

# Steel-Belted Radius<sup>®</sup> Carrier Release Notes

Release 8.6.0R17  
November 2022  
Revision 1

This Release Notes support Release 8.6.0R17 of Steel-Belted Radius Carrier (SBRC). Before you install or use your new software, read these Release Notes in their entirety, especially [“Known Limitations” on page 13](#).

<b>Contents</b>	<b>Release Overview   4</b>
	Before You Start   4
	Documentation   4
	<b>Release Highlights   5</b>
	Support for Red Hat Enterprise Linux Versions   5
	Support for Solaris Versions   5
	MySQL and NDB Upgrade   6
	Security Updates   6
	<b>System Requirements   7</b>
	Software   7
	Perl   8
	LDAP Plug-in   8
	Tested Browsers   9
	External Database Requirements   10
	Signalware and SIM Requirements   10
	<b>Modified Open-Source Software   11</b>
	<b>Migrating from Earlier SBR Carrier Standalone Server Products   12</b>
	<b>Known Limitations   13</b>
	LDAP Authentication   14
	SBRC Core   14
	Logging   14

3GPP AAA Module | 14

Documentation Updates | 15

Resolved Issues, Features, and Limitations (Patch-Wise) | 15

Notations Used to Indicate resolved PRs | 15

PRs fixed in patch R17 | 15

PRs fixed in patch R16 | 16

PRs fixed in patch R15 | 16

PRs fixed in patch R14 | 17

PRs fixed in patch R13 | 17

PRs fixed in patch R12 | 18

PRs fixed in patch R11 | 18

PRs fixed in patch R10 | 18

PRs fixed in patch R9 | 18

PRs fixed in patch R8 | 18

PRs fixed in patch R7 | 19

PRs fixed in patch R6 | 19

PRs fixed in patch R5 | 20

PRs fixed in patch R4 | 20

PRs fixed in patch R3 | 20

PRs fixed in patch R2 | 21

Features and Limitations — Release wise (Notes) | 21

Starting from SBR 8.6.0R2 Release, the following are the features and limitation | 21

Starting from SBR 8.6.0R3 Release, the following features are supported | 22

Starting from SBR 8.6.0R4 Release, the following features are supported | 22

Starting from SBR 8.6.0R5 Release, the following features are supported | 23

Starting from SBR 8.6.0R6 release, the following features are supported | 24

Starting from SBR 8.6.0R7 and 8.6.0R8 release, the following features are supported | 24

Starting from SBR 8.6.0R9 release, the following features are supported | 25

Starting from SBR 8.6.0R10 release, the following features are supported | 26

Starting from SBR 8.6.0R11 release, the following features are supported | 26

Starting from SBR 8.6.0R12 release, the following features are supported | 26

Starting from SBR 8.6.0R13 release, the following are Features and Limitation | 27

SBR 8.6.0R14 Release—Features and Limitations | 30

SBR 8.6.0R15 Release—Features and Limitations | 32

SBR 8.6.0R16 Release—Features and Limitations | 33

Related Documentation | 34

Requests for Comments | 34

3GPP and 3GPP2 Technical Specifications | 37

WiMAX Technical Specifications | 39

Third-Party Products | 39

General Statement of Compliance | 39

SBR Carrier Documentation and Release Notes | 44

Documentation Feedback | 45

Requesting Technical Support | 45

Self-Help Online Tools and Resources | 46

Opening a Case with JTAC | 46

Revision History | 47

# Release Overview

These release notes cover Release 8.6.0 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 Installation Guide</i>	Describes how to install the Steel-Belted Radius Carrier software on the server.
<i>Steel-Belted Radius Carrier 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 Reference Guide</i>	Describes the settings and valid values of the Steel-Belted Radius Carrier configuration files.
<i>Steel-Belted Radius Carrier Performance, Planning, and Tuning Guide</i>	Provides tips, use cases, and tools you need to: <ul style="list-style-type: none"><li>● Improve SBRC performance through planning, analysis, and configuration</li><li>● Increase SBRC throughput and reliability</li><li>● Analyze specific use cases, in the lab or in the production environment, to identify areas of potential performance enhancement and to limit the impact of resource constraints and failure scenarios</li></ul>
<i>Steel-Belted Radius Carrier Release Notes</i>	Contains the latest information about features, changes, known problems, and resolved problems in Release 8.6.0.

**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 webpage, which is located at:

[https://www.juniper.net/documentation/product/en\\_US/sbr-carrier](https://www.juniper.net/documentation/product/en_US/sbr-carrier)

## Release Highlights

In the SBR Carrier Release 8.6.0R17, a few PRs are fixed with the following enhancement:

- While logging errors, SQL plugin name and server identifiers are included.

**NOTE:** SBR Carrier 8.4.1 was the final version to support 32-bit builds. See [https://www.juniper.net/support/eol/carrier\\_aaa\\_sw.html](https://www.juniper.net/support/eol/carrier_aaa_sw.html) for the EOE and EOL dates of SBR Carrier 8.4.1.

### Support for Red Hat Enterprise Linux Versions

The SBR Carrier server has been qualified with Red Hat Enterprise Linux 8.1, 7.8, 7.7, 7.6, 7.5, 7.4, and 7.3 on Intel (Xeon) hardware.

**NOTE:** SBR Carrier 8.6.0 does not support RHEL 6.x, 7.0, 7.1, and 7.2.

### Support for Solaris Versions

SBR Carrier has been qualified on and supports Oracle Solaris 11.3.36.10, 11.3.36.20, and 11.4.25.0.1.75.3.

**NOTE:** Because the Signalware communication stack is not supported on Solaris, the SIM authentication module cannot be used on the Solaris platform to communicate with an HLR to process RADIUS requests. However, the module can be used with an HSS by using the RADIUS to Diameter conversion feature.

SBR Carrier 8.6.0 does not support RHEL 8.1.

## MySQL and NDB Upgrade

MySQL has been upgraded to 5.7.25, and NDB has been upgraded to 7.6.9.

**NOTE:** The **IndexMemory** parameter in **config.ini** file has been deprecated. So, the **IndexMemory** value should now be included in the **DataMemory** value.

SBR Carrier version 8.6.0-R14 supports MySQL and NDB version 8.0.22 for Oracle Solaris 11.4.25.0.1.75.3 and RHEL 8.1 versions.

## Security Updates

The following third-party libraries have been updated to address security vulnerabilities.

### OpenSSL

- OpenSSL has been upgraded to OpenSSL 1.1.1o
- Expat has been upgraded to Expat 2.4.8

**NOTE:** SBR Carrier 8.6.0 does not provide support for TLSv1.3.

SBR Carrier 8.6.0 does not support weak cipher suites: 0x0004, 0x0005, 0x0007, 0x000A, 0x002F, 0x0033, 0x0035, 0x0038, and 0x0039. For the list of tested cipher suites and their TLS protocol versions, see *SBR Carrier Administration and Configuration Guide*.

### Bouncy Castle

Bouncy Castle has been upgraded from 1.45 to 1.60.

### Jetty

Jetty has been upgraded from 9.2.3 to 9.4.14.

**NOTE:** Hard-coded passwords for the Web GUI and COA/DM certificates have been removed and made as random passwords.

## System Requirements

For complete details about the hardware and software requirements for running a standalone Steel-Belted Radius Carrier server or the optional SBR Carrier Session State Register (SSR), see “Meeting System Requirements” in the *Steel-Belted Radius Carrier Installation Guide*.

