

Steel-Belted Radius[®] Carrier Release Notes

Release 8.4.1
January 2018
Revision 1

These Release Notes support Release 8.4.1 of Steel-Belted Radius Carrier (SBRC). Before you install or use your new software, read these Release Notes in their entirety, especially “Known Problems and Limitations” on page 6.

Contents

Release Overview	3
Before You Start	3
Documentation	3
Release Highlights	3
System Requirements	4
Software	4
Perl	4
LDAP Plug-in	4
Tested Browsers	4
External Database Requirements	5
Signalware and SIM Requirements	5
Modified Open-Source Software	5
Migrating from Earlier SBR Carrier Standalone Server Products	6
Known Problems and Limitations	6
LDAP Authentication	7
SBRC Core	7
SIM Authentication	8
Logging	8
Geo-Redundancy	8
Separate Session Database Process	8
3GPP AAA Module	8
Documentation Updates	9
Session State Register Module	9
Resolved Issues	9
Related Documentation	11
Requests for Comments	11
3GPP and 3GPP2 Technical Specifications	14

WiMAX Technical Specifications	15
Third-Party Products	16
General Statement of Compliance	16
SBR Carrier Documentation and Release Notes	20
Documentation Feedback	20
Requesting Technical Support	21
Self-Help Online Tools and Resources	21
Opening a Case with JTAC	22
Revision History	22

Release Overview

These release notes cover Release 8.4.1 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 3 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"> • Improve SBRC performance through planning, analysis, and configuration • Increase SBRC throughput and reliability • 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
<i>Steel-Belted Radius Carrier Release Notes</i>	Contains the latest information about features, changes, known problems, and resolved problems in Release 8.4.1.



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:

<http://www.juniper.net/support/downloads/?p=carrier#docs>

Release Highlights

SBR Carrier 8.4.1 is a maintenance release which resolves several PRs (see the “Resolved Issues” section).



NOTE: SBR Carrier 8.4.1 is the final version to support 32-bit builds. See https://www.juniper.net/support/eol/carrier_aaa_sw.html for the EOE and EOL dates of SBR Carrier 8.4.1.

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 10, 11.0, 11.1, and 11.3 (SPARC) and Red Hat Enterprise Linux 6.1, 6.5, 6.6, 6.7, 7.0, and 7.2 on Intel (Xeon) platforms.

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 included with the SBR Carrier package only for Solaris versions and not for Linux versions. For a Linux machine, you must ensure that you have the SASL package installed before starting SBR.

Tested Browsers

The Web GUI can be launched in different browsers across different platforms. [Table 2 on page 4](#) 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: 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 10, 11, and 12 to connect Oracle database versions 10, 11, and 12 on Solaris.



NOTE: For SBR Carrier to act as an Oracle native client (only on Solaris), the Oracle 32-bit client or 64-bit client must be set up before installing 32-bit or 64-bit version of SBR Carrier respectively, because the Oracle server location is used during installation.

- SBR Carrier has been tested with MySQL version 5.1.69 and Oracle database versions 10.2.0, 11.2.0, and 12.1.0.2.

Signalware and SIM Requirements

To support the optional SIM authentication module, Signalware 9 with Service Pack 6.3 must be installed before installing SBR Carrier.



CAUTION: Service Pack 6.3 must be installed; otherwise, Steel-Belted Radius Carrier cannot use the Signalware communications stack.

For more information, see the *SBR Carrier Installation Guide*.



NOTE: SS7 cards are no longer supported for customers who consider upgrading to SBR Carrier release 8.4.1.

Modified Open-Source Software

Embedded in Steel-Belted Radius Carrier 8.4.1 is open-source software that Juniper Networks has modified. The modified software includes:

- HTTPClient from Innovation GmbH
- sunmd5.c from the OpenSolaris Project
- Spider Monkey 1.7 from Mozilla
- 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 21.

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 8.4.1 environment when installing Steel-Belted Radius Carrier. The corresponding Release 8.4.1 files are also loaded on the system, but are not activated. You are responsible for merging new settings from Release 8.4.1 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 and 8.4.1 use 5.7.18 for Linux (see [Table 3 on page 6](#)), 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 on a Linux machine. 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	Linux: 5.7.18	Linux: 7.5.6
	Solaris: 5.6.36	Solaris: 7.4.15
8.4.1	Linux: 5.7.18	Linux: 7.5.6
	Solaris: 5.6.36	Solaris: 7.4.15

Known Problems and Limitations

This section lists known problems and limitations identified in SBR Carrier 8.4.1. For the most complete and latest information about known defects, use the Juniper Networks online [Problem Report Search](#) application.

