



**Juniper Networks®  
Steel-Belted Radius® Carrier**

## **Release Notes**

*Release 7.2*

**Juniper Networks, Inc.**  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089  
USA  
408-745-2000  
**<http://www.juniper.net>**

Part Number: 530-027240-01

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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 Birdstep Technology. Sun, Sun Microsystems, the Sun logo, Java, Solaris, and all trademarks and logos that contain Sun, Solaris, or Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. MySQL and the MySQL logo are registered trademarks of MySQL AB in the United States, the European Union, 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.

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 (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSe, and SDX-300 software) 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.

Contains software copyright 2000-2009 by MySQL AB, distributed under license.

Portions of this software copyright 1999-2009 Apasphere Ltd. This product includes omniORB CORBA software from Apasphere Ltd, under the LGPL license: The libraries in omniORB are released under the LGPL license.

Portions of this software copyright 2003-2009 Lev Walkin <[vlm@lionet.info](mailto: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:

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

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:

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

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

Portions of this software are copyright © 2001-2009, 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:

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

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

Portions of this software copyright © 1995-2009 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:

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

HTTPClient package Copyright © 1996-2009 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.

Copyright © 2009, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

*Steel-Belted Radius Carrier Release Notes, Release 7.2*  
Writing: Colleen Feerick  
Editing: Ben Mann

Revision History  
14 May 2009—Revision 1

The information in this document is current as of the date listed in the revision history.

## Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at [www.juniper.net/techpubs](http://www.juniper.net/techpubs).

## End User License Agreement

---

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

---

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.
3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
  - a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

- 4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.
- 5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
- 6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.
- 7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.
- 8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.
- 9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.
- 10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.
12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.
13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.
14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.
15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Table of Contents

<b>Steel-Belted Radius Carrier Release 7.2 Release Notes</b>	<b>1</b>
System Requirements .....	2
Stand-Alone SBR Carrier Server Hardware .....	2
Session State Register Host Hardware .....	3
SBR and Management Node Hosts .....	3
Data Node Hosts .....	3
Software .....	4
Perl .....	5
Supported Browsers .....	5
External Database Requirements .....	5
Signalware and SS7 Interface Requirements .....	5
Modified Open-Source Software .....	6
Migrating from Earlier SBR Releases .....	6
Migrating from Earlier SBR Stand-Alone Server Products .....	6
Supported Releases for Stand-Alone Server .....	7
Migrating from SBR Release 5.5 High Availability .....	7
Using a Transition Server .....	7
New Features and Enhancements .....	8
Optional SMS Authentication Module .....	8
Optional CDMA Mobility Module .....	8
Optional Session Control Module .....	8
Optional Session State Register Module .....	9
Optional Concurrency Module .....	9
EAP-TTLS Secondary Authentication Support .....	9
Time-Based SBR Log Rollover .....	9
SNMP Trap When Proxy Realm Goes Out of Service .....	9
Access-Request Discard .....	9
Smart Dynamic Home Agent Assignment for WiMAX .....	9
New Filter Rules .....	10
Disable Strobe Request in FastFail Proxy Realm .....	10
Enhanced Proxy Logging at Debug .....	10
Enhanced Proxy Error Logging .....	10
Added SBR Log File Session Identifier .....	11
Consolidated [Logging] Section .....	11
Modified Advanced Logging Settings .....	12
Higher Granularity Timestamps in Log File .....	12
Improved Diagnostics in Log File .....	12
Thread Id .....	12
Statlog.ini Updated on HUP or USR2 .....	12
Authorize-Only Requests .....	13
Known Problems and Limitations .....	13
CDMA .....	13
CoA/DM .....	13
Filters .....	14

LDAP Authentication .....	14
Oracle.....	15
Replication .....	15
SBR Administrator .....	15
SBR Core .....	16
Session State Register Module .....	17
SIM Authentication .....	17
SNMP .....	18
SQL Authentication.....	18
System Requirements.....	18
WiMAX Module .....	19
Documentation Updates .....	19
account.ini File .....	19
admin.ini File .....	19
Attributes No Longer Editable or Orderable .....	20
CDMA .....	20
classmap.ini File .....	20
Directed Realm Configuration (.dir) File.....	20
HTTP Digest Access Authentication .....	21
JavaScripting.....	21
LDAP .....	21
radius.ini File.....	22
radsql.aut File .....	23
radsqljdbc.aut File .....	23
RFC 5281 .....	23
Session State Register .....	23
SIM Authentication .....	27
Statlog.ini .....	27
ttlsauth.aut File .....	27
Leading Wildcards and Session Queries.....	28
Resolved Issues.....	28
Related Documentation .....	30
Requests for Comments (RFCs) .....	30
3GPP and 3GPP2 Technical Specifications .....	33
WiMAX Technical Specifications.....	33
Third-Party Products.....	33
Obtaining Documentation.....	33
Documentation Feedback .....	34
Requesting Technical Support .....	34
Self-Help Online Tools and Resources.....	34
Opening a Case with JTAC .....	35
General Statement of Compliance .....	36

# Steel-Belted Radius Carrier Release 7.2

## Release Notes

These Release Notes support Release 7.2 of Steel-Belted Radius Carrier. Before you install or use your new software, read these Release Notes in their entirety, especially the “Known Problems and Limitations” section on page 13.

These topics are in the release notes:

- System Requirements on page 2
- Modified Open-Source Software on page 6
- Migrating from Earlier SBR Releases on page 6
- New Features and Enhancements on page 8
- Known Problems and Limitations on page 13
- Documentation Updates on page 19
- Resolved Issues on page 28
- Related Documentation on page 30
- Obtaining Documentation on page 33
- Documentation Feedback on page 34
- Requesting Technical Support on page 34
- General Statement of Compliance on page 36

If the information in these Release Notes differs from the information found in the product documentation, follow the Release Notes.

You can find these release notes in Adobe Acrobat (PDF) format on the Juniper Networks Technical Publications Web page, which is located at [https://www.juniper.net/techpubs/software/carrier\\_aaa/carrier/](https://www.juniper.net/techpubs/software/carrier_aaa/carrier/).

## System Requirements

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

### Stand-Alone SBR Carrier Server Hardware

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

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

**Table 1: Stand-Alone Steel-Belted Radius Carrier Server Hardware Configurations**

Server	RAM	CPUs	Free Disk Space
<b>Stand-Alone SBR Carrier Server (Minimum Configuration)</b>	8 GB RAM.	Two-CPU Ultrasparc IIIi or better, running at 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBR Administrator.
<b>Stand-Alone SBR Carrier Server (Recommended Configuration)</b>	8 GB RAM or more. If the WiMAX or SIM module, or an SS7 communications interface is installed, the Ulticom Signalware communications stack is used. To support the stack and for systems processing a heavier-than-normal load (for instance, with additional session licenses), more memory produces better performance.	Multiple CPU Ultrasparc IIIi or better running at more than 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBR Administrator.