### Software

SBR Carrier has been qualified and is supported on Oracle Solaris 11.3.36.10, 11.3.36.20 (SPARC), and 11.4.25.0.1.75.3; and Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6, 7.7, 8.1 on Intel (Xeon) platforms.

**NOTE:** SBR Carrier does not support RHEL 6.x, 7.0, 7.1, and 7.2.

**NOTE:** You cannot run multiple instances of SBR Carrier on Solaris and Linux platforms.

**NOTE:** Make sure that nss-util, nss, nspr, gcc, openldap, Kerberos, cyrus-sasl, and zlib libraries are installed on your system before installing the SBR Carrier software. The libraries are normally available and installed with the OS base bundle. SBR Carrier supports the package versions of preceding libraries that are provided with Solaris 11.3.36.10.0 or later and RHEL 7.3 or later.

We recommend you to update the OS regularly for security reasons. Any questions concerning vulnerabilities of libraries that are not distributed by Juniper Networks should be addressed to the OS vendor (Red Hat or Oracle).

SBR Carrier supports virtualization on Linux, VMware hypervisor, Kernel-based Virtual Machine (KVM) hypervisor, and logical domains on Solaris. SBR Carrier has been tested with VMware ESXi 5.1, 5.5, 6.0, and 6.5 versions and KVM hypervisor on RHEL 7.3. For more information on planning and tuning the performance of SBR Carrier running on the Linux and Solaris operating systems, see the *Performance, Planning, and Tuning Guide*.

**NOTE:** SSR cluster in virtualized environments is not officially supported. Juniper Networks may still provide support for known issues and for those where you can demonstrate the issue exists on the native OS.

See [“Resolved Issues, Features, and Limitations \(Patch-Wise\)”](#) on page 15 section for RHEL 8.1 and Solaris 11.4 related installation and prerequisite details.

## Perl

Steel-Belted Radius Carrier has been tested with Perl 5.8.4 and 5.8.8. Multiple Perl installations in discrete directories are supported, but attempting to use other versions of Perl with SBR Carrier may cause problems.

## LDAP Plug-in

The LDAP plug-in requires SASL, which is not included with the SBR Carrier package. You must ensure that you have the SASL package installed before starting SBR Carrier.



**NOTE:**

- SBR Carrier does not support the Signalware communication stack on RHEL 8.1. So, the SIM authentication module cannot communicate with an HLR to process RADIUS requests. However, the SIM authentication module can convert RADIUS requests to communicate with an HSS.

SS7 cards are no longer supported.

- The OpenLDAP-2.4.46-15 is NOT supported on RHEL 8.1 due to bug “case ID: 02838485” in RHEL 8.1. Ensure that the OpenLDAP version is 2.4.46-14 or earlier on the RHEL 8.1 machine, where SBR8.60R14 installation is planned.
- In case if the legacy cipher suite is required as mentioned in the section “Starting from SBR 8.6.0R7 and 8.6.0R8 onwards, the legacy cipher suite is not supported”, run the following command to set the RHEL 8.1 to use legacy cipher suites.  
**update-crypto-policies --set LEGACY**
- RHEL 8.1 by default does not support the legacy cipher. Refer the RHEL 8.1 documentation for more detailed information.  
[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/considerations\\_in\\_adopting\\_rhel\\_8/considerations\\_in\\_adopting\\_rhel\\_8\\_see\\_you\\_soon](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/considerations_in_adopting_rhel_8/considerations_in_adopting_rhel_8_see_you_soon)

## Tested Browsers

The Web GUI can be launched in different browsers across different platforms. Table 2 on page 9 lists the tested browser versions and the operating systems.

**Table 2: Web GUI—Tested Browsers**

Browser	Version	Operating System
Google Chrome	36 and later	Windows/UNIX
Internet Explorer	9 and later	Windows
Mozilla Firefox	31 and later	Windows/UNIX
Opera	23 and later	Windows/Mac
Opera	12 and later	UNIX

**NOTE:** Java 1.8.0 or a later version is required to be installed in the server to access the Web GUI.

When you upgrade from an earlier SBR Carrier version to the current version, clear your browser's cache before launching the Web GUI.

## External Database Requirements

Steel-Belted Radius Carrier supports:

- Any external database with a compatible JDBC connector.
- Oracle native client versions 11 and 12 to connect Oracle database versions 11 and 12 on Solaris.
- Oracle native client versions 11 and 12 to connect Oracle database versions 11 and 12 on Linux.

**NOTE:** For SBR Carrier to act as an Oracle native client, the Oracle 64-bit client must be set up before installing 64-bit version of SBR Carrier, because the Oracle server location is used during installation.

- Oracle native client version 19C.
- SBR Carrier has been tested with MySQL version 5.1.69, Oracle database versions 11.2.0 and 12.1.0.2 on Solaris, and Oracle database versions 11.2.0 and 12.2.0 on Linux.

## Signalware and SIM Requirements

To support the optional SIM authentication module, Signalware 9 with Service Pack 6.5 must be installed before installing SBR Carrier.



**CAUTION:** Service Pack 6.5 must be installed; otherwise, Steel-Belted Radius Carrier cannot use the Signalware communications stack.

### *SBR Carrier Installation*

1. Before installing Signalware on RHEL 7.5, you must disable kernel address space layout randomization (KASLR), which is enabled by default on RHEL 7.5. Signalware is incompatible with KASLR and requires the kernel memory address space to be consistent.
2. To disable KASLR, do the following:
  - a. Edit the GRUB\_CMDLINE\_LINUX key in the /etc/default/grub file to add the new parameter nokaslr.

