

Steel-Belted Radius[®] Carrier Release Notes

Release 7.2.3
2 September 2010
Revision 1

These Release Notes support Release 7.2.3 of Steel-Belted Radius Carrier (SBRC). Information for releases 7.2.0, 7.2.1 and 7.2.2 is also included where noted. Before you install or use your new software, read these Release Notes in their entirety, especially “Known Problems and Limitations” on page 12.

Contents

Release Overview	4
Before You Start	4
Documentation	4
System Requirements	4
Standalone SBR Carrier Server Hardware	4
Session State Register Host Hardware	5
SBRC and Management Node Hosts	5
Data Node Hosts	6
Software	7
Required Patches	7
Recommended Patches	7
Perl	8
Supported Browsers	8
External Database Requirements	8
Signalware and SS7 Interface Requirements	8
Modified Open-Source Software	9
Migrating from Earlier SBR Releases	9
Migrating from Earlier SBR Standalone Server Products	9
Supported Releases for Standalone Server	9
Migrating from SBR Release 5.5 High Availability	10
Using a Transition Server	10
Using the SSR Configuration Script	10
Migration and New Installations of SBR Carrier with WiMAX	11
Known Problems and Limitations	12
CDMA	12
CoA/DM	13

Filters	13
LDAP Authentication	13
Oracle	13
Replication	13
SBRC Administrator	14
SBRC Core	14
Session State Register Module	15
SIM Authentication	16
SNMP	17
WiMAX Module	17
Documentation Updates	17
account.ini File	17
admin.ini File	19
Attributes No Longer Editable or Orderable	19
CDMA	19
certinfo.ini File	19
classmap.ini File	19
Dictionary Files	20
Directed Realm Configuration (.dir) File	20
EAP-TTLS Client Certificate	20
HTTP Digest Access Authentication	21
IP Addressing	21
JavaScripting	21
LDAP	22
radius.ini File	22
radsql.aut File	24
radsqljdbc.aut File	24
realm.pro File	24
Replication of RADIUS Configuration Data	24
RFC 5281	25
Session State Register	25
SIM Authentication	32
SMS Authentication	32
Statlog.ini	32
ttlsauth.aut File	33
Ulticom Documentation	33
Uninstalling Signalware 9	33
wimax.ini	35
WiMAX	35
Leading Wildcards and Session Queries	35
Resolved Issues	35
Release 7.2.3	35
Release 7.2.2	40
Release 7.2.1	41
Release 7.2.0	43
Related Documentation	44
Requests for Comments (RFCs)	44
3GPP and 3GPP2 Technical Specifications	46
WiMAX Technical Specifications	46

Third-Party Products	46
General Statement of Compliance	46
SBR Carrier Documentation and Release Notes	51
Documentation Feedback	52
Requesting Technical Support	52
Self-Help Online Tools and Resources	52
Opening a Case with JTAC	53
Revision History	53

Release Overview

These release notes cover Release 7.2.3 of the Juniper Networks Steel-Belted Radius Carrier product.

Before You Start

Before you use your new software, read these *Release Notes* in their entirety, especially the section *Known Problems and Limitations*.

Documentation

Table 1 on page 4 lists and describes the Steel-Belted Radius Carrier documentation set:

Table 1: Steel-Belted Radius Carrier Documentation

Document	Description
<i>Steel-Belted Radius Carrier 7.2 Installation Guide</i>	Describes how to install the Steel-Belted Radius Carrier software on the server and the SBRC Administrator application on a client workstation.
<i>Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide</i>	Describes how to configure and operate the Steel-Belted Radius Carrier and its separately licensed modules.
<i>Steel-Belted Radius Carrier 7.2 Reference Guide</i>	Describes the settings and valid values of the Steel-Belted Radius Carrier configuration files.
<i>Steel-Belted Radius Carrier 7.2.0 Release Notes</i>	Contains the latest information about features, changes, known problems, and resolved problems in Release 7.2.0.



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

You can find these release notes in Adobe Acrobat (PDF) format on the Juniper Networks Technical Publications Web page, which is located at

https://www.juniper.net/techpubs/software/carrier_aaa/carrier/.

System Requirements

This section describes the hardware and software requirements for running a standalone Steel-Belted Radius Carrier server or the optional SBR Carrier Session State Register (SSR) on Sun hardware under the Solaris 10 operating system. For more detailed information, see “Meeting System Requirements” in the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

Standalone SBR Carrier Server Hardware

These basic specifications apply to any standalone Steel-Belted Radius Carrier server — one that does not participate in a Session State Register cluster.

Additional system requirements apply to all Session State Register servers, such as dual Gigabit Ethernet NICs (to provide redundant communication links). See “Supported SBR Carrier SSR Cluster Configurations” in the *Steel-Belted Radius Carrier 7.2 Installation Guide* for these additional requirements.

Table 2: Standalone Steel-Belted Radius Carrier Server Hardware Configurations

Server	RAM	CPUs	Free Disk Space
Standalone SBR Carrier Server (Minimum Configuration)	10 GB RAM.	Two-CPU Ultrasparc IIIi or better, running at 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBRC Administrator.
Standalone SBR Carrier Server (Recommended Configuration)	12 GB RAM or more. If the WiMAX or SIM module, or an SS7 communications interface is installed, the Uticom Signalware communications stack is used. To support the stack and for systems processing a heavier-than-normal load (for instance, with additional session licenses), more memory produces better performance.	Multiple CPU Ultrasparc IIIi or better running at more than 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBRC Administrator.

Session State Register Host Hardware

SBRC and Management Node Hosts

Table 3 on page 5 lists the hardware requirements for Session State Register cluster SBRC and management node hosts.

Table 3: Session State Register SBRC and Management Node Host Hardware Configurations

Server	RAM	CPUs	Free Disk Space	Network Interfaces
SBRC and/or Management Node Host (Minimum Configuration)	2 GB RAM.	Two-CPU Ultrasparc IIIi or better, running at 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBRC Administrator.	Two physical interfaces on a 100 Base-T network. Multipath configuration is required.

Table 3: Session State Register SBRC and Management Node Host Hardware Configurations (*continued*)

Server	RAM	CPUs	Free Disk Space	Network Interfaces
SBRC and/or Management Node Host (Recommended Configuration)	<p>4 GB RAM or more.</p> <p>If the WiMAX or SIM module, or an SS7 communications interface is installed, the Utcicom Signalware communications stack is used. To support the stack and for systems processing a heavier-than-normal load (for instance, with additional session licenses), more memory produces better performance.</p>	<p>Multiple CPU</p> <p>Ultrasparc IIIi or better running at more than 1.5 Ghz.</p>	<p>At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBRC Administrator.</p>	<p>Two physical interfaces on a Gigabit Ethernet network.</p> <p>Multipath configuration is required.</p>

Data Node Hosts

Table 4 on page 7 lists the hardware requirements for Session State Register data node hosts.

All data node hosts in a cluster *must* have the same configuration. Because they collaborate to keep a shared database in virtual shared memory, the processing power, RAM, and communications capability of all the host machines need to be very similar.



NOTE: This free disk space shown in Table 4 on page 7 must be available specifically to the /opt file system for installation of the SSR software.

Table 4: Session State Register Data Node Host Hardware Configurations

Server	RAM	CPUs	Free Disk Space	Network Interfaces
Data Node Host (Minimum Configuration)	10 GB RAM.	Two-CPU UltraSparc IIIi or better, running at 1.5 Ghz.	The local disc space requirement is related to the amount of RAM in the system. To calculate the minimum requirement for the amount of RAM on the system, use the formula: (RAM - 4 GB) * 12 .	Two physical interfaces on a 100 Base-T network. Multipath configuration is required.
Data Node Host (Recommended Configuration)	More than 10 GB RAM. More than the minimum of 10 GB of RAM supports more connections because more of the SSR database can be held in memory. More database in memory may translate into faster processing because disk operations are minimized. Note: In particular, more memory is required if you want the SSR to store more CST data; that is, if <code>config.ini</code> DataMemory and IndexMemory parameters are manually increased. (Refer to PR 495661 in Resolved Issues for more information.)	Multiple CPU UltraSparc IIIi or better running at more than 1.5 Ghz.	For example, a system with 16 GB of RAM requires a minimum of (16 GB - 4 GB) * 12, or 144 GB of local disk storage space.	Two physical interfaces on a Gigabit Ethernet network. Multipath configuration is required.

Software

Steel-Belted Radius Carrier server requires Sun Solaris 10 8/07 for SPARC platforms, with the appropriate patches.

Required Patches

These patches (or higher-numbered equivalents) are required for Solaris 10:

- 117461-08 — ld.so
- 119254-44 — patchadd
- 119963-13 — libC
- 120753-05 — libmtsk
- 120900-04 — libzonecfg
- 121133-02 — zoneadm

Recommended Patches

These patches (or higher-numbered equivalents) are recommended for Solaris 10:

- 113886-48 — OpenGL 1.3 32-bit
- 113887-48 — OpenGL 1.3 64-bit

Perl

Sun ships Solaris 10 with Perl 5.8.4, and Steel-Belted Radius Carrier has been tested with that version. Multiple Perl installations in discrete directories are supported, but attempting to use other versions of Perl with SBR Carrier may cause problems.

Supported Browsers

The SBRC Administrator configuration application can be launched from the browsers listed in Table 5 on page 8:

Table 5: Supported Browsers

Browser	Versions	Operating System
Internet Explorer	6.0, 7.0	Windows XP SP2
Mozilla Firefox	2.0	Windows XP SP2
Mozilla	1.7	Solaris 10 with JRE 1.5.0_11

Java Runtime Environment (JRE) 1.4.2 or newer is required for all browsers, and is available from <http://java.sun.com>.

External Database Requirements

Steel-Belted Radius Carrier supports:

- Oracle 9 and 10; versions 9.2.0 and 10.2.0 are recommended.
- For the Steel-Belted Radius Carrier to act as an Oracle native client, Oracle client must be set up before installing SBR Carrier because the Oracle server location is used during installation.
- The JDBC plug-in has been tested with Oracle on Solaris and the JDBC plug-in for MySQL.

Signalware and SS7 Interface Requirements

If you want the Steel-Belted Radius Carrier server to support the optional SIM authentication module or the optional WiMAX module, Ulticom Signalware 9 with Service Pack 5T needs to be installed in the server before you install SBR Carrier software.

If you want the Steel-Belted Radius Carrier server to communicate with any SS7 legacy equipment, install the Ulticom SS7 communication board and Signalware 9 with Service Pack 5T before you install SBR Carrier software.



CAUTION: Service Pack 5T must be installed, or Steel-Belted Radius Carrier cannot use the Signalware communications stack.

The patch is delivered in the same directory as the SBRC and Signalware 9 .tgz files as SIGNALWARE_9_SP5.T_SOLARIS10_UPGRADE.TGZ.

After the base Signalware 9 software is installed, use the Signalware installation program to install the patch. For specific directions, refer to the Signalware documentation. To see a sample procedure for applying the patch, see “Installing Signalware Service Pack 5T” in the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

The Signalware PH0301 and XH0303 boards are supported.

For more information, see the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

Modified Open-Source Software

Embedded in this version of Steel-Belted Radius Carrier is open-source software that Juniper Networks, Inc. has modified. The modified software includes:

- LDAP C SDK from The Mozilla Foundation
- HTTPClient from Ronald Tschalär
- **sunmd5.c** from The OpenSolaris Project

You can obtain the source code for these modifications by requesting them from Juniper Networks Technical Support. See “Requesting Technical Support” on page 52.

Migrating from Earlier SBR Releases

SBR Carrier Release 7.2.x can run as a standalone server or as part of a Session State Register cluster.

Migrating from Earlier SBR Standalone Server Products

You can use the configuration script to move a number of files from selected previous SBR releases to the Release 7.2.3 environment when installing Steel-Belted Radius Carrier. The corresponding Release 7.2.3 files are also loaded on the system, but are not activated. You are responsible for merging new settings from Release 7.2.3 configuration files into the working (pre-existing) configuration files. To support new features, SBR Carrier uses default values for any new settings that have not been merged into the working configuration files.