## Session State Register Host Hardware

### SBR and Management Node Hosts

Table 2 lists the hardware requirements for Session State Register cluster SBR and management node hosts.

**Table 2: Session State Register SBR and Management Node Host Hardware Configurations**

Server	RAM	CPUs	Free Disk Space	Network Interfaces
<b>SBR and/or Management Node Host (Minimum Configuration)</b>	2 GB RAM.	Two-CPU Ultrasparc IIIi or better, running at 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBR Administrator.	Two physical interfaces on a 100 Base-T network. Multipath configuration is required.
<b>SBR and/or Management Node Host (Recommended Configuration)</b>	4 GB RAM or more. If the WiMAX or SIM module, or an SS7 communications interface is installed, the Ultricom Signalware communications stack is used. To support the stack and for systems processing a heavier-than-normal load (for instance, with additional session licenses), more memory produces better performance.	Multiple CPU Ultrasparc IIIi or better running at more than 1.5 Ghz.	At least 750 MB of local hard disk space (not NFS), including about 81 MB of local disk space for SBR Administrator.	Two physical interfaces on a Gigabit Ethernet network. Multipath configuration is required.

### Data Node Hosts

Table 3 lists the hardware requirements for Session State Register data node hosts.

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



**NOTE:** This free disk space shown in Table 3 must be available specifically to the /opt file system for installation of the SSR software.

**Table 3: Session State Register Data Node Host Hardware Configurations**

<b>Server</b>	<b>RAM</b>	<b>CPUs</b>	<b>Free Disk Space</b>	<b>Network Interfaces</b>
<b>Data Node Host (Minimum Configuration)</b>	8 GB RAM.	Two-CPU Ultrasparc IIIi or better, running at 1.5 Ghz.	The local disc space requirement is related to the amount of RAM in the system. To calculate the minimum requirement for the amount of RAM on the system, use the formula: (RAM - 4 GB) * 12 . For example, a system with 16 GB of RAM requires a minimum of (16 GB - 4 GB) * 12, or 144 GB of local disk storage space.	Two physical interfaces on a 100 Base-T network. Multipath configuration is required.
<b>Data Node Host (Recommended Configuration)</b>	More than 8 GB RAM. More than the minimum of 8 GB of RAM supports more connections because more of the SSR database can be held in memory. More database in memory may translate into faster processing because disk operations are minimized.	Multiple CPU Ultrasparc IIIi or better running at more than 1.5 Ghz.		Two physical interfaces on a Gigabit Ethernet network. Multipath configuration is required.

## Software

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

### Required Patches

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

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

### Recommended Patches

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

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

## Perl

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

## Supported Browsers

The SBR Administrator configuration application can be launched from the browsers listed in Table 4:

**Table 4: Supported Browsers**

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

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

## External Database Requirements

Steel-Belted Radius Carrier supports:

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

## Signalware and SS7 Interface Requirements

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

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



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

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

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

---

The Signalware PH0301 and XH0303 boards are supported.

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

---

## Modified Open-Source Software

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

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

You can obtain the source code for these modifications by requesting them from Juniper Networks Technical Support. See “Requesting Technical Support” on page 34.

---

## Migrating from Earlier SBR Releases

SBR Carrier Release 7.2 can run as a stand-alone server or as part of a Session State Register cluster.

### ***Migrating from Earlier SBR Stand-Alone Server Products***

You can use the configuration script to move a number of files from selected previous SBR releases to the Release 7.2 environment when installing Steel-Belted Radius Carrier. The corresponding Release 7.2 files are also loaded on the system, but are not activated. You are responsible for merging new settings from Release 7.2 configuration files into the working (pre-existing) configuration files. To support new features, SBR Carrier uses default values for any new settings that have not been merged into the working configuration files.

### Supported Releases for Stand-Alone Server

You can migrate configuration files from these SBR server releases to Release 7.2:

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

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

### Migrating from SBR Release 5.5 High Availability

The easiest way to replace an existing SBR Release 5.5 High Availability (SBR HA) cluster with a new Release 7.2 cluster is to fully install and configure the new cluster and then cut over to the new cluster.

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

### Using a Transition Server

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

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

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

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

## New Features and Enhancements

---

Release 7.2 of Steel-Belted Radius Carrier includes a number of new features and improvements in the core software and in optional modules, summarized in this section. For more information, see the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*.

### Optional SMS Authentication Module

For operators who have not yet adopted 802.1X, you can leverage the optional Short Message Service (SMS) module to authenticate hotspot users to the network and deliver services based on out-of-band delivery of a secure one-time password through the Short Message Service (SMS) text messaging protocol. This optional module provides mobile service providers the ability to bill mobile subscribers for wireless hotspot Internet access. Billing integration is provided through RADIUS accounting and Call Detail Record (CDR) generation to enable unified billing.

### Optional CDMA Mobility Module

The optional Code Division Multiple Access (CDMA) Mobility module for Steel-Belted Radius Carrier extends RADIUS functionality to 3GPP2 users on the scale required by Internet Service Providers and carriers. This module meets the AAA service requirements of CDMA wireless operators who are transitioning to next-generation 3G/Mobile IP-based networks. This optional module builds on the features of Steel-Belted Radius Carrier to enable authentication of mobile users, deliver the appropriate level of service to each subscriber, and log and record all subscriber connection data for billing purposes.

### Optional Session Control Module

The optional Session Control module enables you to make changes to active subscriber sessions without requiring the network access server (NAS) to initiate the change. For example, you may want to terminate an active user's session by issuing a Disconnect Message (DM) request to the NAS, or you may want to modify the authorization level of an active user's session issuing a Change of Authorization (CoA) request to the NAS. For example, as a service provider, you may be required to provide legal organizations with voice and data intercept capabilities as mandated by law. These might include access to private communications between organizations or individuals such as phone calls, e-mail, VoIP, or instant messaging. These legal intercept capabilities can be performed by issuing a CoA request.

Using the Session Control module, you can customize the CoA/DM requests you want to support in your network. You can define *actions* that can be invoked on active sessions such as disconnecting an active session, increasing the bandwidth of an active session, or any other action you want to define.

You can control sessions using SBR Administrator, a command-line utility, or you can develop your own client management application to interface with the Steel-Belted Radius Carrier CoA/DM XML interface.