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel_bng-lnx-perf6/root  
rd.lvm.lv=rhel_bng-lnx-perf6/swap rhgb quiet nokaslr"
```
  - b. Run the command **grub2-mkconfig -o /boot/grub2/grub.cfg**.
  - c. Reboot the server.  
This disables the KASLR feature on Linux Kernel.
  - d. Install Signalware.
  - e. Start Signalware.
3. To find out more about KASLR, refer to the RHEL 7.5 kernel release notes.  
If it not 7.5 then refer the Installation guide.

**NOTE:** SBR Carrier does not support the Signalware communication stack on Solaris. So, the SIM authentication module cannot use the SIGTRAN protocol to communicate with an HLR to process RADIUS requests. However, the SIM authentication module can convert RADIUS requests to Diameter requests to communicate with an HSS.

SS7 cards are no longer supported.

## Modified Open-Source Software

SBR Carrier 8.6.0 includes open-source software that Juniper Networks has modified. The modified software includes:

- HTTPClient from Innovation GmbH
- INIH parser from Google Project Hosting

You can obtain the source code for these modifications from Juniper Networks Technical Support. See [“Requesting Technical Support” on page 45](#).

## Migrating from Earlier SBR Carrier Standalone Server Products

You can use the configuration script to move a number of files from selected previous SBR Carrier releases to the Release 8.6.0 environment when installing Steel-Belted Radius Carrier. The corresponding Release 8.6.0 files are also loaded on the system, but are not activated. You are responsible for merging new settings from Release 8.6.0 configuration files into the working (preexisting) 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.

For complete details about migrating from the preceding releases, see the *SBR Carrier Installation Guide*.

**NOTE:** Skipping versions when upgrading the cluster using the rolling restart method is not supported. Since SBR Carrier 8.0.0 uses MySQL 5.5.37, and 8.4.0, 8.4.1, and 8.5.0 use 5.7.18 for Linux (see [Table 3 on page 13](#)), we strongly recommend that you not use the rolling restart method to upgrade the cluster version of SBR Carrier directly from release 8.0.0 to 8.4.x or later on Linux. Similarly, on Solaris, we strongly recommend that you not use the rolling restart method to upgrade the cluster version of SBR Carrier directly from release 8.0.0 to 8.6.0 or later, since SBR Carrier 8.0.0 uses MySQL 5.5.37, and 8.6.0 uses 5.7.25 for Solaris. Instead, use the backup, destroy, and re-create method to upgrade or perform a clean install.

**Table 3: MySQL and NDB Versions Used by SBR Carrier**

SBR Carrier Version	MySQL Version	NDB Version
8.0.0	5.5.37	7.2.16
8.1.0	5.6.22	7.3.8
8.2.0	5.6.28	7.4.10
8.3.0	5.6.29	7.4.11
8.4.0, 8.4.1, and 8.5.0	Linux: 5.7.18 Solaris: 5.6.36	Linux: 7.5.6 Solaris: 7.4.15
8.6.0 (R0 to R14) RHEL 7.x and Solaris 11.3	5.7.25	7.6.9
Starting from 8.6.0R14 onwards for Solaris 11.4.25.0.1.75.3 version and RHEL 8.1	8.0.22	8.0.22

## Known Limitations

This section lists known problems and limitations identified up to SBR Carrier 8.6.0 R15. For the most complete and latest information about known defects, use the Juniper Networks online [Problem Report Search](#) application.

## LDAP Authentication

- Transaction rate of LDAP plug-in is reduced due to changes in the OpenLDAP versions included in RHEL and Solaris. For a workaround, see the PR record. [PR1445212](#)

## SBRC Core

- In the rfc4679.dct file, the names of the Agent-Circuit-Id and Agent-Remote-Id attributes are not defined as mentioned by RFC 4679. Instead, the names are respectively mentioned as DSL-Agent-Circuit-Id and DSL-Agent-Remote-Id.

## Logging

- SBR does not log properly for the Grouped AVP's like Vendor-Specific-Application-ID in Diameter Message. PR1531685.

### CoA/DM

- CoA/DM request - Disconnect multiple users, set variable input for CoA. PR1590846.  
COA/DM disconnect multiple users via XML is supported only using wildcard entries (for all attributes in the session), and for specific session, multiple disconnect can be performed using "Funk-Session-Handle". Funk-Session-Handle refers to the "UniqueSessionId" in the session table.

## 3GPP AAA Module

- The 3GPP AAA module does not initiate subscriber de-registration in the HSS. Subscriber de-registration is performed when SBR Carrier receives an HSS Registration-Termination-Request.
- The Diameter redirection indication is supported only over the SWx reference point. The redirection indication information in an AA-Answer message, received by a proxy server from SBR Carrier over the SWd reference point, is returned to the client without attempting to forward the request to the Redirect-Host. That is, only routing rules configured by a system administrator are enforced.

- The Redirect-Host-Usage value included in a Multimedia-Authentication-Answer message and received over the SWx reference points is ignored. The value is assumed to be DONT\_CACHE.
- In the Web GUI, the **Permanent Failures**, **Transient Failures**, and **Protocol Errors** statistics are updated based on Result-Code attribute values (not based on Diameter Experimental-Result-Code attribute values).

## Documentation Updates

There are no errata or changes in the documentation set published for SBR Carrier 8.6.0 release.

## Resolved Issues, Features, and Limitations (Patch-Wise)

### Notations Used to Indicate resolved PRs

- SBR\_64\_LINUX—64 bit version of SBR on Linux Platform Only.
- SBR\_64\_SOLARIS—64 bit version of SBR on Solaris Platform Only.
- SBR\_64—Fix applicable for 64 bit version of SBR on both platforms i.e., Solaris and Linux.

**NOTE:** If there is no notation at the end of PR title, it indicates the resolution is applicable or available on ALL the SBR 8.6.0 Releases of the tagged patch release.

### PRs fixed in patch R17

- *Interworking-5GS-Indicator* AVP is missing in DEA response sent by EPDG (SWm) and PDG (S6b) Interfaces.   
[\*\* Fix is available in full build only \*\*]. PR1670545
- SBR does not include SQL plug-in name and server identifiers in error logging. PR1674645

- *Configure\_Logs* is misspelled in SIR.sh script. [\*\* Fix is available in full build only \*\*] PR1683669
- XML Import Does Not Import RADIUS Client type <ANY>. PR1683405

## PRs fixed in patch R16

- Warning during sbrd startup displays "VerifyKey.sh: No such file or directory. [\*\* Fix is available in full build only . \*\*] PR1633234
- Added support for Emergency-Services and Emergency-Info AVPs in Diameter. [\*\* Fix is available in full build only. Refer the NOTES Section of SBR 8.6.0 R16 (41) for more information. \*\*] PR1627251

## PRs fixed in patch R15

- User-names with non-printable characters appended are accepted by SQL Auth. PR1481161
