license key for each installation or a site license key.

The SBR Administrator may be deployed 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 Pulse Secure.

# Chapter 3

# Windows Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software 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 7.
- 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.

### Prerequisites for Java Web Server in Windows

Java web server (Jetty) will run as a separate process/service to host the SBR Administrator WebGUI application.

The following are the pre-requisites to run the Java Web server service in Windows:

- Java (version 1.80 or above)
- .NET Framework (version 4)

# Fresh Installation

### Backup of Existing Configuration/User Data

Note: If you are installing Steel-Belted Radius for the first time, skip this step and go to section "Installing the Steel-Belted Radius Server Software.

Note: SBR-E Windows 6.1.7 was supported in Windows 2003 and other lower versions. There may be situations where an Operating System upgrade can happen on the same machine or Steel- Belted Radius getting migrated from one machine to another. The below procedure explains how to carry out Steel-Belted Radius upgrade in each of these scenarios.

Note: If you are using the configuration files of 6.1.7, then back up the configuration files from the directory "C:\Program Files (x86)\Juniper Networks\Steel-Belted Radius\Service".

The backup of the existing configuration and data are to be stored manually whenever you are re-installing the same version or installing a newer version Steel-Belted Radius software. Follow the steps given below for backing up the old configuration data.

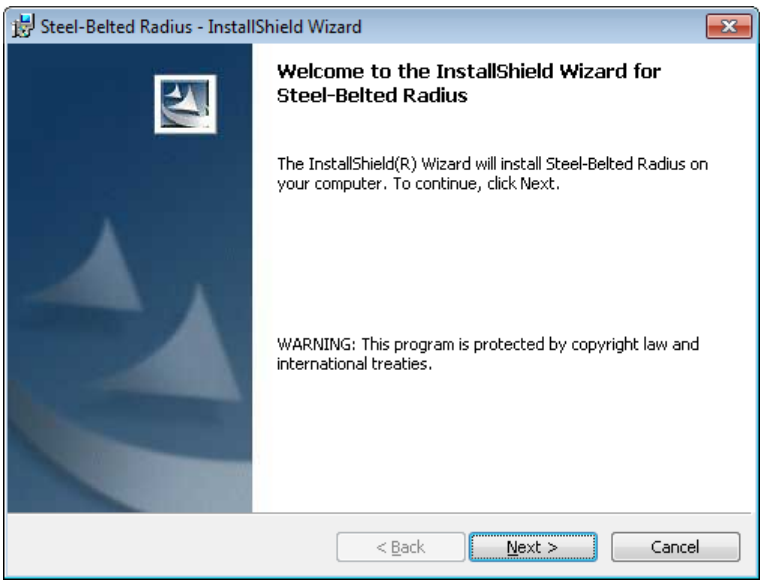
- When you are re-installing the Steel-Belted Radius server software, the installation script saves your existing configuration to a backup directory (Steel-Belted Radius\Service_Date_IDnumber). If you are re- installing the Steel-Belted Radius on the same machine, you can copy the configuration files from the backup directory to the Steel-Belted Radius server directory (Steel-Belted Radius\Service) to restore your previous configuration.
- If you are installing Steel-Belted Radius software in a new machine and you want to use the configuration settings from another machine, you have to manually take a backup of the "Steel-Belted Radius\Service" directory and copythe required configuration files data to the other machine.
- Export your Steel-Belted Radius database to an Extensible Markup Language (.xml) file. Refer to *Steel-Belted Radius Administration Guide* (Appendix E - "Importing and Exporting Data") for information on how to export your Steel-Belted Radius database to an .xml file. You can then import the (.xml) file after installation.

## 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. Make sure you have access to the downloaded Steel-BeltedRadius Windows Installer Package either on the local system or through network share. You can download an evaluation version of Steel-Belted Radius from the Pulse Secure website.
    - Local installation – Copy the Steel-Belted Radius Windows Installer Package (Steel-Belted Radius.msi file) to your computer and run it locally.
    - Network installation – Locate and run the Steel-Belted Radius Windows Installer Package (Steel- Belted Radius.msi file) from a network server.
3. Double click the Steel-Belted Radius.msi package. The following Welcome window opens. To continue, click Next>.

    **Figure 1: Welcome Window**

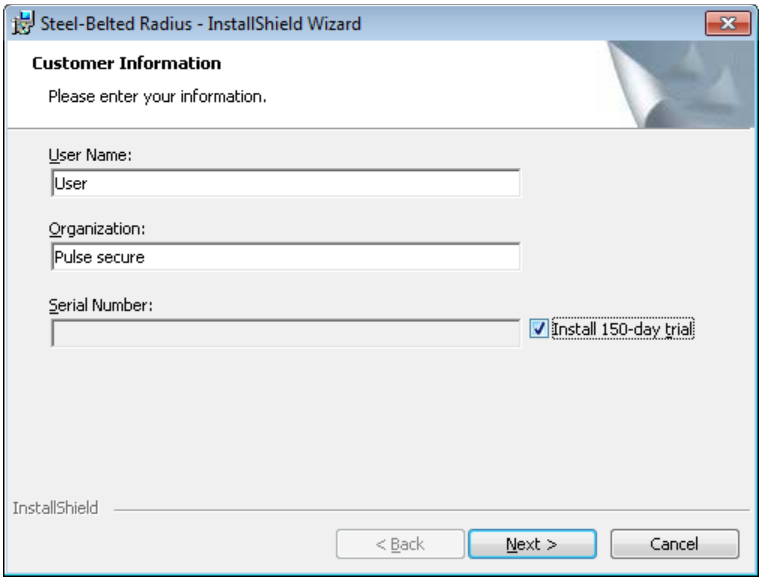
    
    

4. When the Customer Information window opens, enter the following details:
    - Enter your user name in the User Name field.
    - Enter the name of your company in the Organization field.
    - If you are installing a purchased copy of the Steel-Belted Radius server, enter the

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 select the Install 150-Day trial check box (shown in Figure 2). Click Next to continue.

**Figure 2: Customer Information Window**



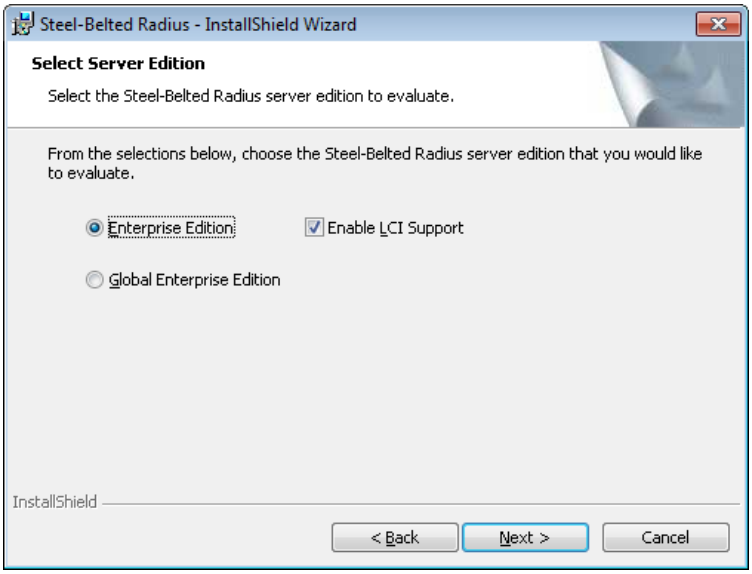

5. If you have selected the Install 150-Day trial check box in 4, use the Select Server Edition window (shown in Figure 3) to specify which edition of the Steel-Belted Radius server software you want to install.

   The Steel-Belted Radius server software is available in two editions:

   - Enterprise Edition (EE) (with optional LDAP Configuration Interface support)
   - Global Enterprise Edition (GEE)

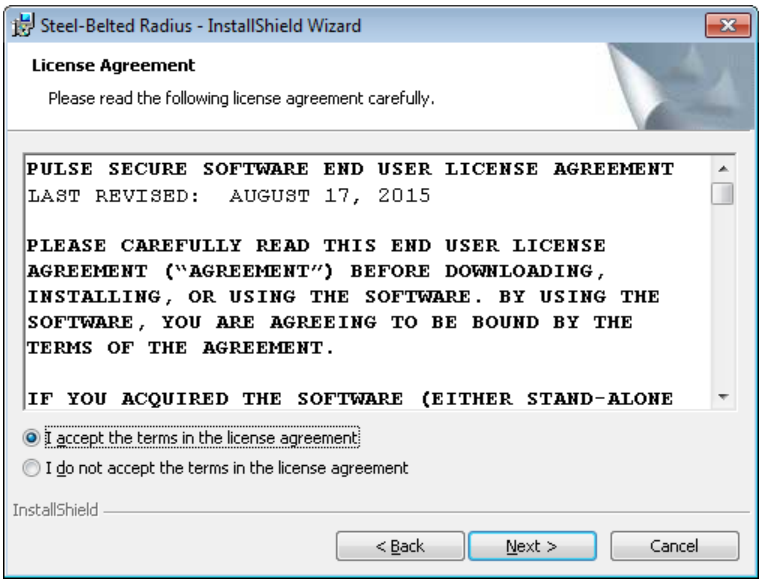
   Select the Enable LCI Support check box for LDAP Configuration Interface. Click Next to continue.

**Figure 3: Select Server Edition**



6. When the License Agreement window (shown in Figure 4) opens, read the agreement, click the radio button I accept the terms in the license agreement, and click Next to continue.

**Figure 4: License Agreement**



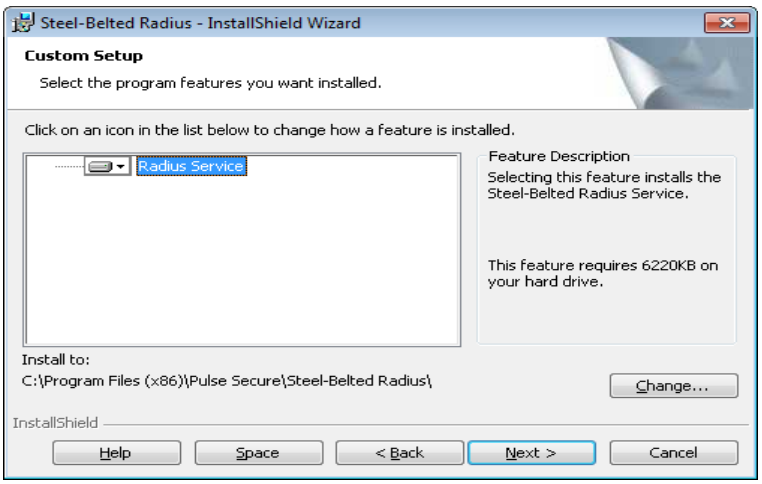

When the Custom Setup window (shown in Figure 5) appears, specify whether you want to change the default settings for installing Steel-Belted Radius.

By default, the Steel-Belted Radius software and documentation are installed in the C:\Program Files (x86)\Pulse Secure\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.

7. Click Next to continue.

Note: If you're using SBR Version 6.1.7, then the installation directory will be "C:\Program Files (x86)\Juniper Networks\Steel-Belted Radius\Service".

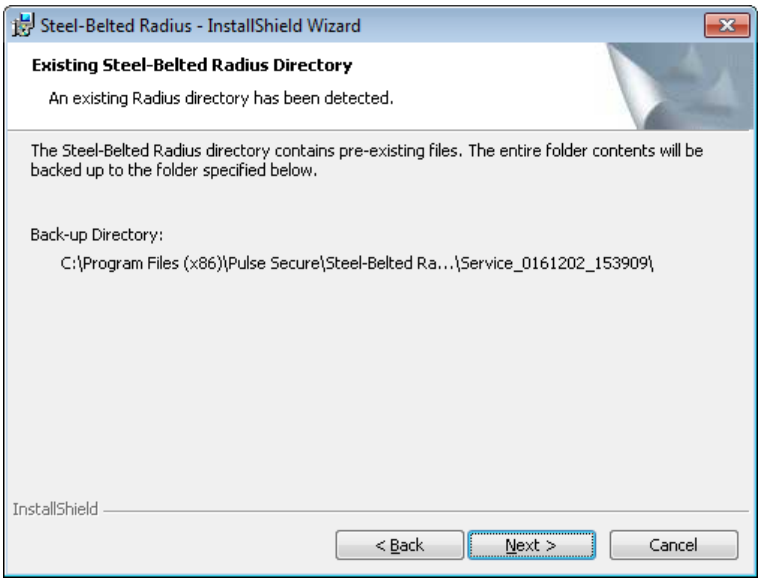
**Figure 5: Custom Setup Window**




If you are updating an existing Steel-Belted Radius installation, a window (shown in Figure 6) identifies the location where your current files will be archived in a Backup directory. 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 (x86)\Pulse Secure\Steel-Belted

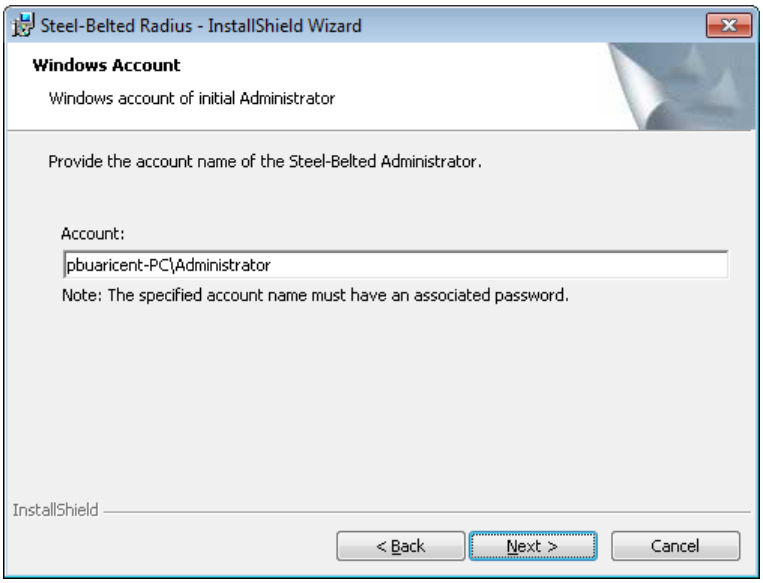
Radius\Service_Date_IDnumber directory. Click Next to continue.

