

Steel-Belted Radius[®] Carrier Release

Notes

Release 7.2.4
13 December 2010
Revision 1

These Release Notes support Release 7.2.4 of Steel-Belted Radius Carrier (SBRC). Before you install or use your new software, read these Release Notes in their entirety, especially “Known Problems and Limitations” on page 7.

Contents

Release Overview	3
Before You Start	3
Documentation	3
Release Highlights	3
SSR Performance Improvements	3
Support for Oracle 11	4
Standalone Server Changes	4
Accounting Log Changes	4
System Requirements	4
Software	4
Perl	4
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 Standalone Server Products	6
Supported Releases for Standalone Server	6
Migrating from SBR Release 5.5 High Availability	7
Using a Transition Server	7
Known Problems and Limitations	7
CDMA	7
CoA/DM	8
Filters	8
Lawful Intercept	8
LDAP Authentication	8
Replication	8

SBRC Administrator	9
SBRC Core	9
Session State Register Module	10
SIM Authentication	13
SMS Authorization	14
SNMP	14
WiMAX Module	14
Documentation Updates	15
Accounting	15
authlog.ini File	15
LDAP	16
Logging	16
Oracle	17
radius.ini File	17
Realm JavaScript	18
Replication	18
SNMP	18
SQL Data Accessor	18
System Requirements	19
wimax.ini File	19
Resolved Issues	20
Release 7.2.4	20
Related Documentation	22
Requests for Comments (RFCs)	22
3GPP and 3GPP2 Technical Specifications	25
WiMAX Technical Specifications	25
Third-Party Products	25
General Statement of Compliance	25
SBR Carrier Documentation and Release Notes	30
Documentation Feedback	30
Requesting Technical Support	31
Self-Help Online Tools and Resources	31
Opening a Case with JTAC	32
Revision History	32

Release Overview

These release notes cover Release 7.2.4 of the Juniper Networks Steel-Belted Radius Carrier product.

Before You Start

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

Documentation

Table 1 on page 3 lists and describes the Steel-Belted Radius Carrier documentation set:

Table 1: Steel-Belted Radius Carrier Documentation

Document	Description
<i>Steel-Belted Radius Carrier Installation Guide</i>	Describes how to install the Steel-Belted Radius Carrier software on the server and the SBRC Administrator application on a client workstation.
<i>Steel-Belted Radius Carrier Administration and Configuration Guide</i>	Describes how to configure and operate the Steel-Belted Radius Carrier and its separately licensed modules.
<i>Steel-Belted Radius Carrier Reference Guide</i>	Describes the settings and valid values of the Steel-Belted Radius Carrier configuration files.
<i>Steel-Belted Radius Carrier 7.2.4 Release Notes</i>	Contains the latest information about features, changes, known problems, and resolved problems in Release 7.2.4.



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

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

Release Highlights

Highlights include the following product enhancements:

SSR Performance Improvements

Performance and reliability improvements have been made to SSR. The performance improvement is enabled by default in a new installation, or after executing the proper upgrade procedure described in “Upgrading Your SSR Cluster” section in the *Steel-Belted Radius Carrier 7.2.4 Installation Guide*. Be sure to follow the steps in your respective upgrade procedure to avoid migration and incompatibility issues with previous releases of Steel-Belted Radius Carrier running the SSR feature.

Support for Oracle 11

Steel-Belted Radius Carrier now has native support for Oracle 11 databases.

Standalone Server Changes

For a standalone server, the current sessions table (CST) is now in local memory, and is configured with the **dbclusterlocal.gen** file when you run the configuration script. You cannot configure field names in the local CST. However, there are three predefined fields and seven generic fields you can configure using the **sessionTable.ini** file. For details, see Chapter 6, “Installation and Basic Configuration of a SBR Carrier Standalone Server,” in the *Steel-Belted Radius Carrier 7.2.4 Installation Guide*, and Chapter 22, “Setting Up the LDAP Directory to Store SMS and CDR Records When Running in Standalone Mode,” in the *Steel-Belted Radius Carrier 7.2.4 Reference Guide*.

- In SBR/HA 5.5 and SBR Carrier Release 7.0, the settings for storing CDR and SMS records in a remote LDAP server were configured in the **ss7ldapdb.gen** file. When running SBR Carrier Release 7.2.4 in the standalone mode, these settings are configured in the **ss7db.gen** file. When migrating from SBR/HA 5.5 or SBRC Release 7.0, to Release 7.2.4, you need to move these settings from the **ss7ldapdb.gen** file to the **ss7db.gen** file.

Accounting Log Changes

Failed accounting requests are now logged by configuring the **acctReport.ini** file. The accounting log records all accounting request failures by logging them in a comma-delimited text file. While viewing the logs, you can sort, search, and filter the log records. Each record includes details of what happened during the accounting request. The accounting log records failures due to bad shared secrets and unknown clients.