- Native user with single quotes is not getting deleted in SBR GUI. [\*\* Fix is available in full build only.\*\*] PR1527957
- Description of proxy realms is incomplete. [\*\* Fix is available in full build only. Please refer the NOTES Section of SBR 8.6.0 R15 (36) for more information \*\*] PR1499704
- SBR Carrier Core dumps when enhanced EAP logging is enabled. PR1599169
- "Current Sessions Count" showing strange values after applying SBR 8.6.0 R14 patch . [\*\* Impacted for SBR 8.6.0 R14 patch applied variants on RHEL 7 only. The fix is NOT applicable for SBR 8.6.0 R14 Full build installed on RHEL8.1.\*\*] PR1603537
- Session Control script client connection to SBR results in TLS Handshake failure. -- [\*\* Fix is available in full build only.\*\*] PR1602482
- Support of 5G AVP's Core-Network-Restrictions (1704),UE-Usage-Type (1680) and Interworking-5GS-Indicator (1706) in SWm interface. – [\*\* Fix is available in full build only.Please refer the NOTES Section (37) for more information \*\*] PR1608897
- radiusd watchdog fails to properly start on RHEL 7 and 8. [\*\* Fix is available in full build only.\*\*] PR1612225
- radius process frequently disconnects from data nodes when Geo-redundancy is enabled. PR1615299
- GeoRedundancy Replicated Session Doesn't get Deleted via GUI and CLI. [\*\* Fix is available in full build only.\*\*] PR1583511
- SBR Geo Redundancy Replication Messages are not being Parsed Properly On Solaris Platform. PR1585124



## PRs fixed in patch R14

- jnprsnmpd process high memory usage. [\*\* The fix is available in both the patch and full builds for RHEL7.X and Solaris 11.3, and available in the full builds \*only\* for RHEL 8.1 and Solaris 11.4. \*\*]. PR1566472

## PRs fixed in patch R13

- Sessions authenticated by proxy module are not counted toward concurrency login limit. [\*\* Fix is available in full build only . Please refer NOTES SECTION (22) for more information.\*\*]. PR857901
- LCI returns incorrect information for any RAS client. PR1219722
- radius process crashes when both WiMAX module and JavaScript filters are configured. PR1349575
- Support for the Terminal-Information AVP added for Diameter SWm, STa interfaces. -- [\*\* Fix is available in full build only.\*\*] PR1424137
- Concurrency ID enhanced to support greater differentiation among plug-ins for login limit calculation and logging. -- [\*\* Fix is available in full build only. Please refer NOTES SECTION (27) for more information.\*\*] PR1468996
- Static accounting SNMP traps are not available for realm-based static accounting. -- [\*\* Please refer NOTES SECTION (23) for more information.\*\*] PR1481402
- JavaScript performance degraded with JSEngineRuntimeMemory = 32. -- [\*\* Fix is available in full build only. Please refer NOTES SECTION (24) for more information.\*\*] PR1491312
- SBR incorrectly reports that SWx response did not contain an Origin-Host.-- [\*\* Fix is available in full build only. \*\*] PR1527254
- radius process crashed due to worker thread stack size. -- [\*\* Fix is available in full build only. Please refer NOTES SECTION (25) for more information.\*\*] PR1531129
- 9s6C Signalware Upgrade Support for RHEL 7. -- [\*\* Please refer NOTES SECTION (26) for more information.\*\*] PR1531990
- A default value for acct-session-id is stored in the SSR for authentication requests and may cause subsequent requests to be rejected if GenerateUniqueld = acct-session-id-plus-nas is configured. PR1533255

## PRs fixed in patch R12

- The Redirect-Host AVP is not formatted as a Diameter URI in DEA responses. PR1513175
- Webserver fails to start when using a custom SSL certificate imported with the configure script. PR1529095

## PRs fixed in patch R11

- Optimization of proxy attribute mapping. PR1451291

## PRs fixed in patch R10

- Accounting response is received even if the smart static accounting realm does not respond and is set to Primary in the proxyrl.ini configuration file. -- **[\*\* Please refer to the Notes section (16) for more information. \*\*]** PR1478650
- The attributes related to Diffie-Hellman parameters are incorrectly logged in the RADIUS log file. PR1443456

## PRs fixed in patch R9

- Authentications are rejected when JavaScript data conversion fails . -- **[\*\* Fix is available in full build only . Please refer NOTES SECTION (14 and 15) for more information.\*\*]** PR1090357
- The authReport reject log message for rejects due to exceeding the concurrency limit is "Unavailable" in cluster environment instead of "User usage limit exceeded". PR1476776

## PRs fixed in patch R8

- Some MIB files are missing from installation. -- **[\*\* Fix is available in full build only \*\*]**. PR1483957
- JDBC .jar files are not collected by SIR.sh script. -- **[\*\* Fix is available in full build only \*\*]**. PR1482494
- Legacy clients that require unsupported weak cipher suites fail EAP authentication. -- **[\*\* Please refer the NOTES SECTION (12,13) for more information \*\*]**. PR1492338

- Add support for Oracle 19C. -- **[\*\* Fix is available in full build only \*\*]**. PR1479994
- Framed-IP-Address not returned in accept when Framed-IPv6-Address is returned from profile. PR1489520

## PRs fixed in patch R7

- Some MIB files are missing from installation. -- **[\*\* Fix is available in SBR\_64\_LINUX full build only \*\*]** PR1483957
- JDBC .jar files are not collected by SIR.sh script. -- **[\*\* Fix is available in SBR\_64\_LINUX full build only \*\*]** PR1482494
- Legacy clients that require unsupported weak cipher suites fail EAP authentication. -- **[\*\* Fix is available in SBR\_64\_LINUX only. Please refer the NOTES SECTION (12,13) for more information \*\*]** PR1492338

**NOTE:** The SBR 8.6.0.R-7.51589 Full Build and 8.6.0.R-7 Patch are supported only on Linux Platforms.

## PRs fixed in patch R6

- UDP Ports 2000 and 2002 are bound even if DIAMETER is not licensed. PR1293117
- The Funk-Peer-Cert-Subject is populated from the client issuer field rather than the client device field. PR1476888
- Added support to collect .eap configuration files in SIR.sh script. -- **[\*\* Fix is available in full build only \*\*]** PR1476836
- SSL Record Layer tracing for Enhanced EAP Logging is not supported for TLS version 1.2. -- **[\*\*Please refer the NOTES SECTION (11) for more information \*\*]** PR1219412
- Framed-Interface-ID attribute from accounting request overwrites Framed-IP-Address in CST. PR1469389

## PRs fixed in patch R5

- SBR auth reject report logs error code AUTH\_ERR\_004 instead of error code AUTH\_ERR\_048 when configured max-concurrent value is exceeded. PR1474738
- SBR logs error code "AUTH\_ERR\_004" instead of error code "AUTH\_ERR\_048" for EAP NAK received. PR1475213
- SBR logs AUTH\_ERR\_004,"Unable to find user with matching password" instead of "AUTH\_ERR\_048","Unavailable" when DHCP pool IP-Addresses are unavailable. PR1475534