**Figure 6: Existing Steel-Belted Radius Directory Window**




When the Windows Account window (shown in Figure 7) opens, enter your Windows administrator account name in the Account field. Click Next to continue. The Windows account you enter is the default login account for SBR Administrator. You must use this account name the first time you log into SBR Administrator.

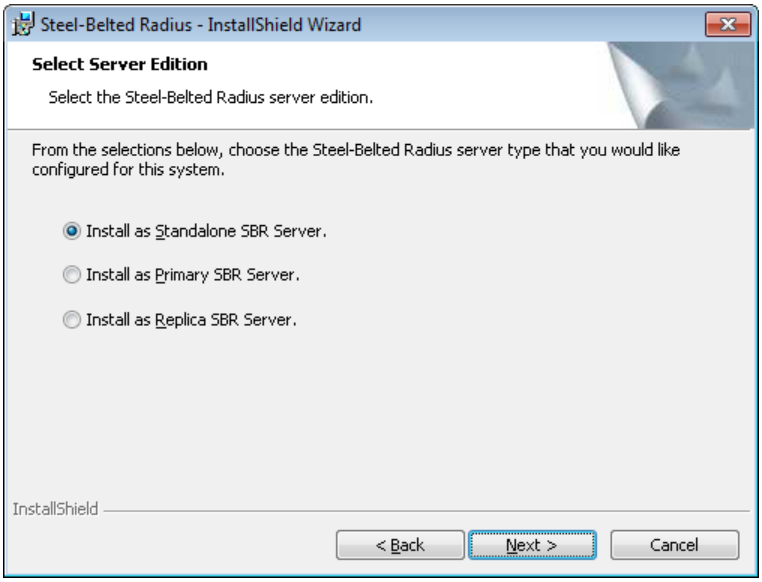
**Figure 7: Windows Account Window**




Note: Make sure the login system 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.

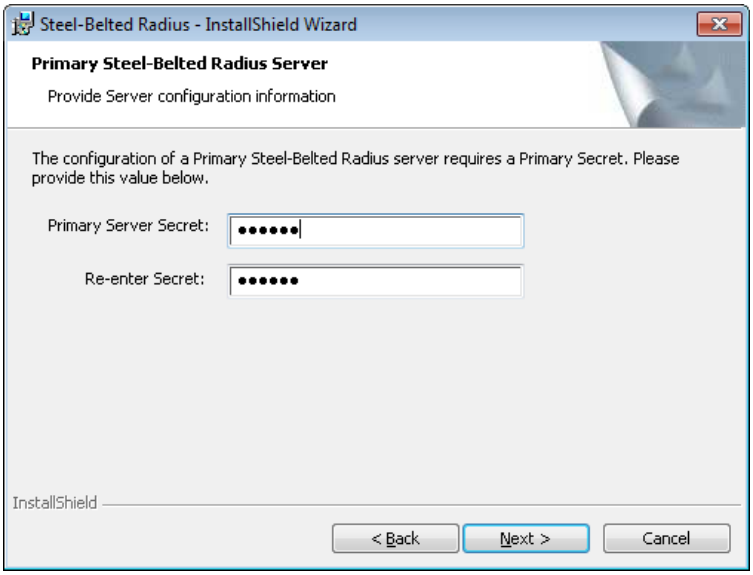
8. When the Select Server Edition window (shown in Figure 8) opens, specify whether you want to install a standalone server, a primary server, or a replica server.

**Figure 8: Select Server Edition Window**




- 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 another window (shown in Figure 9) 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.

**Figure 9: Primary Steel-Belted Radius Server Window**

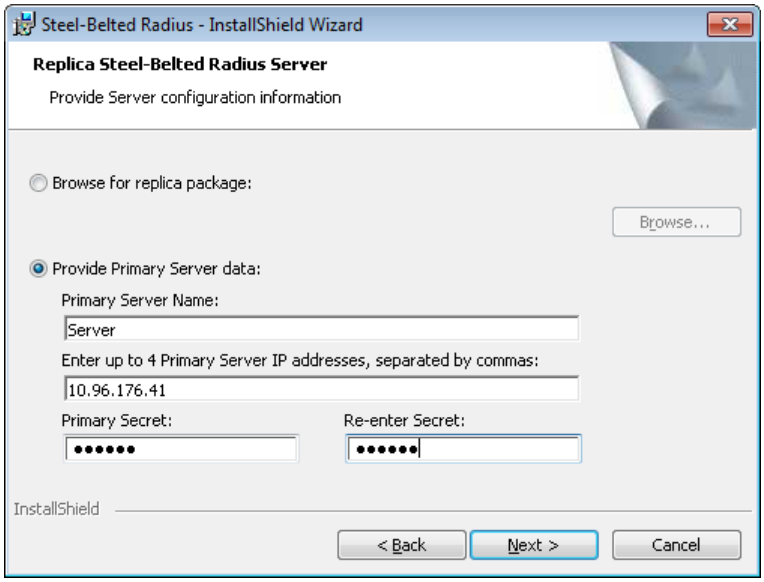



If you click the Install as Replica SBR Server button and click Next, you are prompted to another Window (shown in Figure 10). Specify how the replica server can locate the replica package containing your Steel- Belted Radius replication settings.

- 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.

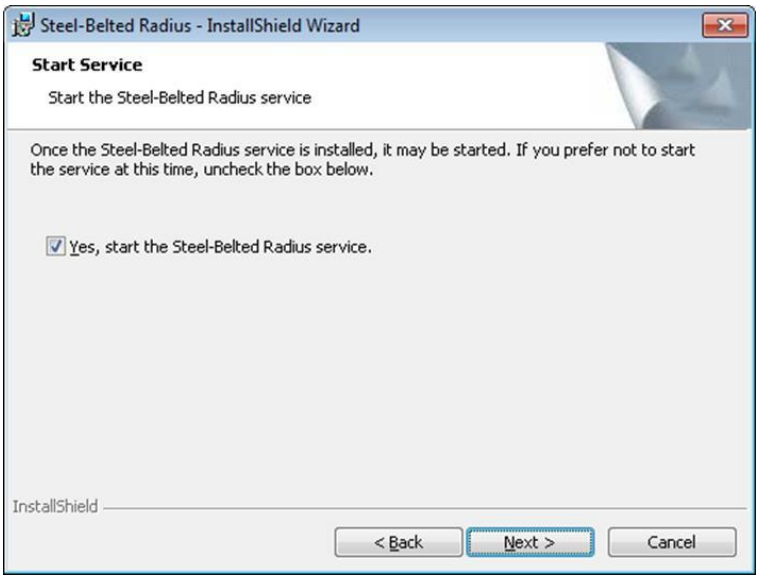
- If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), click the Provide Primary Server data button, and specify the name, IP address (es), and replication secret of the primary server.
- Click Next to continue.

**Figure 10: Replica Steel-Belted Radius Server Window**



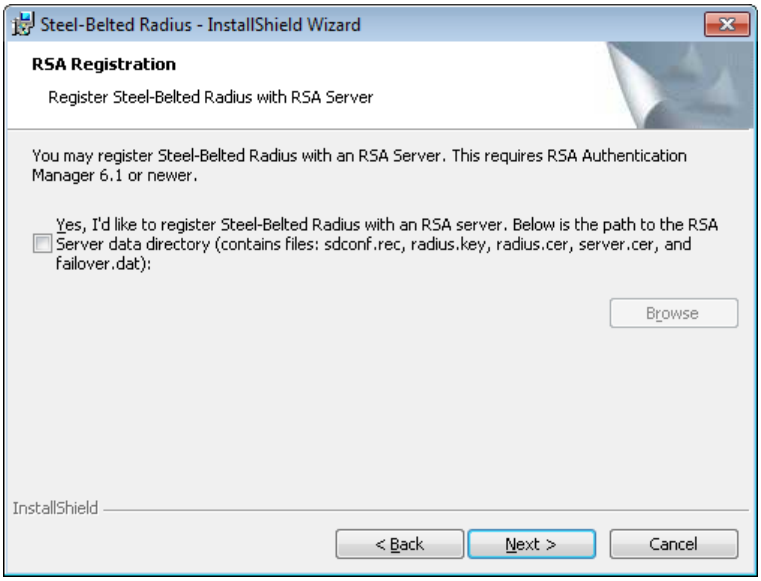

9. When the Start Services window opens, select the Yes, start the Steel-Belted Radius service check box if you want the Steel-Belted Radius service to start immediately. Click Next to continue.

**Figure 11: Start Service Window**




10. In the RSA Registration Window (shown in Figure 12), if you want to register the Steel-Belted Radius server as an Agent Host with an RSA SecurID server, select the Yes, I'd like to register check box, click the Browse button, and navigate to the directory containing the sdconf.rec, radius.cer, server.key and failover.dat files.

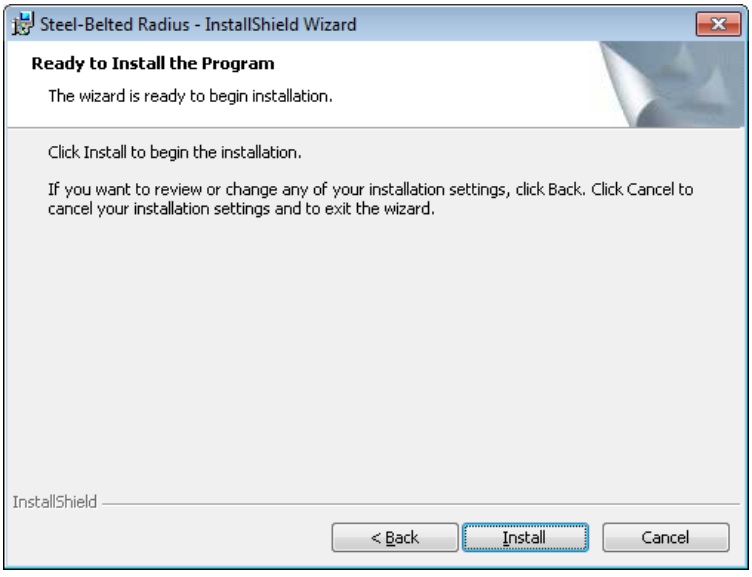
**Figure 12: RSA Registration Window**




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.

11. When the Ready to Install the Program window (shown in Figure 13) opens, click Install to begin the installation.

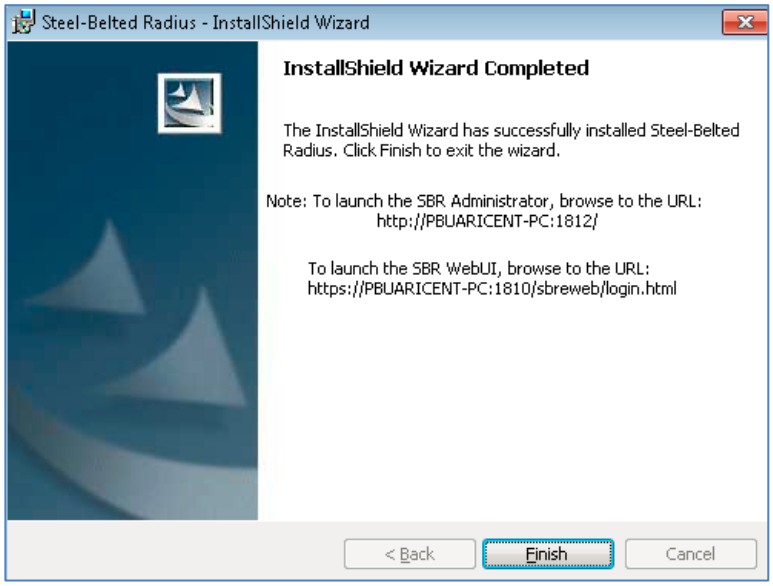
**Figure 13: Ready to Install the Program Window**




As the installation proceeds, the Installation Status window displays the progress. This might take over a minute or two to complete.