Supported Releases for Standalone Server

You can migrate configuration files from these SBR server releases to Release 7.2.3:

- Mobile IP Module (MIM) Release 5.32
- SIM Server Release 5.4
- SBR Service Provider Edition Release 6.0 and Release 6.1
- SBR Carrier Release 7.0

For complete details on migrating from these releases, see the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

Migrating from SBR Release 5.5 High Availability

The easiest way to replace an existing SBR Release 5.5 High Availability (SBR HA) cluster with a new Release 7.2.3 cluster is to fully install and configure the new cluster and then cut over to the new cluster.

Doing this causes a brief service disruption that you can mitigate by allowing both clusters to run online in parallel long enough for existing sessions to naturally drop off the old cluster as they end. Because no new sessions are added to the old cluster, after some period of time, most active sessions are managed by the new cluster. Any remaining long-term sessions are terminated when the old cluster is brought down. When they reconnect to the network, they connect to the new cluster.

Using a Transition Server

Some sites may not have enough servers to support two clusters running simultaneously. To address this issue, we developed a migration strategy that uses a transition server. A *transition server* is a single machine that temporarily takes the place of your existing, working cluster while you take the servers from that cluster offline, install Release 7.2.x software on them, and then bring them back online as a Release 7.2.x cluster.

Use a transition server in addition to the four servers that a basic cluster installation requires to ensure redundancy. The fifth server performs the work of the entire cluster while you take the four existing SBR/HA Release 5.5 servers offline, update them, and bring them back online in an SSR Starter Kit configuration.

If a fifth host machine is not available and you must work only with the four servers that currently make up the SBR/HA Release 5.5 cluster, you can adapt the transition server strategy and borrow one server from the existing cluster to use as the transition server. Doing this increases the risk of cluster failure during the switchover because some level of redundancy or capacity is removed from the existing, working cluster when you take one host machine offline.

For details about migrating from SBR Release 5.5 High Availability, see the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

Using the SSR Configuration Script

When running the SSR configuration script, option "2. Generate Cluster Definition" always generates a 16 digit random number that is saved in `dbcluster.dat` as the `CLUSTER_DEFAULT_KEY`. Upon selecting configure script option "3. Configure Cluster Node" the following occurs:

1. The `CLUSTER_DEFAULT_KEY` is used to configure `spi.ini` [Keys] if:
 - `CurrentKey=` has not already been configured.
 - and
 - The first key `1=` has not already been configured.
2. Any IP addresses previously specified for nodes in the cluster are added to the `spi.ini` [Hosts] section if they are not already present. (PR 481510)



NOTE: If you are migrating from an older `spi.ini` then:

1. It is likely that [Keys] have already been configured and it is up to you to maintain [Keys] in this case.
2. Node IP addresses may still be added to [Hosts] but pre-existing (and possibly obsolete) addresses will not be removed.

Also note that the IP addresses specified for nodes during cluster configuration are primarily intended for SSR as opposed to RADIUS-specific configuration. If RADIUS traffic utilizes different IP addresses from SSR traffic then it is up to the user to maintain `spi.ini` [Hosts].

Migration and New Installations of SBR Carrier with WiMAX

Release 7.2.3 of SBR Carrier includes improvements in the WiMAX processing software. This change improves both performance and scalability. The improvements include different logic for assigning primary keys to WiMAX tables and for generating the Class attribute in the Access-Accept response. To control these improvements, a new parameter, `EnableWiMAXUniqueSessionIdFromNAI`, has been added to the `radius.ini` file. (PR 454398, PR 475897)



NOTE: When the `EnableWiMAXUniqueSessionIdFromNAI` parameter is enabled, new session records in the database and the Class attribute in Access-Accept messages are incompatible with the WiMAX logic in previous releases of SBR Carrier. For this reason, this parameter is disabled by default.

For new installations of the Release 7.2.3 software running the optional WiMAX module, we recommend that you enable this parameter as part of your installation procedure. It must be enabled on all SBR Carrier servers in your network.

If you are currently running a previous release of SBR Carrier and using WiMAX, the new WiMAX logic is backward compatible with the previously released WiMAX logic; that is, it understands the older session records and Class attributes. However, the older WiMAX logic does not comprehend the new session records or Class attribute in the Access-Accept messages. Due to this incompatibility, when you have multiple SBR Carrier servers in your network, you need to upgrade each server before enabling the `EnableWiMAXUniqueSessionIdFromNAI` parameter.



NOTE: If you are running the Session State Register (High Availability) cluster, this upgrade does not require any changes to the session database schema, and does not require any stopping or starting of nodes in the cluster. Therefore, it is nondisruptive.

For networks running multiple SBR Carrier servers follow this procedure to upgrade:



NOTE: Upgrading the SBR Carrier software does not interrupt service.

1. Upgrade the first server with the Release 7.2.3 software. Do not enable the EnableWiMAXUniqueSessionIdFromNAI parameter.
2. Upgrade the next server with the Release 7.2.3 software. Do not enable the EnableWiMAXUniqueSessionIdFromNAI parameter.
3. Repeat until all servers are running the Release 7.2.3 software.

At this point, all servers are running the Release 7.2.3 software, but the EnableWiMAXUniqueSessionIdFromNAI parameter is disabled on all servers. The next step is to enable the EnableWiMAXUniqueSessionIdFromNAI parameter on all servers one by one.

1. Select the first server.
2. Edit the [Configuration] section of the **radius.ini** file and set EnableWiMAXUniqueSessionIdFromNAI =1.
3. Restart the server (sbrd restart). (The EnableWiMAXUniqueSessionIdFromNAI parameter is not updated on receipt of a HUP.)

After the server is back up, repeat this process on each and every server in the network one by one.

Known Problems and Limitations

These issues have been identified in Steel-Belted Radius Carrier 7.2.x. The identifier in parentheses is the Problem Report number in our bug database.

CDMA

- **Because prepaid session IDs are kept in memory, if SBR Carrier stops, these session IDs are lost.** If prepaid session IDs are lost, the sessions must be deleted from the prepaid server; otherwise new prepaid sessions may not be available. (PR 248265, PR 444460)
- **To set session timeout, use the SessionTimeoutSeconds in the prepaid.att file or a Session-Timeout attribute in a profile.** A session timeout cannot be set using a filter in the **3GPP2.ini** file. (PR 248448, PR 306397)

CoA/DM

- **If a NAS client is configured without saving the RFC3576 CoA/DM Shared Secret password, a password appears to be configured when the client is subsequently viewed.** If unexpected results such as invalid signatures occur, make sure that the password is set correctly. (PR 420409)

Filters

- **Changing a rule in SBRC Administrator with Filter>Edit Rule from Exclude or Add to Replace has no effect.** Instead of changing the rule type, delete the attribute and then add a new attribute with the correct **Replace** type. (PR 298086)
- **A filter with an index that is configured to replace a parent attribute with multiple instances of a single subattribute does not always work correctly.** To avoid this, set up the configuration so that it uses multiple separate attributes that each contain the same subattribute. (PR 298631)

LDAP Authentication

- **Setting the MaxConcurrent setting in the ldapauth configuration files to very large values can cause Steel-Belted Radius Carrier to run out of memory and crash.** As a workaround, use smaller values of MaxConcurrent, for example less than 1000. (PR 249953)

Oracle

- **The native Oracle plug-ins (radsql_accessor_ora*.so, radsql_acct_ora*.so, radsql_auth_ora*.so) utilize the modern Oracle Call Interface version 8 API that is specified by Oracle.** Because calls to this API do not accept any timeout parameters, and because even explicitly cancelling outstanding Oracle transactions is not guaranteed to succeed in a timely fashion, the following configuration parameters do not have any effect when they appear in the configuration files (***gen, *acc, *aut**) for native Oracle plug-ins: (PR 410616)

```
[Settings]
ConnectTimeout=25
QueryTimeout=25

[Server/*]
ConnectTimeout=25
QueryTimeout=25
```

Replication

- **After a server is configured as non-replicating, it cannot be converted to a primary server.** You must reinstall the server to set it up as a primary server. (PR 436725)
- **Replica servers that are offline when the primary server publishes configuration data may not update correctly.** (PR 284279) To correct this:

1. Execute on the replica:

```
# sbrsetuptools -identity REPLICA -primary name address secret
```

where:

name is the DNS name of the primary server

address is the IP address of the primary server

secret is the shared secret that authenticates configuration downloads

2. Restart the replica.
- **There is a slow memory leak on the replica during replication.** (PR 510698)

SBRC Administrator

- **When a profile is configured in SBRC Administrator, the value entered in a checklist can exceed the maximum length for the value that is specified in the dictionary file.** This does not cause any problems in Steel-Belted Radius Carrier, but if any external applications require a value with a specific length, the external application may generate an error. (PR 306944)
- **The Auth Logs dialog in the Reports section of the SBRC Administrator does not correctly allow searching for events before a particular time and date.** An error is displayed if the To field is used in this dialog. (PR 461691)

SBRC Core

- **The UseMasterDictionary feature may add or allow unknown attributes.** This can result in the dispatch of an incorrect packet. The problem occurs if two vendor-specific dictionaries associate the same attribute number with different types (such as string and integer). (PR 248477)
- **To open the audit log in a browser, the close-tag of the root element ("`</auditRecords>`") must be manually moved to the end of the file.** (PR 435027)
- **The proxy logging enhancement features introduced in Release 7.2.2 apply only to extended proxy or to realms defined in the proxy.ini file.** They do not apply to legacy proxy, including Proxy-As-Authentication-Method. (PR 444675)
- **If SBR Carrier receives an Accounting-Start message after the Accounting-Stop message for the same session has already been processed, SBR Carrier will create a new session that will only be removed by stale session purging.** (PR 447739)
- **PEAP with inner TLS may fail with Windows supplicants.** Microsoft technical support reports that in EAP-PEAP phase 2, MS PEAP does not support fragmentation on the outer packets. To prevent this, set the inner TLS packet fragmentation so that no outer fragmentation is necessary during the negotiation. Edit `tlsauth.aut`, and in the `[Server_settings]` section, set `TLS_Message_Fragment_Length=900`. (PR 254219)
- **If the location of the logging directory is changed from the default, make sure that the directory exists before starting SBRC.** Otherwise, SBRC may fail to function correctly. (PR 437583)
- **When a subattribute string with a length of 244 characters is specified, the expected response is not returned.** To avoid this situation, edit the string to reduce the number of characters to fewer than 244. (PR 298055)

- If RADIUS vendor-specific attributes (VSAs) are added to the session database schema, they should be defined as VARBINARY type. (PR 412255)
- AcctCarryOver is no longer supported because the expanded capacity of the database makes it unreasonable to write all existing sessions to a log file at one time. (PR 297789)
- If user concurrency is enabled after user sessions have been established, those sessions are not counted toward concurrency limits. (PR 431438)
- Configuration of large checklists or return lists via the LDAP configuration interface (LCI) can result in a crash of the server. If the total permissible size of a configuration object (64 KB) is exceeded by adding many checklist or return list attributes to a native user or profile object, then SBRC will crash trying to process the LCI transaction. A workaround with better performance characteristics is to avoid very large checklists and use multiple native users or Dialed Number Identification Service (DNIS) mapping instead. Very large return lists are not likely to be required in any valid configuration because a RADIUS packet can only contain less than 4 KB of return attributes. (PR 451518)
- If multiround (challenge) authentication is used, the AddFunkClientGroupToRequest feature adds the Funk-Radius-Client-Group attribute-value pair (AVP) to only the first access request. Subsequent challenge responses will not have this attribute added, and, therefore, cannot use this attribute in checklist processing when EAP or other challenge-based protocols are used. (PR 460109)
- In either cluster or standalone mode, SBR Carrier will crash on startup if the session database exists but no tables have been created. During normal installation, the database processes are installed and started, and database tables are then automatically created. Manually installing the product or aborting the installation process can result in an uninitialized database. The CreateDB.sh administration script can be run to correct this situation. (PR 451019)
- In scenarios where SBR Carrier proxies requests to downstream authentication and accounting servers, Class attributes are handled incorrectly if the downstream RADIUS server returns more than one Class attribute. In such scenarios, the downstream accounting servers will not receive the correct Class attributes. The support for Class attributes in proxy scenarios works correctly only if the downstream server returns less than two Class attributes in the Access-Accept message. (PR 465894)