### **Optional Session State Register Module**

The Steel-Belted Radius Carrier Session State Register (SSR) module implements a stateless high-availability AAA platform. Multiple servers of different types (data, management, and SBR Carrier) perform certain aspects of SBR Carrier operation. The servers collaborate to share a common session database and a common IP address pool, and to provide a high level of redundancy. Up to 20 SBR Carrier servers can access the common shared resources simultaneously.

### **Optional Concurrency Module**

The optional Concurrency module works in the Session State Register environment and provides tools that can limit the number of active connections on a per-user per-cluster basis on any attribute or realm. Users can also be grouped based on attributes or realms.

### **EAP-TTLS Secondary Authentication Support**

EAP TTLS Secondary Authentication support includes verification of MAC address with Calling-Station-Id, as well as the population of various Juniper Networks VSAs with fields from the Client certificate.

### **Time-Based SBR Log Rollover**

You can now specify rollover time in minutes for the `yyymmdd.log` file of SBR Carrier. Previously only daily rollover and rollover based on file size were supported.

### **SNMP Trap When Proxy Realm Goes Out of Service**

You can now signal when all targets of a proxy realm go out of service, and again when any target comes back into service.

### **Access-Request Discard**

You can now discard an Authentication-Request based on the presence of attributes in the Access-Request (as determined through JavaScripting) or on the Found/Not Found return of an LDAP or SQL authentication method. No response is sent to the NAS. Previously only Access-Requests from unknown NASs were ignored.

### **Smart Dynamic Home Agent Assignment for WiMAX**

The smart dynamic home agent assignment feature works by reading various configuration files and creating round-robin groups as specified in those files. You can assess the load status of the home agents in your network and populate the associated configuration files in a way that balances the load across home agents. When SBR Carrier receives a HUP signal, it reads these configuration files and updates the round-robin groups.

### **New Filter Rules**

A new filter called EXCLUDE-UNKNOWN deletes all attributes that are not included in the dictionary of the sending NAS before proxying the message to the target (outbound filters) or before returning the proxy response (inbound filters). Optionally, a Vendor Id may accompany the directive to limit the exclusion to attributes with that Vendor Id.

In addition, the inverse rule ALLOW-UNKNOWN filter rule has been added, also optionally with a Vendor Id. This is useful to override a global EXCLUDE-UNKNOWN for a particular Vendor Id.

### **Disable Strobe Request in FastFail Proxy Realm**

You can now enable or disable the sending of strobe requests.

When a target in a proxy realm goes into fastfail (in the [FastFail] section of the realm.pro file), it can be put back into operation by any of two events:

- Timer expiration (ResetSeconds)
- Target response to strobe request

### **Enhanced Proxy Logging at Debug**

Transactions between SBR Carrier and proxy targets are now formatted into human-readable form when TraceLevel is set to 2. Previously, transactions between SBR Carrier and proxy targets were only displayed in raw format.

The formatted messages include the client name, source address and port, the type of packet (code), the id, authenticator (*vector*), and decoded attributes. For example:

```
04/02/2008 14:26:26 Authentication Request
04/02/2008 14:26:26 Received From: ip=172.28.76.30 port=4095
04/02/2008 14:26:26 Packet : Code = 0x1 ID = 0x0
04/02/2008 14:26:26 Client Name = KENMOBILE Dictionary Name = Radius.dct
04/02/2008 14:26:26 Vector =
04/02/2008 14:26:26 000: f4df07c9 024b46c2 33a3b451 3e9bca58
|.....KF.3..Q>..X|
```

### **Enhanced Proxy Error Logging**

In order to help troubleshoot proxy issues, logging has been enhanced to show the target or realm names. Previously, proxy error messages did not specify what target was at fault.

For example:

```
08/28/2007 05:35:44 Proxy timeout on accounting request for USER1, proxy
target WAGTARGET101 (198.16.4.4), proxy realm AOLBILLING
08/28/2007 05:35:44 Sending fastfail strobe to target WAGTARGET101
08/28/2007 05:35:44 CProxyRequest::ExecForwardEx(): fastFail failed for
realm AOLBILLING
08/28/2007 05:35:44 Target WAGTARGET101 has responded to fastfail strobe
```

Target names are the actual targets that failed. These targets are configured in SBR Administrator and assigned to realms in the \*.pro files.



**NOTE:** Some log messages related to proxy continue to be sent without targets or realms, such as Proxy accounting failed, because there is no specific information at the level they are issued. For example, a proxy accounting failure may involve several realms if static accounting is used. Specific failures are logged.

### Added SBR Log File Session Identifier

A session identifier has been added to the log file entry so that you can track entries related to the same session more easily. This capability is enabled by setting the LogSessionId = yes in the [Logging] section of radius.ini. Example:

```
11/05/2008 09:51:52.262 (0056) TxId 0x485c5f8a4911b1fa00000002: Unable to
find user test with matching password

MM/DD/YYYY hh:mm:ss:nnn (Thread Id) TxId 0x0000000000000000:00000000:
LOG-MESSAGE
```

### Consolidated [Logging] Section

Logging features have been consolidated in a new [Logging] section of the radius.ini file. These parameters were previously dispersed in multiple configuration files. The new [Logging] section includes:

```
[Logging]
LogLevel = <"0"|"1"|"2">
TraceLevel = <"0"|"1"|"2">
LogAccept = <"0"|"1">
LogReject = <"0"|"1">
EnhancedDiagnosticLogging = <"yes"|"no">
LogfileMaxMBytes = <size in megabytes>
LogfilePermissions = <owner:group permissions>
LogHighResolutionTime = <"yes"|"no">
Log-Thread-ID = <"yes"|"no">
Log-Flush-To-System = <"yes"|"no">
LogUsesUtc = <"yes"|"no">
LogSessionId = <"yes"|"no">
MaxSize = <size in bytes>
Rollover = <frequency server log file is rolled over in minutes>
```

## Modified Advanced Logging Settings

Multiple advanced logging settings are now available, some of which were previously not documented, and which were scattered in various configuration files. In addition, you previously had to restart SBR Carrier after a problem occurred in order to enable these advanced logging features.

### Higher Granularity Timestamps in Log File

The option to include higher resolution timestamps in the standard server log file (`yyyymmdd.log`) is now available. When this option is enabled, the timestamp is recorded as `hh:mm:ss.xxx`, where `xxx` expresses the number of elapsed milliseconds since the `ss` value last changed. This option is enabled by specifying `LogHighResolutionTime = yes` in the `radius.ini` file. This setting was previously in the [Configuration] section of `radius.ini`.