12. When the Setup Complete window (shown in Figure 14) opens, click Finish to complete the installation process.

**Figure 14: Setup Complete Window**




## Start the Steel-Belted Radius

- Before you can run SBR Administrator, you must start the RADIUS service if not started already. Refer to “Starting the Steel-Belted Radius Service” for information on starting the RADIUS service.
- On starting the Steel-Belted Radius Service, another service called "Steel-Belted Radius Jetty Server" (Java Web Server) will be created and started automatically. If it does not get started automatically, refer to Appendix H from Steel-Belted Radius Administration Guide for information on starting the Jetty Server.

## Launch the Steel-Belted Radius Administrator

- After starting the service, you can launch the SBR Administrator using the URL:

  http::///<Server name>:1812/

- You can launch the SBR Administrator Web GUI using the URL:

  https://<Server name>:1810/sbreweb/login.html

## Configure Steel-Belted Radius Server

- You must now complete 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 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.
- Refer to Steel-Belted Radius Administration Guide for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

Note: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

Note: If it is fresh installation and you do not have any backup data to be restored, then skip the next section. You have completed the Installation procedure.

### Restoration of Backed-Up Data

1. For restoring the previous configuration follow the steps below:
    - If you are re-installing the Steel-Belted Radius on the same machine, you can copy the configuration files from the backup directory Steel-Belted Radius\Service_Date_IDnumber which will be created during installation to the Steel-Belted Radius server ("Steel-Belted Radius\Service") directory to restore your previous configuration.
    - If you are installing the Steel-Belted Radius server in different machine, copy the backed up configuration files/data from "Steel-Belted Radius\Service" directory to the other machine's server directory in which you have installed SBR.
    - Refer to "Restoration of Previous Configuration" for further information.
2. To Import all the saved database configuration data, follow the steps given below:
    - Start the Steel-Belted Radius service. For more information, refer to the section "Starting the Steel-Belted Radius Service".
    - Launch the SBR administrator.
    - Import the saved database configurations by importing the XML file you have saved earlier. Refer to Steel-Belted Radius Administration Guide (Appendix E - "Importing and Exporting Data") for information on how to import your Steel-Belted Radius database from an .xml file.
3. Restart the Steel-Belted Radius service.

   Choose Start > Control Panel > Administrative Tools > Services. Select the Steel-Belted Radius entry. Click Restart the service.
4. Run SBR Administrator and verify that your configuration settings are complete and correct.

Note: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

# Upgrading the Steel-Belted Radius

Note: Steel-Belted Radius v6.2 supports upgrades from v6.1.1 or above. If you have an SBR installation earlier than v6.1.1, you must first upgrade to v6.1.7 before you attempt to move to v6.2.

Note: Do not uninstall your existing version of SBR before upgrading to v6.2.x versions.

### Backup of Existing Configuration/User Data

Note: If you are using the configuration files of 6.1.7, then back up the configuration files from the directory "C:\Program Files (x86)\Juniper Networks\Steel-Belted Radius\Service".

- Export your Steel-Belted Radius database to an Extensible Markup Language (.xml) file. Refer to *Steel-Belted Radius Administration Guide* (Appendix E - "Importing and Exporting Data") for information on how to export the Steel-Belted Radius database to an .xml file.
- Back up your Steel-Belted Radius\Service directory and the exported .xml file to an archive location.

  This step ensures that you have a clean copy of the existing Steel-Belted Radius configuration files so that you could merge it with the new configuration files after upgrade.

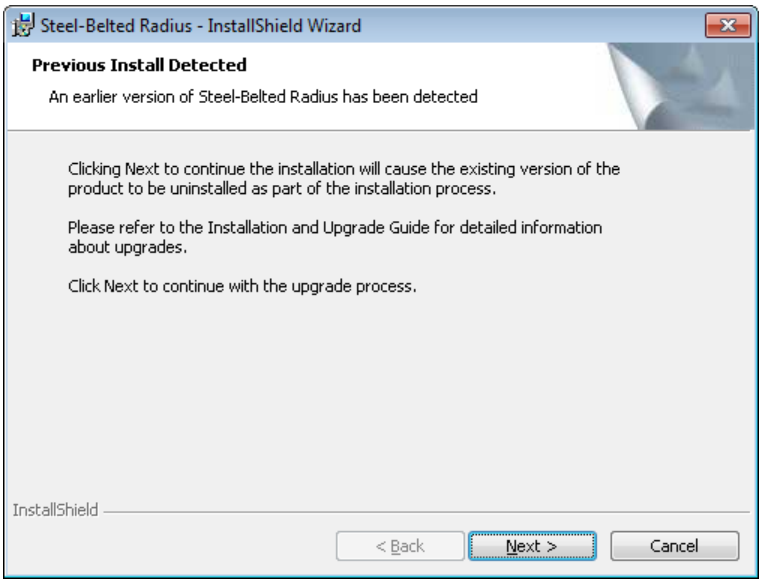
## Installation of Steel-Belted Radius – Upgrade

Verify that you have your Steel-Belted Radius version 6.2.x license number.

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

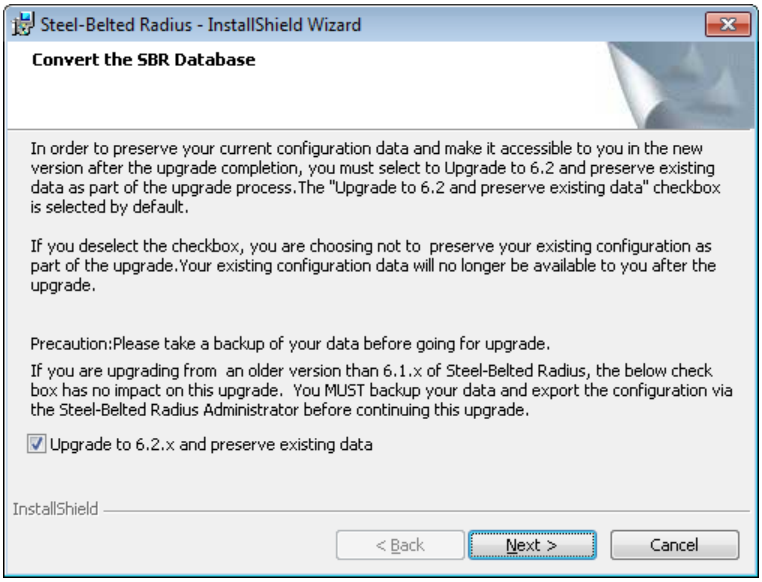
   You do not need to stop the Steel-Belted Radius service when you upgrade the Steel-Belted Radius server software.
2. Start the installation for Steel-Belted Radius version 6.2.x server software on your server by double clicking the Steel-belted Radius.msi package.
3. When the installation program detects the presence of a previous version of SBR installed on the system, you are prompted with information detailing what must happen next as part of the upgrade. The "Previous Install Detected" window (shown in Figure 15) will be displayed. Click Next to continue.

   **Figure 15: Previous Install Detected Window**




4. When Convert the SBR Database window appears (shown in Figure 16), the check box Upgrade to 6.2.x and preserve existing data will be selected by default to preserve the current configuration data which will be available in the new version after the upgrade. Click Next to continue.

**Figure 16: Convert the SBR Database**




5. Then follow the same installation procedure for installing the Steel-belted Radius. For more information, refer to “Installing the Steel-Belted Radius Server Software”.
6. When you have finished entering the necessary configuration settings, the upgrade program is ready to proceed with the installation. You are presented with the “Ready to Install the Program” prompt. Here you are again warned that the previous installation will be uninstalled as part of the upgrade. Click the Install button to proceed.

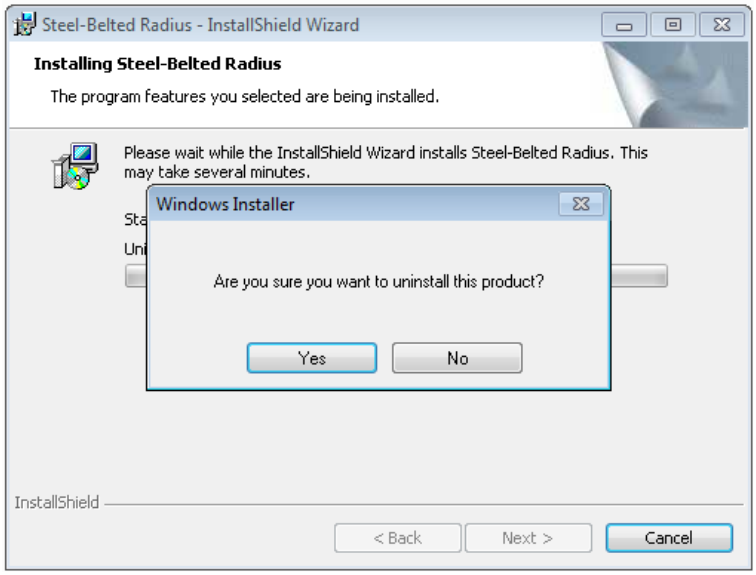
   Note: Do not cancel the Steel-Belted Radius installer after you start running it. Doing so may result in loss of data.

7. The upgrade program starts the uninstall process for the previous version. You must click the Yes button when the “Are you sure you want to uninstall this product?” pop-up window appears. If you click the No button, you are cancelling the v6.2 upgrade and nothing you have configured is instantiated.

   This is shown in Figure 1.

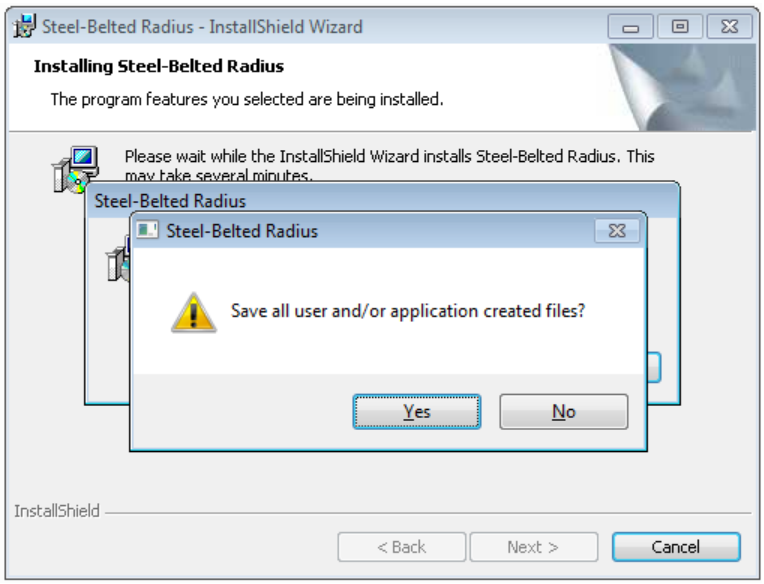
   Note: The Steel-Belted Radius v6.2 upgrade must uninstall the previous version in order to complete successfully.

**Figure 17: Uninstallation of Previous Version**




When you start the uninstall program for the previous version after clicking Yes, you are asked if you would like to save all user and\or application created files from the previous version (shown in Figure 18). Click Yes to save the user/application created files.

**Figure 18: Save user/application created files**




8. When the v6.2.x upgrade is complete and the "InstallShield Wizard Completed" window appears, click the Finish button. Now the upgrade is completed.

## Start the Steel-Belted Radius Service

Before you can run SBR Administrator, you must start the RADIUS service if not started already. Refer to "Starting the Steel-Belted Radius Service" for information on starting the RADIUS service.

## Launch the Steel-Belted Radius Administrator/WebGUI

After starting the service, you can launch the SBR Administrator using the URL: http://<Server name>:1812/.

You can launch the SBR Administrator WebGUI using the URL:

https://<Server name>:1810/sbreweb/login.html

- Import the saved database configurations by importing the XML file you have saved earlier. Refer to *Steel- Belted Radius Administration Guide* (Appendix E - "Importing and Exporting Data") for information on how to import the Steel-Belted Radius database from an .xml file.
- For restoring the previous configuration, refer to "Restoration of Previous Configuration".
- Restart the Steel-Belted Radius service.
    - Choose Start > Control Panel > Administrative Tools > Services. Select the Steel-Belted Radius entry. Click Restart the service.
    - Run SBR Administrator and verify that your configuration settings are complete and correct.

# Restoration of Previous Configuration

In order to restore to the previous configurations in the newly installed or upgraded Steel-Belted radius server some manual work is needed.

## Manual Migration of Configuration Files

You must manually migrate the following configuration files by merging any changed values into the corresponding configuration files that are shipped with the new Steel-Belted Radius software installation:

- *.ini
- *.aut
- *.dir
- *.pro
- *.rr
- *.eap

Note: It is recommended not to merge the settings from the archived version of few files (such as *tlsauth.aut, ttlsauth.aut, peapauth.aut, eap.ini*) to the newly installed files. Use SBR Administrator to apply the settings you were using before the upgrade.