System Requirements

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

Software

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

- Solaris Update 6 is required
- Update 8 is recommended, for Oracle 11 support

Perl

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

Supported Browsers

The SBRC Administrator configuration application can be launched from the browsers listed in Table 2 on page 5.

Table 2: 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, 10, and 11 are supported; version 11.2.0 is recommended.
- For the Steel-Belted Radius Carrier to act as an Oracle native client, the 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 must be installed in the server before you install SBR Carrier software.

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



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

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

After the base Signalware 9 software is installed, use the Signalware installation program to install the patch. For specific directions, refer to the Signalware documentation. To see a sample procedure for applying the

patch, see “Installing Signalware Service Pack 5T” in the *SBR Carrier Installation Guide*.

.....
The Signalware PH0301 and XH0303 boards are supported.

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

Modified Open-Source Software

Embedded in this version of Steel-Belted Radius Carrier is open-source software that Juniper Networks 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 31.

Migrating from Earlier SBR Releases

SBR Carrier Release 7.2.4 can run as a standalone server or as part of a Session State Register cluster.

Migrating from Earlier SBR Standalone Server Products

You can use the configuration script to move a number of files from selected previous SBR releases to the Release 7.2.4 environment when installing Steel-Belted Radius Carrier. The corresponding Release 7.2.4 files are also loaded on the system, but are not activated. You are responsible for merging new settings from Release 7.2.4 configuration files into the working (pre-existing) configuration files. To support new features, SBR Carrier uses default values for any new settings that have not been merged into the working configuration files.

Supported Releases for Standalone Server

You can migrate configuration files from these SBR server releases to Release 7.2.4:

- 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 and previous 7.2.x releases

For complete details on migrating from these releases, see the *SBR Carrier 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 7.2.4 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 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 the sessions 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 7.2.4 software on them, and then bring them back online as a Release 7.2.4 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 *SBR Carrier Installation Guide*.

Known Problems and Limitations

These issues have been identified in Steel-Belted Radius Carrier 7.2.4. The identifier in parentheses is the Problem Report number in our bug database.

CDMA

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

CoA/DM

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

Filters

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

Lawful Intercept

- **Lawful Intercept is not operational when Juniper Networks MX Series or ERX Series devices are deployed.** (PR 568968 and PR 390311)

LDAP Authentication

- **Setting the MaxConcurrent setting in the ldapauth configuration file 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)