Session State Register Module

- A HUP signal reinitializes the cluster, causing SBR Carrier to enter Management mode and any IP address caches to be reinitialized. During this reinitialization, authentication requests exhibit longer than normal latency if IP address assignment is configured. To prevent this behavior, set UpdatePlugins = 0 in the [HUP] section of update.ini file. To use theUSR2 signal instead of HUP to reinitialize the cluster, set UpdatePlugins = 1 in the [USR2] section. (PR 416232)
- Configuring redirection and concurrency together causes sessions that are rejected due to concurrency limitations to be redirected and to populate the database and may interfere with correct operation of concurrency. (PR 422987)

- **Although WimaxAcctFlows is included in the session table, it is not displayed by the ShowSessions script.** This is normal, as it consists of binary data and is not readable. (PR 440624)
- **SBR Carrier Cluster IP address allocation is limited to caching 30,000 IP addresses per SBRC front-end node.** If any front-end node is configured to cache more than a total of 30,000 IP addresses via `dbclusterndb.gen`, then this SBRC node cannot correctly clear up cached addresses on a restart. These failed restarts can lead to large amounts of leaked IP addresses that are no longer available for use until manually cleaned up via SQL. The `ClearCache.sh` administration script cannot correct this situation since it will also fail to clear the address cache in this situation. Customers should cap their total caching at 30,000 IP addresses for each front-end node, proportionally reducing the recommended cache sizes for their pools until the total is less than 30,000 IP addresses. (PR 486733)

SIM Authentication

- **The performance of the SIM module in Release 7.2.3 is degraded compared to that of SBR SIM 5.4.** (PR 548118)
- **When the optional SIM Module is in use and SIMAUTH is used as an EAP method, changing the order of EAP methods in SBRC Administrator does not take effect.** Manually edit the `eap.ini` file to make the change. (PR 306868)
- **For EAP-SIM and EAP-AKA requests, the first byte of the request contains the EAP-Identifier that SBR Carrier uses to select the EAP method.** If this byte is incorrect, SBR Carrier cannot properly identify and select the EAP method. In this case, SBR Carrier may respond with a protocol the client cannot support. If the client does not support NAK, and thus cannot respond with a NAK, the request fails. (PR 303268)
- **When using the SIM authentication module with EAP-helper enabled and a profile checklist with subattributes is in use, a false authorization can be returned.** There is no workaround. In some cases, you might be able to implement a valid check if the helping authentication method is LDAP, because LDAP scripting may be able to workaround the checklist issue. (PR 310988)
- **CDR: the event timestamp value is incorrect in the CdrAccounts table.** Although the event timestamp in CDRs is always erroneously set to 1970-01-01 00:00:01 (TZ=+00:00), the actual start time is present in `AccStartTimeUTC`. (PR 435470)
- **Do not specify the `-host <hostname>` option in the Signalware MML CREATE-PROCESS command, which is responsible for starting the authGateway process used by the SIM Authentication module.** Doing so may cause the authGateway process to fail in environments where IP multipath is enabled. (PR 403141)
- **The Ulticom Signalware communications stack that is accessed by the SIM authentication module may generate false error messages in the Signalware log.** When the stack is first accessed, an 8057 message is generated if everything is working properly:
 - > 008057 26-Aug-2008 10:58:25 mercury.POP Info Signalware Application(s)
 - > Authorized.
 - >

After that, messages such as this example may be generated periodically as a countdown timer expires:

```
> 008056 26-Aug-2008 11:00:17 mercury.POP Critical Signalware
> Application(s) Not Authorized: 60 Minutes Remaining to Authenticate
>
```

These are false warnings that you can ignore.

SNMP

- **When address pools and ranges are configured in the database (instead of configured locally), the following traps behave differently and indicate when the cache for a pool enters *emergency* state (the size becomes zero).** The emergency continues until the cache size reaches or exceeds the configured low-water mark. The traps are sent under the following conditions: (PR 249876)
 - `funkSbrTrapIPAddrPoolLow` — Servicing a RADIUS request, SBR Carrier attempts to get a new address from the pool and finds the cache is empty. The cache enters emergency state and SBR Carrier tries to refill it synchronously.
 - `funkSbrTrapIPAddrPoolNormal` — In the cache-fill thread, the size of the queue has reached or exceeded the low-water mark.

WiMAX Module

- **WiMAX accounting records are too cryptic in the accounting log.** Because Class attributes are presented in a binary format, some users may prefer not to log them. (PR 291646)
- **Care must be taken to ensure the `.aut` file used for authentications is separate from the `.aut` file used for Authorize-Only requests, even though the two files may be using the same database table.** Also the `authorizeOnly.aut` file should not be able to handle or pass any authentications. (PR 411144)
- **Smart Dynamic Home Agent (HA) Assignment can be used by the HAAA to assign the hHA-IP-MIP4 address.** The feature cannot currently be used by the VAAA to assign the vHA-IP-MIP4 address. (PR 415662)

Documentation Updates

Information in this section updates the published Steel-Belted Radius Carrier 7.2.x documentation set. The identifier in parentheses is the Problem Report number in our bug database.

account.ini File

- **The default settings for the [Settings] section of the `account.ini` file in the *Steel-Belted Radius Carrier 7.2 Reference Guide* are incorrect; these are the correct default settings:** (PR 431214)

```
[Configuration]
LogDir =
```

```
[Settings]
Enable = 1
LineSize = 4096
LogfilePermissions = owner:group mode
MaxSize = 0
QuoteBinary = 1
QuoteInteger = 1
QuoteIPAddress = 1
QuoteText = 1
QuoteTime = 1
RollOver = 0
RollOverOnStartup = 0
Titles = 1
UTC = 0
```

- The *Steel-Belted Radius Carrier 7.2 Reference Guide* incorrectly states that accounting logging is enabled by default. The Enable parameter in the `account.ini` file is disabled (Enable=0) by default. To enable accounting logging, set Enable=1 and restart SBR Carrier. (PR 434062)

admin.ini File

- Due to interdependencies in configuration, to enable an administrator to configure users, the following settings are required in the [AccessLevel] section of the admin.ini file: (PR 445858)

Users=rw

IP-Pools=r

Profiles=r

This change applies to the *Steel-Belted Radius Carrier 7.2 Reference Guide*.

Attributes No Longer Editable or Orderable

- If dictionary entries are changed after tunnel, user, or profile attributes have been entered, existing attributes may become no longer editable or orderable. The following note should be added to the “Editing Dictionary Files” section of Chapter 4, Attribute Processing Files, in the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 435279)



NOTE: If dictionary entries are changed after tunnel, user, or profile attributes have been entered, existing attributes may become no longer editable or orderable. To edit such attributes, delete and re-enter them. This is working as designed.

CDMA

- Because prepaid session IDs are kept in memory, if SBR Carrier stops, the prepaid session IDs are lost. The following note should be added to the section “Components of the Prepaid Data Services” in Chapter 31, Configuring the Advanced Features of the CDMA Module, in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*: (PR 248266)



NOTE: Because prepaid session IDs are kept in memory, if SBR Carrier stops, the prepaid session IDs are lost. If prepaid session IDs are lost, the sessions must be deleted from the prepaid server; otherwise new prepaid sessions may not be available.

certinfo.ini File

- The “certinfo.ini File” section in Chapter 2, Operations Files, in the *Steel-Belted Radius Carrier 7.2 Reference Guide* should be removed from the manual. (PR 445232)

classmap.ini File

- **SBR Carrier can embed upstream Class attributes within an Access-Accept when it is acting as a proxy.** Upon receipt of a subsequent accounting request, SBR Carrier decapsulates and forwards the upstream server's Class attribute. This action can result in two Class attributes being present in the proxied accounting request. In the following example, the encapsulated Class attribute replaces the existing Class attribute in the accounting request to prevent the Class attribute for SBR Carrier from being forwarded. (PR 394317)

```
[Class]
```

```
replace = Class
```

This information should be added to the **classmap.ini** file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*.

Dictionary Files

- **The bundling flag option must be specified in all dictionaries using the same Vendor ID.** The following note should be added to the description of the flag character b or B in Table 56, Flag Characters, in the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 443441)



NOTE: The bundled option must be specified in all dictionaries that use the same Vendor ID.

Directed Realm Configuration (.dir) File

- **In the *Steel-Belted Radius Carrier 7.2 Reference Guide*, add the following under the [Auth] section of the .dir file:** (PR 428124)

For the FilterIn and FilterOut parameters, name the attribute or subattribute filters you want applied to request and response packets, respectively.

Add the following to Table 95, RealmName.dir [Auth] Syntax:

Parameter	Function
FilterOut = <i>name</i>	The FilterOut=<i>name</i> parameter causes Steel-Belted Radius Carrier to apply the filtering rules found in the [<i>name</i>] section of filter.ini . These rules are applied while Steel-Belted Radius Carrier is processing the <i>incoming</i> RADIUS request packet, and <i>before</i> it directs the packet <i>out</i> to the destination realm. You may also think of this as filtering various attributes and values <i>out</i> of the request before directing it to the realm.
FilterIn = <i>name</i>	The FilterIn=<i>name</i> parameter causes Steel-Belted Radius Carrier to apply the filtering rules found in the [<i>name</i>] section of filter.ini . These rules are applied <i>after</i> Steel-Belted Radius Carrier has received a response <i>in</i> from the destination realm, and while it is preparing the RADIUS response packet for its client. You may also think of this as filtering various attributes and values <i>in</i> to the response before returning it to the client.

EAP-TTLS Client Certificate

- **The following statement should be added to Step 9 of “Configuring Client Certificate**

Validation” on page 237 of the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*:

Special-purpose VSAs carry the certificate information and must be filtered into the inner authentication method in order to be made available for validation. For example, these lines could be added to the ttls transfer filter: (PR 416548)

```
Allow Funk-Peer-Cert-Subject
Allow Funk-Peer-Cert-Principal
Allow Funk-Peer-Cert-Hash
Allow Funk-Peer-Cert-Issuer
```

HTTP Digest Access Authentication

- **References to HTTP Digest Access Authentication should be labeled as Early Field Trial, including the following sections:** (PR 446214)

The “HTTP Digest Access Authentication” section in Chapter 2, RADIUS Basics, of the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*.

The following parameters in the **radius.ini** file described in Chapter 2, Operations Files, of the *Steel-Belted Radius Carrier 7.2 Reference Guide*:

- EnableEricssonViGHTTTPDigestSupport
- EnableHTTTPDigestSupport

IP Addressing

- **The following note should be added to the “Overlapping Address Ranges” section of Chapter 2, RADIUS Basics, in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*:** (PR 490016)



NOTE: Overlapping IP Address ranges are supported only in the standalone version of SBR Carrier.