## Manual Migration of XML Configuration

You must manually migrate the following XML files by merging any changed values into the corresponding XML files that are shipped with the new Steel-Belted Radius software installation (you should never modify any other *.xml files):

- Service\sbr_administration.xml
- Service\sbr_ccm.xml
- Service\sbr_id.xml
- Service\system\config\logging_mgr.xml

## Manual Migration of Java scripts

JavaScript files (*.jsi) are stored in the Service\scripts subdirectory. Any JavaScript files must be migrated manually to v6.1 by copying them to the new Steel-Belted Radius software installation.

## Manual Migration of Certificates

The certificates are managed by the Steel-Belted Radius server, and the SBR Administrator is used to add and delete certificates. You must manually migrate certificates by using the SBR Administrator to the new Server directory.

### Manual Migration of Dictionaries

If you have stored any modified or third-party dictionary files (*.dci, *.dcm, *.dct) in the radius directory, then you must manually migrate these either by merging each of the modifications with the corresponding files that are shipped with the new Steel-Belted Radius software, or by copying the third-party dictionary files to the new Server directory.

### Manual Migration of Third-Party Plugins and other Binaries

If you have stored any third-party plug-ins (*.dll) and/or other binaries in the radius directory, then you must manually migrate them by copying the files to the new Server directory.

### Inclusion of Newly Added/Deleted Parameters

- If Steel-Belted Radius is being upgraded to 6.22 version or higher, it is important to add the following parameters manually at the end of “radius.ini” file.

  [EapSettings]

  ;Allows Backward compatibility in SSL/TLS protocol suite( Options - 1/0 )

  ;AllowTLSFallback = 1

  ;Specifies the SSL/TLS protocol version to be used.

  ;Options - TLSv10,TLSv11,TLSv12

  ;MinimumProtocolVersion = TLSv12

- If Steel-Belted Radius is being upgraded to 6.24-R3 version or higher, it is important to modify the following parameters manually in the file "sbr_administration.xml" that is present on the Steel-Belted Radius installed directory

  Edit Line 40 and 41: under program_id radAdmin.RadAdminTlsSessionMgr with the following values.

  minimumProtocolVersion="33" (Earlier it was 31 by default)

  ciphersuites="0x3C,0x3D,0x67,0x6B,0x40,0x6A,0x9C,0x9D,0x9E,0x9F,0xA2,0xA3" (Earlier it was TLS 1.0 ciphers by default)

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

# 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 the 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.

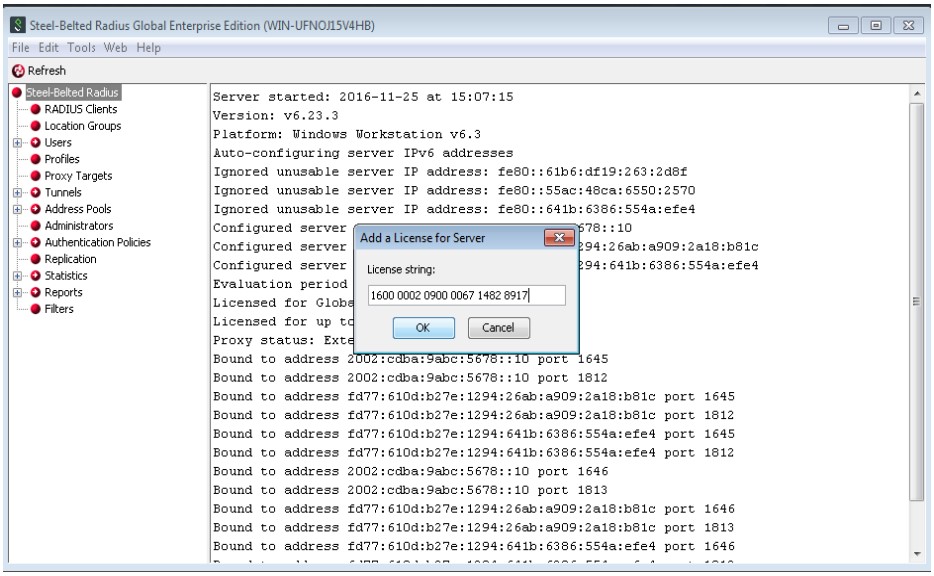
   Note: To Start/Stop Java Web Server (Jetty) individually, refer to Steel-Belted Radius Administration guide (Appendix G: Stopping and starting Steel-Belted Radius Jetty Server).

# Upgrading from a 30-Day Trial Installation

If you want to continue using the product at the end of the 30-Day evaluation period, you need not re-install the software. You can just 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 Pulse Secure. 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 (shown in Figure 19) opens, enter your license number and click OK.

   **Figure 19: Pulse Connect Secure Configuration Workflow**




   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.
7. Refer to *Steel-Belted Radius Administration Guide* for information on using Legacy SBR Administrator or WebGUI Administrator.

# Chapter 4

# Linux Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software on a Linux server. This chapter also describes how to install the optional SNMP software for use with the GEE 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 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.

# Fresh Installation

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.

Note: 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).

## Installing the RPM in SUSE Platform

Perform the following steps to install RPM in SUSE platform (**up to SUSE12**).

1. Log into the Linux server as root.
2. Copy the Steel-Belted Radius installation files to the Linux server.

   Make sure to copy them to a local or remote hard disk partition that is readable by root.

   The following example copies the files to the **/opt/PSsbr/temp** directory.

   **mkdir -p /opt/PSsbr/temp**

   **cp -pR /cdrom/sbr/linux/* /opt/PSsbr/temp**

3. In SUSE, the installation can be carried out using Zypper. While using Zypper, all the dependencies are automatically installed. Use the following command to install the SBR RPM in SUSE.

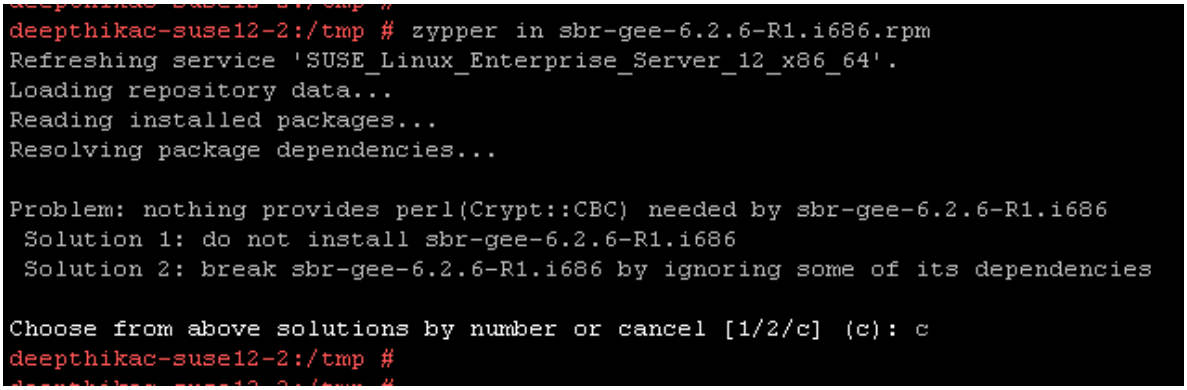
   **zypper in sbr-gee-6.2.6-R1.i686.rpm**

Note: In GEE package, the following dependencies are required for Tacacs+ server:

- **Perl(LDAP)**
- **Perl(Crypto::CBC)**
- **Perl(Crypto::DES)**

You might get the following dependency error with Perl(Crypto::CBC) during installation:

**Figure 20: Dependency Error**




Note: Choose "Solution 2: break sbr-gee-6.2.6-R1 by ignoring some of its dependencies" and proceed with installation if you are not using the **Tacacs+** server of SBR.

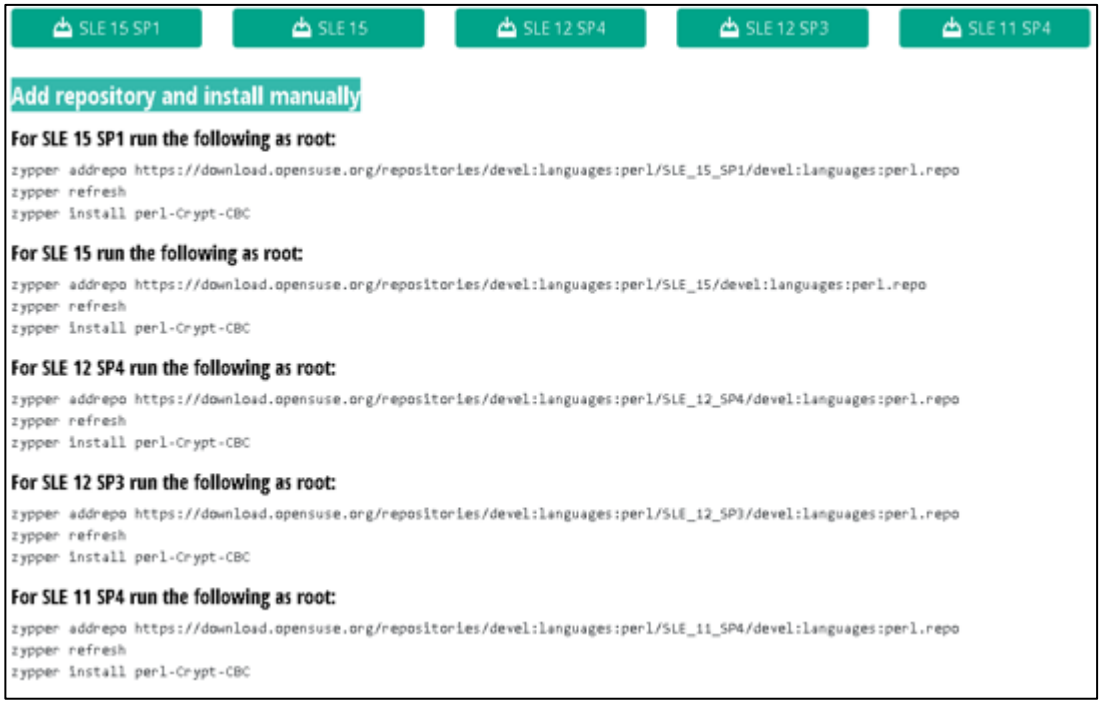
If you plan to install **Tacacs+** server, then proceed with the following steps to install the perl crypto-cbc library:

a. Go to the following link: https://software.opensuse.org/download.html?project=devel%3Alanguages%3Aperl&package=perl-Crypt-CBC

b. Select **SUSE SLE** > **Add repository** and install manually.

A list of zipper commands to add repository will be displayed as shown below:

**Figure 21: List of Zipper Commands**




c. Use the commands based on the SLE version.

   If you are using SUSE 12 SP4, then run the following commands:

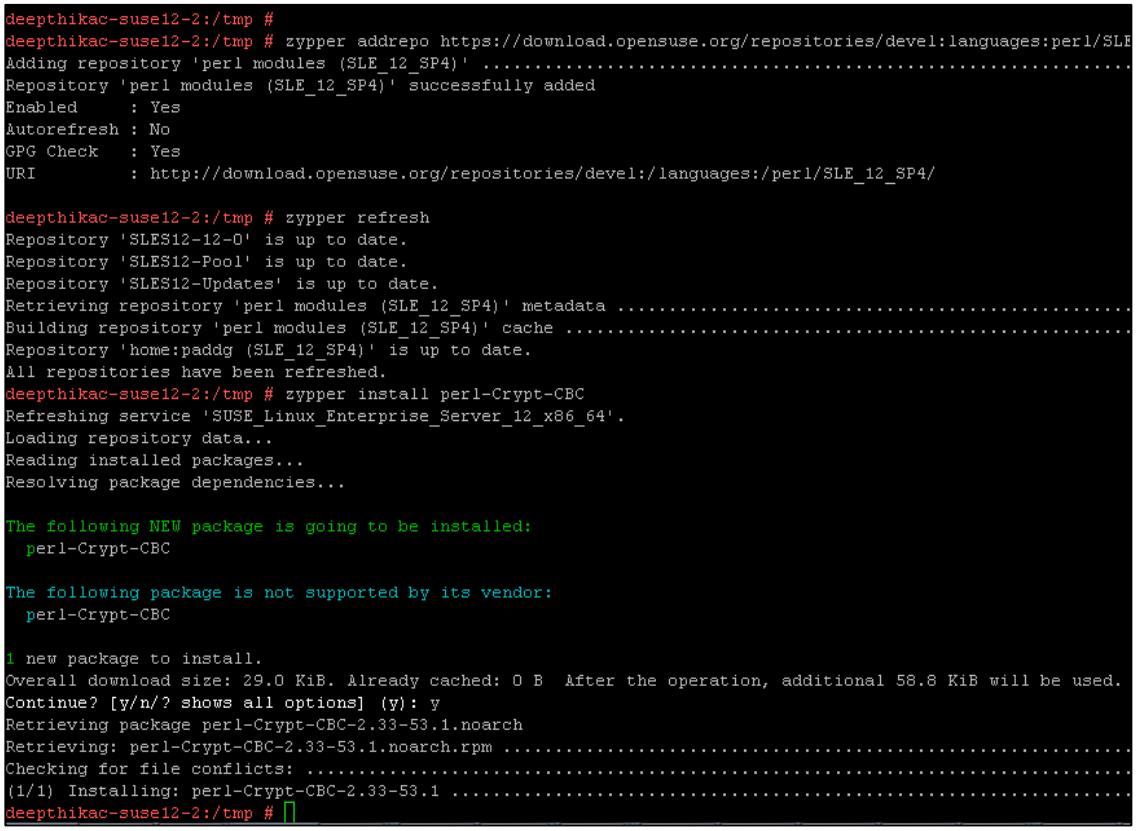
   **zypper addrepo https://download.opensuse.org/repositories/devel:languages:perl/SLE_12_SP4/devel:languages:perl.repo**