### Improved Diagnostics in Log File

The option to include improved diagnostics in the server log file is now available. This feature was previously not documented. When this option is enabled, more extensive logging for proxy initial requests, retries, and failures, and LDAP retries and timeouts is emitted at log level 0. (All other logging messages remain subject to the `LogLevel` setting.) This option is enabled by specifying `EnhancedDiagnosticLogging = yes` in the `radius.ini` file.

### Thread Id

The option to output thread ids in the server log file (at all log levels) is now available. This option is enabled by specifying `Log-Thread-ID = yes` in the `radius.ini` file.

Thread IDs appear in parentheses immediately after the date and time. For example:

```
08/12/2008 18:31:08 (44)Configuring licenses: licensed component =
'SynchronousRequestProvider', feature = 'functional', now enabled
08/12/2008 18:31:08 (44)Configuring licenses: licensed component =
'SynchronousRequestProvider', feature = 'number of requests within one HTTP
POST body', now allows unlimited
08/12/2008 18:31:08 (1)DCF system started
08/12/2008 18:31:08 (1)Steel-Belted Radius is operational.
08/12/2008 18:31:18 (13)Authentication Request
08/12/2008 18:31:18 (13)Received from IpAddr=172.28.81.227 Port=4851
```

## Statlog.ini Updated on HUP or USR2

The `statlog.ini` file can now be updated on a HUP or USR2 signal by setting `UpdateStatLog = 1` in the `update.ini` file.

## Authorize-Only Requests

Authorize-Only requests are supported for WiMAX and 3GPP2 (CDMA) sessions using the LDAP, SQL, or other authentication method. To support Authorize-Only requests, you need to set `AuthorizeOnly = 1` in the [Configuration] section of `radius.ini` and the request must also satisfy *all* of these conditions:

- The Access-Request contains the Service-Type attribute with a value = Authorize-Only
- Message-Authenticator is present and valid
- A session already exists in SBR Carrier for the AAA session ID (WiMAX or 3GPP2)
- The authentication method (usually SQL or LDAP) must have the `AcceptsAuthorizeOnly = 1` in the [Bootstrap] section.

## Known Problems and Limitations

---

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

### CDMA

- **Because Prepaid session IDs are kept in memory, if SBR Carrier stops, these session IDs are lost.** If this happens, the sessions must be deleted from the prepaid server; otherwise new prepaid sessions may not be available. (PR 248266)
- **To set session timeout, use the SessionTimeoutSeconds in the prepaid.att file or a Session-Timeout attribute in a Profile.** Session timeout cannot be set using a filter in the 3GPP2.ini file. (PR 248448/PR 306397)

### CoA/DM

- **If no CoA/DM license is present, the message "License check failed: ControlledDeviceMgr is disabled" appears for every client at startup.** This message is normal and does not indicate any loss of functionality. (PR 395033)
- **SBR Carrier may experience a core dump when the scscli.sh script is run if the "OnFailure" section of deviceModels.xml file contains no data.** To prevent this problem, remove the entire section instead. (PR 414255)
- **If a NAS client is configured without saving the RFC3576 CoA/DM Shared Secret password, a password appears to be configured when the client is subsequently viewed.** If unexpected results such as invalid signatures occur, make sure that the password is correctly set. (PR 420409)

- **Tagged attribute-value pairs cannot be emitted as part of a CoA/DM. Such AVPs are emitted onto the wire without the tag.** This includes JUNOS service activation VSAs such as: (PR 260849)

```
ATTRIBUTE Unisphere-Activate-Service-tag1
ERX-TAGGED-STRING-VSA(65, 1) rt
```

As a workaround, create these AVPs as hexadecimal attributes and enter the value and tag manually:

```
ATTRIBUTE Unisphere-Activate-Service-tag1
ERX-VSA(65, hexadecimal) rt
```

## Filters

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

## LDAP Authentication

- **User names with special characters such as ( ' ) may cause problems when using LDAP authentication.** If using such user names, set FilterSpecialCharacterHandling to 1 in the [Settings] section of the ldapauth.aut file. (PR 409675)
- **Careful configuration may be required to achieve maximum performance from SBR Carrier with LDAP authentication in order to divide SBR Carrier LDAP processing among the SBR Carrier server cores.** This is most important on hardware such as the Sun T-series, which has a high number of low-power virtual cores. (PR 438956)
- **Setting the MaxConcurrent setting in the ldapauth configuration files to very large values can cause Steel-Belted Radius Carrier to run out of memory and crash.** As a workaround, use smaller values of MaxConcurrent, for example less than 1000. (PR 249953)
- **Attributes are not returned when an LDAP search by user (radiusstatus = sessions\_by\_user) is performed, such as in this query:** (PR 419631)

```
./ldapsearch -p 667 -h 65.83.228.58 -D "cn=admin,o=radius" -V 2 -w radius -s
sub -b "user=ace@diamonds.net,radiusstatus=sessions_by_user,o=radius"
objectclass=*
```

To work around this issue, include the client in the search, for example:

```
./ldapsearch -p 667 -h 65.83.228.58 -D "cn=admin,o=radius" -V 2 -w radius -s
sub -b "client=hearts.com,user=ace@diamonds.net,radiusstatus=sessions_
by_user,o=radius" objectclass=*
```

## Oracle

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

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

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

## Replication

- After enabling the IP range field of a RADIUS client and performing the initial publish, further publishes and changes are no longer updated on the replica server until the range is disabled. (PR 391225)
- After a server is configured as non-replicating, it cannot be converted to a primary server. You must reinstall the server to set it up as a primary server. (PR 436725)
- Replica servers that are offline when the primary server publishes configuration data may not update correctly. (PR 284279)  
To correct this:

1. Execute on the replica:
 

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

 where:  
*name* is the DNS name of the primary server  
*address* is the IP address of the primary server  
*secret* is the shared secret that authenticates configuration downloads
2. Restart the replica.