Replication

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

1. Execute on the replica:

```
# 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.

SBRC Administrator

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

SBRC Core

- **The UseMasterDictionary feature may add or allow unknown attributes.** This can result in the dispatch of an incorrect packet. The problem occurs if two vendor-specific dictionaries associate the same attribute number with different types (such as string and integer). (PR 248477)
- **To open the audit log in a browser, the close-tag of the root element ("`</auditRecords>`") must be manually moved to the end of the file.** (PR 435027)
- **The proxy logging enhancement features introduced in Release 7.2.2 apply only to extended proxy or to realms defined in the proxy.ini file.** They do not apply to legacy proxy, including Proxy-As-Authentication-Method. (PR 444675)
- **If SBR Carrier receives an Accounting-Start message after the Accounting-Stop message for the same session has already been processed, SBR Carrier will create a new session that will only be removed by stale session purging.** (PR 447739)
- **PEAP with inner TLS may fail with Windows supplicants.** Microsoft technical support reports that in EAP-PEAP phase 2, MS PEAP does not support fragmentation on the outer packets. To prevent this, set the inner TLS packet fragmentation so that no outer fragmentation is necessary during the negotiation. Edit `tlsauth.aut`, and in the `[Server_settings]` section, set `TLS_Message_Fragment_Length=900`. (PR 254219)
- **If the location of the logging directory is changed from the default, make sure that the directory exists before starting SBRC.** Otherwise, SBRC may fail to function correctly. (PR 437583)
- **When a subattribute string with a length of 244 characters is specified, the expected response is not returned.** To avoid this situation, edit the string to reduce the number of characters to fewer than 244. (PR 298055)
- **If RADIUS vendor-specific attributes (VSAs) are added to the session database schema, they should be defined as VARBINARY type.** (PR 412255)
- **AcctCarryOver is no longer supported because the expanded capacity of the database makes it unreasonable to write all existing sessions to a log file at one time.** This issue applies to servers running standalone and in an SSR cluster. (PR 297789)
- **If user concurrency is enabled after user sessions have been established, those sessions are not counted toward concurrency limits.** (PR 431438)

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

Session State Register Module

- **The OverwriteCstDataOnFailure feature that was introduced as a hotfix to the SBR/HA Release 5.5x is not functional in Release 7.2.4. This hotfix was introduced to enable session database constraint violations to trigger replacement of old sessions by new sessions when Accounting-Stops are dropped by the network.** (PR 309958)
- **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)
- **Although WimaxAcctFlows is included in the session table, it is not displayed by the ShowSessions script.** This is normal, as it consists of binary data and is not readable. (PR 440624)

- **SBR Carrier Cluster IP address allocation is limited to caching 30,000 IP addresses per SBRC front-end node.** If any front-end node is configured to cache more than a total of 30,000 IP addresses via `dbclusterndb.gen`, then this SBRC node cannot correctly clear up cached addresses on a restart. These failed restarts can lead to large amounts of leaked IP addresses that are no longer available for use until manually cleaned up via SQL. The `ClearCache.sh` administration script cannot correct this situation since it will also fail to clear the address cache in this situation. Customers should cap their total caching at 30,000 IP addresses for each front-end node, proportionally reducing the recommended cache sizes for their pools until the total is less than 30,000 IP addresses. (PR 486733)
- NDB nodes for the MySQL versions that ship with SBRC release 7.4 cluster perform better when the number of virtual processors equals the number of physical processors. Care must be taken to turn off the right virtual processors, to avoid turning an entire physical CPU off and having two virtual processors run on one physical processor. For an M3000 (a recommended platform), which defaults with eight virtual processors, the command to disable the extra processors is `psradm -f 1357`. This command turns off every other virtual processor, leaving one virtual processor per physical processor. (PR 488756)
- **A new setting in the config.ini file for HeartBeatOrder may alleviate certain issues. This is not set by default; it must be configured manually. This change can be applied with rolling restarts for most customers.**

For proper functioning, a certain proportionality must exist between each OSI stack level failure condition, specifically between the NAS clients to the RADIUS front ends, the RADIUS S node to the D nodes, and among the ndb and dbapi nodes (M nodes to D nodes). That dependency has to do with timeout values associated within the network and the NDB itself.

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

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

- If using IPMP, the IPMP probe value should be lower than twice the heartbeat timeout appropriate for the connection. (Defaults for the S or M nodes to the D nodes are controlled by the `/opt/JNPRhadm/config.ini` file on the M nodes; the value is set by `HeartBeatIntervalDbApi` and is 1500ms by default, and the inter-D node timeout is `HeartBeatIntervalDbDb` and is 200ms by default.) Widely divergent values may impact performance in the failure case, leading to unexpected outage.
- HeartBeats are implemented in and among the D nodes so that failures are more quickly detected than the underlying TCP failure mechanism can detect. The initial

detection of fault happens after four times the HeartBeatInterval. After that is detected, the D nodes attempt to repartition and form a valid cluster. This operation can take several to many seconds, depending on the type and mode of failure: single D node hard failures or hard networking loss are generally quickest; complete cluster splits (which, under the correct network design, require two underlying faults to happen) and serious network faults (dropped connections and interfaces that are down are detectable more easily than intermittent or one-way failing connection scenarios) take longer to detect and compensate for.