   **zypper refresh**

   **zypper install perl-Crypt-CBC**

The installation process is shown in the following figure:

**Figure 22: Installation Process**




4. Now proceed with the installation of SBR package using Zypper. Use the following command:

   zypper in sbr-gee-6.2.6-R1.i686.rpm

   **Note:**
   You might get the following error with the package **perl LDAP**.

   **"Problem: Nothing provides perl-LDAP needed by sbr-gee-6.2.6-R1.i686".**

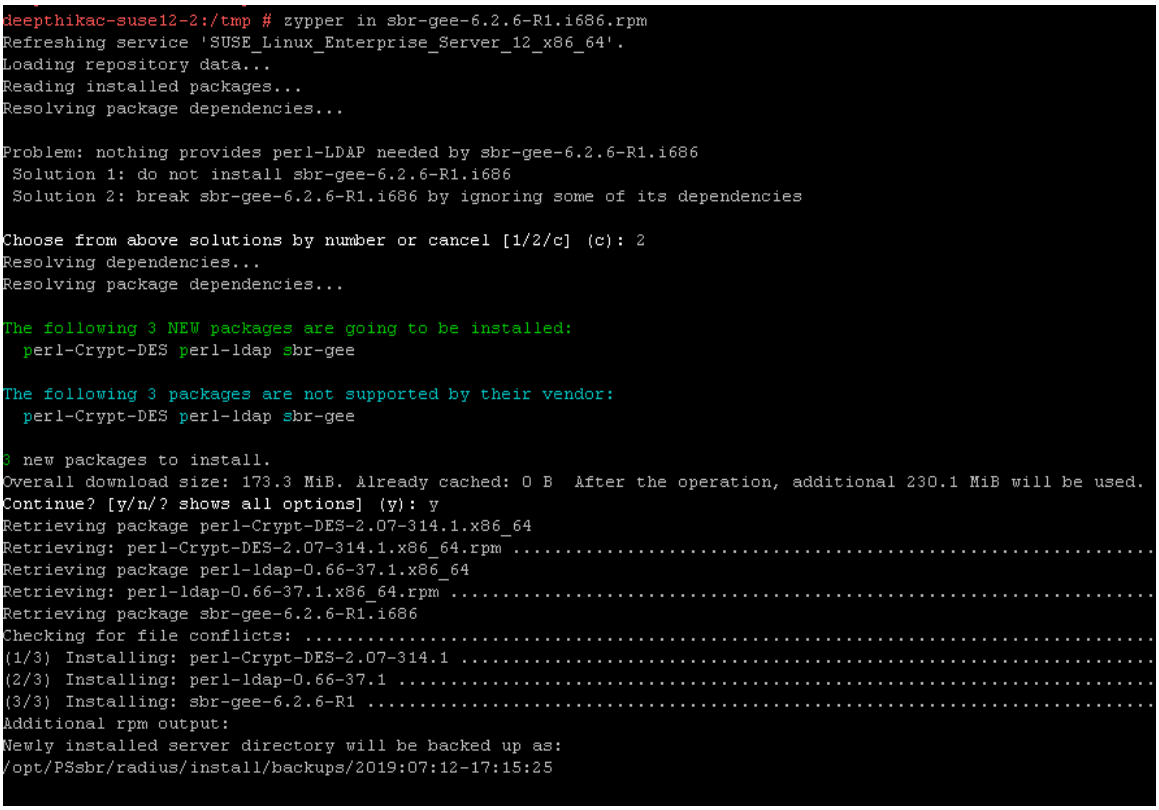
   Ignore the above problem and choose "Solution 2". **Perl-ldap** will be installed properly without any issue.

   **Note:**
   Ignore the following log message during installation:

   "**The following packages are not supported by their vendor**".

   Press **y** to continue the installation.
   Successful installation with all dependencies is shown in the following figure:

**Figure 23: Successful Installation**




## Installing the RPM in SUSE 15 Platform

Only signed RPM packages can be installed in SUSE15 platform. Therefore SBR-E Global Enterprise Edition (GEE) and Enterprise Edition (EE) RPMs are signed and maintained exclusively for SUSE15 platform apart from the RPMs maintained for other Linux platforms.

Now the signed RPMs require public key to be imported to the RPM database prior to package installation. Importing the public key and installing the SBR package using RPM has been automated via the shell script "sbr_suse15_install_script.sh". The shell script takes RPM name and the public key file as input arguments. There is a README file which gives the details on the shell script execution. All the files (RPM, Publickey, Shell Script and README) are compressed and available as '.gz' file in the PulseSecure download website.

1. Download the applicable edition (sbr-ent-6.2.6-R1.tar.gz/sbr-gee-6.2.6-R1.tar.gz) from the PulseSecure download website.
2. Extract the compressed file

### Enterprise Edition

tar zxvf sbr-ent-6.2.6-R1.tar.gz

The following files must be present in the newly extracted directory sbr-ent-6.2.6-R1:

- sbr_suse15_install_script.sh
- README.txt

- sbr-ent-6.2.6-R1.i686.rpm
- RPM-GPG-KEY-pulse-adminscl

**Global Enterprise Edition**

tar zxvf sbr-gee-6.2.6-R1.tar.gz

The following files must be present in the newly extracted directory sbr-gee-6.2.6-R1:

- sbr_suse15_install_script.sh
- README.txt
- sbr-gee-6.2.6-R1.i686.rpm
- RPM-GPG-KEY-pulse-adminscl

3. Navigate to the above extracted directory. Execute the shell script for RPM installation in SUSE15 platform.

**Enterprise Edition**
sh sbr_suse15_install_script.sh sbr-ent-6.2.6-R1.i686.rpm RPM-GPG-KEY-pulse-adminscl

**Global Enterprise Edition**
sh sbr_suse15_install_script.sh sbr-gee-6.2.6-R1.i686.rpm RPM-GPG-KEY-pulse-adminscl

Look out for the Zypper installation logs displayed on the screen to confirm if the package has been successfully installed.

## Installing the RPM in RHEL Platform

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.

   Make sure to copy them to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/PSsbr/temp directory.

   **mkdir -p /opt/PSsbr/temp**

   **cp -pR /cdrom/sbr/linux/* /opt/PSsbr/temp**
3. Linux installation can be carried out in the following two ways:
   While using Yum, all dependencies are automatically installed

   **yum localinstall sbr-gee**

   Note: In GEE package, the following dependencies are required for Tacacs+ server configuration:

   **Perl(Crypto::CBC)**

   **Perl(Crypto::DES)**

   Use the below mentioned procedure, if the above dependencies do not get resolved using **yum**.

   The above modules are available in **rhel-optional-rpms**, we have to enable this before

installing SBR package with yum.

Use the following command to enable:

**subscription-manager repos --enable=rhel-7-server-optional-rpms (in rhel-7)**

**subscription-manager repos --enable=rhel-6-server-optional-rpms (in rhel-6)**

Then proceed with yum install.

If you are not using Tacacs+ server of SBR, then you can skip the installation of above perl dependencies using the following command:

**--skip-broken command**

Using rpm, without checking any dependencies

rpm -ivh --nodeps sbr-gee-6.2-0.i386.rpm

Using rpm and specifying the Installation path

rpm -i /path/ sbr-gee-6.2-0.i386.rpm

Table 6 provides the useful package management commands.

**Table 6 Useful Package Management Commands**

| Command | Function |
|---|---|
| rpm -q -a \|egrep "FUNK\|SBR\|RSAR" | Report any pre-existing packages and patches |
| rpm -q -i sbr-gee-6.2.3-i386.rpm | Report high level description for specified package |
| rpm -q --queryformat {INSTALLPREFIX}" sbr-gee-6.2.3-i386.rpm | Show installed directory |
| rpm -i [--prefix /path] sbr-gee.6.2.3- i386.rpm | Install Steel-Belted Radius [at the specified /path].<br>Note: The rpm -i command cannot be used to overwrite an existing installation |
| rpm -U [--prefix /path] sbr-gee.6.2.3- i386.rpm | Upgrade an existing Steel-Belted Radius installation [in the specified /path] |
| rpm -e sbr-gee-6.1.0-0 | Uninstall Steel-Belted Radius |

Note: SBR uses a lot of third party software and hence it is recommended to use "Yum" so that it automatically installs the required dependencies.

## Configuring the Radius Application

1. Navigate to the directory where you installed Steel-Belted Radius. cd /opt/PSsbr/radius/install
2. Execute the following command to run the configuration script for Steel-Belted Radius: ./configure
3. 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
4. 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 have purchased a 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 150-Day evaluation package, allowing use of the product's full feature set for a limited period.

5. 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

6. 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

7. 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

8. 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. If the machine is RHEL6, it prompts as "Configuring for RedHat6" and if the machine is RHEL7, it prompts as "Configuring for RedHat7"

   Configuring for RedHat6

   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.

9. 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 standalone (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.

10. The configure script proceeds with configuring Java Web Server.

    Configure Admin UI Web Server

    a. It searches for the Java 1.8.0 or later version in the default system path and displays a confirmation message, if found.

    Compatible version found

    b. If java is not available in the system, then the script displays the following error message:
    - ERROR: No JRE available. Unable to configure Webserver.
    - Supported Java version: 1.8.0 or above.

    c. If the compatible Java version is not found, then the script displays the following error message:
    - [ERROR]: Compatible java version not Found.
    - Unable to configure Java Web server.
    - Supported Java version: 1.8.0 or above.

    In both the error cases (b and c), the script prompts, if the user wants to continue with other configurations.
    - Do you want to continue with other configurations? [n]
    - Press 'y' or 'Y' to continue with other configurations and 'n' or 'N' to quit.

11. 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.

12. If you are installing the Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional TACAS+ server to enable the additional support of AAA functionalities through TACACS+ protocol.

    Do you want to configure TACACS+ Server? [n]:

    If you do not want to configure the optional TACACS+ Server, press Enter to proceed to the next prompt.

    If you want to install the optional TACACS+ Server, type y and press Enter. The following message

will be displayed after configuration and proceed to the next prompt Configuration of TACACS+ Server is complete.

13. If you are installing the 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 pssnmpd.conf and startsnmp.sh files.

    - 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

    - 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

    - 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 *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

    Note: In SUSE platform, you have to install "bc" package "zypper in bc" to configure SNMP.

14. 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.

15. 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 auto boot 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.dboot script and deletes old Steel-Belted Radius auto boot settings, thereby enabling auto booting for Steel-Belted Radius v6.1.
    - 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 auto boot settings, thereby disabling auto booting 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 auto boot settings, thereby leaving your previous autoboot settings unchanged.

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.

### Start the Application

- Refer to *Steel- Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel- Belted Radius server. 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 *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

Before you can run SBR Administrator, you must start the RADIUS process. Refer to "**Starting the RADIUS Server"** section for information on starting the RADIUS process.

Note: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

### Launch the SBR Administrator

- 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.

# Upgrade

The Linux release of Steel-Belted Radius v6.2 is supported on Red Hat 6 and 7. Older Steel-Belted Radius versions were supported on Red Hat 4. If you are upgrading a version of Steel-Belted Radius that is running on Red Hat 4 and you want to preserve and use your existing configuration data, you must move it to the new operating system.

Note: If you are planning to upgrade the Steel-Belted Radius cluster, the existing primary node should always be upgraded first. Once the newly migrated primary node is functioning, delete all existing replica nodes from the newly upgraded primary node's CCM server list. The existing replica nodes should be upgraded last, and the newly upgraded primary node specified when the newly upgraded replicas are installed and configured. Once functioning, the newly upgraded replica nodes will contact the newly upgraded primary node, thus re-populating the primary node's CCM server list and re-synchronizing the newly upgraded Steel-Belted Radius cluster. Once the newly upgraded Steel-Belted Radius cluster is functioning, you can decommission the existing Steel-Belted Radius cluster.

Note: If this is a primary node, be sure to delete all existing replica nodes from the newly migrated primary node's CCM server list. If this is a replica node, verify that it has contacted the newly migrated primary node as opposed to the existing primary node.