- MySQL Password Stored in Global Configuration File. -- **[\*\* Fix is available in full build only. Please refer the NOTES SECTION(9) for more information \*\*]** PR1263109
- To extend the trusted root certificate expiration time. -- **[\*\* Please refer the NOTES SECTION(10) for more information \*\*]** PR1468555
- Wrong UDP port number is logged in authentication/accounting response from SBR. PR1457895
- SBR with Net SNMP 5.8 generates "Cannot find module" logs in snmpd logfile. -- **[\*\* Fix is available in full build only \*\*]** PR1475784

## PRs fixed in patch R4

- Incorrect value recorded to CST Ipv4Address field. -- **[\*\*Please refer the NOTES SECTION (7) for more information \*\*]** PR1465028
- Enhanced the reject logging for TTLS for invalid username and noUserNameProvided. -- **[\*\*Please refer the NOTES SECTION (8) for more information \*\*]** PR1468597

## PRs fixed in patch R3

- Double and single quotation marks are not escaped in CSV-style logs. PR1463491
- SBR may core if reject logging enabled. PR1460377
- UTF-8 multi-byte characters may be logged incorrectly. -- **[\*\* Fix is available in full build only \*\*]** PR1463693
- Two new items added to reject logging for TTLS. -- **[\*\*Please refer the NOTES SECTION (4) for more information \*\*]** PR1459297
- SBR may reset after receiving a malformed VSA in a RADIUS packet.-- **[\*\*Please refer the NOTES SECTION (5) for more information \*\*]** PR1458584

## PRs fixed in patch R2

- SBR cores when tracelevel is set to 2 for Proxy COA Disconnect triggered from Proxy Target. PR1457614
- 9SP6A Signalware Upgrade for Linux. -- **[\*\* Fix is available in SBR\_64\_LINUX build only. Please refer the NOTES SECTION (1 to 3) for more information \*\*]** PR1459287

## Features and Limitations — Release wise (Notes)

### Starting from SBR 8.6.0R2 Release, the following are the features and limitation

#### *Features*

1. Before installing Signalware on RHEL 7.5, you must disable kernel address space layout randomization (KASLR), which is enabled by default on RHEL 7.5. Signalware is incompatible with KASLR and requires the kernel memory address space to be consistent.
2. To disable KASLR:
  - a. Edit the GRUB\_CMDLINE\_LINUX key in the `/etc/default/grub` file to add the new parameter `nokaslr`.  
Example: `GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel_bng-lnx-perf6/root rd.lvm.lv=rhel_bng-lnx-perf6/swap rhgb quiet nokaslr"`.
  - b. Run `grub2-mkconfig -o /boot/grub2/grub.cfg`.
  - c. Reboot the server.  
This disables the KASLR feature on Linux Kernel.
  - d. Install Signalware.
  - e. Start Signalware.
3. To know more about KASLR, refer to the RHEL 7.5 kernel release notes.

### Limitation

1. SBR does not log the Grouped AVP's like **Vendor-Specific-Application-ID** in **Diameter Message** due to design constraint.

## Starting from SBR 8.6.0R3 Release, the following features are supported

4. The following error code and reject reason will be logged in `rejects_YYYYMMDD.csv` under `radius_installed/authreports` directory for *Invalid Password* scenario in proxy directed realm case, instead of printing **Tunneled authentication reject** for TTLS.

Two error codes and reject reasons are added to reject logging:

- a. **AUTH\_ERR\_044** and **ldap auth user not authenticated** for TTLS with LDAP.
  - b. **AUTH\_ERR\_043** and **user found, but password validation failed** for TTLS with SQL.
5. A new parameter "RejectMalformedPacket" is introduced in `radius_installed/radius.ini` file to check whether to reject malformed packet or not.
    - **RejectMalformedPacket** - When this Parameter is enabled, SBR will reject if any malformed packet is received.
    - Default value is 0.
    - If **RejectMalformedPacket** is set to 1, SBR will reject the malformed request received.
    - If set to 0, SBR will skip the malformed attribute and continue parsing.

**NOTE:** If the packet is so severely malformed that it is not usable, then it would be dropped.

## Starting from SBR 8.6.0R4 Release, the following features are supported

### Features

6. A new configuration parameter has been introduced as part of fix for PR 1465028 in `radius.ini` for cases where both **Framed-Interface-Id** and **Framed-IP-Address** attributes are present in an accounting request. Setting **ExcludeFramedInterfaceId=1** in `radius.ini` will prevent SBR from recording the **Framed-Interface-Id** value to the **Ipv4Address** CST field. By default the parameter

**ExcludeFramedInterfaceId = 0** is disabled. A new setting will be created in a future patch to store **Framed-Interface-Id** separately.

7. The following error code and reject reason will be logged in “rejects\_YYYYMMDD.csv” under **radius\_installed/authreports** directory for invalid username and no username scenario in proxy directed realm case, instead of printing **Tunneled authentication reject** for TTLS.
  - a. Invalid Username—“AUTH\_ERR\_004” and “Unable to find user with matching password”.
  - b. No Username—“AUTH\_ERR\_019” and “Missing User Name attribute in request”.

#### *Known Issues*

The following are known issues related to retaining the backward compatibility, which is planned to be fixed in the future patch releases.

- a. PR 1474738-1: SBR auth reject report logs error code AUTH\_ERR\_004 instead of error code AUTH\_ERR\_048 when configured max-concurrent value is exceeded.
  - b. PR 1475213-1: SBR logs error code “AUTH\_ERR\_004” instead of error code “AUTH\_ERR\_048” for EAP NAK received.
  - c. PR 1475534-1: SBR logs AUTH\_ERR\_004, “Unable to find user with matching password” instead of “AUTH\_ERR\_048”, “Unavailable” when DHCP pool IP-Addresses are unavailable.
8. SBR is supported on the Linux RHEL 7.7 variant.

## Starting from SBR 8.6.0R5 Release, the following features are supported

9. Starting from 8.6.0R5, the “expect” package needs to be pre-installed on RHEL and Solaris version before executing SBR “configure” script from <radius\_installed>/install/ path.

The “expect” package versions validated for SBR variants are:

- expect 5.44 for RHEL6
- expect 5.45 for RHEL7

**NOTE:** The expect package for Solaris 11 is available along with the OS.

- expect 5.45 for Solaris 10 with Generic\_147147-26 sun4u sparc SUNW

**NOTE:**

The expect package for Solaris 10 can be downloaded from the following URLs:

- <https://www.opencsw.org/packages/expect/>
- <https://solaris-scripting-judi.blogspot.com/2018/05/install-expect-and-tcl-package-on-solaris-10.html>

10. Starting from 8.6.0R5, the below mentioned steps have to be followed before applying the patch. The below steps are for the manual renewal of expiration time stamp.

- a. Stop the SBR using the command **./sbrd stop radius** from **radius\_install\_path**.