JavaScripting

- The “Tunneled Authentication Plug-in Realm Selection Scripts” section of Chapter 49, Creating Realm Selection Scripts, in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide* fails to mention that when using JavaScripting, setting the disposition of an inner authentication request (for example, in TTLS) to discard does not suppress the sending of an Access-Reject by the outer request. (PR 404877)
- When JavaScripting is used and the number of SBRC worker threads is set to a high value, authentication failures may occur due to the inability to allocate Java script hosts. A new setting has been added **radius.ini** to limit the number of Java script host allocations which can be attempted. When set, worker threads will wait for a host to become available. The optimum setting for this parameter may vary depending on machine configuration and RADIUS traffic. (PR 483631)

[Configuration]

MaxEngines = n (default is 0, no limit)

LDAP

- The LDAP Configuration Interface schema documented in the “LDAP Virtual Schema” section of Chapter 24, *Using the LDAP Configuration Interface*, of the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*, incorrectly lists Tribe as an available attribute for session queries. This attribute should be removed from the LDAP schema. (PR 427161)
- The following information should be added to the description of FilterSpecialCharacterHandling parameter in Chapter 12, LDAP Authentication File, Table 138, *aut [Settings] Syntax, on page 265 of the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 446561)

In support of RFC 2254, the following substitutions are made when set:

- replace '(' with "\\28"
 - replace '>' with "\\29"
 - replace '*' with "\\2a"
 - replace '\' with "\\5c"
- A [RejectResponse] section should be added to the ldapauth.aut file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*. This section defines the attributes you want to return in an Access-Reject message. (PR 394690)

Example:

```
[Response]
Kineto-UMA-Reg-Reject-Cause = Kineto-UMA-Reg-Reject-Cause
Service-Type= Service-Type
```

```
[RejectResponse]
Kineto-UMA-Reg-Reject-Cause = Kineto-UMA-Reg-Reject-Cause
Filter-ID = Filter-ID
```

- In the *Steel-Belted Radius Carrier 7.2 Reference Guide*, the Search parameter should be removed from Table 137: *aut [Server/name] Syntax in the [Server/name] Sections of the LDAP Authentication Header (.aut) file. The search function is not supported. (PR 250248)

radius.ini File

The following corrections apply to the **radius.ini** file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*:

- **The *Steel-Belted Radius Carrier 7.2 Reference Guide* misnames the attribute that specifies the location of server log files as PrivateDir and lists it in the [Configuration] section of the radius.ini file.** The correct attribute is LogDir and it should be listed in the [Logging] section of the **radius.ini** file. The description shown for the PrivateDir attribute is correct; only the name of the attribute and location in **radius.ini** are incorrect. (PR 435013)

- **LogUsesUTC should be added to the radius.ini file as follows:** (PR 435735)

LogUsesUTC = <"yes"|"no"> (no is the default)

Configures whether log times are in UTC or local time. Use of local time causes timestamps to be automatically adjusted for seasonal adjustments, such as Daylight Saving Time in the United States, if applicable.

- **The description for the PhantomTimeout parameter in the radius.ini file [Configuration] section should be updated to reflect the same operation for an Accounting-Start message and an interim accounting packet as follows:** (PR 406182)

Specifies the maximum number of seconds for a phantom session record. When a phantom session is created, its expiration timestamp (Sbr_ExpirationTime) is set to its creation timestamp (Sbr_CreationTime) plus the PhantomTimeout value. If a corresponding Accounting-Start or an interim accounting packet is received before the expiration timestamp, the phantom record is upgraded to active status, and its expiration timestamp is upgraded according to the StaleSessionTimeoutSecs setting. If no Accounting-Start or interim accounting packet is received before the expiration timestamp, the phantom record is purged according to settings for stale session purge threads. This highlights the importance of synchronizing clocks amongst SBR Carrier servers in a Session State Register cluster.



NOTE: This parameter is applicable to standalone servers and servers running in a Session State Register cluster.

- **The ProxyPortCount parameter should be added to Table 23, radius.ini [Ports] Syntax, on page 44 of the *Steel-Belted Radius Carrier 7.2 Reference Guide*.** The ProxyPortCount parameter is used to configure SBR Carrier for load when Proxy's are being used. The setting of ProxyPortCount instructs SBR Carrier how many ports to use from within the number of possible ports defined within UDPProxyPortBlockLength starting with the port value set at UDPProxyPortBlockStart. (PR 455797)
- **A new parameter: EnableWIMAXUniqueSessionIdFromNAI is added to the [Configuration] section of the radius.ini file, which enables WIMAX performance and scalability enhancements.**
 - When EnableWIMAXUniqueSessionIdFromNAI=1 enhancements are enabled.
 - When EnableWIMAXUniqueSessionIdFromNAI=0 enhancements are disabled.

See Migration and New Installations of SBR Carrier with WIMAX on page 11 for a complete description of these enhancements. (PR 454398, PR 475897)
- **The [Status] report section of the radius.ini file should be documented.** To clear the Threads and Floods status report counters when [HUP] or [USR2] signals are sent,

set "UpdateThreadsAndFloods = 1" in the [HUP] and/or [USR2] sections of **update.ini** file. To set the status interval time, set "UpdateStatusPeriodAndInfo = 1". (PR 489756)

radsq1.aut File

- Support has been added for binary cleartext passwords by setting the **ClearTextBinary** attribute under the [Settings] section of the **radsq1.aut** file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide* to a non-zero value. (PR 249963)

radsq1jdbc.aut File

- A new parameter called **MaxHardErrorRetries** should be added to the [Settings] section of the **radsq1.aut** file. This parameter is added to resolve an issue where the database disconnected due to inactivity timeout. The **MaxHardErrorRetries** parameter enables the connection to be reestablished without failing the authentication by allowing you to set the number of additional attempts you want to make after hard errors have been encountered. Default is 0. This new parameter should be added to the *Steel-Belted Radius Carrier 7.2 Reference Guide*. (PR 410408)
- **QueryTimeout** is not supported in the jdbc plug-in. The setting is removed from **radsq1jdbc.aut**. (PR 410893)
- Binary passwords should not be cased to VARCHAR — Instead, they should remain as binary (VARBINARY). (PR 477643)

In addition, in the .aut file, the setting **ClearTextBinary** must be set to the length of the binary passwords in operation.

```
[Settings]
ClearTextBinary=16
```

realm.pro File

- The following note should be added to the [SpooledAccounting] Section of the **RealmName.pro** file described in Chapter 7, Realm Configuration Files, of the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 415927)



NOTE: Because Account Spooling guarantees sequential delivery of proxied accounting packets through a single-threaded mechanism, its use can adversely affect performance in systems that may sustain heavy load.

- The default value for the **Directory** parameter in the [SpooledAccounting] section of the **RealmName.pro** file should read "Default is ./Realm-Name." This needs to be corrected in Table 94, RealmName.pro [SpooledAccounting] Syntax, of the *Steel-Belted Radius Carrier 7.2 Reference Guide*. (PR 284582)

Replication of RADIUS Configuration Data

The information under the "Publishing Server Configuration Information" section of Chapter 16, Configuring Replication, in the *Steel-Belted Radius Carrier 7.2 Administration*

and Configuration Guide should be replaced with the following information: (PR 507496)

If you change the configuration of your primary server and want to push that data to your replicas, you must manually publish the modified configuration so that your replica servers can download the modified settings. The replication engine is not automated; it will always entail manual intervention to push the data to the replicas.

The following configurations are published to the replicas:

- Server information
- RADIUS client information
- User information
- Profile information
- Proxy target information
- EAP method configurations
- Filters
- RADIUS tunnel information
- Name parsing information
- Authentication method information
- Authentication realm information
- Rejection messages
- Javascript (.jsi) files

To publish the server configuration information:

1. Open the **Replication** panel.
2. Click the **Publish** button on the toolbar.

This creates a file called `/radius/packages/timestamp_RSA.ccmpkg` (Solaris/Linux) or `\Radius\Service\packages\timestamp_RSA.ccmpkg` (Windows), where `timestamp` reflects the date and time the package was created.

RFC 5281

- **The following RFC should be added to the table titled, “RFCs Related to Steel-Belted Radius Carrier” in the chapter, “About This Guide” in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*, *Steel-Belted Radius Carrier 7.2 Reference Guide*, and *Steel-Belted Radius Carrier 7.2 Installation Guide*:**

RFC 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), P. Funk, S. Blake-Wilson. August 2008.

Session State Register

- **For those customers with geodiversity use-cases or any form of multi-tiered LAN environment interconnecting the NDB nodes, JTAC has a patch to mysql to be able to better manage heartbeat topology - also known as the HeartBeatOrder.** This does not ship by default with Steel-Belted Radius Carrier Release 7.2.3 and requires some manual configuration of the `config.ini` associated with it. This can be applied with rolling restarts for most customers. [The filename is `mysql-cluster-com-6.3.34-br37718-solaris10-sparc-64bit.tar.gz`.]

There is a dependency for proper functioning of a certain proportionality between each OSI stack level's failure conditions, specifically between the NAS clients to the RADIUS front ends; the RADIUS S node to the D nodes; and among the ndb and dbapi nodes (M nodes to D nodes). That dependency has to do with timeout values associated within the network and the NDB itself.

RADIUS uses UDP as its transport. Network devices and OS stacks can be expected to drop UDP packets under load conditions, and it is up to the application-level retransmits to take effect. SBRC implements a packet cache to optimize responding to a retransmitted RADIUS request. So, it does not have to do the authentication and back-end work to process the request a second time. Although values may change in some use cases, normal RADIUS retransmit values are: three retries to the same SBRC front end with a 5-second delay between retries before attempting to transmit to another front end. For values widely divergent from that, check with your sales engineer or JTAC.

The network between the S nodes and the D nodes has several timeout dependencies as follows:

- If using IPMP, the IPMP probe value should be lower than two times the heartbeat timeout appropriate for the connection. (Defaults for the S or M nodes to the D nodes are controlled by the /opt/JNPRhadm/config.ini file on the M nodes; the value is set by HeartBeatIntervalDbApi and is 1500ms by default, and the inter-D node timeout is HeartBeatIntervalDbDb and is 200ms by default.) Widely divergent values may impact performance in the failure case, leading to unexpected outage.
- HeartBeats are implemented in and among the D nodes so that failures are more quickly detected than the underlying TCP failure mechanism can detect. The initial detection of fault happens after four times the HeartBeatInterval. After that is detected, the D nodes attempt to repartition and form a valid cluster. This operation can take several to many seconds, depending on the type and mode of failure: single D node hard failures or hard networking loss are generally quickest; complete cluster splits (which, under the correct network design, require two underlying faults to happen) and serious network faults (dropped connections and interfaces that are down are detectable more easily than intermittent or one-way failing connection scenarios) take longer to detect and compensate for.

Overall system load plays a part in fault recovery performance: many outstanding transactions take longer to roll back than few outstanding transactions.

- During an extended loss of service due to significant failure (such as loss of connectivity between two halves of a cluster), SBRC might need to reconnect to the new cluster to continue processing, and failures of reconnection are managed by timers set by the [Ndb] values DelayBetweenConnectRetriesSec and ReconnectRetriesin in the **dbclusterndb.gen** file. Setting these values higher than the defaults may make the system more resilient at the expense of a period of dropped RADIUS traffic. Setting TimeoutForFirstAliveSec and TimeoutAFterFirstALiveSec lower may also increase resiliency.
- During processing, some ndb operations are designed to be retried to attempt to avoid lock contention. Setting dbclusterndb.gen's [Database] section's Retries and

DelayBetweenRetriesMillisec higher may improve effective performance and decrease delays in a case where the underlying network is prone to latency or dropped packets.

- In cases where the underlying network is prone to short or long periods of latency, fault or other unexpected cases, setting the values of HeartBeatInterval higher (and setting all the proportionally related values appropriately) may make the system more resilient. The tradeoff is fast detection of serious failures (and after a failure spending extra time setting up connections again) against the acceptance of temporary processing delays due to minor fault that is otherwise survivable.
- There is a known error in ndb for serious cluster failure (requiring automatic restarts of a node) under extended one-way traffic failure of the inter-D and SM-D network. Correct network design should not permit this to happen: IPMP probes with the correct values, for instance, cause this to fail over to a working link. A ticket has been entered with Oracle and we are working closely with NDB engineers on addressing this problem; the HeartBeatOrder fix mentioned previously addresses temporary instances of this type of failure.
- There is a known bug in ndb for automatically restarting nodes. Certain, limited failure conditions (usually associated with serious, extended, and pathological network disfunctions, mentioned previously) at restart time may require a manual restart. A ticket has been entered with Oracle and we are working closely with NDB engineering on addressing this problem.