If you are planning to upgrade from 6.1.7 to 6.23 version, it requires Operating System Upgrade. Following

scenarios can occur while upgrading Operating System:

1. Upgrading OS in the same machine, therefore SBR upgrade will happen on the same machine.
2. Using a new machine with RHEL6 or RHEL7 OS, which means SBR data has to be migrated from the old machine to new machine.

If you are planning to upgrade from 6.1.7 to 6.2 versions or within 6.2 versions, SBR upgrade remains the same, which is listed in the following sections.

## Back up of Existing Radius Directory

1. Connect to the server where Steel Belted Radius Server is installed. ssh root@xxx.xxx.xxx.xxx
2. Take backup of the radius directory and store it in a temporary location. cd /opt/JNPRsbr/
   Take file count:
   ls -ltr /opt/JNPRsbr/radius | wc -l
   tar -cvf radius_617_backup.tar.gz
   ./radius mv
   radius_617_backup.tar.gz to
   /opt/temp

## Installing the RPM in SUSE Platform

Perform the following steps to install RPM in SUSE platform (**up to SUSE12**).

1. Log into the Linux server as root.
2. Copy the Steel-Belted Radius installation files to the Linux server.

   Make sure to copy them to a local or remote hard disk partition that is readable by root.

   The following example copies the files to the **/opt/PSsbr/temp** directory.

   **mkdir -p /opt/PSsbr/temp**

   **cp -pR /cdrom/sbr/linux/* /opt/PSsbr/temp**

3. In SUSE, the installation can be carried out using Zypper. While using Zypper, all the dependencies are automatically installed. Use the following command to install the SBR RPM in SUSE.

   **zypper in sbr-gee-6.2.6-R1.i686.rpm**

   Note: In GEE package, the following dependencies are required for Tacacs+ server:

   - **Perl(LDAP)**
   - **Perl(Crypto::CBC)**
   - **Perl(Crypto::DES)**

   You might get the following dependency error with Perl(Crypto::CBC) during installation:

**Figure 24: Dependency Error**

```
deepthikac-suse12-2:/tmp # zypper in sbr-gee-6.2.6-R1.i686.rpm
Refreshing service 'SUSE_Linux_Enterprise_Server_12_x86_64'.
Loading repository data...
Reading installed packages...
Resolving package dependencies...

Problem: nothing provides perl(Crypt::CBC) needed by sbr-gee-6.2.6-R1.i686
 Solution 1: do not install sbr-gee-6.2.6-R1.i686
 Solution 2: break sbr-gee-6.2.6-R1.i686 by ignoring some of its dependencies

Choose from above solutions by number or cancel [1/2/c] (c): c
deepthikac-suse12-2:/tmp #
```

**Note:** Choose "Solution 2: break sbr-gee-6.2.6-R1 by ignoring some of its dependencies" and proceed with installation if you are not using the **Tacacs+** server of SBR.

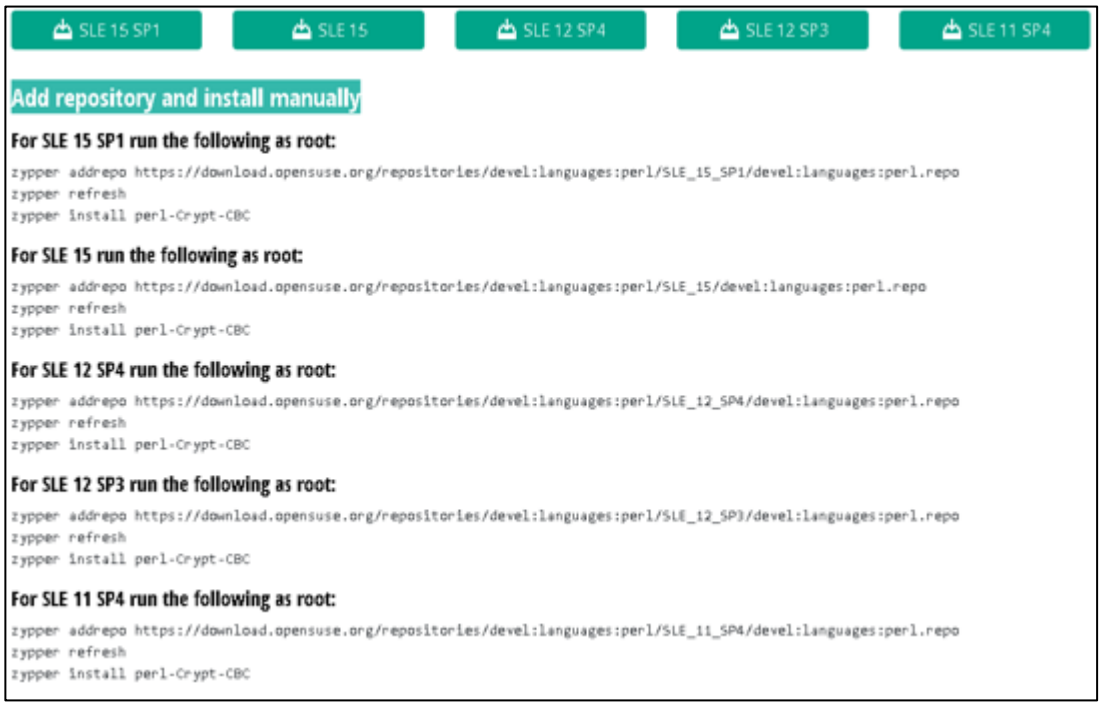
If you plan to install **Tacacs+** server, then proceed with the following steps to install the **perl crypto-cbc** library:

a. Go to the following link: https://software.opensuse.org/download.html?project=devel%3Alanguages%3Aperl&package=perl-Crypt-CBC

b. Select **SUSE SLE** > **Add repository** and install manually.

A list of zipper commands to add repository will be displayed as shown below:

**Figure 25: List of Zipper Commands**




c. Use the commands based on the SLE version.

   If you are using SUSE 12 SP4, then run the following commands:

**zypper addrepo https://download.opensuse.org/repositories/devel:languages:perl/SLE_12_SP4/devel:languages:perl.repo**

**zypper refresh**

**zypper install perl-Crypt-CBC**

The installation process is shown in the following figure:

**Figure 26: Installation Process**

```
deepthikac-suse12-2:/tmp #
deepthikac-suse12-2:/tmp # zypper addrepo https://download.opensuse.org/repositories/devel:languages:perl/SLE
Adding repository 'perl modules (SLE_12_SP4)' ..........................................................
Repository 'perl modules (SLE_12_SP4)' successfully added
Enabled     : Yes
Autorefresh : No
GPG Check   : Yes
URI         : http://download.opensuse.org/repositories/devel:/languages:/perl/SLE_12_SP4/

deepthikac-suse12-2:/tmp # zypper refresh
Repository 'SLES12-12-0' is up to date.
Repository 'SLES12-Pool' is up to date.
Repository 'SLES12-Updates' is up to date.
Retrieving repository 'perl modules (SLE_12_SP4)' metadata .............................................
Building repository 'perl modules (SLE_12_SP4)' cache ..................................................
Repository 'home:paddg (SLE_12_SP4)' is up to date.
All repositories have been refreshed.
deepthikac-suse12-2:/tmp # zypper install perl-Crypt-CBC
Refreshing service 'SUSE_Linux_Enterprise_Server_12_x86_64'.
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following NEW package is going to be installed:
  perl-Crypt-CBC

The following package is not supported by its vendor:
  perl-Crypt-CBC

1 new package to install.
Overall download size: 29.0 KiB. Already cached: 0 B  After the operation, additional 58.8 KiB will be used.
Continue? [y/n/? shows all options] (y): y
Retrieving package perl-Crypt-CBC-2.33-53.1.noarch
Retrieving: perl-Crypt-CBC-2.33-53.1.noarch.rpm ........................................................
Checking for file conflicts: ..........................................................................
(1/1) Installing: perl-Crypt-CBC-2.33-53.1 .............................................................
deepthikac-suse12-2:/tmp #
```

4. Now proceed with the installation of SBR package using Zypper. Use the following command:

   zypper in sbr-gee-6.2.6-R1.i686.rpm

**Note:**
You might get the following error with the package **perl LDAP**.

**"Problem: Nothing provides perl-LDAP needed by sbr-gee-6.2.6-R1.i686".**

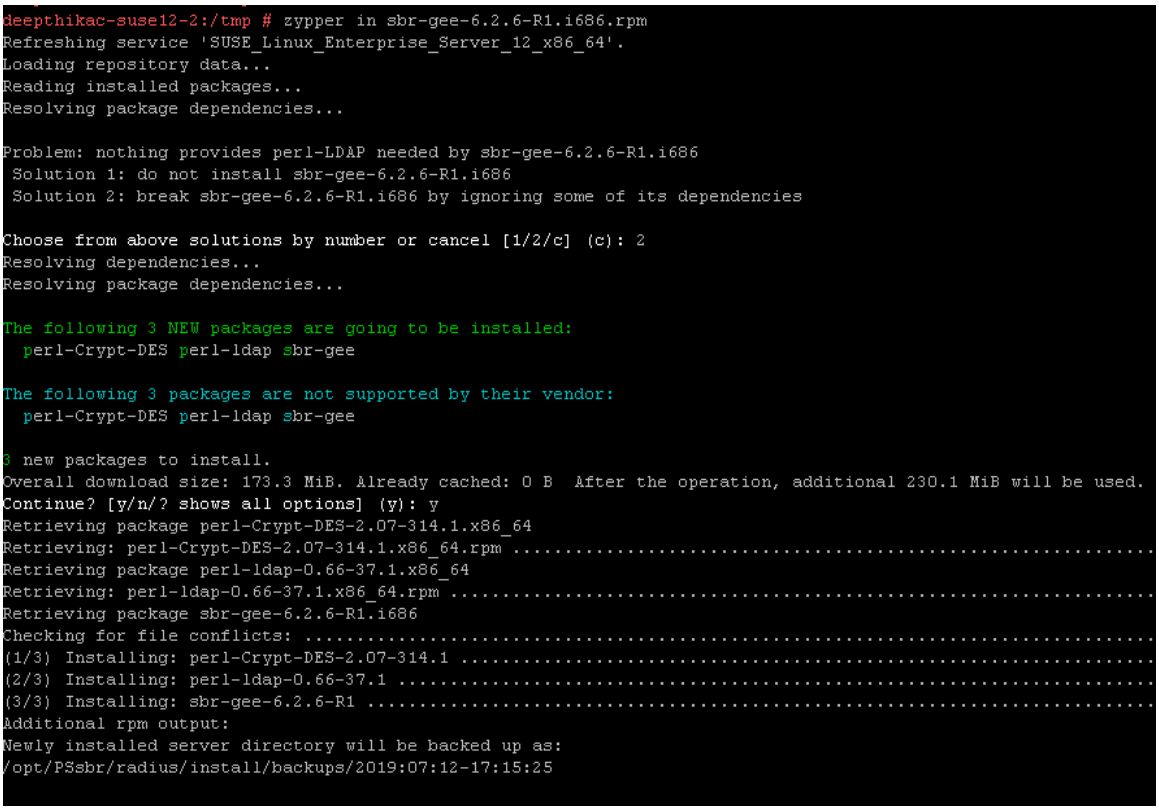
Ignore the above problem and choose "Solution 2". **Perl-ldap** will be installed properly without any issue.

**Note:**
Ignore the following log message during installation:

"**The following packages are not supported by their vendor**".

Press **y** to continue the installation.
Successful installation with all dependencies is shown in the following figure:

**Figure 27: Successful Installation**




## Installing the RPM in SUSE15 platform

Only signed RPM packages can be installed in SUSE15 platform. Therefore SBR-E Global Enterprise Edition (GEE) and Enterprise Edition (EE) RPMs are signed and maintained exclusively for SUSE15 platform apart from the RPMs maintained for other Linux platforms.

Now the signed RPMs require public key to be imported to the RPM database prior to package installation. Importing the public key and installing the SBR package using RPM has been automated via the shell script "sbr_suse15_install_script.sh". The shell script takes RPM name and the public key file as input arguments. There is a README file which gives the details on the shell script execution. All the files (RPM, Publickey, Shell Script and README) are compressed and available as '.gz' file in the PulseSecure download website.

1. Download the applicable edition (sbr-ent-6.2.6-R1.tar.gz/sbr-gee-6.2.6-R1.tar.gz) from the PulseSecure download website.
2. Extract the compressed file

### Enterprise Edition

tar zxvf sbr-ent-6.2.6-R1.tar.gz

The following files must be present in the newly extracted directory sbr-ent-6.2.6-R1:

- sbr_suse15_install_script.sh
- README.txt

- sbr-ent-6.2.6-R1.i686.rpm
- RPM-GPG-KEY-pulse-adminscl

**Global Enterprise Edition**

tar zxvf sbr-gee-6.2.6-R1.tar.gz

The following files must be present in the newly extracted directory sbr-gee-6.2.6-R1:

- sbr_suse15_install_script.sh
- README.txt
- sbr-gee-6.2.6-R1.i686.rpm
- RPM-GPG-KEY-pulse-adminscl

3. Navigate to the above extracted directory. Execute the shell script for RPM installation in SUSE15 platform.

**Enterprise Edition**
sh sbr_suse15_install_script.sh sbr-ent-6.2.6-R1.i686.rpm RPM-GPG-KEY-pulse-adminscl

**Global Enterprise Edition**
sh sbr_suse15_install_script.sh sbr-gee-6.2.6-R1.i686.rpm RPM-GPG-KEY-pulse-adminscl

Look out for the Zypper installation logs displayed on the screen to confirm if the package has been successfully installed.