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

- During an extended loss of service due to significant failure (such as loss of connectivity between two halves of a cluster), SBRC might need to reconnect to the new cluster to continue processing, and failures of reconnection are managed by timers set by the [Ndb] values DelayBetweenConnectRetriesSec and ReconnectRetriesin in the **dbclusterndb.gen** file. Setting these values higher than the defaults may make the system more resilient at the expense of a period of dropped RADIUS traffic. Setting TimeoutForFirstAliveSec and TimeoutAFterFirstALiveSec lower may also increase resiliency.
- During processing, some ndb operations are designed to be retried to attempt to avoid lock contention. Setting the dbclusterndb.gen [Database] section Retries and DelayBetwenRetriesMillisec value higher may improve effective performance and decrease delays in cases where the underlying network is prone to latency or dropped packets.
- In cases where the underlying network is prone to short or long periods of latency, fault, or other unexpected cases, setting the values of HeartBeatInterval higher (and setting all the proportionally related values appropriately) may make the system more resilient. The trade-off is fast detection of serious failures (and after a failure, spending extra time setting up connections again) against the acceptance of temporary processing delays due to minor faults that are otherwise survivable.
- There is a known error in ndb for serious cluster failure (requiring automatic restarts of a node) under extended one-way traffic failure of the inter-D and SM-D network. Correct network design should not permit this to happen: IPMP probes with the correct values, for instance, cause this to fail over to a working link. A ticket has been entered with Oracle and we are working closely with NDB engineers on addressing this problem. The HeartBeatOrder fix mentioned previously addresses temporary instances of this type of failure.
- There is a known bug in ndb for automatically restarting nodes. Certain, limited failure conditions (usually associated with serious, extended, and pathological network dysfunctions, mentioned previously) at restart may require a manual restart. A ticket has been entered with Oracle and we are working closely with NDB engineering on addressing this problem.
- The default settings of CacheLowWater, CacheHighWater, and CacheChunkSize may cause badly degraded performance. The defaults cannot be made higher because one S node can pre-cache all the addresses in a small pool if the

CacheLowWater is set higher than the number of addresses in a pool. Default to a CacheLowWater and CacheChunkSize related to the transaction rate of new address allocations for your installation so you are not too likely run out of addresses before the threads can fill up cache, and use Per-Pool settings to set any small pools much lower than the default.

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

- **If you start a management (m or sm) node without running the “configure 2 (create a new cluster definition)” option, as you would in the case of a rolling restart upgrade from Release 7.2.x to Release 7.2.4, you will see multiple warnings such as the following:**



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

These warnings can be safely ignored.

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

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

SIM Authentication

- **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 the optional SIM Module is in use and SIMAUTH is used as an EAP method, changing the order of EAP methods in SBRC Administrator does not take effect.** Manually edit the `eap.ini` file to make the change. (PR 306868)
- **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)
- **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)

- **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)
- **The Call Detail Record (CDR) accounting module is not functional in Release 7.2.4.** (PR 571405)
- **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.

SMS Authorization

- **SMS authorization is not enabled in Release 7.2.4 of SBR Carrier. This is a known issue for which there is no known workaround.** (PR 566092)

SNMP

- **For the cluster version of SBRC, 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:
 - 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. (PR 249876)

WiMAX Module

- **WiMAX accounting records are too cryptic in the accounting log.** Because Class attributes are presented in a binary format, some users may prefer not to log them. (PR 291646)
- **Care must be taken to ensure the .aut file used for authentications is separate from the .aut file used for Authorize-Only requests, even though the two files may be using the same database table.** Also the authorizeOnly.aut file should not be able to handle or pass any authentications. (PR 411144)

- **Smart Dynamic Home Agent (HA) Assignment can be used by the HAAA to assign the hHA-IP-MIP4 address.** The feature cannot currently be used by the VAAA to assign the vHA-IP-MIP4 address. (PR 415662)

Documentation Updates

Information in this section updates the published Steel-Belted Radius Carrier 7.2.4 documentation set. The identifier in parentheses is the Problem Report number in our bug database.

Accounting

- In the *Steel-Belted Radius Carrier 7.2.4 Reference Guide*, the default setting for the **Enable** parameter in the [Settings] section of the `account.ini` file should say: "Default value is 1 for enabled." The line that reads: "To enable accounting logging, set Enable =1 and restart the SBRC server" should be removed. (PR 505728)
- The following note should be added to the "LDAP Configuration Interface Overview" section on page 339 of the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide*: (PR 539207)



NOTE: The LDAP-SQL bridge, previously shipped as part of SBR HA 5.5, has been replaced by SBRC's LDAP Command Interface (LCI).

To use, enter a search query such as:

```
1dapsearch -V2 -h localhost -p667 -D "cn=admin, o=radius" -w radius -s
sub -b "framed-ip-address=10.1.105.122, radiusstatus=sessions_by_ipaddress,
o=radius" framed-ip-address="*"
```

This search produces the following output:

```
dn:acct-session-id=f9248bc54c60230c003d9fbd00000000,
client=10.13.101.201,framed-ip-address=10.1.105.122,
radiusstatus=sessions_by_ipaddress,o=radius
objectclass: top
objectclass: radiusstatus
radiusstatus: sessions_by_ipaddress
client: 10.13.101.201
acct-session-id: 13
nas-ip-address: 192.168.1.16
nas-port: 0
framed-ip-address: 10.1.105.122
session-start-time: 1281473604
fullname: TEST
elapsed: 616
```

authlog.ini File

- A new parameter called `LogAssignedIpAddress` should be added to the [Settings] section of the `authlog.ini` file in the *SBR Carrier Reference Guide*. This parameter is added to resolve the issue where the framed IP address is not written to the `authlog.ini` file. The default value is 0 (Disable). To enable this parameter, set it to 1. (PR 532978)

If this parameter is disabled, the framed IP address will not be displayed in the **authlog.ini** file as Assigned-IP-Address. If this parameter is enabled, the framed IP address will be displayed in the **authlog.ini** file as Assigned-IP-Address. Here is a sample output displaying the header and log message:

Header:

```
"Date", "Time", "RAS-Client", "Full-Name", "Acc/Rej", "User-Name", "NAS-IP-Address", "NAS-Port",
"Service-Type", "Framed-Protocol", "Framed-IP-Address", "Framed-IP-Netmask", "Framed-Compression",
"Login-IP-Host", "Callback-Number", "State", "Called-Station-Id", "Calling-Station-Id", "NAS-Identifier",
"Proxy-State", "Event-Timestamp", "NAS-Port-Type", "Port-Limit", "Login-LAT-Port", "Assigned-IP-Address"
```

Log Message:

```
"11/11/2010", "01:42:51", "<ANY>", "ROOT", "ACCEPT", "ROOT",
"10.206.144.123", "1975",,,,,, "t1.internet",,,,, "2",,, "10.206.144.1"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1976",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.5"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1977",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.7"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1978",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.8"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1979",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.10"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1980",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.14"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1981",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.15"
"11/11/2010", "01:43:06", "<ANY>", "ROOT", "ACCEPT", "ROOT", "10.206.144.123", "1982",,,,,, "
t1.internet",,,,, "2",,, "10.206.144.16"
```

LDAP

- Usernames with special characters such as (') may cause problems when using LDAP authentication. If using such usernames, set FilterSpecialCharacterHandling to 1 in the [Settings] section of the ldapauth.aut file. (PR 409675)
- A new parameter has been added to the [CRL_Checking] section of the tlsauth.aut, tlsauth.eap, and ttlsauth.aut files to enable the selection of the LDAP protocol when binding to an LDAP server:

```
LDAP_Bind_Version=['2'|'3']
```

The default is 2 (LDAP version 2). (PR 565940)

Logging

- The first sentence of the last paragraph on page 697 of the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide* in the “Using the Server Log File” section, should read as follows: (PR 478308)

If a maximum file size is set, the server log filename identifies the date and time it was opened. Log files are named as follows: *yyyymmdd_xxxxx.log*, where *xxxxx* is the sequence beginning with 00000.

- The following changes should be made to Table 19: radius.ini [Logging] Syntax in the *Steel-Belted Radius Carrier 7.2.4 Reference Guide*: (PR 478308)

For the LogHighResolutionTime parameter, the descriptions should read:

- If set to no, the timestamp for entries in the Steel-Belted Radius Carrier log file (*yyyymmdd.log*) are recorded as MM/DD/YYYY hh:mm:ss (month/date/year/hour:minutes:seconds).
- If set to yes, the timestamp for entries in the Steel-Belted Radius Carrier log file (*yyyymmdd.log*) are recorded as MM/DD/YYYY hh:mm:ss.xxx, where xxx represents the number of elapsed milliseconds since the ss value changed.

For the LogFileMaxMBytes parameter, the second bullet should read:

- If set to a value in the range 1–2047, the current server log file is closed when it reaches the specified number of megabytes (1024 x 1024 bytes), and a new server log file is opened using the file format YYYYMMDD_NNNNN.log, where NNNNN is a sequence number.

Oracle

- **The following patch information should be added to Table 14: Required Patches on page 52 of the *Steel-Belted Radius Carrier 7.2.4 Installation Guide*:**

To use Oracle 11, Update 6 is required, and Update 8 is recommended.

radius.ini File

- **Table 12: radius.ini [Configuration] Syntax on page 30 of the *Steel-Belted Radius Carrier 7.2.4 Reference Guide*, incorrectly lists the DiscardAccessRequestOnCstFailure parameter. This parameter should be replaced with the following: (PR 411391)**

AuthResponseOnCstFailure

Specifies how the SBRC server responds to requests when the session database cannot be contacted.

If set to Reject, the SBRC server sends an Access-Reject when there is a CST failure.

If set to Accept, the SBRC server sends an Access-Accept in spite of a CST failure.

Discard - do not send any response

Default value is Reject.

Realm JavaScript

- The `SetLocationGroupProfile` method with the following description should be added to the “RealmSelector Methods” section in the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide*. (PR 441981)

`SetLocationGroupProfile()`

Purpose—The `SetLocationGroupProfile()` method is used to set the profile to be returned upon successful authentication.

Syntax—`selector.SetLocationGroupProfile(profile)`

Parameters—`profile`: Specifies the location group profile name.

Returns—Nothing.

Example—`selector.SetLocationGroupProfile("Profile1");`

Replication

- The last paragraph in the “Publishing Server Configuration Information” section on page 272 of the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide* should read: (PR 507496)

This creates a file called `/opt/JNPRsbr/radius/packages/timestamp_RSA.ccmpkg`, where `timestamp` reflects the date and time the package was created.

SNMP

- If you have used the Solstice Enterprise Agents (SEA) SNMP utility in the past, this package is obsolete. It is possible to use the SNMP trap command supplied with Solaris SNMP as a replacement. The `radiusd` plug-in `radiusd.net-snmp-5.0.9.sh` is now included as a sample script in the `/opt/JNPRsbr/radius/samples/radiusd` directory. (PR 520180)
- The following note should be added to the “`jnrnsnmpd.conf` File Overview” section of Chapter 14, “SNMP Configuration Overview” in the *Steel-Belted Radius Carrier 7.2.4 Reference Guide*: (PR 542421)



NOTE: The “`clientaddr`” needs to be placed under `[snmp]` in the `jnrnsnmpd.conf` file, otherwise an error is logged in the `jnrnsnmpd.log`. To avoid this issue, place “`clientaddr`” under the `[snmp]` header in the `jnrnsnmpd.conf` file.

SQL Data Accessor

- Part 11, “Optional Scripting Module” of the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide* incorrectly mentions `LibraryName=sqlaccessor.dll`. All references to the `LibraryName` should read `LibraryName=sqlaccessor.so`. In addition, the SQL query samples shown in this section mention the

ConnectTimeout and QueryTimeout parameters. These parameters are not supported for Oracle, and may or may not be supported for jdbc, depending on the driver used. (PR 410616)

- **The following corrections apply to the “[Bootstrap]” subsection of the “SQL Data Accessor Configuration” section, in the *Steel-Belted Radius Carrier 7.2.4 Administration and Configuration Guide*: (PR 567511)**

- The text under the “[Bootstrap]” section should be replaced with the following information:

You can configure more than one SQL data accessor plug-in instance. Each requires its own **.gen** file in the /radiusdir directory. The [Bootstrap] section of each **.gen** file must include one of these libraries as the LibraryName entry:

```
radsqL_accessor_ora9.so
```

```
radsqL_accessor_ora10.so
```

```
radsqL_accessor_ora11.so
```

or

```
radsqL_accessor_jdbc.so
```

```
[Bootstrap]
```

```
LibraryName=radsqL_accessor_ora11.so
```

```
Enable=1
```

- The function for the “LibraryName” parameter in the table “[Bootstrap] Syntax” should be replaced with the following information:

LibraryName Specifies the name of one SQL data accessor plug-in. It may be:

```
radsqL_accessor_ora9.so
```

```
radsqL_accessor_ora10.so
```

```
radsqL_accessor_jdbc.so
```

System Requirements

- Under the RAM column of Table 11: Standalone Steel-Belted Radius Carrier Server Hardware Configurations on page 49 of the *Steel-Belted Radius Carrier 7.2.4 Installation Guide*, the minimum configuration should list 1 GB RAM and the recommended configuration should list 4 GB RAM or more. (PR 568188)

wimax.ini File

- **The following two parameters should be added to “Table 191: wimax.ini [ASNGW-Requests] Syntax” in the *SBR Carrier Reference Guide*: (PR 511639)**

The description for the ASNGW-Accept-Filter parameter should read:

Specifies the name of the attribute filter to be applied to the ASN-GW Access-Accept parameter before the session is recorded. You can use this parameter to specify regular or scripted filters. If no filter is specified, all attributes are returned unchanged.

The description for the ASNGW-PostSession-Filter parameter should read:

Specifies the name of the attribute filter to be applied to the ASN-GW Access-Accept parameter after the session is recorded. You can use this parameter to specify regular or scripted filters. If no filter is specified, all attributes are returned unchanged.



NOTE: You must define all filters using the SBR Administrator. Do not edit the `filter.ini` file manually. For more information, see the *SBR Carrier Administration and Configuration Guide*. The default value is no filter.

- **SBR Carrier does not acknowledge accounting requests for WiMAX when the session does not exist in the current sessions table (CST).** Class attributes are sent in Access-Accept packets and contain state information regarding the user session. This Class attribute is then returned by the NAS in subsequent Accounting-Requests to convey the information back to SBR. Depending on your configuration, a cookie may be sent instead of a full Class attribute. In this case, the full Class attribute is stored in the CST and retrieved using the cookie when an Accounting-Request is received. When this lookup fails, normally an Accounting-Ack is not returned to the NAS. To work around this problem, the `AckOnCookieFailure` parameter has been added to the [Configuration] section of the `radius.ini` file. When this parameter is set to yes, SBR Carrier sends an acknowledgement back for every accounting request it receives. To configure an acknowledgment to be sent despite the error, set `AckOnCookieFailure = without_session` (which will not create a new session for an `Accounting_Start`) or `AckOnCookieFailure = with_session` (which will create a new session). `AckOnCookieFailure = no` is the default and will neither create a new session nor send an Accounting-Ack. This parameter should be added to the “[Configuration] section” of the `radius.ini` file in the *SBR Carrier Reference Guide*. (PR 514667)

Resolved Issues

Release 7.2.4

- The `sbrsetuptool` command to replicate the primary server configuration does not work. (PR 284279)
- The message "device will be disabled" appears if a client was not configured in `deviceModels.xml` file. This message pertains to only CoA/DM functionality and will now clearly state so. (PR 395013)
- A Primary CCM server cores if no file descriptor was available for replication. (PR 405584)
- In the `ldapauth.aut` file, the `FilterSpecialCharacterHandling` parameter is now set to 1 in the [Settings] section to prevent usernames with special characters (such as ')') from causing problems when using LDAP authentication. (PR 409675)
- Proxied attributes that are not present in the client's dictionary appear as "Unknown" in the log and are not available for filtering. (PR 454059)

- Some international characters, such as é, ö, or à, are not supported as passwords for users in the SBR native user database. (PR 461739 and PR 535283)
- SBR can exit unexpectedly after a CCM update of proxy targets. (PR 467760)
- HUP processing is delayed by 60 seconds if Spooled Proxy Accounting is enabled. (PR 472655)
- During a routed proxy authentication, inserted attributes are dropped when the authentication includes a Challenge/Response sequence. (PR 480663)
- SNMP traps 10042, 10046, and 10047 are no longer sent, as these are intended for internal use only. (PR 483558)
- The StartPartialTimeout setting is no longer applicable to the SBR Carrier servers running as standalone. From Release 7.2.4, the standalone servers use the LDAP directory to store sessions. (PR 487454)
- When an invalid IP address is configured for a client, the following message is now logged: "Invalid configuration for CoA/DM device 'ARMSTST', no range configurable." The previous message "Invalid IPv4 address in configuration of controlled device 'ARMSTST'; ignoring" was ambiguous. (PR 487459)
- Memory is leaked during HUP when TTLS or TLS is configured. (PR 494123)
- More than 100,000 sessions cannot be deleted at one time by the session control module. (PR 495689)
- Hexadecimal attributes are not supported by the JDBC plug-ins. (PR 503770)
- Incorrect values for the Global Application Context are sent to HLRs. (PR 508579)
- Memory can be leaked during CCM publication. (PR 510698)
- Accounting Interim-Update is not updating the phantom session if no Start has been received. Added the following information to the *SBRC Release 7.2.4 Reference Guide*. (PR 515389)

UpdateOnInterim

Specifies whether or not to update the session from phantom to active when the SBRC server receives an accounting packet with the Acct-Status-Type attribute set to a value of interim-update:

- If set to 1, the server changes the state of the session from phantom to active when it receives an interim update.
- If set to 0, the server does not change the state of the session from phantom to active when an interim update is received.

The default value is 0.

- Subscriber requests using MAC addresses for usernames result in non-unique session keys. (PR 517944)
- Changes to the WiMAX ASNGW-PostSession-Filter do not take effect until SBR is restarted. (PR 518163)

- **Setting DiscardAccountingRequestOnCstFailure to 1 will now cause Accounting request to be discarded (that is, no response will be sent).** (PR 518466 and PR 534561)
 - **The running scsClient script goes into an infinite loop while the SBR is stopped.** (PR 519167)
 - **Behavior of JavaScript has been improved. Problems such as “unexpected termination of SBR” or “failure to execute scripts” will not occur.** (PR 523834)
 - **The Days-To-Keep GUI setting is not applied to directed realm accounting files.** (PR 525653)
- When the SSR connection manager is not used, the SNMP traps are not sent if the SSR failed.** (PR 526857)
- **Typo in the funkrate.mib file, which can cause errors when using certain snmp agents, has been corrected.** (PR 527527)
 - **The SDK API can return an incorrect WiMAX BEK value.** (PR 530379)
 - **Typos in the events.ini file have been corrected.** (PR 533068)
 - **Juniper Networks dictionaries have been updated.** (PR 535285)
 - **WiMAX TLVs are not logged correctly.** (PR 537584)
 - **Duplicate IP addresses can be assigned after restarting the Standalone SBR.** (PR 548164)
 - **Tunneled TTLS attributes can be unavailable to the Auth-Final-Response control point plug-in.** (PR 549983)
 - **SBR sends Access-Accept responses for WiMAX Access-Requests when a Session-Timeout attribute is not available.** (PR 553357)
 - **Files necessary for LDAP SSL connections are not installed.** (PR 553696)
 - **When the maximum number of concurrent connections is reached for a WiMAX user on a standalone SBR Carrier server, no further Access-Requests are accepted.** (PR 555997)
 - **Due to a mutex being held too long, proxy responses are delayed during post response activity, such as attribute filtering, IP address assignment, Control Point invocation, or the use of JavaScript.** (PR 556167)
 - **The use of %login-limit from a stored procedure during SQL authentication is not functional.** (PR 557599)

Related Documentation

Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFC)s online at <http://www.ietf.org/rfc.html>. Table 3 on page 23 lists the RFCs that apply to Steel-Belted Radius Carrier.