The default settings of CacheLowWaterMark, CacheHighWaterMark, and CacheChunkSize, which are set in the dbclusterndb.gen file under the [IpAddressPool] section, may cause badly degraded performance. The defaults cannot be made higher because one S node can pre-cache all the addresses in a small pool if the CacheLowWaterMark is set higher than the number of addresses in a pool. Default to a LowWaterMark and ChunkSize related to the transaction rate of new address allocations for your installation so you are not to likely run out of addresses before the threads can fill up cache, and use Per-Pool settings to set any small pools much lower than that default.

If performance is degraded, setting CacheThreadVerbose=1 and inspecting the logs for "Emergency" allocations indicates that the LowWaterMark and ChunkSize may be too low. Another indicator is low CPU utilization on the front ends and high CPU utilization on ndb. (PR 543334)

- **Clarification of terminology used in the *Steel-Belted Radius Carrier 7.2 Installation Guide* and the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*.** The following information serves as clarification on the use of various terms as they relate to the SSR feature in Release 7.2.

The term *SBR Cluster* should be replaced with the term *SSR cluster*. The term *SSR Cluster* refers only to the set of machines that host SSR processes.

In some cases, the terms *node* and *machine* have been used interchangeably. The term *node* refers to software processes that can be collocated on the same machine.

- Machines that host the RADIUS process are known as *SBRC nodes*.
- Machines that host the *SSR management process* are known as *SSR management nodes*.
- Machines that host the *SSR data process* are known as *SSR data nodes*.
- Machines that host both a *RADIUS process* and an *SSR management process* are known as *SBRC and SSR management nodes*.

Each machine in the front end and the SSR cluster is assigned a *node type* which indicates what processes it hosts: s (SBRC), sm (SBRC and management), m (management), d (data). Thus, the following terms may be used to describe machines that are members of either the front end or the SSR cluster: *s node*, *sm node*, *m node*, and *d node*.

The SBRC Temporary Cluster, also termed *the transition server*, and the SBRC Standalone Server, also termed *the standalone*, are exceptional nodes in the sense that they execute all processes on one machine. The transition server is assigned the node type= smdt and the standalone is assigned the node type=smdl. The transition server and standalone differ in the operational sense that on the transition server, the **CreateDB.sh** and configuration of pool(s) needs to be done manually just like in a cluster, where as in a standalone, **CreateDB.sh** is not required to be run, and the IP pools are configured via the SBRC Administrator.

Clarification is required as to the meaning of the term *SBRC Standalone Server* in Release 7.2 documentation versus the meaning associated with the Centralized Configuration Management (CCM) feature of the SBRC product as it is discussed in older documentation. The CCM feature of the SBRC product allows you to designate a RADIUS process as an *SBRC primary*, from which configuration is published to other RADIUS processes that are designated as *SBRC replicas*. Older documentation often refers to these as simply *primaries* and *replicas*. It should be made clear that SBRC replicas are unrelated to SSR cluster data replication and node groups; the latter are technical concepts involved in implementing the high availability feature of the SSR feature in Release 7.2.2. Thus, CCM-specific topics should always be qualified with *CCM*, for example, *CCM replica*, and SSR-specific topics should always be qualified with *SSR*, for example *SSR replication*. (PR 440583)

- **By default, accounting requests are acknowledged even if the session database cannot be contacted.** To cause accounting requests to be discarded when the session database cannot be contacted, as may be desirable when using load balancing equipment, modify **radius.ini** as follows: (PR 403793)

[Configuration] Section

DiscardAccountingRequestOnCstFailure = 1

- If set to 1, accounting requests (start, stop, on, off, and interim) are discarded when the session database cannot be contacted.
- If set to 0, accounting requests (start, stop, on, off, and interim) are acknowledged when the session database cannot be contacted.

Similarly, to cause the discard of authentication requests that contact the session database to assign resources (such as IP address assignment or concurrency), modify **radius.ini** as follows:

```
[Configuration] Section
DiscardAccessRequestOnCstFailure = 1
```

- If set to 1, authentication requests requiring access to the session database are discarded when the session database cannot be contacted.
- If set to 0, SBR Carrier sends an Access-Reject when the session database cannot be contacted.



NOTE: Operation is unaffected for requests not requiring session database access.

This information should be added to the **radius.ini** file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*.

- **The `./configure` script prompts you to enable or disable the autoboot option. If you disable it, you cannot start the SSR process on the node (`./sbrd start ssr`) from the `/etc/init.d/sbrd` directory.** If the autoboot option is disabled, you must start the SSR process from the `/opt/JNPR sbr/radius` directory. The `./configure` script prompts are described in the *Steel-Belted Radius Carrier 7.2 Installation Guide*. (PR 417927)

- **In the *Steel-Belted Radius Carrier 7.2 Installation Guide*, the description for the `CacheHighWater` parameter in the `dbclusterndb.gen` file should read as follows:**

`CacheHighWater` - Specifies the number of addresses that must be available in a server's IP address cache for an IP address pool before it stops adding addresses to the cache. The `CacheHighWater` value must be greater than or equal to the `CacheLowWater` value.

Default value is 250.

- **The *Steel-Belted Radius Carrier 7.2 Installation Guide* should be updated to reflect the following:** (PR 444456)

When executing `./sbrd clean ssr` you see the following prompts:

```
WARNING: Cleaning the SSR lock on this node may be destructive.
Do not use this function unless you are attempting to start the
entire cluster for the first time, or for recovery purposes.
Clean the SSR lock on this node? (y,n): y
Are you sure? (y,n): y Really? (y,n): y
Cleaning SSR lock
```

- **Chapter 3, "Planning Your Session State Register Cluster" of the *Steel-Belted Radius Carrier 7.2 Installation Guide* describes a "Best Practice" whereby host (machine) names, IP addresses, and so forth are determined as a function of the node IDs that are assigned to the SSR processes that will run on those machines.** The general scheme for node IDs currently documented in this Best Practice should be updated as follows: (PR 440803)

Guidelines for the assignment of node IDs:

- 0 is for internal use.
- 1–48 are for clustered data nodes (41–48 for standalone or transition servers).
- 49 is for SBRC nodes on standalone or transition servers.
- 50 is for management nodes on standalone or transition servers.
- 51–59 are for clustered management nodes.
- 60 is for management nodes on standalone or transition servers.
- 61–69 are for clustered management nodes (a function of base node ID + 10).
- 70–99 are reserved for future use.
- 100–149 are for clustered SBRC nodes.
- 150–255 are reserved for future use.
- 256 and higher are not supported and are illegal.



NOTE: If striping is enabled, you are restricted to the range 1–N for data node IDs where N is the total number of data nodes in the cluster. See [Striping Data Nodes \(PR 440803\)](#).

- **Striping Data Nodes (PR 440803)**

The *Steel-Belted Radius Carrier 7.2 Installation Guide* should be updated with the following information:

For performance reasons, the data stored in the Session State Register (SSR) should be striped. If you choose not to enable striping, the SBR Carrier software operates in demonstration mode without enforcing minimum memory requirements. When operating in *demonstration mode*, the SBR Carrier software makes a best effort attempt to operate in spite of various deficiencies that would normally prevent operation due to poor performance.

The choice of whether or not to stripe must be answered when the `./configure` script (typically found in `/opt/JNPR/sbr/radius/install`) is executed in order to create a new cluster definition. When you execute the `./configure` script, and select option 2, "Generate Cluster Definition", you are presented with the following prompts:

```
...
Enter number of management nodes to be paired with SBR nodes [2]: 2

Your license allows striping sun4v class hardware for performance.
However, striping requires at least 8GB memory on all data nodes.
The software will operate in demonstration mode with degraded
performance if you do not enable striping.  Enable striping? [y]: y

Creating cluster blue{0s,2sm,0m,2d}
will require 4 machines total.  Do you wish to continue? [y]: y
...
```

If the prompts related to striping are not answered correctly (for example, striping is enabled but one or more data nodes has less than 8GB memory, then you will not be able to configure all of the data nodes. In this case, when you execute the `./configure` script, and select option 3, "Configure Cluster Node", and then select the (c) Create option, you are prompted as follows:

```
...
Create (c) new or update (u) existing node configuration? [u]: c
...
WARNING: d nodes require at least 8 GB physical memory
         whereas this machine has only 4 GB installed.
ERROR: Insufficient hardware
HINT: You may wish to reconfigure for demonstration mode instead.
...
```

Similar prompts appear when configuring standalone SBR Carrier servers.

The number of stripes is presently a fixed parameter, always being set to either 1 (striping disabled for demonstration mode), 4 (striping enabled for cluster), or 8 (striping enabled for standalone server or transition server). After the number of stripes is configured, it cannot be changed without destroying and then re-creating the entire SBR Carrier cluster, or the standalone SBR Carrier server. Again, because striping is a global parameter with respect to cluster geometry, all data nodes must always have the same number of stripes.

Each stripe is implemented by a separate SSR data process requiring its own unique node ID. Thus eight node IDs are required for each data node in a standalone or transition server when striping is enabled. However, the `./configure` script only prompts for one base node ID per data node regardless of whether striping is enabled because higher order node IDs are determined by an algorithm related to the number of data nodes and the number of stripes. (The node IDs for standalone SBR Carrier servers are determined automatically and cannot be changed.) Also, the `./sbrd` script (typically found in `/opt/JNPR/sbr/radius`) operates upon all of the SSR data processes on a particular node as if they were one entity.

If any SSR data processes diverge from the group, the `./sbrd` script may detect this and warn you if you attempt to restart them. (You are not likely to encounter this unless you are having trouble starting the software in the first place.):

```
sbrd: WARNING: some ssr data processes failed, stop the survivors first
```

If you see this warning, use the `./sbrd status` command to verify whether or not any data processes have failed. If any data processes have failed while other data processes still persist, then execute `./sbrd stop ssr` followed by `./sbrd start ssr` and finally `./sbrd status` again to verify that the problem has been resolved.

When `./sbrd status` is executed as either root or hadm on a running management node (or SBRC/management node), or for a cluster that is striped, you should observe 4 times (because 4 is the number of stripes) as many `[nbd(NDB)]` nodes as there are actual data nodes. When `./sbrd status` is executed on a running data node, you should observe 2 times as many `nbd` processes (the SSR data processes) as stripes because each working `nbd` process is paired with a watchdog instance of itself to guard against failure.

SIM Authentication

- In the *Steel-Belted Radius Carrier 7.2 Reference Guide*, these parameters should be added under the [Settings] section of the `locspec.ctrl` file: (PR 433201)
 - OperatorNameAttribute = TeliaSonera-Operator-Name
 - VisitedOperatorIdAttribute = TeliaSonera-Visited-Operator-ID
 - LocationInformation = TeliaSonera-Location-Information
 - LocationNameAttribute = TeliaSonera-Location-Name
- On a multipathed SBRC server running SIM, the AuthGateway can fail to communicate with SBR Carrier. Because a single SCTP connection can have multiple addresses associated with each endpoint, the `sctp_addr_populate` call that translates the hostname into IP address actually results in multiple IP addresses — all of the local addresses that supported SCTP. A single TCP connection only has one address associated with each endpoint. The new `agw_addr_populate` call must translate the hostname into one IP address. (PR 392425)
- The following note should be added to the PseudonymSecret parameter in the [Settings] section of the `simauth.aut` file in the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 414526)



NOTE: If running the SIM authentication option in an SBR Carrier cluster, all pseudonym passwords should be the same throughout the cluster.

SMS Authentication

- In section “Password Format” in Chapter 18, *Configuring the SMS Authentication Module Files* in the *Steel-Belted Radius Carrier 7.2 Reference Guide*, the following line should be removed from the document: (PR (249510)

If the *language* is not specified, the default value is used. The default value is the value of `DefaultAccountProvisionRequestSeconds` in the `smsprov.aut` field.