## SBR Administrator

- Some hexadecimal values are not displayed when editing in SBR Administrator. While you are editing within a hexadecimal string, the string may not appear in the Edit Field Value dialog. If this happens, select and retype the entire value instead of trying to modify just part of the string. (PR 300841)

- **When a profile is configured in SBR Administrator, the value entered in a checklist can exceed the maximum length for the value that is specified in the dictionary file.** This does not cause any problems in Steel-Belted Radius Carrier, but if any external applications require a value with a specific length, the external application may generate an error. (PR 306944)

## SBR Core

- **The UseMasterDictionary feature may add or allow unknown attributes.** This can result in the dispatch of an incorrect packet. The problem occurs if two vendor-specific dictionaries associate the same attribute number with different types (such as string and integer). (PR 248477)
- **To open the audit log in a browser, the close-tag of the root element ("`</auditRecords >`") must be manually moved to the end of the file.** (PR 435027)
- **The proxy logging enhancement features introduced in Release 7.2 apply only to extended proxy or to realms defined in the `proxy.ini` file.** They do not apply to legacy proxy, including Proxy-As-Authentication-Method. (PR 444675)
- **The `LogSessionId` parameter in the [Logging] section of the `radius.ini` file does not function for non-WiMAX Accounting requests.** (PR 447446)
- **To allow Access-Requests with no User-Name attribute, set `AllowNoUserName = Yes` in the [Configuration] section of `radius.ini`.** (PR 390984)
- **PEAP with inner TLS may fail with Windows supplicants.** Microsoft technical support reports that in EAP-PEAP phase 2, MS PEAP does not support fragmentation on the outer packets. To prevent this, set the inner TLS packet fragmentation so that no outer fragmentation is necessary during the negotiation. Edit `tlsauth.aut`, and in the [Server\_settings] section, set `TLS_Message_Fragment_Length = 900`. (PR 254219)
- **Specifying a non-existent directory for `LogDir` in the `radius.ini` file may cause SBR Carrier to function incorrectly.** (PR 437583)
- **When a subattribute string with a length of 244 characters is specified, the expected response is not returned.** To avoid this, edit the string to reduce the number of characters to fewer than 244. (PR 298055)
- **After SBR Carrier authenticates a session and returns an Access-Accept, a RADIUS client might send an Accounting-Stop to signal that the session was not allowed for some other reason.** However, SBR Carrier does not clear a phantom session upon receiving an Accounting-Stop. The phantom session times out, but under heavy load this can lead to SBR Carrier resource depletion. (PR 423703)
- **If RADIUS VSAs are added to the session database schema, they should be defined as VARBINARY type.** (PR 412255)

- **AcctCarryOver is no longer supported because the expanded capacity of the database makes it unreasonable to write all existing sessions to a log file at one time.** (PR 297789)
- **If user concurrency is enabled after user sessions have been established, those sessions are not counted toward concurrency limits.** (PR 431438)
- **If a non-multivalued checklist attribute is added to an authentication as a response attribute prior to profile processing, the requirement that the attribute be present in the request is not enforced.** (PR 432489)

### **Session State Register Module**

- **A HUP signal reinitializes the cluster, causing SBR Carrier to enter Management mode and any IP address caches to be reinitialized.** During this reinitialization, authentication requests exhibit longer than normal latency if IP address assignment is configured. To prevent this behavior, set UpdatePlugins = 0 in the [HUP] section of update.ini file. To use the USR2 signal instead of HUP to reinitialize the cluster, set UpdatePlugins = 1 in the [USR2] section. (PR 416232)
- **Configuring redirection and concurrency together causes sessions that are rejected due to concurrency limitations to be redirected and to populate the database and may interfere with correct operation of concurrency.** (PR 422987)
- **SBR Carrier loses its connection to the database cluster if the cluster restarts for any reason.** If there is an outage of the cluster, or it is restarted, each SBR node must be restarted in order to reestablish its connection to the cluster. (PR 443694)

### **SIM Authentication**

- **When the optional SIM Module is in use and SIMAUTH is used as an EAP method, changing the order of EAP methods in SBR Administrator does not take effect.** Manually edit the eap.ini file to make the change. (PR 306868)
- **For EAP-SIM and EAP-AKA requests, the first byte of the request contains the EAP-Identifier that SBR Carrier uses to select the EAP method.** If this byte is incorrect, SBR Carrier cannot properly identify and select the EAP method. In this case, SBR Carrier may respond with a protocol the client cannot support. If the client does not support NAK, and thus cannot respond with a NAK, the request fails. (PR 303268)
- **When using the SIM authentication module with EAP-helper enabled and a profile checklist with subattributes is in use, a false authorization can be returned.** There is no workaround. In some cases, you might be able to implement a valid check if the helping authentication method is LDAP, because LDAP scripting may be able to work around the checklist issue. (PR 310988)
- **CDR: the event timestamp value is incorrect in the CdrAccounts table.** Although the event timestamp in CDRs is always erroneously set to 1970-01-01 00:00:01 (TZ = + 00:00), the actual start time is present in AccStartTimeUTC. (PR 435470)

- **Do not specify the "-host <hostname >" option in the Signalware MML "CREATE-PROCESS" command, which is responsible for starting the authGateway process used by the SIM Authentication module.** Doing so may cause the authGateway process to fail in environments where IP multipath is enabled. (PR 403141)
- **The Ulticom Signalware communications stack that is accessed by the SIM authentication module may generate false error messages in the Signalware log.** When the stack is first accessed, an 8057 message is generated if everything is working properly:
 

```
> 008057 26-Aug-2008 10:58:25 mercury.POP Info Signalware Application(s)
> Authorized.
>
```

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

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

 These are false warnings that you can ignore.

## SNMP

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

## SQL Authentication

- **Careful configuration may be required to achieve maximum performance from SBR Carrier with SQL authentication in order to divide SBR Carrier SQL processing among the SBR Carrier server cores.** This is most important on hardware such as the Sun T-series, which has a high number of low-power virtual cores. (PR 439436)

## System Requirements

- **Stand-alone servers and transition servers require 8 GB of physical memory unless configured for demonstration mode with degraded performance.** When operating in demonstration mode, the SBR Carrier software makes a best effort attempt to operate in spite of various deficiencies that would normally prevent operation due to poor performance. (PR 443318)

## WiMAX Module

- **WiMAX accounting records are too cryptic in the accounting log.** Because Class attributes are presented in a binary format, some users may prefer not to log them. (PR 291646)
- **Smart dynamic HA assignment can be used by the HAAA to assign the hHA-IP-MIP4 address.** The feature cannot currently be used by the VAAA to assign the vHA-IP-MIP4 address. (PR 415662)

## Documentation Updates

---

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

### account.ini File

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

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

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

### admin.ini File

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

```
Users = rw
IP-Pools = r
Profiles = r
```

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

### Attributes No Longer Editable or Orderable

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



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

---

### CDMA

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



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

---

### classmap.ini File

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

```
[Class]
replace = Class
```

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

### Directed Realm Configuration (.dir) File

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

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

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

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

## HTTP Digest Access Authentication

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

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

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

- EnableEricssonViGHTTPEDigestSupport
- EnableHTTPEDigestSupport

## JavaScripting

- The “JavaScripting” section in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide* fails to mention that when using JavaScripting, setting the disposition of an inner authentication request (for example, in TTLS) to discard does not suppress the sending of an Access-Reject by the outer request. (PR 404877)