```
bash-3.00# cd /opt/JNPRsbr/radius/
bash-3.00# ./sbrd stop radius
```

- b. Execute the following commands from **radius\_install\_path**.

```
bash-3.00# cd /opt/JNPRsbr/radius/
bash-3.00# mv root root_bkp
bash-3.00# mv my my_bkp
```

**NOTE:** After the execution of these steps apply the patch and start SBR.

## Starting from SBR 8.6.0R6 release, the following features are supported

11. As part of PR 1219412, Enhanced EAP Logging support is provided only for TLS version 1.2. Logging for TLS version 1.1 still remains unsupported.

## Starting from SBR 8.6.0R7 and 8.6.0R8 release, the following features are supported

12. The following weak cipher suites are now optionally available to support legacy clients.



- [0x2f] AES128-SHA RSA AES 128 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- [0x35] AES256-SHA RSA AES 256 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- [0x3c] AES128-SHA256 RSA AES 128 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- [0x3d] AES256-SHA256 RSA AES 256 TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

13. If the above cipher suites are needed to support legacy devices, they may be added.

By default, SBR is configured to use the following cipher suites for TLS and TTLS  
0x0067,0x006B,0xC030,0xC028,0xC014,0xC013.

If needed, the weak cipher suites mentioned above can be configured in the Web GUI under RADIUS Configuration > Authentication Policies > EAP Methods > EAP-TLS/EAP-TTLS > Advanced Server Settings tab

## Starting from SBR 8.6.0R9 release, the following features are supported

14. The Parameter “DisableMetaData” is added in the following files

- **sqlaccessor\_jdbc.gen**
- **radsqldb.aut**
- **radsqldb.acc**

15. *DisableMetaData*

- Set this parameter to avoid data type conversion in the input container between JavaScript and MySQL when using the generic string type in the container (\*.gen) file and varchar in the MySQL DB function, and then converting the received varchar value in the DB to its corresponding type using the 'cast' function.
- Enable this Parameter while using MYSQL driver to avoid errors while using the integer as the data type argument.
- Default Value is 0.

Consider an input variable MaxSessions of type varchar(20) which holds an integer value. It can be converted to its corresponding type by using the following:

```
DECLARE maxSess DECIMAL;

set maxSess=(SELECT CAST(MaxSessions as DECIMAL));
```

**NOTE:** If DisableMetaData is set to 0 (disabled), the value “maxSess” will be NULL and an error (**CDataAccessorClassObject::getOutputVariable(): failed to get variable (result) from container**) will be logged.

To avoid this error and to set the proper value for “maxSess”, set DisableMetaData set to 1 (enabled).

## Starting from SBR 8.6.0R10 release, the following features are supported

16. To discard accounting requests if one or more target realms marked as “Primary” fail to respond, you must set the parameter **SuppressResponseSelfStaticAcctFails = yes** in the Configuration section of the proxy.ini file.

## Starting from SBR 8.6.0R11 release, the following features are supported

17. SBR Carrier has been qualified on Sparc Solaris 11.3.36.20.0.
18. Testing of SBR Carrier 8.6.0:R11 full build versions has been performed successfully on the Red Hat Enterprise Linux 7.3 - 7.7 and Solaris 11.3.36.10.0, 11.3.36.20.0 operating systems in the Juniper standard laboratory environment.
19. For performance improvement, Solaris install packages now include OpenLDAP 2.4.50.

## Starting from SBR 8.6.0R12 release, the following features are supported

20. Starting from SBR 8.6.0R12 release, SBR Carrier has been qualified with RHEL 7.8.
21. • The following third-party package upgrades have been made in the SBR 8.6.0R12 full build versions.
  - OpenSSL has been upgraded to OpenSSL 1.1.1g.

- Expat has been upgraded to Expat 2.2.9.

## Starting from SBR 8.6.0R13 release, the following are Features and Limitation

22. UserConcurrency—A new parameter has been introduced to configure an active session limit for users authenticated by the proxy authentication method.

To configure a session limit, uncomment UserConcurrency in the proxy configuration (.pro) file, and provide a value for the number of active sessions allowed for users authenticated by this method.