Statlog.ini

- The `statlog.ini` file can now be updated on a HUP or USR2 signal by setting `UpdateStatLog=1`. The following is added to the `update.ini` file: (PR 401632)

Parameter: UpdateStatLog

Description:

- If set to 0, do not update settings in the `statlog.ini` file when a HUP or USR2 signal is received.
- If set to 1, update settings in the `statlog.ini` file when a HUP or USR2 signal is received.

Default value is 1 in the [HUP] section.

Default value is 0 in the [USR2] section.

This information should be added to the **update.ini** file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*.

ttlsauth.aut File

- In the *Steel-Belted Radius Carrier 7.2 Reference Guide*, the **[Integrity_Settings]** section, of the **ttlsauth.aut** file should be removed. Also, disregard this section in the “Sample ttlsauth.aut File” section of Chapter 8, EAP Configuration Files. (PR 433423)

Ulticom Documentation

- On page xxxvii, section “Third-Party Products,” the statement “Ulticom documentation can be obtained through the Juniper Networks Technical Assistance Center (JTAC) (See ‘Requesting Technical Support’ on page xxxviii for contact information.)” should be removed from the documentation. The following statement replaces this statement: (PR 483329)

For information about configuring your Ulticom software and hardware, or your access servers and firewalls, consult the manufacturer’s documentation.

Uninstalling Signalware 9

In the *Steel-Belted Radius Carrier 7.2 Installation Guide*, the procedure for uninstalling Signalware 9 should be added. (PR 541778)



NOTE: This procedure provides the basic steps to uninstall the software. Refer to the Signalware documentation for complete details.

To uninstall Signalware 9:

1. Start the Signalware uninstallation.
Execute:
swsetup
The script prompts you for a user identifier.
2. Enter the unique user that you created in the initial installation.
The Signalware Main Menu is displayed.
The script prompts you for a scheduling priority.
3. Press **Enter** to accept the default value 10.
The system checks for previous installations, a valid package file, and updates. Then it prompts for an ECN update.
4. Enter **N**.
The Main Menu is displayed.

To uninstall the required software packages:

1. From the Main Menu, enter **1** to select Signalware.
The Product Menu is displayed.
2. Enter **1** to select Signalware ... Develop/Deploy SS7 Services.
The Signalware Main Menu is displayed.
3. Enter **1** to select Install/Configure.
The Install/Configure menu is displayed.
4. Enter **4** to select **Replace Signalware (replace an existing installation with a new GA)**.
5. Press **Enter** to accept the default value.
The Uninstall Menu is displayed.
6. Enter **3 -override** to select **Delete old instance**.

wimax.ini

- The description of the [ASNGW-Requests/name] section in wimax.ini should state that this section only applies to the WiMAX VAAA configuration. (PR 428112)

WiMAX

- The following note should be added to the Configuring the Home Agent and DHCP Server Assignment section of Chapter 28: Configuring the WiMAX Mobility Module in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*: (PR 409198)



NOTE: For DHCP server keys to be generated, the DHCP server IP address needs to be returned as part of the ASNGW Access-Accept either through a profile or filter. We recommend using a filter so that based on the user@NAI, the appropriate DHCP server IP address is returned.

Leading Wildcards and Session Queries

- The *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide* incorrectly states that leading wildcards (*) may be used when performing session queries. These incorrect statements appear in Chapter 38, Using SBRC Administrator to Manage and Control Sessions, in the section, "Searching for Sessions Using SBRC Administrator", and in Chapter 39, Using the Command Line Utility to Manage and Control Sessions, in the section, "Action Arguments." These statements should be clarified as follows: (PR 416945)

Leading wildcards are supported only in a trailing position. For example, "*bcd" matches any value and "abc*def" matches any value beginning with "abc".

Resolved Issues

Release 7.2.3

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier Release 7.2.3. The identifier in parentheses is the Problem Report number in our bug database.

- **SBR Carrier may experience a core dump when the scscli.sh script is run if the OnFailure section of the deviceModels.xml file contains no data.** To prevent this problem, remove the entire section instead. (PR 414255)
- **If no CoA/DM license is present, the message "License check failed: ControlledDeviceMgr is disabled" appears for every client at startup.** This message is normal and does not indicate any loss of functionality. (PR 395033)
- **The LogSessionId parameter in the [Logging] section of the radius.ini file does not function for non-WiMAX accounting requests.** (PR 447446)

- **There was a potential memory leak when adding response attributes to a TTLS transaction by inbound filter or JavaScript.** (PR 544254)
- **Failover between servers in a single LDAP authentication plug-in file could take too long.** (PR 413585)
- **SSR Cluster: several issues related to reconnecting to a cluster due to network errors or cluster failure are fixed.** (PR 426500)
 - `./sbrd hup` when SBRC fails to connect to the data nodes, no longer causes a core.
 - Fixed a cached IP address leak due to addresses that could not be written as 'InUse' due to database failure/disconnect.
 - SBRC supports a new reconnection mechanism, enabled by default, that can be disabled in the [Database] section of the `dbclusterndb.gen` file, with the value `UseConnectionManager=<bool>`. It should always be set to true unless a change is recommended by Juniper Networks Technical Support. This might have a minor performance impact on throughput, bandwidth-bound installations - contact your sales engineer or Juniper Networks Technical Support for more information.
- **The Authentication rejection log (configured with the `authReport.ini` file) did not report locked-out as a reject reason.** (PR 427381)
- **MaxSize parameter was missing from the [Logging] section of the default `radius.ini` file.** (PR 430802)
- **Log messages were not properly generated even though `LogAccept=1` in the [Logging] section of the `radius.ini` file.** (PR 439746)
- **Local time was always reflected in the main SBRC accounting log, even though "UTC = 1" in the `account.ini` file. UTC time was always reflected in the directed accounting log, even though "UTC = 0" in the `account.ini` file.** (PR 451348)
- **International characters as a password for Native Users did not work.** (PR 461739)
- **Native user password validation did not work when special characters were used.** (PR 462000)
- **Occasionally, errors could occur when replacing attributes by using a JavaScript.** (PR 467251)
- **SBRC fails to start after a crash when a significant number of pool addresses were cached.** (PR 475100)
- **Symbol collisions with Oracle libraries could result in a SBRC crash when using LDAP authentication. This applies only when using versions of the radius binaries linked with Oracle libraries (`radius_ora9` or `radius_ora10`).** (PR 475102)
- **SBRC does not support HUPs when SBRC is started under CRON.** (PR 475538)
- **LDAP authentication with JavaScript and EAP-TLS helper will reject all attempts.** (PR 476463)
- **When `LogfileMaxMBytes` is set, the first log of the day does not have `_hhmm` (now has `xxxxx`).** (PR 478308)
- **In release 7.2, some SNMP OIDs fail on walks.** (PR 478756)

- **TimeTra.dct file has multiple attributes with same name and different parameters.** The following dictionary entries have been changed to avoid duplication issues: (PR 480549)
 - In Timetra.dct, changed
 - < ATTRIBUTE Timetra-Profile Timetra-Attr(6, string) R
 - to
 - > ATTRIBUTE Timetra-Command Timetra-Attr(6, string) R
 - In hiperarc.dct, marc.dct, and netservr.dct, changed
 - < ATTRIBUTE Prompt 64 integer
 - to
 - > ATTRIBUTE 3COM-Prompt 64 integer
 - In hiperarc.dct and marc.dct, deleted
 - < ATTRIBUTE MP-EDO USR-VSA(0x9841, integer) c
 - In totlctrl.dct, changed
 - < ATTRIBUTE TC-Compression-Type USR-VSA(0x00C7, integer)
 - < VALUE TC-Compression-Type none 1
 - < VALUE TC-Compression-Type ccittV42bis 2
 - < VALUE TC-Compression-Type mnpLevel5 3
 - < VALUE TC-Compression-Type v44 4
 - to
 - ATTRIBUTE TC-Modem-Compression-Type USR-VSA(0x00C7, integer)
 - > VALUE TC-Modem-Compression-Type none 1
 - VALUE TC-Modem-Compression-Type ccittV42bis 2
 - VALUE TC-Modem-Compression-Type mnpLevel5 3
 - VALUE TC-Modem-Compression-Type v44 4
 - In shiva.dct, changed
 - < ATTRIBUTE Shiva-User-Attributes 51 string r
 - to
 - > ATTRIBUTE Shiva-User-Attributes-Non-Conforming 51 string r
- **Attributes whose name contained a '/' could not be added to a plug-in enumeration filter.** (PR 485981)
- **An "out of space in buffer" error occurs when certain return list attributes are set.** (PR 487941)
- **When debugging logging is enabled and an EAP authentication is routed through a plugin, for example, ldapauth, SBRC cores.** (PR 487978)
- **In some cases, responses to Authenticate-Only requests may have included unnecessary attributes.** (PR 488086)
- **SBR Carrier startup fails with DCF errors about "conversion to BSTR not implemented".** (PR 488429)

- **XML import of earlier version's configuration adds check to check box for 'range' when original check box was empty. This causes an error in the logs because CoA/DM clients cannot use a range.** (PR 489012)
- **Concurrency limits not enforced (introduced in 7.2.1).** (PR 491943)
- **There was an apparent delay in RADIUS request processing due to large granularity in millisecond logging.** (PR 494710)
- **SBRC does not rollover logs after HUP signal.** (PR 495288)
- **For performance reasons, the SSR ndbd processes on DATA nodes are now configured to execute under the UNIX root account by default, as opposed to the UNIX hadm account.** In particular this allows the ndbd processes to lock data in physical memory (faster) as opposed to allowing the OS to use swap space on disk (slower). UNIX root account privilege is required in order to lock data in physical memory.

The relevant configuration item is `/opt/JNPRhadm/my.cnf` section `"[nbd]"` parameter `"#sbrd-nbd-run-as-root = true"`. Note that the leading `"#"` character is required to distinguish this parameter as an sbrd script parameter, this parameter is NOT a comment and is always active. When the value of this parameter is true, the ndbd processes will execute under the UNIX root account. When the value of this parameter is false (or if the parameter is missing entirely), the ndbd processes will execute under the UNIX hadm account. The value of this parameter may only be changed immediately after configuring a DATA node; that is, it cannot be changed after SSR processes have been executed. We recommend, although it is not necessary, that the parameter be configured the same on all DATA nodes. In order to change the value of this parameter at a later time, you must unconfigure the DATA node and then reconfigure it again.

When ndbd processes are executed under the UNIX root account, it is extremely important that the `/opt/JNPRhadm/config.ini` section `"[nbd default]"` parameters `"DataMemory = ..."` and `"IndexMemory = ..."` be configured properly with respect to the amount of physical memory that is actually available on the DATA node. If the DATA node does not have enough physical memory available, then it is possible for the ndbd processes to starve the entire machine, including the OS itself, for memory. By default, the software is configured under the assumption that at least 8GB is available SOLELY for ndbd processes. In practice more than 8GB is required to support the OS and other applications. (PR 495661)

- **In SBRC 7.2 release, there is a very large drop in RADIUS TPS processing when Debug logs are enabled.** (PR 497771)
- **Complex structured attributes may cause JavaScripts to fail.** (PR 500124)
- **SNMP queries could result in memory leaks.** (PR 502731)
- **JavaScripts could not return request attribute values.** (PR 504976)
- **On shutdown, SBRC 7.2 clears the LARGE pool cache before closing network connections.** (PR 506256)
- **SBRC Carrier does not acknowledge accounting requests for WiMAX when the session does not exist in the current sessions table (CST).** To work around this problem, the `AckOnCookieFailure` parameter has been added to the `radius.ini` file. When this

parameter is set to yes, SBR Carrier sends an acknowledgement back for every accounting request it receives. (PR 514667)

- **Placing node into management mode with load on a SBRC causes it to hang/core dump.** (PR 515140)
- **Stopping SSR and hupping causes packets to be rejected.** If a HUP is sent to SBR Carrier when the database cluster is disconnected or down, the IP pool initialization code will not be able to determine the names of the pools configured in the SSR. This may result in authentication requests getting rejected. Sending a HUP to SBR Carrier when the database cluster is operational and connected will return SBR Carrier to normal operation. A new setting has been added to the [database] section of **dbclusterndb.gen**: `ReconnectOnHUP=<0|1>` (0=false, 1=true); default=0. ReconnectOnHUP controls whether the database cluster will be disconnected and reconnected after a HUP signal is sent to the dbcluster plugin. (PR 517838)
- **Non SBRC state attributes containing a ':' would be truncated.** (PR 519938)
- **Using an inbound proxy filter to add an orderable multi-value attribute could result in a SBRC crash.** (PR 520430)
- **SBRC responds with an LDAP RESULTCODE of success for LCI queries against the CST fields if the CST is down.** (PR 522999)
- **Writing an attribute value which contains "%" to the authlog could cause a SBRC crash.** (PR 526544)
- **Update of WiMAX configuration by a HUP could cause a SBRC crash.** (PR 527031)
- **The libumem script does not work for SBRC 7.2 standalone.** (PR 531321)



CAUTION: Must only be installed on standalone or SBR Carrier nodes.