Table 3: RFCs Related to Steel-Belted Radius Carrier

RFC Number	Title
RFC 1035	<i>Domain Names - Implementation and Specification.</i> P. Mockapetris. November 1987.
RFC 1155	<i>Structure and Identification of Management Information for TCP/IP-based Internets.</i> M. Rose, K. McCloghrie, May 1990.
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II.</i> K. McCloghrie, M. Rose, March 1991.
RFC 2006	<i>The Definitions of Managed Objects for IP Mobility Support using SMIv2.</i> D. Cong and others. October 1996.
RFC 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.

Table 3: RFCs Related to Steel-Belted Radius Carrier (*continued*)

RFC Number	Title
RFC 2882	<i>Network Access Servers Requirements: Extended RADIUS Practices</i> . D. Mitton. July 2000.
RFC 3046	<i>DHCP Relay Agent Information Option</i> . M. Patrick. January 2001.
RFC 3118	<i>Authentication for DHCP Messages</i> . R.Droms and others. June 2001.
RFC 3162	<i>RADIUS and IPv6</i> . B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3344	<i>IP Mobility Support for IPv4</i> . C. Perkins. August 2002.
RFC 3539	<i>Authentication, Authorization, and Accounting (AAA) Transport Profile</i> . B. Aboba, J. Wood. June 2003.
RFC 3575	<i>IANA Considerations for RADIUS (Remote Authentication Dial-In User Service)</i> . B. Aboba, July 2003.
RFC 3576	<i>RFC3576 - Dynamic Authorization Extensions to Remote to Remote Authentication Dial In User Service</i> . Network Working Group, 2003
RFC 3579	<i>RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)</i> . B. Aboba, P. Calhoun, September 2003.
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i> . P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.
RFC 3748	<i>Extensible Authentication Protocol</i> . B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. 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.

Table 3: RFCs Related to Steel-Belted Radius Carrier (*continued*)

RFC Number	Title
RFC 5281	<i>Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)</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 Uticom software and hardware, or your access servers and firewalls, consult the manufacturer's documentation.

General Statement of Compliance

Table 4 on page 25 lists Steel-Belted Radius Carrier 7.2.x compliance with applicable RFCs.

Table 4: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs

RFC Number	Name	Notes
1155	Structure and Identification of Management Information for TCP/IP-based Internets	—
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	—
2058	Remote Authentication Dial In User Service	Obsoleted by RFC 2138
2059	RADIUS Accounting	Obsoleted by RFC 2139
2107	Ascend Tunnel Management Protocol	—
2138	Remote Authentication Dial In User Service	Obsoleted by RFC 2865
2139	RADIUS Accounting	Obsoleted by RFC 2866
2271	An Architecture for Describing SNMP Management Frameworks	Obsoleted by RFC 2271

Table 4: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
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	—
2989	Criteria for Evaluating AAA Protocols for Network Access	—
3012	Mobile IPv4 Challenge/Response Extensions	—

Table 4: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
3162	RADIUS and IPv6	—
3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	—
3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	—
3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	—
3748	Extensible Authentication Protocol (EAP)	—
3770	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks	—
4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	—
4017	Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs	—
4072	Diameter Extensible Authentication Protocol (EAP) Application	Not supported
4137	State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator	—
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	—

Table 4: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
4668	RADIUS Authentication Client MIB for IPv6	Previous version (RFC 2618) supported
4669	RADIUS Authentication Server MIB for IPv6	Previous version (RFC 2619) supported
4670	RADIUS Accounting Client MIB for IPv6	Previous version (RFC 2220) supported
4671	RADIUS Accounting Server MIB for IPv6	Previous version (RFC 2221) supported
4672	RADIUS Dynamic Authorization Client MIB	Not supported
4673	RADIUS Dynamic Authorization Server MIB	Not supported
4675	RADIUS Attributes for Virtual LAN and Priority Support	Not supported
4679	DSL Forum Vendor-Specific RADIUS Attributes.	Not supported
4746	Extensible Authentication Protocol (EAP) Password Authenticated Exchange	Not supported
4763	Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)	Not supported
4764	The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method.	Not supported
4793	The EAP Protected One-Time Password Protocol (EAP-POTP)	EAP-32
4818	RADIUS Delegated-IPv6-Prefix Attribute.	—
4849	RADIUS Filter Rule Attribute	—
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	Not supported
4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management	—
5030	Mobile IPv4 RADIUS Requirements	—
5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes	—
5106	The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method	—
5169	Handover Key Management and Re-Authentication Problem Statement	—

Table 4: Compliance of Steel-Belted Radius Carrier 7.2.x with Applicable RFCs (*continued*)

RFC Number	Name	Notes
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 5 on page 29 lists the protocols supported in Steel-Belted Radius Carrier 7.2.x.

Table 5: Protocols Supported in SBR Carrier 7.2.x

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	—

Table 5: Protocols Supported in SBR Carrier 7.2.x (continued)

Protocol	Notes
3GPP	RADIUS only
23.234 (RADIUS)	WLAN UE
29.061 (RADIUS)	G1 and Pk reference points
TISPAN	RADIUS only Interface E5
ES282.001	—
ES282.004	—
ES283.034	—
ES283.035	—

SBR Carrier Documentation and Release Notes

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

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings:
<http://www.juniper.net/customers/support/>
- Search for known bugs:
<http://www2.juniper.net/kb>
- Find product documentation:
<http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base:
<http://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager:
<http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

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

When you contact technical support, be ready to provide:

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

Revision History

December 2010—FRS SBR Carrier Release 7.2.4

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

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

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

Ulticom, Signalware, Programmable Network, Ultimate Call Control, and Nexworx are registered trademarks of Ulticom, Inc. Kineto and the Kineto Logo are registered trademarks of Kineto Wireless, Inc. Software Advancing Communications and SignalCare are trademarks and service marks of Ulticom, Inc. CORBA (Common Object Request Broker Architecture) is a registered trademark of the Object Management Group (OMG). Raima, Raima Database Manager and Raima Object Manager are trademarks of 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.

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> All rights reserved.

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

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

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

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

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

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

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

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

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

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

3. The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

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

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

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

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

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

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

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

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

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

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