LDAP Authentication

- Entering more than 124 characters for a native user password results in an erroneous rejection. [PR771505](#)
- In previous versions of SBR Carrier in Solaris, LDAP used the Mozilla libraries for LDAP communication. When LDAP is used, this requires the Cert7.db and Key3.db files as the certificate store for trusted root certificates. Starting with SBR Carrier version 7.4.0 Linux and 7.5.0 Solaris, SBR Carrier uses the OpenLDAP libraries to process LDAP requests. For SBR to process LDAP requests, you must configure OpenLDAP to accept the server certificate.
- When you have a large number of LDAP connections configured, SBR Carrier may hang or take several minutes to shut down, and the sbrd script may display a shutdown failure message in the terminal. [PR847961](#)

SBRC Core

- Sessions are not handled correctly when the length of Acct-Session-Id is greater than 24 octets. For a workaround, see the PR record. [PR719218](#)
- The User Concurrency table does not display proxy realm names. [PR857901](#)
- The Inbound-from-Proxy control point is called after, not before, the inbound filters are applied. [PR889762](#)
- 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.
- Response for the SendRoutingInfoForLCS message from the HLR or HSS may not be received by authGateway if the HLR or HSS sends the message with the routing indicator in CalledPartyAddress set to "Route based on SSN". For a workaround, see the PR record. [PR987162](#)
- Enhanced performance counters initialize peak-rate counter to total-requests counter's value when a HUP signal is sent. [PR1052592](#)
- When the **Framed-IPv6-Address** attribute is configured in both the user and profile return lists, the IPv6 addresses in both the return lists are returned if the **FramedIPv6AddressHint** parameter is set to **no**. For a workaround, see the PR record. [PR1303671](#)
- SBR Carrier cores when the HST file size exceeds the system RAM limit. For a workaround, see the PR record. [PR1306886](#)
- In Web GUI, the **Location Group** pane displays only the first 50 RADIUS clients and includes non-location group clients. For a workaround, see the PR record. [PR1237011](#)

SIM Authentication

- The authGateway and GWrelay processes must be restarted whenever SBR restarts. This is applicable only on a Linux platform. [PR1011144](#)

Logging

- Detailed EAP logging is supported only for TLS protocol version 1.0, and not for versions 1.1 or 1.2. [PR1219412](#)
- The **KPI/High-Challenge-Objects-Since-Reset** statistics logged in the statistics log file may display an additional count. [PR1219732](#)
- Transaction IDs are not logged for accounting packets when a Class attribute is not present in the packet. [PR917748](#)

Geo-Redundancy

- Geo-redundancy server populates some CST fields with NULL values. [PR1308295](#)



.....
CAUTION:

If you are using the Geo-redundancy feature, we recommend that you do not upgrade to Release 8.4.0. This issue will be resolved in a future patch.
.....

Separate Session Database Process

- When you upgrade SBR Carrier from releases earlier than 7.6.0, SBR Carrier automatically converts the standalone session store file (radads.hst) to a new format. This conversion delays the SBR startup for the first time after the upgrade. The approximate time taken for converting the 1-GB persistent session store file (radads.hst) to a new format (radadcst.hst) is 8–10 minutes.

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 SBR Diameter Administrator, 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).
- SBR Carrier fails to generate CoA/DM messages when a request is sent for RADIUS to Diameter conversion. [PR1053462](#)
- Diameter packets are not routed to the HSS based on the IMSI prefix routing rule.

Documentation Updates

Information in this section updates the published Steel-Belted Radius Carrier 8.4.1 documentation set.

Session State Register Module

- If you start a management (M or SM) node without running the “configure 2 (create a new cluster definition)” option, as you would in the case of a rolling restart upgrade from Release 7.2.x to Release 8.4.1, you will see multiple warnings such as the following:



.....
WARNING: 2010-11-30 15:25:23 [MgmtSrvr] WARNING -- at line 68: [api] Id is deprecated, use NodeId instead

These warnings can be safely ignored.

To avoid these warnings, make the following change in the /opt/JNPRhadm/config.ini file:

Change lines that read Id=<number> to NodeId=<number> on each management node.

Resolved Issues

This section lists the issues fixed in Steel-Belted Radius Carrier 8.4.1. For the most complete and latest information about resolved issues, use the Juniper Networks online [Problem Report Search](#) application.