Installation: Solaris

To install the libumem script:

1. Stop the SBRC software, for example, `/etc/init.d/sbrd stop`.
2. Copy the following files from the HOTFIX directory into the install subdirectory of the SBRC installation directory: typically `/opt/JNPRsbr/radius/install`:
radius.template
3. Switch to the `/opt/JNPRsbr/radius/install` directory and execute the configure script. Answer the SBRC specific prompts the same way as when you previously executed the configure script. This step will update the sbrd scripts.
4. Switch to the `/opt/JNPRsbr/radius` directory and edit the sbrd.conf file. Insert the following line immediately after the line that specifies
`RADIUS_PRIVATE_DIR="$RADIUSDIR":#RADIUS_LD_PRELOAD="/usr/lib/libumem.so"`
5. Perform any additional configuration as described in notes that follow Step 6.
6. Restart the SBRC software, e.g. `/etc/init.d/sbrd start`



NOTE: Perform the following configuration on SBRC nodes only (node types s, sm, transition server, and stand-alone). Note that the SBRC software must be stopped and restarted for this configuration to take effect:

1. Use "man -s 3MALLOC umem_debug" to review online Solaris documentation that describes the ENVIRONMENT VARIABLES that may be configured when libumem is enabled, for example, UMEM_DEBUG and UMEM_LOGGING.
2. When you want to enable libumem, edit the sbrd.conf file to uncomment the RADIUS_LD_PRELOAD line and insert any related UMEM lines as needed, immediately below, to specify the desired libumem behavior, for example:
`RADIUS_LD_PRELOAD="/usr/lib/libumem.so" UMEM_DEBUG=default; export UMEM_DEBUG UMEM_LOGGING=transaction; export UMEM_LOGGING`
3. When you want to disable libumem, edit the sbrd.conf file to comment out the RADIUS_LD_PRELOAD line and any related UMEM lines.

- **SBR Carrier does not have an option to use WiMAX-MSK.** To add the WiMAX-MSK to the Access-Accept, set Add-Keys-To-Access-Accept = 1 in the [Setting] of the `wimax.ini` file. The default value is 0. (PR 534364)
- **Data from earlier transaction recorded in new authlog entry.** For multi-round challenge authentications, SBRC stores state information in a cache indexed by a challenge session index which is returned in the State attribute in an Access-Challenge. To avoid false matches when a server incorrectly responds to a different SBRC server, this session id is now prefaced by the server id. (PR 534375)
- **Juniper.dct dictionary has been updated.** (PR 535285)
- **LogDir does not work in all the log.ini files.** (PR 537054)
- **Use of a challenge method, for example, EAP-TTLS within a directed realm could result in a memory leak.** (PR 541608)

Release 7.2.2

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier Release 7.2.2. The identifier in parentheses is the Problem Report number in our bug database.

- **SBR Carrier intermittently loses its server certificate while processing a HUP.** (PR 490588)
- **When Java scripting is used and the number of SBRC worker threads is set to a high value, authentication failures may occur due to the inability to allocate Java script hosts.** A new setting has been added `radius.ini` to limit the number of Java script host allocations that can be attempted. When set, worker threads will wait for a host to become available. (PR 483631)

```
[Configuration]
MaxEngines = n (default is 0, no limit)
```

- **While publishing to replica servers, replication of filters could be delayed, possibly causing authentication rejects.** (PR 488855)
- **Oracle plug-ins would not load in release 7.2.1.** (PR 483946)
- **When NoNullTermination was configured, use of echo reply attributes could cause SBRC to crash.** (PR 480450)
- **Certain combinations of proxy and thread configurations could cause SBRC to crash.** (PR 465067)
- **In Release 7.2.1, multivalue attributes in an inbound proxy filter could be lost.** (PR 482664)
- **In Release 7.2.1, SBR Carrier could crash during a failover if an accounting request was received from an unrecognized server (that is, not listed in spi.ini).** (PR 480825)
- **If LeaseTime is less than MinLeaseTime as specified in the pool.dhc file, the DISCOVER message in PostResponse fails when it receives back a LeaseTime less than the minimum and only logs "DHCP Requester: No response to DISCOVER."** This problem has been fixed. (PR 298954)
- **SBR Carrier crashes when User-Name is excluded by outbound-directed realm filter.** (PR 454767)
- **Setting clientaddr in the jnprsnmp.conf file creates an error.** (PR 477155)
- **SSR configure script does not ask you to configure the spi.ini file.** This problem is fixed. See "Using the SSR Configuration Script" on page 10 for more information on this fix. (PR 481510)
- **The QueryTimeout parameter is not supported in the jdbc plug-in.** The parameter is removed from the radsqljdbc.aut file. (PR 410893)
- **Attributes are not returned when an LDAP search by user (radiusstatus=sessions_by_user) is performed.** (PR 419631)
- **SBR Carrier loses its connection to the database cluster if the cluster restarts for any reason.** If there is an outage of the cluster, or it is restarted, each SBRC node must be restarted in order to reestablish its connection to the cluster. This problem is resolved. (PR 443694)

Release 7.2.1

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier Release 7.2.1. The identifier in parentheses is the Problem Report number in our bug database.

- **Once an IP range is specified for a RADIUS client, further modifications are not replicated.** (PR 391225)
- **The GuardStdioDescriptors setting has been removed from .aut files.** This feature is obsolete and should no longer be used. (PR 405191)
- **Plug-ins can not add attributes that are not flagged as reply-list attributes to an Access-Accept.** A new setting has been added to the [Configuration] section of

- radius.ini.** Set EnumAttrsWithoutMvpFlagUpdate = 1 to enable this behavior. (PR 427380)
- **Checklist attributes are ignored if they already exist in response attributes.** (PR 432489)
- **The WiMAX-AAA-Session-ID attribute is attached by VAAA to the first proxied response, even if that response is an Access-Challenge.** (PR 435248)
- **Framed-IP-Addresses from IP pools assigned by a filter in a directed realm are not released by matching Accounting-Stop messages.** (PR 435787)
- **In certain situations, under extreme conditions, SBR Carrier could crash under load if auth logging is enabled.** (PR 448584)
- **SBR Carrier only returns one attribute from a proxy response if the attribute is flagged as orderable.** (PR 448812)
- **MaxHardErrorRetries in radsqldb.aut did not function properly when MySQL Server timed out the connection to SBR Carrier.** (PR 449442)
- **The Acct-Delay-Attribute was not sent to a downstream target when spooling was in use.** (PR 449691)
- **The MaxConcurrent setting has been removed from radsqldb.acc. This setting is no longer supported.** (PR 450763)
- **There was an extra set of double quotes surrounding quoted fields in auth logs.** (PR 451699)
- **WiMAX-AAA-Session-ID attributes were added to Access-Reject responses.** (PR 452057)
- **In certain situations under rare conditions SBR Carrier had the potential to crash when thread limits were reached.** (PR 452679)
- **Unnecessary index scan log messages have been removed when logging in Debug (LogLevel = 2) mode.** (PR 453537)
- **WiMAX performance has been improved.** See Migration and New Installations of SBR Carrier with WiMAX on page 11 for complete details. (PR 454398)
- **In certain situations, under rare conditions, SBR Carrier could crash when specific, unusual native user records were accessed by the SBRC Administrator.** (PR 454405)
- **Adding attributes using a filter could result in duplicate, instead of different, attributes being added.** (PR 455150)
- **Events that would result in SNMP traps would cause a memory leak if the SBR Carrier SNMP Agent was not running.** This memory leak could occur when SNMP was not configured. (PR 456087)
- **Various functional issues in the SSR have been corrected and improved.** This fix requires an upgrade of the SSR cluster. (PR 459093, PR 476418)
- **Log messages were occasionally written to incorrect log files.** (PR 461080)
- **Profiles were not retrieved when assigned by using JavaScript when EAP-TTLS or EAP-PEAP was used with EAP-MSCHAP-v2.** (PR 462016)

- **CCM replication would report an error if SSR cluster licenses were not unique.** (PR 462575)
- **The LADP Configuration Interface (LCI) did not display the entire contents of customized Current Session Tables (CSTs).** Now, all fields added by CST customization are enumerated to LDAP without any processing or conversion; string fields are presented as strings whereas all others are presented as binary data. (PR 464229)
- **The LCI did not display the full subtree scope of sessions records and could not search into subtrees.** (PR 465806)
- **LCI queries failed when returning more than 1300 entries.** (PR 466292)
- **In certain situations, under rare conditions, SBR Carrier could crash when importing large XML files with specific, unusual contents.** (PR 467152)
- **The LDAP authentication method now uses LDAPv3 by default when connecting to LDAP back-end databases.** (PR 467377)
- **SBRC Administrator erroneously reported IP range overlap errors.** (PR 467418)
- **The value for the Funk-Radius-Client-Group checklist attribute was not added to challenge responses.** (PR 467436)
- **The configuration script could hang when IPMP was used.** (PR 468649)
- **WiMAX phantom sessions were not deleted when an Accounting-Stop was received instead of an Accounting-Start.** (PR 470919)
- **SBR Carrier returned only one of the attributes from a directed realm response if the attribute was flagged as orderable.** (PR 472449)
- **Use of the scscli script had the potential to cause a memory leak.** (PR 472494)
- **Under rare conditions, an incomplete subattribute fragment could potentially cause SBR Carrier to crash.** (PR 473211)
- **Excessive log messages about AuthReqPools have been removed.** (PR 474779)
- **One memory leak and general stability issues were addressed by switching to a later Juniper Networks internal SDK.** (PR 476393)

Release 7.2.0

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier Release 7.2.0. The identifier in parentheses is the Problem Report number in our bug database.

- **User names with special characters such as (') may cause problems when using LDAP authentication.** (PR 409675)
- **SBRC rejects Authentication request if no User-Name attribute is present in the Access Request.** To allow Access-Requests with no User-Name attribute, set AllowNoUserName = Yes in the [Configuration] section of **radius.ini**. (PR 390984)
- **SBRC will not install if a machine has 8 GB of RAM which is the minimum requirement.** (PR 443318)

- Careful configuration may be required to achieve maximum performance from SBR Carrier with LDAP authentication in order to divide SBR Carrier LDAP processing among the SBR Carrier server cores. (PR 438956, PR 439436)
- Stored procedures may prevent correct server initialization. (PR 256084)
- The LDAP to SQL Bridge feature is no longer supported. (PR 407753)

Related Documentation

Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFC)s online at <http://www.ietf.org/rfc.html>. Table 6 on page 44 lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 6: RFCs Related to Steel-Belted Radius Carrier

RFC Number	Title
RFC 1035	<i>Domain Names - Implementation and Specification</i> . P. Mockapetris. November 1987.
RFC 1155	<i>Structure and Identification of Management Information for TCP/IP-based Internets</i> . M. Rose, K. McCloghrie, May 1990.
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II</i> . K. McCloghrie, M. Rose, March 1991.
RFC 2006	<i>The Definitions of Managed Objects for IP Mobility Support using SMIPv2</i> . D. Cong and others. October 1996.
RFC 2246	<i>The TLS Protocol</i> . T. Dierks, C. Allen. January 1999.
RFC 2271	<i>An Architecture for Describing SNMP Management Frameworks</i> . D. Harrington, R. Presuhn, B. Wijnen, January 1998.
RFC 2284	<i>PPP Extensible Authentication Protocol (EAP)</i> . L. Blunk, J. Vollbrecht, March 1998.
RFC 2433	<i>Microsoft PPP CHAP Extensions</i> . G. Zorn, S. Cobb, October 1998.
RFC 2548	<i>Microsoft Vendor-specific RADIUS Attributes</i> . G. Zorn. March 1999.
RFC 2607	<i>Proxy Chaining and Policy Implementation in Roaming</i> . B. Aboba, J. Vollbrecht, June 1999.
RFC 2618	<i>RADIUS Authentication Client MIB</i> . B. Aboba, G. Zorn. June 1999.
RFC 2619	<i>RADIUS Authentication Server MIB</i> . G. Zorn, B. Aboba. June 1999.
RFC 2620	<i>RADIUS Accounting Client MIB</i> . B. Aboba, G. Zorn. June 1999.
RFC 2621	<i>RADIUS Accounting Server MIB</i> . G. Zorn, B. Aboba. June 1999.