## LDAP

- The LDAP Configuration Interface schema documented in the “LDAP Virtual Schema” section of Chapter 24, Using the LDAP Configuration Interface of the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*, incorrectly lists Tribe as an available attribute for session queries. This attribute should be removed from the LDAP schema. (PR 427161)

- A [RejectResponse] section should be added to the `ldapauth.aut` file described in the *Steel-Belted Radius Carrier 7.2 Reference Guide*. This section defines the attributes you want to return in an Access-Reject message. (PR 394690)

Example:

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

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

## radius.ini File

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

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

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

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

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

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

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



**NOTE:** This parameter is applicable to stand-alone servers and servers running in a Session State Register cluster.

---

**radsq1.aut File**

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

**radsq1jdbc.aut File**

- A new parameter called `MaxHardErrorRetries` should be added to the [Settings] section of the **radsq1.aut** file. This parameter is added to resolve an issue where the database disconnected due to inactivity timeout. The `MaxHardErrorRetries` parameter enables the connection to be reestablished without failing the authentication by allowing you to set the number of additional attempts you want to make after hard errors have been encountered. Default is 0. This new parameter should be added to the *Steel-Belted Radius Carrier 7.2 Reference Guide*. (PR 410408)

**RFC 5281**

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

*RFC 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TLSv0)* P. Funk, S. Blake-Wilson. August 2008.

**Session State Register**

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

[Configuration] Section

`DiscardAccountingRequestOnCstFailure = 1`

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

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

[Configuration] Section

`DiscardAccessRequestOnCstFailure = 1`

- If set to 1, authentication requests requiring access to the session database are discarded when the session database cannot be contacted.

- If set to 0, SBR Carrier sends an Access-Reject when the session database cannot be contacted.



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

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

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

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

Default value is 250.

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

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

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

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

Guidelines for the assignment of node IDs:

- 0 is for internal use.
- 1–48 are for clustered data nodes (41-48 for stand-alone or transition servers).
- 49 is for SBR nodes on stand-alone or transition servers.

- 50 is for management nodes on stand-alone or transition servers.
- 51–59 are for clustered management nodes.
- 60 is for management nodes on stand-alone or transition servers.
- 61–59 are for clustered management nodes (a function of base node ID + 10).
- 70–99 are reserved for future use.
- 100–149 are for clustered SBR nodes.
- 150–255 are reserved for future use.
- 256 and higher are not supported and are illegal.



**NOTE:** If striping is enabled, you are restricted to the range 1–N for data node IDs where N is the total number of data nodes in the cluster. See “Striping Data Nodes (PR 440803)” on page 25.

---

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

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

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

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

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

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

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

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

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

Similar prompts appear when configuring stand-alone SBR Carrier servers.

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

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

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

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

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

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

## SIM Authentication

- In the *Steel-Belted Radius Carrier 7.2 Reference Guide*, these parameters should be added under the [Settings] section of the `locspec.ctrl` file: (PR 433201)

```

OperatorNameAttribute    = TeliaSonera-Operator-Name
VisitedOperatorIdAttribute = TeliaSonera-Visited-Operator-ID
LocationInformation      = TeliaSonera-Location-Information
LocationNameAttribute    = TeliaSonera-Location-Name

```

- The following note should be added to the `PseudonymSecret` parameter in the [Settings] section of the `simauth.aut` file in the *Steel-Belted Radius Carrier 7.2 Reference Guide*: (PR 414526)



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

---

## Statlog.ini

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

**Parameter:** UpdateStatLog

**Description:**

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

Default value is 1 in the [HUP] section.  
 Default value is 0 in the [USR2] section.

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

## ttlsauth.aut File

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

## Leading Wildcards and Session Queries

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

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

## Resolved Issues

---

These issues were identified in previous releases of Steel-Belted Radius and have been resolved in Steel-Belted Radius Carrier Release 7.2. The identifier in parentheses is the Problem Report number in our bug database.

- The default `filter.ini` does replicate successfully. (PR 249955)
- During installation of Steel-Belted Radius Carrier as a primary server, false error messages in the log may report that the primary designation did not succeed. (PR 304413)
- Accounting Start is not classified as WiMAX Acct Request in ASN-GW initial accounting-start request and ASN-GW Reauth accounting-start and accounting-stop. (PR 297773)
- Stored procedures may prevent correct server initialization. (PR 256084)
- SIM-functionality: EAP-Helper with profile checklist containing subattributes is not working. (PR 310988)
- Some Accounting Start commands are not correctly classified as WiMAX Acct Request in ASN-GW initial accounting-start request, ASN-GW Reauth accounting-start, and accounting-stop. To avoid this, ensure that the Accounting Request contains the NAS-Identifier or configure the RADIUS client for the specific client (not ANY) and ensure that the configured client name is the expected NAS-Identifier. (PR 297773)
- LCI sessions query now returns the first 100 sessions by NAS Name, which allows the use of browsers for testing and exploration of the schema; however, it is not useful in production. We recommend you use the `sessions_by_x` command in a production environment. (PR 418922)
- A macro setting has been added to support VSAs that require a Continuation field (in subattributes) for support of CoA/DM. `cbytes` specifies the length in octets of the continuation field (typically 1). In this release, the field is always filled with 0. To disable use of the field, remove the `cbyte` attribute from the macro: (PR 425281)

```
MACRO WiMAX-VSA(t,s) 26 [vid = 24757 type1 = %t% len1 = + 3 fill1 = 0
cbytes = 1 data = %s%]
```

- **SBR Carrier is disconnecting the ODBC connection to the SQL server unnecessarily when one of the following three error types occurs:**

(PR 249927)

- The data being written is too long for the field that SBR Carrier is trying to write to.
- The data being written to SQL does not match the specified data-type in SQL.
- Some databases only allow a certain record to be written once.

SBR Carrier no longer disconnects in any of these cases. It now drops the data, logs the error, and continues processing.

- **(CoA/DM) It was not previously possible to look up sessions by all documented searchable attributes using the command-line utility (`scscli.sh`).** All searchable attribute fields now operate correctly. These fields include: (PR 410489)

Acct-Multi-Session-Id  
 Acct-Session-Id  
 Called-Station-Id  
 Calling-Station-Id  
 Framed-IP-Address  
 NAS-Identifier  
 NAS-IP-Address  
 User-Name  
 Funk-Session-Handle  
 Funk-Attribute-Range



**NOTE:** Funk-Session-Handle is used to refer to the *unique session ID* of the session, and it must match the format of the *handle* returned in the response to a Query action. This attribute is used to target a specific session exactly.