- Authentication logs are not searchable through the Web GUI, and non-default filenames are not handled correctly. [PR1297832](#)
- Use of an empty CoA/DM XML request causes SBR Carrier to core. [PR1310206](#)
- Performance improvements have been made to the standalone version by enabling the use of more threads. [PR1276673](#)
- The GWrelay process does not wait for the authGateway process to start and goes down immediately after startup. [PR1282484](#)
- 64-bit version of SBR Carrier hangs and stops processing requests when any incoming request attributes are mapped under [Request] section in the *.dhc file. [PR1307962](#)

- RADIUS User-Name attributes larger than 234 characters are not supported for authentication methods. [PR1300337](#)
- RADIUS process may crash under load when an Accounting-Interim is received with either Framed-IP-Address or Framed-IPv6-Address attribute in the request and the **UpdateOnInterim** parameter is enabled in **radius.ini**. [PR1314811](#)
- Scroll bar is not available while importing XML configurations. [PR1213382](#)
- Web GUI allows creation of RADIUS clients and proxy targets with no shared secret. [PR1248396](#)
- Web GUI allows users to configure Echo feature for Multi-Valued-Pair attributes though the Multi-Valued-Pair attribute has no support for Echo feature. [PR1306874](#)
- The RADIUS process is not starting when the **radius.ini** file copied from the backup to the RADIUS is for a different flavor (i.e., cluster to standalone) than the newly installed version. [PR1232398](#)
- SBR Carrier incorrectly allows pseudonym secret with length more than 32 characters in the **simauth.aut** file. [PR794123](#)
- SBR Carrier fails to bind to LCI interfaces in the [LDAPAddresses] section of **radius.ini** which are duplicated. [PR1052583](#)
- When the Geo-redundancy feature is enabled, SBR Carrier on the receiving server fails to restart under load. [PR1070836](#)
- LDAP authentication plug-in logs an accept when the password does not match during EAP-TTLS or EAP-MS-CHAP-V2 authentication using the directed realm. [PR1143396](#)
- If you have already added the **<ANY>** RADIUS client or a RADIUS Client with an IPv6 address, you cannot configure another RADIUS Client with an IPv6 address. [PR1072032](#)
- Some CST fields might be populated with incorrect values on the Geo-redundancy server when the corresponding RADIUS attributes are not present in the accounting request. [PR1070837](#)
- Bundled AVPs in the accept response from a proxy target are not parsed in the proxy response. [PR1289314](#)
- While starting the RADIUS process, SBR Carrier logs an irrelevant error: "route provider 'AcctMethodListMgr' does not provide routes". [PR1280802](#)
- ***gen** files contain configuration parameters related to the deprecated DMU feature of Mobile IP Module. [PR1088438](#)
- Incorrect UniqueSessionId is logged in the latency log file when using IP pools with **GenerateUniqueld** as **ipaddr** or **ipaddr-plus-nas** in **sessionTable.ini**. [PR931628](#)
- In the WiMAX device scenario, the session table is updated abnormally if the **OuterNAIPlusMAC** parameter is set to ON. Accounting-Start fails to match the phantom session if the **GenerateUniqueld** parameter in the **sessionTable.ini** file is set to outernai-plus-mac. [PR849401](#)
- The CST restoration blocking mode (CSTRestorationBlock = 0 in the **dbclusterlocal.gen** file) has been removed. [PR1232558](#)

- The Web GUI does not allow configuring IP pools with empty address ranges. [PR1309088](#)
- SBR Carrier may core while creating native users with non-English language characters. [PR1266503](#)
- Reject messages are erroneously logged for successful requests when the **Filter** parameter is set to **MostRelevant** in the [AuthRejectLog] section of **radius.ini**. [PR1022042](#)
- The presence of a leading "00" in a NasIpv6Address, Ipv6InterfaceId, IPv6Address, or Framed-Ipv6-Prefix attribute prevents the Geo-redundancy server from replicating a session. [PR1277339](#)
- The value of Termination-Action for TLS and TTLS authentication methods and the TLS helper cannot be set correctly through the GUI. [PR583905](#)
- SBR Carrier cores when Acct-Session-Id is fetched with a JavaScript which is not present in the authentication request. [PR928215](#)
- SQL logging messages for successful SQL queries are not written to the log file. [PR852049](#)
- Usage description in the **proxyrl.ini** file requires clarification. [PR1275639](#)
- Enabling RealTimeScheduler by default for Data nodes may cause internal cluster database errors. [PR1255989](#)
- Connectivity errors can result in termination of the authGateway process. [PR1305900](#)
- Oversized return list attributes imported from XML files cause SBR Carrier to crash. [PR896673](#)

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 4 on page 11](#) lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 4: 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.