## Installing the RPM RHEL Platform

Note: If Steel-Belted Radius Server upgrade is occurring on the same machine, before you can start the upgrade, refer to "Uninstalling Steel-Belted Radius on Linux" for information on stopping the RADIUS process, uninstalling the package and removing the RADIUS directory.

1. Linux installation can be carried out in the following ways:
   - While using Yum, all dependencies are automatically installed. yum localinstall sbr-gee-6.2-0.i386.rpm
   - Using rpm, without checking any dependencies. rpm -ivh --nodeps sbr-gee-6.2-0.i386.rpm
   - Using rpm and specifying the Installation path. rpm -i /path/ sbr-gee-6.2-0.i386.rpm

Table 7 provides the useful package management commands.

**Table 7 Package management commands**

| Command | Function |
|---|---|
| rpm -q -a \|egrep "FUNK\|SBR\|RSAR" | Report any pre-existing packages and patches |

| | |
|---|---|
| rpm -q -i sbr-gee-6.2.3-i386.rpm | Report high level description for specified package |
| rpm -q --queryformat {INSTALLPREFIX}" sbr-gee-6.2.3-i386.rpm | Show installed directory |
| rpm -i [--prefix /path] sbr-gee.6.2.3- i386.rpm | Install Steel-Belted Radius [at the specified /path].<br>Note: The rpm -i command cannot be used to overwrite an existing installation |
| rpm -U [--prefix /path] sbr-gee.6.2.3- i386.rpm | Upgrade an existing Steel-Belted Radius installation [in the specified /path]. |
| rpm -e sbr-gee-6.1.0-0 | Uninstall Steel-Belted Radius |

Note: SBR uses a lot of third party software and hence it is recommended to use "Yum" so that it automatically installs the required dependencies.

## Configuring the Radius Application

Note: Before configuring the RADIUS application, it is important to place the backed up RADIUS directory in /opt location in order for SBR to search and list the old directories.

1. Extract backed up 6.1.7 radius
   directory. cd /opt/temp
   mv radius_617_backup.tar.gz
   radius_617_backup.tar tar -xvf
   radius_617_backup.tar
   Take file count: ls -ltr /opt/temp/radius | wc –l
2. Navigate to the directory where you installed Steel-Belted
   Radius. cd /opt/PSsbr/radius/install
3. Execute the following command to run the configuration script for Steel-Belted Radius.
   ./configure
4. 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
5. 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 have 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 150-Day evaluation package, allowing use of the product's full feature set for a limited period.
   - 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).
6. Specify whether you are upgrading an existing Steel-Belted Radius installation or configuring

a new installation. In this scenario, it is upgrade, therefore choose s to search for the existing directory.

- 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] s

7. By default, the radius directories in /opt directory will be listed and you can choose to provide the radius directory from which to be backed up.

   Please enter backup or radius directory from which to migrate. Enter n for new configuration, s to search, or q to quit [/opt/temp/radius]: /opt/temp/radius

8. Indicate to stop the old server process.

   It is strongly recommended that the old server be stopped for migration. Stop old server processes now? [y] y

9. Since the data is already backed up and pre-existing software is already completed, indicate 'n' to manually back up and remove pre-existing software.

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

10. Configuring Admin UI Web server

    a. It searches for the Java 1.8.0 or later version in the default system path and displays a confirmation message, if found.

    Compatible version found

    b. If java is not available in the system, then the script displays the following error message:
       - ERROR: No JRE available. Unable to configure Webserver.
       - Supported Java version: 1.8.0 or above.

    c. If the compatible java version is not found, then the script displays the following error message:

       - [ERROR]: Compatible java version not Found.
       - Unable to configure Java Web server.
       - Supported Java version: 1.8.0 or above.

       In both the error cases (b and c), the script prompts, if the user wants to continue with other configurations.
       - Do you want to continue with other configurations? [n]
       - Press 'y' or 'Y' to continue with other configurations and 'n' or 'N' to quit.

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. If the machine is

RHEL6, it prompts as "Configuring for RedHat6" and if the machine is RHEL7, it prompts as "Configuring for RedHat7"

Configuring for RedHat6

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 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.
13. If you are installing the Global Enterprise Edition (GEE) of Steel- Belted Radius, specify whether you want to install the optional TACACS+ Server to enable the additional support of AAA functionalities through TACACS+ protocol.

    Do you want to configure TACACS+ Server[n]:

    If you do not want to configure the optional Tacacs+ server, press Enter to proceed to the next prompt.

    If you want to install the optional Tacacs+ server, type y and press Enter. The following message will be displayed after configuration and proceed to the next prompt Configuration of TACACS+ Server is complete
14. If you are installing the 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 pssnmpd.conf and startsnmp.sh files.
    - 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
    - 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
    - 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 is complete.

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

agent.

Note: In SUSE platform, you have to install "bc" package "zypper in bc" to configure SNMP.

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

    Do you want to 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 auto boot 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.dboot script and deletes old Steel-Belted Radius auto boot settings, thereby enabling auto booting for Steel-Belted Radius v6.1.
    - 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 auto boot settings, thereby disabling auto booting 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 auto boot settings, thereby leaving your previous autoboot settings unchanged.

    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 is complete

## Inclusion of Newly Added/Deleted Parameters

- If Steel-Belted Radius is being upgraded to 6.22 version or higher, it is important to add the following parameters manually at the end of "radius.ini" file.

  1. Navigate to the directory where you installed Steel-Belted Radius. By default, it is '/opt/PSsbr/radius' cd /opt/PSsbr/radius
  2. Edit the file "radius.ini" using vim editor
     a. If you are using the Global Enterprise Edition (GEE) then add the following entries at the end of [Configuration] section available at the top.

        Note: EnableTACACSPlusServer parameter is applicable only for Linux Global

        ;Enterprise Edition. It is not applicable for Windows platform.

        ;EnableTACACSPlusServer = 0

     b. And append the following [EapSettings] entries at the end of the file and save the file. [EapSettings]

        ;Allows Backward compatibility in SSL/TLS protocol suite( Options - 1/0 )

        ;AllowTLSFallback = 1

        ;Specifies the SSL/TLS protocol version to be used.

;Options - TLSv10,TLSv11,TLSv12

;MinimumProtocolVersion = TLSv12

- If Steel-Belted Radius is being upgraded to 6.24-R3 version or higher, it is important to modify the following parameters manually in the file "sbr_administration.xml" that is present on the Steel-Belted Radius installed directory.

  Edit Line 40 and 41: under program_id radAdmin.RadAdminTlsSessionMgr with the following values.

  minimumProtocolVersion="33" (Earlier it was 31 by default)

  ciphersuites="0x3C,0x3D,0x67,0x6B,0x40,0x6A,0x9C,0x9D,0x9E,0x9F,0xA2,0xA3" (Earlier it was TLS 1.0 ciphers by default)

## Start the Application

Before you can run SBR Administrator, you must start the RADIUS process. Refer to "Starting the Radius Server" section for information on starting the RADIUS process.

## Launch the SBR Administrator

You can run SBR Administrator to verify the old configurations are present in the upgraded Steel-Belted Radius version

## Starting the RADIUS Server

Use the following command to start the RADIUS server

manually. cd server-directory

./sbrd start

If you change configuration settings on Steel-Belted Radius server, you may need to restart Steel-Belted Radius to make the changes effective. As an alternative to issuing a sbrd stop command immediately followed by a 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 RADIUS server process.

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 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

## Displaying RADIUS Status Information

You can use the sbrd status command to display status information for the RADIUS process. cd server-directory
./sbrd status
The output of the sbrd status command.

```
------ Essential Network Status ------
Protocol        Local Address        Foreign Address
tcp       0     0 0.0.0.0:1812       0.0.0.0:*          LISTEN
tcp       0     0 0.0.0.0:1813       0.0.0.0:*          LISTEN
udp       0     0 10.96.176.7:1812   0.0.0.0:*
udp       0     0 10.96.176.7:1813   0.0.0.0:*
udp       0     0.10.96.176.7:1645   0.0.0.0
udp       0     0.10.96.176.7:1646   0.0.0.0


root    26848 radius
sbr.xml radius
processes are active
radius lock files exist
radius state is
running radius status
1100

--------- WebServerStatus --------
root    31795 jetty
Java WebServer is active

watchdog processes are
inactive watchdog state is
stopped watchdog status
1000

aggregate state is running
```

## Unconfiguring the RADIUS Server

You can use the unconfigure command to unconfigure the RADIUS server. cd server-directory/install
/unconfigure

**Note**: To start/stop Java Web Server individually refer to "Appendix G: Stopping and starting Steel-Belted Radius Jetty Server" in the Steel-Belted Radius Administration guide.

## Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Pulse Secure website (https://www.pulsesecure.net/products/). 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 Pulse Secure. 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 *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.
5. After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.
6. Click OK to close the confirmation window.
7. 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 Steel-Belted Radius Service"** section for information on how to restart your Steel-Belted Radius server.

# Chapter 5

# Migrating Steel-Belted Radius from Solaris to Linux

This chapter describes how to migrate Steel-Belted Radius 6.17 in Solaris platform to higher versions in Linux platform.

## Steps to Migrate Steel-Belted Radius from Solaris to Linux

1. Back-up the Steel -Belted Radius 6.17 directory in Solaris platform.
2. Freshly Install Linux higher version of Steel-Belted Radius 6.2 and complete the configuration.
3. Manual restoration of Solaris Steel-Belted Radius 6.17 files into Linux platform.

## Back-up the Solaris Steel-Belted Radius 6.17

1. Connect to the Solaris Server where Steel Belted Radius Server is

   installed. ssh root@xxx.xxx.xxx.xxx
2. Take backup of the radius directory and store it in a temporary

   location. cd /opt/JNPRsbr/

   Take file count: (The purpose of taking file count is to verify if the same count exists while restoring the radius directory in the Linux machine)

   ls -ltr /opt/JNPRsbr/radius | wc -l

   tar -cvf radius_617_backup.tar.gz

   ./radius mv

   radius_617_backup.tar.gz to

   /opt/temp
3. Transfer the tarred file to the Linux machine via scp or any other secure

   means. cd /opt/temp

   scp radius_617_backup.tar.gz root@<Linux Machine IP>:<path to be placed, eg: /opt/temp>
4. Connect to the Server from where the SBR Administrator is launched. Export your Steel-Belted Radius database to an Extensible Markup Language (.xml) file. Refer to the *Steel-Belted Radius Administration guide* (Appendix E – "Importing and Exporting Data" for information on how to export your Steel-Belted Radius database to an .xml file).

WARNING: Since it is Solaris to Linux Migration, current Sessions in SBR Administrator or the data in radads.hst file will not be restored in the Linux platform. Also accounting and Log files present in Solaris platform will not be migrated to Linux platform.

## Fresh Installation of Steel-Belted Radius in Linux

Note: For fresh installation of higher version of SBR in Linux platform, refer Chapter 4 "Linux Installation" section "Fresh Installation" – Installing the Linux RPM and

Configuring the Radius Application.

## Manual Restoration of Steel-Belted Radius Files

1. In the example demonstrated in section "Back-up the 6.17 Solaris Steel-Belted Radius", the tarred file was placed in /opt/temp. If you have placed in a different directory, change to the corresponding directory

   cd /opt/temp

   mv radius_617_backup.tar.gz

   radius_617_backup.tar tar -xvf

   radius_617_backup.tar

   Take file count: ls -ltr /opt/temp/radius | wc –l (Verify if the count matches to the one that was taken in Solaris machine while backing up the radius files).

2. Connect to the Server from where the SBR Administrator in Linux platform is going to be launched.

   - If it is the same server where the SBR Administrator Solaris was launched, then exported .xml file is already available in the stored location. However, for launching the SBR Administrator in the Linux Platform, Solaris SBR Administrator files have to be uninstalled. For uninstalling the SBR Administrator refer Chapter 6: "*Uninstalling Steel-Belted Radius*", section "Uninstalling SBR Administrator Files".

   - If it is the different server where the SBR Administrator Linux is going to be launched, then transfer the exported .xml file to a certain location in that server. This .xml file will be used later for importing of data.

   Migrating from Solaris to Linux requires manual upgrading of configuration files. The files and file types listed in this section are those that require manual migration.

### Manual Migration of Configuration files

The following configuration files in Solaris backed up radius directory have to be manually over-written to the new configuration files present in the Linux Server radius directory.