Table 6: RFCs Related to Steel-Belted Radius Carrier (*continued*)

RFC Number	Title
RFC 2622	<i>PPP EAP TLS Authentication Protocol</i> . B. Aboba, D. Simon, October 1999.
RFC 2809	<i>Implementation of L2TP Compulsory Tunneling via RADIUS</i> . B. Aboba, G. Zorn. April 2000.
RFC 2865	<i>Remote Authentication Dial In User Service (RADIUS)</i> . C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
RFC 2866	<i>RADIUS Accounting</i> . C. Rigney. June 2000.
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support</i> . G. Zorn, B. Aboba, D. Mitton. June 2000.
RFC 2868	<i>RADIUS Attributes for Tunnel Protocol Support</i> . G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. June 2000.
RFC 2869	<i>RADIUS Extensions</i> . C. Rigney, W. Willats, P. Calhoun. June 2000.
RFC 2882	<i>Network Access Servers Requirements: Extended RADIUS Practices</i> . D. Mitton. July 2000.
RFC 3046	<i>DHCP Relay Agent Information Option</i> . M. Patrick. January 2001.
RFC 3118	<i>Authentication for DHCP Messages</i> . R.Droms and others. June 2001.
RFC 3162	<i>RADIUS and IPv6</i> . B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3344	<i>IP Mobility Support for IPv4</i> . C. Perkins. August 2002.
RFC 3539	<i>Authentication, Authorization, and Accounting (AAA) Transport Profile</i> . B. Aboba, J. Wood. June 2003.
RFC 3575	<i>IANA Considerations for RADIUS (Remote Authentication Dial-In User Service)</i> . B. Aboba, July 2003.
RFC 3576	<i>RFC3576 - Dynamic Authorization Extensions to Remote to Remote Authentication Dial In User Service</i> . Network Working Group, 2003
RFC 3579	<i>RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)</i> . B. Aboba, P. Calhoun, September 2003.
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i> . P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.
RFC 3748	<i>Extensible Authentication Protocol</i> . B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz. June 2004.
RFC 3957	<i>Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4</i> . C. Perkins and P. Calhoun. March 2005.

Table 6: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
RFC 4017	<i>Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs.</i> D. Stanley and others. March 2005.
RFC 4186	<i>Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).</i> H. Haverinen, J. Salowey. January 2006.
RFC 4187	<i>Extensible Authentication Protocol Method for Global System for 3rd Generation Authentication and Key Agreement (EAP-AKA).</i> J. Arkko, H. Haverinen. January 2006.
RFC 4282	<i>The Network Access Identifier.</i> B. Aboba and others. December 2005.
RFC 4284	<i>Identity Selection Hints for the Extensible Authentication Protocol (EAP).</i> F. Adrangi, V. Lortz, F. Bari, P. Eronen. January 2006.
RFC 4372	<i>Chargeable User Identity.</i> F. Adrangi and others. January 2006.
RFC 4510	<i>Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map.</i> K. Zeilenga, June 2006.
RFC 5281	<i>Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TLSv0)</i> P. Funk, S. Blake-Wilson. August 2008.

3GPP and 3GPP2 Technical Specifications

The 3rd Generation Partnership Project (3GPP) and (3GPP2) maintains an online repository of Technical Specifications and Technical Reports online at <http://www.3gpp.org> and <http://www.3gpp2.org>, respectively.

WiMAX Technical Specifications

The WiMAX Forum Networking Group (NWG) maintains a repository of technical documents and specifications online at <http://www.wimaxforum.org>. You can also view the WiMAX IEEE standards, 802.16e-2005 for mobile WiMAX and 802.16-2004 for fixed WiMAX, online at <http://www.ieee.org>.

Third-Party Products

For information about configuring your Ulticom software and hardware, or your access servers and firewalls, consult the manufacturer's documentation.

General Statement of Compliance

Table 7 on page 47 lists Steel-Belted Radius Carrier 7.2.x compliance with applicable RFCs.

Table 7: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs

RFC Number	Name	Notes
1155	Structure and Identification of Management Information for TCP/IP-based Internets	—
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	—
2058	Remote Authentication Dial In User Service	Obsoleted by RFC 2138
2059	RADIUS Accounting	Obsoleted by RFC 2139
2107	Ascend Tunnel Management Protocol	—
2138	Remote Authentication Dial In User Service	Obsoleted by RFC 2865
2139	RADIUS Accounting	Obsoleted by RFC 2866
2271	An Architecture for Describing SNMP Management Frameworks	Obsoleted by RFC 2271
2284	PPP Extensible Authentication Protocol (EAP)	Updated by RFC 2484
2433	Microsoft PPP CHAP Extensions	—
2548	Microsoft Vendor-specific RADIUS Attributes	—
2607	Proxy Chaining and Policy Implementation in Roaming	—
2618	RADIUS Authentication Client MIB	Obsoleted by RFC 4668
2619	RADIUS Authentication Server MIB	Obsoleted by RFC 4669
2620	RADIUS Accounting Client MIB	Obsoleted by RFC 4670
2621	RADIUS Accounting Server MIB	Obsoleted by RFC 4671
2716	PPP EAP TLS Authentication Protocol	Obsoleted by RFC 5216
2809	Implementation of L2TP Compulsory Tunneling via RADIUS	—
2865	Remote Authentication Dial In User Service (RADIUS).	—
2866	RADIUS Accounting	—
2867	RADIUS Accounting Modifications for Tunnel Protocol Support	—
2868	RADIUS Attributes for Tunnel Protocol Support	—

Table 7: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
2869	RADIUS Extensions	—
2882	Network Access Servers Requirements: Extended RADIUS Practices	—
2903	Generic AAA Architecture	—
2904	AAA Authorization Framework	—
2905	AAA Authorization Requirements	—
2906	AAA Authorization Requirements	—
2977	Mobile IP Authentication, Authorization, and Accounting Requirements	—
2989	Criteria for Evaluating AAA Protocols for Network Access	—
3012	Mobile IPv4 Challenge/Response Extensions	—
3162	RADIUS and IPv6	—
3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	—
3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	—
3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	—
3748	Extensible Authentication Protocol (EAP)	—
3770	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks	—
4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	—
4017	Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs	—
4072	Diameter Extensible Authentication Protocol (EAP) Application	Not supported
4137	State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator	—

Table 7: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)	—
4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	—
4284	Identity Selection Hints for the Extensible Authentication Protocol (EAP)	—
4334	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	—
4372	Chargeable User Identity	—
4590	RADIUS Extension for Digest Authentication	Obsoleted by RFC 5090
4603	Additional Values for the NAS-Port-Type Attribute	—
4668	RADIUS Authentication Client MIB for IPv6	Previous version (RFC 2618) supported
4669	RADIUS Authentication Server MIB for IPv6	Previous version (RFC 2619) supported
4670	RADIUS Accounting Client MIB for IPv6	Previous version (RFC 2220) supported
4671	RADIUS Accounting Server MIB for IPv6	Previous version (RFC 2221) supported
4672	RADIUS Dynamic Authorization Client MIB	Not supported
4673	RADIUS Dynamic Authorization Server MIB	Not supported
4675	RADIUS Attributes for Virtual LAN and Priority Support	Not supported
4679	DSL Forum Vendor-Specific RADIUS Attributes.	Not supported
4746	Extensible Authentication Protocol (EAP) Password Authenticated Exchange	Not supported
4763	Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)	Not supported
4764	The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method.	Not supported
4793	The EAP Protected One-Time Password Protocol (EAP-POTP)	EAP-32

Table 7: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
4818	RADIUS Delegated-IPv6-Prefix Attribute.	—
4849	RADIUS Filter Rule Attribute	—
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	Not supported
4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management	—
5030	Mobile IPv4 RADIUS Requirements	—
5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes	—
5090	RADIUS Extension for Digest Authentication	—
5106	The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method	—
5169	Handover Key Management and Re-Authentication Problem Statement	—
5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	—
5216	The EAP-TLS Authentication Protocol	Previous version (RFC 2716) supported
—	3GPP2 X.S0011-D, Version: 1.0, Version Date: February, 2006	MIPv6 not supported
5281	Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TLSv0) P. Funk, S. Blake-Wilson. August 2008.	—

Table 8 on page 50 lists the protocols supported in Steel-Belted Radius Carrier 7.2.x.

Table 8: Protocols Supported in SBR Carrier 7.2.x

Protocol	Notes
UDP	—
IPv4	—
IPv6	NAS-server only
DHCP v2	—

Table 8: Protocols Supported in SBR Carrier 7.2.x (*continued*)

Protocol	Notes
DHCP v3	—
LDAP v2	—
LDAP v3	Not LCI
JDBC	—
Oracle (SQL)	—
XML	Configuration
HTTP v1.1	Admin
LEAP	—
WiMAX NWG 1.2.2	<i>Except CRs 801, 823, OMA/DM</i>
3GPP2	—
3GPP2 X.S0011-D	—
3GPP	RADIUS only
23.234 (RADIUS)	WLAN UE
29.061 (RADIUS)	G1 and Pk reference points
TISPAN	RADIUS only Interface E5
ES282.001	—
ES282.004	—
ES283.034	—
ES283.035	—

SBR Carrier Documentation and Release Notes

For a list of related SBR Carrier documentation, see <http://www.juniper.net/support/products/carrier/carrier/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Steel-Belted Radius Carrier Release Notes*.

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at <http://www.juniper.net/techpubs/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- **JTAC Policies**—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/customers/support/downloads/710059.pdf>
- **Product Warranties**—For product warranty information, visit <http://www.juniper.net/support/warranty/>
- **JTAC Hours of Operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings:
<http://www.juniper.net/customers/support/>
- Search for known bugs:
<http://www2.juniper.net/kb>
- Find product documentation:
<http://www.juniper.net/techpubs/>

- Find solutions and answer questions using our Knowledge Base:
<http://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager:
<http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

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

- Use the Case Manager tool in the CSC at <http://www.juniper.net/cm/>
- Call 1-888-314-JTAC (1-888-314-5822 – toll free in the USA, Canada, and Mexico)

For international or direct-dial options in countries without toll-free numbers, visit <http://www.juniper.net/support/requesting-support.html>

When you are running SBRC Administrator, you can choose **Web > Steel-Belted Radius Carrier User Page** to access a special home page for Steel-Belted Radius Carrier users.

When you contact technical support, be ready to provide:

- Your Steel-Belted Radius Carrier release number (for example, Steel-Belted Radius Carrier Release 7.x).
- 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.
- A detailed description of the problem.
- Any documentation that may help in resolving the problem, such as error messages, core files, compiler listings, and error or RADIUS log files.

Revision History

August 2010—FRS SBR Carrier Release 7.2.3

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.