```
[Auth]

UserConcurrency = 2
```

**NOTE:** Default value is 0, which means there is no session limit.

23. The following SNMP traps have been added for static proxy accounting timeouts and failures, supporting smart static accounting and static accounting configured in realm files.

- RADMSG\_STATIC\_ACCT\_PROXY\_TIMEOUT
- RADMSG\_STATIC\_ACCT\_PROXY\_FAILURE

24. The default value of "JSEngineRuntimeMemory" is changed from 32 to 8.

Increasing the value of JSEngineRuntimeMemory will decrease the frequency of garbage collection but negatively affect performance.

```
radius_installed_path/JNPRsbr/radius.ini:

[JavaScript]

;JSEngineRuntimeMemory=8
```

25. The default value of "WorkerThreadStackSize" in <radius\_installed\_path>/JNPRsbr/radius/radius.ini is changed from 512KB to 1MB, to prevent stack corruption.

26. Consider the following points, if your planning for to Install or upgrade Signalware version to 9s6C on RHEL 7.6 or later version.

- a. Before installing Signalware on RHEL 7.6 or later version, you must disable the Hardened User-copy feature, which is enabled by default on RHEL 7.6 or later versions.
- b. Signalware is incompatible with Hardened User-copy feature, and the feature MUST be disabled to ensure the Omnimon debugger is 100% safe to run in production network.
- c. Please refer <https://supportmavenir.com/sites/croc/TechPub/SWAR/Documentation/LINUX%20Installation%20Manual%20Version%2020200.pdf> for detailed information of system perquisites and installing procedure for Signalware installation or upgrade.

27. The generic plug-in Ids are updated and the following two new parameters are introduced.

- a. SerialNum
- b. LegacyPluginConcurrency

**NOTE:** PR:1468996 fix is available starting from SBR 8.6.0R13 full builds.

SBR 8.6.0R13 addresses the following limitation in previous builds.

If we consider the generic custom plug-ins like LDAP, TLS, TTLS, PEAP, SQL-JDBC, and ORACLE, the same Prefix ID ("200") is used.

Let us consider a scenario, where same User-Name "test" is authenticated by SBR via both LDAP and ORACLE plug-ins. In the previous builds(with out fix)the same Prefix ID "200" will be shown in the ".ShowUserConc -a" output. To overcome this issue SBR should maintain unique ID's for each plug-in. The following are the updated Prefix IDs for each generic plug-in.

Component	New Plug-In ID
LDAP	400
TLS	500
TTLS	600
PEAP	700

Component	New Plug-In ID
SQL-JDBC	800
ORACLE	900

**NOTE:** The updated behavior will function only when the parameter *LegacyPluginConcurrency* is set to False.

*LegacyPluginConcurrency*—If this parameter is set to "False" the latest plug-in's ID will be used, else the SBR behavior will be similar to prior releases. Default Value of "LegacyPluginConcurrency" is "False".

*SerialNum*—The parameter is added to "[Bootstrap]" section of \*.aut file of the generic plug-ins. Range: 1 through 99. By Default the parameter "SerialNumber" is commented.

```
[Bootstrap]

;SerialNumber=0
```

**NOTE:** In case of multiple plug-ins of the same type, the Ids can be differentiated by adding "SerialNumber" is configured in each corresponding "aut" file.

The Final Value of "Id" in the **./ShowUserConc -a** calculation is done as below.

$\text{Id} = \text{New Plug-In ID value} + \text{SerialNum configured in the *.aut file of the plug-in.}$

If the above mentioned scenario of limitation is considered, with the latest patch full build, we may notice the below out put in the **./ShowUserConc.sh -a**.

```
Id value for ORACLE in "./ShowUserConc -a" = 900 (ORACLE ID ) + 1
(SerialNum configured in *.aut file of ORACLE) = 901

Id value for LDAP in "./ShowUserConc -a" = 400 (LDAP ID ) + 1
(SerialNum configured in *.aut file of LDAP) = 401
```

hadm@<host\_name>:~> ./ShowUserConc.sh -a

Table 4: UserConcurrency

Id	Count
901-Test	3
401-Test	4

**NOTE:** Different values of <serialnum> should be used to differentiate different instances of the same generic plug-in. For example, ldapauth1.aut and ldapauth2.aut. However, if different instances are used in the same backend, <serialnum> should be the same to properly support concurrency limitations.

## SBR 8.6.0R14 Release—Features and Limitations

### LINUX

28. SBR Carrier has been qualified with RHEL 8.1.

29. SBR Carrier support MySQL and NDB version 8.0.22 for RHEL 8.1.

30. The following is the naming convention introduced for differentiating the RHEL 8.1 of SBR:8.6.0R14 Full build:

- Cluster Variant Full build: sbr-cl-8.6.0.R-14.el8.x86\_64.rpm
- Standalone Variant Full Build: sbr-sa-8.6.0.R-14.el8.x86\_64.rpm

**NOTE:** The tag **el8** is present in the name of RHEL 8.1 build of SBR to differentiate between RHEL7.x build which will have **el7** tag within the name.

### 31. Prerequisite for SBR 8.6.0R14 Installation on RHEL 8.1

In Addition to the required packages for RHEL 7.x the following packages **MUST** be installed on the RHEL 8.1 machine, where SBR 8.6.0R14 installation is planned.

- expect
- ncurses-compat-libs

- OpenLDAP-2.4.46-11

**NOTE:**

- The OpenLDAP-2.4.46-15 is NOT supported on RHEL 8.1 due to bug “case ID: 02838485” in RHEL 8.1. Please refer the bug link present on the RHEL 8.1 machine, where SBR8.60R14 installation is planned.
- In case if the legacy cipher suits is required as mentioned in the section (Starting from SBR 8.6.0R7 and 8.6.0R14 onwards is supported), run the command **update-crypto-policies --set LEGACY** to set the RHEL 8.1 to use legacy cipher suits.
- RHEL 8.1 by default doesn't support the legacy cipher. Kindly, refer the RHEL 8.1 documentation for more details.

Link:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/considerations\\_in\\_adopting\\_rhel\\_8\\_1/considerations\\_in\\_adopting\\_rhel\\_8\\_1](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/considerations_in_adopting_rhel_8_1/considerations_in_adopting_rhel_8_1)

### *Limitation*

1. The Signalware communication stack is not supported on RHEL 8.1 and the SIM authentication module cannot be used on the RHEL 8.1 platform to communicate with an HLR to process RADIUS requests. However, the module can be used with an HSS by using the RADIUS to Diameter conversion feature.

### *SOLARIS*

32. SBR Carrier has been qualified with Solaris 11.4.25.0.1.75.3 version.

33. SBR Carrier support MySQL and NDB version 8.0.22 for Solaris 11.4.25.0.1.75.3 version.

34. The following is the naming convention introduced for differentiating the Solaris 11.4 Full build for SBR:8.6.0R14

- Cluster Variant Full build: sbr-cl-8.6.0.R-14.SPARCV9.tgz
- Standalone Variant Full Build: sbr-sa-8.6.0.R-14.SPARCV9.tgz

**NOTE:** The tag "SPARCV9" (\*UPPER CASE\*) is present in the name of Solaris 11.4 Full build of SBR to differentiate between the < 11.4 Solaris builds which will have "sparcv9" (\*lower case\*) in their name.

35. In Addition to the required packages lesser than Solaris 11.4 version, the following packages **MUST** be installed on the Solaris 11.4 machine, where SBR 8.6.0R14 installation is planned.

- a. expect
- b. ncurses-compat-libs
- c. developerstudio-126 runtime libraries

**NOTE:**

- a. The developerstudio-126 runtime libraries related six libraries **MUST** be installed successfully on the Solaris 11.4 machine where SBR8.6.0R14 installation is planned.
- b. The following is the example command for installing the six libraries related to developerstudio-126 runtime libraries.
  - pkg install --accept developerstudio-126/library/c++-libs \
  - developerstudio-126/library/c-libs \
  - developerstudio-126/library/f90-libs \
  - developerstudio-126/library/math-libs \
  - developerstudio-126/library/perflib \
  - developerstudio-126/library/studio-gccrt

## SBR 8.6.0R15 Release—Features and Limitations

36. The **StaticTarget** parameter is introduced to \*.pro files as part of fix for PR 1499704.

StaticTarget configures SBR to not revert to a previously down target when it comes back up.

"0", (default) SBR reverts to previously down target when it comes back up.

"1", SBR will not revert to the previously down target even after it comes back up.



37. Starting from SBR 8.6.0 R15 release onwards, the support for following Diameter SWm interface attributes is provided on RHEL7.x and RHEL 8.1 SBR variants.

*Core-Network-Restrictions (1704)*

*UE-Usage-Type (1680)*

*Interworking-5GS-Indicator (1706)*

38. The following third-party package upgrades have been made in the SBR 8.6.0R15 full build versions of SBR .

SBR:8.6.0 R15 supported Linux and SunOS:

- OpenSSL has been upgraded to OpenSSL 1.1.1k for Linux and SunOS.
- Jetty has been upgraded to 9.4.43.
- OpenLDAP has been upgraded from 2.4.50 to 2.4.58 version.

39. Special Notes for RHEL 8.1 1024-bit RSA certificates:

Due to security considerations of RHEL 8.1 version OS, starting from SBR:8.6.0 R15 version lesser than 2047-bit RSA certificates are NOT supported. 1024-bit RSA certificates are considered too weak by RHEL 8 cryptographic policies.

According to RHEL 8 release notes, the default system-wide cryptographic policy accepts RSA keys and Diffie-Hellman parameters if larger than 2047 bits.

40. *Special Notes for upgrade using SBR 8.6.0 R15 on RHEL 8.1 and Solaris 11.4.25.0.1.75.3.*

In SBR 8.6.0 R15 RHEL 8.1 and Solaris 11.4.25.0.1.75.3 variants the size of "Name" column which represents the Pool Name present in the table "Sbr\_lpPools" is modified from 24 varchar to 84 varchar.

To accommodate and synchronize this change between the existing and planned upgrade SBR version (SBR 8.6.0 R15 on RHEL 8.1), the following command MUST be executed only once on the first upgrade planned cluster node.