---



**NOTE:** Funk-Attribute-Range is a special attribute used exclusively in SBR Administrator to query for a range of Framed-IP-Addresses or NAS-IP-Addresses.

---

If any additional search fields are required, the Current Sessions Table (CST) customization procedure must be used to add a single-valued index to the field in the `CurrentSessions.sql` file, followed by customization of `dbc_mapping.xml` to map a RADIUS attribute name to the field in a queryAttribute statement. This procedure is shown in the CoA deployment example for WiMAX in “Example CoA/DM Configuration” in the *Steel-Belted Radius Carrier 7.2 Administration and Configuration Guide*. The CST customization procedure is described in “Customizing the SSR Database Current Sessions Table” in the *Steel-Belted Radius Carrier 7.2 Installation Guide*.

If a query is executed that contains *no* supported search attributes, then all attributes presented are interpreted as *action* attributes and added to the CoA engine session request. The query is unconstrained in this case, and the first *limit* sessions from the CST is affected by the query. For this reason, we recommend you set a small limit parameter during testing of new scscli command lines during development.



**NOTE:** If a non-existent attribute is used in a search, SBR Carrier does not send Disconnect Messages to the NAS. Instead, the reply sent to the client contains the list of sessions with the session result as being incomplete, a non-zero resultcode and result message saying “need more info...”. The resulting log message reads as follows (for example):

"Action 'DM' was completed against device 'PFARRELL-755' with result: 'need more information to format session control request'"

## Related Documentation

Table 5 lists and describes the Steel-Belted Radius Carrier documentation set:

**Table 5: Steel-Belted Radius Carrier Documentation**

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



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

## Requests for Comments (RFCs)

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

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

RFC Number	Title
RFC 1035	<i>Domain Names - Implementation and Specification</i> . P. Mockapetris. November 1987.
RFC 1155	<i>Structure and Identification of Management Information for TCP/IP-based Internets</i> . M. Rose, K. McCloghrie, May 1990.

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

<b>RFC Number</b>	<b>Title</b>
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II.</i> K. McCloghrie, M. Rose, March 1991.
RFC 2006	<i>The Definitions of Managed Objects for IP Mobility Support using SMIPv2.</i> D. Cong and others. October 1996.
RFC 2246	<i>The TLS Protocol.</i> T. Dierks, C. Allen. January 1999.
RFC 2271	<i>An Architecture for Describing SNMP Management Frameworks.</i> D. Harrington, R. Presuhn, B. Wijnen, January 1998.
RFC 2284	<i>PPP Extensible Authentication Protocol (EAP).</i> L. Blunk, J. Vollbrecht, March 1998.
RFC 2433	<i>Microsoft PPP CHAP Extensions.</i> G. Zorn, S. Cobb, October 1998.
RFC 2548	<i>Microsoft Vendor-specific RADIUS Attributes.</i> G. Zorn. March 1999.
RFC 2607	<i>Proxy Chaining and Policy Implementation in Roaming.</i> B. Aboba, J. Vollbrecht, June 1999.
RFC 2618	<i>RADIUS Authentication Client MIB.</i> B. Aboba, G. Zorn. June 1999.
RFC 2619	<i>RADIUS Authentication Server MIB.</i> G. Zorn, B. Aboba. June 1999.
RFC 2620	<i>RADIUS Accounting Client MIB.</i> B. Aboba, G. Zorn. June 1999.
RFC 2621	<i>RADIUS Accounting Server MIB.</i> G. Zorn, B. Aboba. June 1999.
RFC 2622	<i>PPP EAP TLS Authentication Protocol.</i> B. Aboba, D. Simon, October 1999.
RFC 2809	<i>Implementation of L2TP Compulsory Tunneling via RADIUS.</i> B. Aboba, G. Zorn. April 2000.
RFC 2865	<i>Remote Authentication Dial In User Service (RADIUS).</i> C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
RFC 2866	<i>RADIUS Accounting.</i> C. Rigney. June 2000.
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support.</i> G. Zorn, B. Aboba, D. Mitton. June 2000.
RFC 2868	<i>RADIUS Attributes for Tunnel Protocol Support.</i> G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. June 2000.
RFC 2869	<i>RADIUS Extensions.</i> C. Rigney, W. Willats, P. Calhoun. June 2000.
RFC 2882	<i>Network Access Servers Requirements: Extended RADIUS Practices.</i> D. Mitton. July 2000.
RFC 3046	<i>DHCP Relay Agent Information Option.</i> M. Patrick. January 2001.
RFC 3118	<i>Authentication for DHCP Messages.</i> R. Droms and others. June 2001.
RFC 3162	<i>RADIUS and IPv6.</i> B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3344	<i>IP Mobility Support for IPv4.</i> C. Perkins. August 2002.
RFC 3539	<i>Authentication, Authorization, and Accounting (AAA) Transport Profile.</i> B. Aboba, J. Wood. June 2003.
RFC 3575	<i>IANA Considerations for RADIUS (Remote Authentication Dial-In User Service).</i> B. Aboba, July 2003.
RFC 3576	<i>RFC3576 - Dynamic Authorization Extensions to Remote to Remote Authentication Dial In User Service.</i> Network Working Group, 2003
RFC 3579	<i>RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).</i> B. Aboba, P. Calhoun, September 2003.
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.</i> P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.