- *.acc
- *.aut
- *.conf
- *.dat
- *.dhc
- *.dir
- *.ini
- *.pro
- *.rr

Note: If in Solaris platform, certain parameters like LogFilePath in configuration files were modified from the default value, it should be taken care that the same value holds good in Linux platform. Few examples as follows,

Radius.ini file

;PrivateDir = <file system location>

If there was a separate PrivateDir mentioned in Solaris platform, the same log path should exist in Linux platform too.

Authlog.ini

;LogDir = <pathname>

If there was a separate LogDir mentioned in Solaris platform, the same LogDir should exist in Linux platform too.

### Manual Migration of JRE extensions

Steel-Belted Radius ships its own Java Runtime Environment (JRE) to facilitate JDBC plug-ins and Java Scripting. You can extend the JRE by installing third-party .jar files in the radius/jre/lib/ext subdirectory. You must place the corresponding third party .jar files suiting to the Linux requirements. Refer to Release Notes "System Requirements – Database Servers" for more details.

Note: Steel-Belted Radius Application in Solaris used to support native Oracle plugins for connecting to Oracle Database. However, Steel-Belted Radius Application in Linux makes use of JDBC connection and the Oracle instant client driver for x86_64 is used for connecting to Oracle Database. Hence the Solaris Oracle Client Libraries need not be transferred to the Linux platform.

### Manual Migration of SNMP Configuration

SNMP configuration is contained in the radius/snmp/conf directory (for example in 6.1.7, radius/snmp/conf/jnprsnmpd.conf). While migrating to 6.20 and higher releases, SNMP configuration file exists as radius/snmp/conf/pssnmpd.conf. You must manually migrate this configuration by merging the contents of the files into the files that are shipped with the new Steel-Belted Radius software installation. But if you choose not to configure SNMP, then the new radius/snmp/conf directory should remain empty.

Note: The syntax of the radius/snmp/conf/pssnmpd.conf file is particularly sensitive to the ordering of the parameters, malformed IP address CIDR notation, and stray white space. Misconfiguring this file will typically result in a broken SNMP agent. If you have stored any modified or third-party MIB files in the radius/snmp/mibs directory, these files should be migrated manually by copying them to the new Steel-Belted Radius software installation.

### Manual Migration of Dictionaries

If you have stored any modified or third-party dictionary files (*.dci, *.dcm, *.dct) in the radius directory, then you must manually migrate these either by merging each of the modifications with the corresponding files that are shipped with the new Steel-Belted Radius software, or by copying the third-party dictionary files to the new radius directory.

### Manual Configuration of JavaScript files

All JavaScript files (*.jsi) are stored in the radius/scripts directory. Any JavaScript files must be migrated manually by copying them to the new Steel-Belted Radius software installation.

### Manual Migration of Third-party plugins and other Binaries

If you have stored any third-party plug-ins (*.so) and/or other binaries in the radius directory, then you must manually migrate them by copying the files to the new radius directory.

### Inclusion of newly added/deleted parameters

- If Steel-Belted Radius is being upgraded to 6.22 version or higher, it is important to add the following parameters manually at the end of "radius.ini" file.

1. Navigate to the directory where you installed Steel-Belted Radius. By default, it is '/opt/PSsbr/radius'

   cd /opt/PSsbr/radius

2. Edit the file "radius.ini" using vim editor

a. If you are using the Global Enterprise Edition (GEE) then add the following entries at the end of [Configuration] section available at the top.

   ; Note: EnableTACACSPlusServer parameter is applicable only for Linux Global
   ;Enterprise Edition. It is not applicable for Windows platform.
   ;EnableTACACSPlusServer = 0

b. And append the following [EapSettings] entries at the end of the file and save the file. [EapSettings]
   ;Allows Backward compatibility in SSL/TLS protocol suite( Options - 1/0 )
   ;AllowTLSFallback = 1
   ;Specifies the SSL/TLS protocol version to be used.
   ;Options - TLSv10,TLSv11,TLSv12
   ;MinimumProtocolVersion = TLSv12

- If Steel-Belted Radius is being upgraded to 6.24-R3 version or higher, it is important to modify the following parameters manually in the file "sbr_administration.xml" that is present on the Steel-Belted Radius installed directory.
  Edit Line 40 and 41: under program_id radAdmin.RadAdminTlsSessionMgr with the following values.
  minimumProtocolVersion="33" (Earlier it was 31 by default)
  ciphersuites="0x3C,0x3D,0x67,0x6B,0x40,0x6A,0x9C,0x9D,0x9E,0x9F,0xA2,0xA3" (Earlier it was TLS 1.0 ciphers by default)

## Starting Steel-Belted Radius Application

Once all the manual migration is completed, you must start the RADIUS process. Refer to "Radius version Starting the RADIUS Server" section for information on starting the RADIUS process.

## Launch the Steel-Belted Radius Administrator/WebGUI

Connect the server from where the Steel-Belted Radius Administrator/ Web GUI is going to be launched. You can launch the SBR Administrator using the URL: https://<Server name>:1812/.

You can launch the SBR Web GUI using the URL: https://<Server name>:1810/sbreweb/login.html.

Once the SBR Administrator/Web GUI is running successfully, following Steel-Belted Radius Database configurations" must be executed.

### Manual Migration of Licenses

The license keys have to be reloaded to Steel-Belted Radius Administrator. Refer to "Adding License Keys" section for information on adding License Keys.

### Migrating Configuration Data in SBR Administrator

Import the saved database configurations by importing the XML file you have saved earlier. Refer to the *Steel-Belted Radius Administration guide* (Appendix E – "Importing and Exporting Data" for information on how

to import your Steel-Belted Radius database from an .xml file).

### Manual Migration of ROOT Certificates

The storage of root certificates is managed by the Steel-Belted Radius server and the SBR Administrator is used to add and delete root certificates. You must manually migrate root certificates by using the SBR Administrator to add them from the old root directory.

Note: If any UNIX users are imported, it is advisable to delete them and create them newly as per the UNIX users available in the Linux platform.

# Chapter 6

# Uninstalling Steel-Belted Radius

This chapter describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows or Linux host.

## Uninstalling Steel-Belted Radius on Windows

Use the Windows "Programs and Features" under control panel to uninstall the Steel-Belted Radius server software and Steel-Belted Radius Administrator.

Note: Stop the "Steel-Belted Radius" service before uninstalling the server.

## Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from a Windows host:

1. Choose Start > Control Panel > Programs and Features.
2. When the Programs and Features window opens, select Steel-Belted Radius.
3. Click Uninstall.
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 (x86)\Pulse Secure\Steel-Belted Radius\Service directory.

## Uninstalling the Legacy 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:\Users\Administrator\AppData\Roaming\PulseSecure
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 Steel-Belted Radius on Linux

This section describes how to uninstall the Steel-Belted Radius server software and SBR Administrator configuration application on a Linux 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/PSsbr):

1. Log into the Linux server as root.
2. Stop the Radius process by issuing the following commands:

   # cd /opt/PSsbr/radius

   # ./sbrd stop
3. Back up your Steel-Belted Radius server directory.

   Create a new archive directory to ensure that you do not overwrite an existing backup.

   # cd /opt/PSsbr

   # mkdir /opt/backups

   # tar cf - radius | ( cd /opt/backups; tar xfBp - )
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/PSsbr/radius/install

   # ./unconfigure
6. Execute the following command to uninstall the Steel-Belted Radius server software:

   # rpm -e sbr-ent-6.2-0.i386.rpm

   Where edition specifies the Steel-Belted Radius edition (Global Enterprise Edition (gee); 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 6.1, you would enter the following:

   # rpm -e sbr-gee-6.2-0.i386.rpm

   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/PSsbr

## Uninstalling the Legacy 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/.pulsesecure/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.

# Glossary

| Terms | Description |
|---|---|
| 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 its 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. Refer **Table 8** CIDR Translation. |

| Terms | Description |
|---|---|
| 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.<br>1. The read community string allows an SNMP management station to issue Get and GetNext messages.<br>2. 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. |
| DHCP | 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. |
| DNIS | Dialed number identification service. A telephone service that identifies what number was dialed by a caller. |
| DNS | Domain Name Service. Internet protocol for mapping host names, domain names, and aliases to IP addresses. |
| EAP | Extensible Authentication Protocol. An industry-standard authentication protocol for network access that acts as a transport for multiple authentication methods or types. Defined by RFC 2284. |
| EAP-32 | See POTP. |
| EAP-TTLS | Authentication method that uses EAP (Extensible Authentication Protocol) and TTLS (Tunneled Transport Layer Security). |
| GTC | Generic Token Card. |
| IEEE | Institute of Electrical and Electronics Engineers. |
| IETF | Internet Engineering Task Force. Technical subdivision of the Internet Architecture Board that coordinates the development of Internet standards. |
| IPv4 | Implementation of the TCP/IP suite that uses a 32-bit addressing structure. |
| IPv6 | Implementation of the TCP/IP suite that uses a 128-bit addressing structure. |
| Java | Programming language designed for use in distributed environments such as the Internet. |

| Terms | Description |
|---|---|
| JDBC | Java Database Connectivity. Application programming interface for accessing a database from programs written in Java. |
| LDAP | Lightweight Directory Access Protocol. An IETF standard protocol for updating and searching directories over TCP/IP networks. |
| LDIF | LDAP Data Interchange Format. The format used to represent directory server entries in text form. |
| 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. |
| MPPE | Microsoft Point-to-Point Encryption. A means of representing point-to-point packets in an RC4 encrypted format. Defined in RFC 3078. |
| 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.<br>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 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. |

| Terms | Description |
|---|---|
| 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. |
| SHA-1 | Secure Hash Algorithm-1. A one-way cryptographic function that takes a message of any length and produces a 160-bit message digest. |
| session ID | Session Identifier. A string of characters uniquely identifying the session. |
| SHA-1 | Secure Hash Algorithm-1. A one-way cryptographic function that takes a message of any length and produces a 160-bit message digest. |
| shared secret | An encryption key known only to the sender and receiver of data. |
| silent discard | The process of discarding a packet without further processing and without notification to the sender. |
| SNMP | Simple Network Management Protocol. |
| SSL | Secure Sockets Layer. Program layer that manages the security of messages on a network. |
| supplicant | The client in an 802.1X-authenticated network. |
| TACACS+ | 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. |
| TLS | Transport Layer Security. |
| trap | An SNMP message that reports a significant event, such as a problem, error, or change in state that occurred within a managed device. |
| trap sink | The destination for trap messages sent by an SNMP agent on a managed device. |
| TTLS | Tunneled Transport Layer Security. |
| user database | A database where a RADIUS server keeps information about users, such as authentication information and network access permissions. |
| user profile | A record in the user database that describes how a particular user or class of users should be configured during authentication and authorization. |
| VSA | Vendor Specific Attributes. |
| WEP | Wired Equivalent Privacy. An encryption method designed to encrypt traffic between a WLAN client and an access point. |
| WLAN | Wireless Local Area Network. |

Table 8: CIDR Translation

| CIDR Format | First Address | Last Address | Number of Usable IP Addresses[a] | Comparable IP Subnet Mask |
|---|---|---|---|---|
| **10.0.0.0/8** | 10.0.0.0 | 10.255.255.255 | 16,777,214 | 255.0.0.0 |
| **10.0.0.0/16** | 10.0.0.0 | 10.0.255.255 | 65,534 | 255.255.0.0 |
| **192.168.0.0/24** | 192.168.0.0 | 192.168.0.255 | 254 | 255.255.255.0 |
| **.l192.168.0.0/25** | 192.168.0.0 | 192.168.0.127 | 126 | 255.255.255.128 |
| **192.168.0.0/26** | 192.168.0.0 | 192.168.0.63 | 62 | 255.255.255.192 |
| **192.168.0.0/27** | 192.168.0.0 | 192.168.0.31 | 30 | 255.255.255.224 |
| **192.168.0.0/28** | 192.168.0.0 | 192.168.0.15 | 14 | 255.255.255.240 |
| **192.168.0.0/29** | 192.168.0.0 | 192.168.0.7 | 6 | 255.255.255.248 |
| **192.168.0.9/29** | 192.168.0.8 | 192.168.0.15 | 6 | 255.255.255.248 |
| **192.168.0.10/30** | 192.168.0.8 | 192.168.0.11 | 2 | 255.255.255.252 |
| **192.168.0.10/31** | 192.168.0.10 | 192.168.0.11 | 0 | 255.255.255.254 |
| **192.168.0.10/32** | 192.168.0.10 | 192.168.0.10 | 1 | 255.255.255.255 |

# Index

I

IAS, 20
Installing the Linux RPM,

37 L

LDAP, 58
license number, 19
Linux, 37
Linux,upgrade,

41 M

Microsoft IAS,

20 O

ODBC,

59 cxP

pre-installation checks administrator
account access 19

host name resolution,

13 R

radiusdir,

40 S

SBR Administrator, 41
sbrd, 45
sbrd restart, 46
sbrd start, 46
sbrd status, 47
sbrd stop,

46 U

uninstall sbr on linux, 55
uninstall sbr on windows, 54
upgrade sbr, 30

W

Windows, new install, 20