```
$ su - hadm
```

```
perl ./UpdateSchema.pl 8.6 ColumnUpdate:Name
```

This command should be executed from "hadm" mode after successful installation and configuration of the Node. Refer the installation guide for detailed procedure for the Rolling-Restart Upgrade.

## SBR 8.6.0R16 Release—Features and Limitations

41. The following Diameter AVPs are available in the SBR 8.6.0R16 full build versions for SWm(ePDG) and S6b(PDG) interfaces.

- Emergency-Services
- Emergency-Info

42. The following third-party package upgrades are available in the SBR 8.6.0R16 full build versions.

- OpenSSL has been upgraded to OpenSSL1.1.1.o
- Expat has been upgraded to Expat 2.4.8

## Related Documentation

### Requests for Comments

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFCs) at <http://www.ietf.org/rfc.html>. Table 5 on page 34 lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 5: 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 SMIv2</i> . D. Cong and others. October 1996.
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i> . H. Krawczyk, M. Bellare, R. Canetti. February 1997.
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.

Table 5: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
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.
RFC 2622	<i>PPP EAP TLS Authentication Protocol.</i> B. Aboba, D. Simon, October 1999.
RFC 2719	<i>Framework Architecture for Signaling Transport.</i> L. Ong et al., 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 2960	<i>Stream Control Transmission Protocol.</i> R. Stewart and others. October 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.

Table 5: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
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. Roesse, September 2003.
RFC 3588	<i>Diameter Base Protocol</i> . P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko. 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.
RFC 4005	<i>Diameter Network Access Server Application</i> . P. Calhoun, G. Zorn, D. Spence, D. Mitton. August 2005.
RFC 4017	<i>Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs</i> . D. Stanley and others. March 2005.
RFC 4072	<i>Diameter Extensible Authentication Protocol (EAP) Application</i> . P. Eronen, G. Zorn, T. Hiller. August 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.

Table 5: RFCs Related to Steel-Belted Radius Carrier (continued)

RFC Number	Title
RFC 4306	<i>Internet Key Exchange (IKEv2) Protocol</i> . C. Kaufman. December 2005.
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 4666	<i>Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)</i> . K. Morneault, J. Pastor-Balbas. September 2006.
RFC 4668	<i>RADIUS Authentication Client MIB for IPv6</i> . D. Nelson. August 2006.
RFC 4669	<i>RADIUS Authentication Server MIB for IPv6</i> . D. Nelson. August 2006.
RFC 4670	<i>RADIUS Accounting Client MIB for IPv6</i> . D. Nelson. August 2006.
RFC 4671	<i>RADIUS Accounting Server MIB for IPv6</i> . D. Nelson. August 2006.
RFC 5281	<i>Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)</i> P. Funk, S. Blake-Wilson. August 2008.
RFC 5448	<i>Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)</i> . J. Arkko, V. Lehtovirta, P. Eronen. May 2009.
RFC 5997	<i>Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol A</i> . DeKok. August 2010.
RFC 6733	<i>Diameter Base Protocol</i> . V. Fajardo, J. Arkko, J. Loughney, G. Zorn. October 2012.
RFC 6911	<i>RADIUS Attributes for IPv6 Access Networks</i> . W. Dec, B. Sarikaya, G. Zorn, D. Miles, B. Lourdelet. April 2013.

## 3GPP and 3GPP2 Technical Specifications

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

Table 6 on page 38 lists the 3GPP Technical Specifications that apply to Steel-Belted Radius Carrier.

Table 6: 3GPP Technical Specifications

3GPP TS Number	Title	Applicable Sections
3GPP TS 22.234 Version 12.0.0	<i>Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking</i>	<ul style="list-style-type: none"> <li>• Section 5.1.7: Interworking between PLMN and WLANs</li> </ul>
3GPP TS 23.003 Version 12.6.0	<i>Numbering, addressing, and identification</i>	<ul style="list-style-type: none"> <li>• Section 2.2: Composition of IMSI</li> </ul>
3GPP TS 23.008 Version 12.6.0	<i>Organization of subscriber data</i>	<ul style="list-style-type: none"> <li>• Section 3B: Definition of subscriber data I-WLAN domain</li> </ul>
3GPP TS 23.234 Version 12.0.0	<i>3GPP system to Wireless Local Area Network (WLAN) interworking; System description</i>	<ul style="list-style-type: none"> <li>• Section 6.1: Reference Model</li> <li>• Section 6.2: Network Elements</li> </ul>
3GPP TS 23.402 Version 12.8.0	<i>Architecture enhancements for non-3GPP accesses</i>	<ul style="list-style-type: none"> <li>• Section 4.1: Concepts</li> <li>• Section 4.3: Network Elements</li> </ul>
3GPP TS 24.302 Version 14.4.0	<i>Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3</i>	<ul style="list-style-type: none"> <li>• Section 6: UE – EPC Network protocols</li> <li>• Section 8: PDUs and parameters specific to the present document</li> </ul>
3GPP TS 29.002 Version 12.7.0	<i>Mobile Application Part (MAP) specification</i>	<ul style="list-style-type: none"> <li>• Section 6: Requirements concerning the use of SCCP and TC</li> <li>• Section 7.1: Terminology and definitions</li> <li>• Section 7.2: Modelling principles</li> <li>• Section 7.3: Common MAP service</li> </ul>
3GPP TS 29.273 Version 12.7.0	<i>Evolved Packet System (EPS); 3GPP EPS AAA interfaces</i>	<ul style="list-style-type: none"> <li>• Section 4: SWa Description</li> <li>• Section 5: STa Description</li> <li>• Section 6: SWd Description</li> <li>• Section 7: SWm Description</li> <li>• Section 8: SWx Description</li> <li>• Section 9: S6b and H2 Description</li> <li>• Section 10: Result-Code and Experimental-Result Values</li> </ul>

Table 6: 3GPP Technical Specifications (*continued*)

3GPP TS Number	Title	Applicable Sections
3GPP TS 33.402 Version 14.2.0	<i>3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses</i>	<ul style="list-style-type: none"> <li>• <i>Section 6: Authentication and key agreement procedures</i></li> <li>• <i>Section 7: Establishment of security contexts in the target access system</i></li> <li>• <i>Section 8: Establishment of security between UE and ePDG</i></li> <li>• <i>Section 9: Security for IP based mobility signalling</i></li> <li>• <i>Section 14: Temporary identity management</i></li> </ul>

## 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 39 lists Steel-Belted Radius Carrier Release 8.6.0 compliance with applicable RFCs.

Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs

RFC Number	Name	Notes
1155	Structure and Identification of Management Information for TCP/IP-based Internets	—

Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs (*continued*)

RFC Number	Name	Notes
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
2104	HMAC: Keyed-Hashing for Message Authentication	—
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 2571
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).	—



Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs (*continued*)

RFC Number	Name	Notes
2866	RADIUS Accounting	—
2867	RADIUS Accounting Modifications for Tunnel Protocol Support	—
2868	RADIUS Attributes for Tunnel Protocol Support	—
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)	—

Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs (*continued*)

RFC Number	Name	Notes
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	—
4137	State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator	—
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)	—
4306	Internet Key Exchange (IKEv2) Protocol. C. Kaufman. December 2005.	—
4334	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	—
4372	Chargeable User Identity	—
4603	Additional Values for the NAS-Port-Type Attribute	—
4668	RADIUS Authentication Client MIB for IPv6	—

Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs (*continued*)

RFC Number	Name	Notes
4669	RADIUS Authentication Server MIB for IPv6	—
4670	RADIUS Accounting Client MIB for IPv6	—
4671	RADIUS Accounting Server MIB for IPv6	—
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	—
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
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	Not supported

Table 7: Compliance of Steel-Belted Radius Carrier Release 8.6.0 with Applicable RFCs (*continued*)

RFC Number	Name	Notes
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	—
—	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-TTLSv0) P. Funk, S. Blake-Wilson. August 2008.	—
5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'). J. Arkko, V. Lehtovirta, P. Eronen. May 2009.	—
5997	Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol. A. DeKok. August 2010.	—
6733	Diameter Base Protocol. V. Fajardo, J. Arkko, J. Loughney, G. Zorn. October 2012.	—
6911	RADIUS Attributes for IPv6 Access Networks. W. Dec, B. Sarikaya, G. Zorn, D. Miles, B. Lourdelet. April 2013.	—

## SBR Carrier Documentation and Release Notes

For a list of related SBR Carrier documentation, see

[https://www.juniper.net/documentation/product/en\\_US/sbr-carrier](https://www.juniper.net/documentation/product/en_US/sbr-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 website at <https://www.juniper.net/documentation/>.

## 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](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/documentation/feedback/>. 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 <https://www.juniper.net/customers/support/downloads/710059.pdf>
- **Product Warranties**—For product warranty information, visit <https://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:

<https://www.juniper.net/customers/support/>

- Find product documentation:

<https://www.juniper.net/documentation/>

- Find solutions and answer questions using our Knowledge Base:

<https://kb.juniper.net/>

- Download the latest versions of software and review release notes:

<https://support.juniper.net/support/downloads/>

- Search technical bulletins for relevant hardware and software notifications:

<https://kb.juniper.net/InfoCenter/index?page=subscriptions>, "Manage My Subscriptions"

- Open a case online in the Juniper Networks Customer Service Portal:

<https://my.juniper.net>

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

For commercial inquiries (such as license purchase), contact your Juniper Networks representative or visit <https://www.juniper.net/us/en/how-to-buy/form/>.

## Opening a Case with JTAC

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

- Use the Juniper Networks Customer Service Portal at <https://my.juniper.net>
- 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 <https://www.juniper.net/support/requesting-support.html>

When you contact technical support, be ready to provide:

- Your Steel-Belted Radius Carrier release number (for example, Steel-Belted Radius Carrier Release 8.6.0).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- 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

### November 2022—SBR Carrier Release 8.6.0 R17

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.

Ulticom, Signalware, Programmable Network, Ultimate Call Control, and Nexworx are registered trademarks of Ulticom, Inc. Kineto and the Kineto Logo are registered trademarks of Kineto Wireless, Inc. Software Advancing Communications and SignalCare are trademarks and service marks of Ulticom, Inc. CORBA (Common Object Request Broker Architecture) is a registered trademark of the Object Management Group (OMG). Raima, Raima Database Manager, and Raima Object Manager are trademarks of Raima, Inc. Sun, Sun Microsystems, the Sun logo, Java, Solaris, MySQL, and all trademarks and logos that contain Sun, Solaris, MySQL, or Java are trademarks or registered trademarks of Oracle America, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Contains software copyright 2000–2014 by Oracle America, Inc., distributed under license.

Portions of this software copyright 2003-2009 Lev Walkin <vlm@lionet.info> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

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

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

Portions of this software copyright 1989, 1991, 1992 by Carnegie Mellon University  
Derivative Work-1996, 1998-2009 Copyright 1996, 1998-2009. The Regents of the University of California All Rights Reserved. Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

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

Portions of this software copyright © 2001-2009, Networks Associates Technology, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

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

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



Portions of this software are copyright © 2001–2009, Cambridge Broadband Ltd. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

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

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

Portions of this software copyright © 1995–2009 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

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

HTTPClient package Copyright © 1996–2009 Ronald Tschalär (ronald@innovation.ch)

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

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

Copyright (c) 2000–2009 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy,

modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Contains software copyright 2000–2014 by Oracle America, Inc., distributed under license.

Steel-Belted Radius uses Thrift, licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the license at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

Steel-Belted Radius uses Cyrus SASL under the following license:

Copyright © 1994-2012 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

Office of Technology Transfer  
Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213-3890  
(412) 268-4387, fax: (412) 268-7395  
[tech-transfer@andrew.cmu.edu](mailto:tech-transfer@andrew.cmu.edu)

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

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

Steel-Belted Radius uses OpenSSL version 1.1.1, which have the following terms:

Copyright © 1998-2018 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.  
(<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit  
(<http://www.openssl.org/>)"

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

The "inix" library is distributed under the New BSD license:

Copyright © 2009, Brush Technology. All rights reserved.

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

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