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

<b>RFC Number</b>	<b>Title</b>
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II.</i> K. McCloghrie, M. Rose, March 1991.
RFC 2006	<i>The Definitions of Managed Objects for IP Mobility Support using SMIPv2.</i> D. Cong and others. October 1996.
RFC 2246	<i>The TLS Protocol.</i> T. Dierks, C. Allen. January 1999.
RFC 2271	<i>An Architecture for Describing SNMP Management Frameworks.</i> D. Harrington, R. Presuhn, B. Wijnen, January 1998.
RFC 2284	<i>PPP Extensible Authentication Protocol (EAP).</i> L. Blunk, J. Vollbrecht, March 1998.
RFC 2433	<i>Microsoft PPP CHAP Extensions.</i> G. Zorn, S. Cobb, October 1998.
RFC 2548	<i>Microsoft Vendor-specific RADIUS Attributes.</i> G. Zorn. March 1999.
RFC 2607	<i>Proxy Chaining and Policy Implementation in Roaming.</i> B. Aboba, J. Vollbrecht, June 1999.
RFC 2618	<i>RADIUS Authentication Client MIB.</i> B. Aboba, G. Zorn. June 1999.
RFC 2619	<i>RADIUS Authentication Server MIB.</i> G. Zorn, B. Aboba. June 1999.
RFC 2620	<i>RADIUS Accounting Client MIB.</i> B. Aboba, G. Zorn. June 1999.
RFC 2621	<i>RADIUS Accounting Server MIB.</i> G. Zorn, B. Aboba. June 1999.
RFC 2622	<i>PPP EAP TLS Authentication Protocol.</i> B. Aboba, D. Simon, October 1999.
RFC 2809	<i>Implementation of L2TP Compulsory Tunneling via RADIUS.</i> B. Aboba, G. Zorn. April 2000.
RFC 2865	<i>Remote Authentication Dial In User Service (RADIUS).</i> C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
RFC 2866	<i>RADIUS Accounting.</i> C. Rigney. June 2000.
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support.</i> G. Zorn, B. Aboba, D. Mitton. June 2000.
RFC 2868	<i>RADIUS Attributes for Tunnel Protocol Support.</i> G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. June 2000.
RFC 2869	<i>RADIUS Extensions.</i> C. Rigney, W. Willats, P. Calhoun. June 2000.
RFC 2882	<i>Network Access Servers Requirements: Extended RADIUS Practices.</i> D. Mitton. July 2000.
RFC 3046	<i>DHCP Relay Agent Information Option.</i> M. Patrick. January 2001.
RFC 3118	<i>Authentication for DHCP Messages.</i> R. Droms and others. June 2001.
RFC 3162	<i>RADIUS and IPv6.</i> B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3344	<i>IP Mobility Support for IPv4.</i> C. Perkins. August 2002.
RFC 3539	<i>Authentication, Authorization, and Accounting (AAA) Transport Profile.</i> B. Aboba, J. Wood. June 2003.
RFC 3575	<i>IANA Considerations for RADIUS (Remote Authentication Dial-In User Service).</i> B. Aboba, July 2003.
RFC 3576	<i>RFC3576 - Dynamic Authorization Extensions to Remote to Remote Authentication Dial In User Service.</i> Network Working Group, 2003
RFC 3579	<i>RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).</i> B. Aboba, P. Calhoun, September 2003.
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.</i> P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.

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

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

### **3GPP and 3GPP2 Technical Specifications**

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

### **WiMAX Technical Specifications**

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

### **Third-Party Products**

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

### **Obtaining Documentation**

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

## 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/cgi-bin/docbugreport>. If you are using e-mail, be sure to include the following information with your comments:

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

## Requesting Technical Support

---

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

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

## Self-Help Online Tools and Resources

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

- Find CSC offerings:  
<http://www.juniper.net/customers/support/>
- Search for known bugs:  
<http://www2.juniper.net/kb/>
- Find product documentation:  
<http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base:  
<http://kb.juniper.net/>
- Download the latest versions of software and review release notes:  
<http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:  
<https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager:  
<http://www.juniper.net/cm/>

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

### **Opening a Case with JTAC**

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

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

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

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

When you contact technical support, be ready to provide:

- Your Steel-Belted Radius Carrier release number (for example, Steel-Belted Radius Carrier Release 7.x).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- A detailed description of the problem.
- Any documentation that may help in resolving the problem, such as error messages, core files, compiler listings, and error or RADIUS log files.

## General Statement of Compliance

Table 7 lists Steel-Belted Radius Carrier Release 7.2 compliance with applicable RFCs.

**Table 7: Compliance of Steel-Belted Radius Carrier Release 7.2 with Applicable RFCs**

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

**Table 7: Compliance of Steel-Belted Radius Carrier Release 7.2 with Applicable RFCs**

<b>RFC Number</b>	<b>Name</b>	<b>Notes</b>
2989	Criteria for Evaluating AAA Protocols for Network Access	—
3012	Mobile IPv4 Challenge/Response Extensions	—
3162	RADIUS and IPv6	—
3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	—
3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	—
3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	—
3748	Extensible Authentication Protocol (EAP)	—
3770	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks	—
4005	Diameter Network Access Server Application	—
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)	—
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	h3Sumal	Previous version (RFC 2618) supported
4669	RADIUS Authentication Server MIB for IPv6	Previous version (RFC 2619) supported
4670	RADIUS Accounting Client MIB for IPv6	Previous version (RFC 2220) supported
4671	RADIUS Accounting Server MIB for IPv6	Previous version (RFC 2221) supported
4672	RADIUS Dynamic Authorization Client MIB	Not supported

**Table 7: Compliance of Steel-Belted Radius Carrier Release 7.2 with Applicable RFCs**

<b>RFC Number</b>	<b>Name</b>	<b>Notes</b>
4673	RADIUS Dynamic Authorization Server MIB	Not supported
4675	RADIUS Attributes for Virtual LAN and Priority Support	Not supported
4679	DSL Forum Vendor-Specific RADIUS Attributes.	Not supported
4746	Extensible Authentication Protocol (EAP) Password Authenticated Exchange	Not supported
4763	Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)	Not supported
4764	The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method.	Not supported
4793	The EAP Protected One-Time Password Protocol (EAP-POTP)	EAP-32
4818	RADIUS Delegated-IPv6-Prefix Attribute.	—
4849	RADIUS Filter Rule Attribute	—
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	Not supported
4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management	—
5030	Mobile IPv4 RADIUS Requirements	—
5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes	—
5090	RADIUS Extension for Digest Authentication	—
5106	The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method	—
5169	Handover Key Management and Re-Authentication Problem Statement	—
5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	—
5216	The EAP-TLS Authentication Protocol	Previous version (RFC 2716) supported
—	3GPP2 X.S0011-D, Version: 1.0, Version Date: February, 2006	MIPv6 not supported
5281	Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) P. Funk, S. Blake-Wilson. August 2008.	—

Table 8 lists the protocols supported in Steel-Belted Radius Carrier Release 7.2.

**Table 8: Protocols Supported in SBR Carrier Release 7.2**

Protocol	Notes
UDP	—
IPv4	—
IPv6	NAS-server only
DHCP v2	—
DHCP v3	—
LDAP v2	—
LDAP v3	Not LCI
JDBC	—
Oracle (SQL)	—
XML	Configuration
HTTP v1.1	Admin
LEAP	—
WiMAX NWG 1.2.2	<i>Except CRs 801, 823, OMA/DM</i>
3GPP2	—
3GPP2 X.S0011-D	—
3GPP	RADIUS only
23.234 (RADIUS)	WLAN UE
29.061 (RADIUS)	G1 and Pk reference points
TISPAN	RADIUS only Interface E5
ES282.001	—
ES282.004	—
ES283.034	—
ES283.035	—