Table 4: RFCs Related to Steel-Belted Radius Carrier (*continued*)

RFC Number	Title
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.
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.

Table 4: RFCs Related to Steel-Belted Radius Carrier (*continued*)

RFC Number	Title
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 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. Levkowitz. 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 4: 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-TLSv0)</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</i> . A. 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 5 on page 14 lists the 3GPP Technical Specifications that apply to Steel-Belted Radius Carrier.

Table 5: 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"> Section 5.1.7: Interworking between PLMN and WLANs

Table 5: 3GPP Technical Specifications (*continued*)

3GPP TS Number	Title	Applicable Sections
3GPP TS 23.003 Version 12.6.0	<i>Numbering, addressing, and identification</i>	<ul style="list-style-type: none"> • Section 2.2: Composition of IMSI
3GPP TS 23.008 Version 12.6.0	<i>Organization of subscriber data</i>	<ul style="list-style-type: none"> • Section 3B: Definition of subscriber data I-WLAN domain
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"> • Section 6.1: Reference Model • Section 6.2: Network Elements
3GPP TS 23.402 Version 12.8.0	<i>Architecture enhancements for non-3GPP accesses</i>	<ul style="list-style-type: none"> • Section 4.1: Concepts • Section 4.3: Network Elements
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"> • Section 6: UE – EPC Network protocols • Section 8: PDUs and parameters specific to the present document
3GPP TS 29.002 Version 12.7.0	<i>Mobile Application Part (MAP) specification</i>	<ul style="list-style-type: none"> • Section 6: Requirements concerning the use of SCCP and TC • Section 7.1: Terminology and definitions • Section 7.2: Modelling principles • Section 7.3: Common MAP service
3GPP TS 29.273 Version 12.7.0	<i>Evolved Packet System (EPS); 3GPP EPS AAA interfaces</i>	<ul style="list-style-type: none"> • Section 4: SWa Description • Section 5: STa Description • Section 6: SWd Description • Section 7: SWm Description • Section 8: SWx Description • Section 9: S6b and H2 Description • Section 10: Result-Code and Experimental-Result Values
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"> • Section 6: Authentication and key agreement procedures • Section 7: Establishment of security contexts in the target access system • Section 8: Establishment of security between UE and ePDG • Section 9: Security for IP based mobility signalling • Section 14: Temporary identity management

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 Juniper software and hardware, or your access servers and firewalls, consult the manufacturer's documentation.

General Statement of Compliance

Table 6 on page 16 lists Steel-Belted Radius Carrier Release 8.4.1 compliance with applicable RFCs.

Table 6: Compliance of Steel-Belted Radius Carrier Release 8.4.1 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
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

Table 6: Compliance of Steel-Belted Radius Carrier Release 8.4.1 with Applicable RFCs (continued)

RFC Number	Name	Notes
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	—
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 6: Compliance of Steel-Belted Radius Carrier Release 8.4.1 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	Not supported
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	—
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	—
4669	RADIUS Authentication Server MIB for IPv6	—
4670	RADIUS Accounting Client MIB for IPv6	—
4671	RADIUS Accounting Server MIB for IPv6	—

Table 6: Compliance of Steel-Belted Radius Carrier Release 8.4.1 with Applicable RFCs (continued)

RFC Number	Name	Notes
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	—
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

Table 6: Compliance of Steel-Belted Radius Carrier Release 8.4.1 with Applicable RFCs (continued)

RFC Number	Name	Notes
5281	Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TLSv0) 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 <http://www.juniper.net/support/downloads/?p=carrier#docs>.

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 <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 <http://www.juniper.net/techpubs/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 <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/>.

For commercial inquiries (such as license purchase), contact your Juniper Networks representative or visit <http://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 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 contact technical support, be ready to provide:

- Your Steel-Belted Radius Carrier release number (for example, Steel-Belted Radius Carrier Release 8.4.1).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- 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

January 2018—SBR Carrier Release 8.4.1

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

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 versions 1.0.2j, which have the following terms:

Copyright © 1998-2016 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.
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 "inih" 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.