FEATURES AND STANDARDS SUPPORT MATRIX

Ruckus SmartZone RFC Support and Standards Compliance Report, 5.1.2

Supporting Release 5.1.2

Part Number: 800-72361-001 Rev A
Publication Date: August 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Report

Introduction

The *SmartZone RFC Support and Standards Compliance Report* lists the RFCs supported by the SmartZone and Virtual SmartZone (vSZ) platforms. This document also provides SNMP, GTP, and 3GPP compliance test reports for the controller, including the test topology and compliance support matrix.

This report is for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE
This guide assumes that the controller has already been installed as described in the *Getting Started Guide*.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus support web site at https://support.ruckuswireless.com/contact-us.

What's New in This Document

The following are the new RFCs for this guide in 5.1.2 release

- RFC 6614 Transport Layer Security (TLS) Encryption for RADIUS
- RFC 2737 Entity MIB (Version 2) for FIPS
- RFC 2818 HTTP Over TLS
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec
- RFC 4945 The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- RFC 4251 The Secure Shell (SSH) Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4253 The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254 The Secure Shell (SSH) Connection Protocol
- RFC 5656 Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
- RFC 6668 SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
- RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 3268 Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)

- RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
- RFC 5288 AES Galois Counter Mode (GCM) Cipher Suites for TLS
- RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 1981 Path MTU Discovery for IP version 6
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 3879 Deprecating Site Local Addresses
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- RFC 2462 IPv6 Stateless Address Auto configuration
- RFC 4862 IPv6 Stateless Address Auto configuration
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Terminology

The following table lists the terms used in this guide.

TABLE 2 Terminology used in this guide

Term	Description
Fully compliant	Implemented as specified in the section including optional aspects of the specification.
Compliant	Implemented all mandatory aspects of the functionality. Optional aspects may not be supported.
Partially compliant	Some aspects of the mandatory part have not been implemented.
Non-compliant	Not implemented as specified. If applicable, proprietary implementations are explained with a note.
Not applicable	Refers to requirements but is not relevant to this version of the controller.
No requirement	Indicates that there are no requirements to be implemented or the section is empty.

RFCs

Supported RFCs

The following table lists the RFCs that are supported by the SmartZone and Virtual SmartZone (vSZ) controllers. In the Release field, SmartZone 5.0 is used as the baseline release. This means RFCs listed as being introduced in release 5.0 were actually introduced in 5.0 or an earlier release.

RFC Number	RFC Name	Release in which Support was Introduced
RFC 768	User Datagram Protocol	5.0
RFC 793	Transmission Control Protocol	5.0
RFC 959	File Transfer Protocol	5.0
RFC 1122	Requirements for Internet Hosts - Communication Layers	5.0
RFC 1180	TCP/IP tutorial	5.0
RFC 1212	Concise MIB Definitions	5.0
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II	5.0
RFC 1215	SNMP Generic Traps	5.0
RFC 1256	ICMP Router Discovery Messages	5.0
RFC 1305	Network Time Protocol (Version 3)	5.0
RFC 1492	An Access Control Protocol, Sometimes Called TACACS	5.0
RFC 1643	Definitions of Managed Objects for the Ethernet-like Interface Types	5.0
RFC 1812	Requirements for IP Version 4 Routers	5.0
RFC 1901	Introduction to Community-based SNMPv2	5.0
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework	5.0
RFC 2307	An Approach for Using LDAP as a Network Information Service	5.0
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	5.0
RFC 2511	Internet X.509 Certificate Request Message Format	5.0
RFC 2548	Microsoft Vendor-Specific RADIUS Attributes	5.0
RFC 2578	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	5.0
RFC 2579	Textual Conventions for SMIv2	5.0
RFC 2581	TCP Congestion Control	5.0
RFC 2597	Assured Forwarding PHB Group	5.0

RFC Number	RFC Name	Release in which Support was Introduced
RFC 2600	Internet Official Protocol Standards	5.0
RFC 2616	HTTP 1.1	5.0
RFC 2660	HTTPs (compliant)	5.0
RFC 2665	Definitions of Managed Objects for the Ethernet-like Interface Types	5.0
RFC 2759	Microsoft PPP CHAP Extensions, Version 2	5.0
RFC 2819	Remote Network Monitoring Management Information Base	5.0
RFC 2863	The Interface Group MIB	5.0
RFC 2865	Remote Authentication Dial In User Service (RADIUS) [June 2000]	5.0
RFC 2866	RADIUS Accounting [June 2000]	5.0
RFC 2867	RADIUS Tunnel Accounting	5.0
RFC 2869	RADIUS Extensions [June 2000]	5.0
RFC 2882	Network Access Servers Requirements: Extended RADIUS Practices	5.0
RFC 3164	The BSD Syslog Protocol (This RFC is obsoleted by RFC 5424)	5.0
RFC 3246	An Expedited Forwarding PHB (Per-Hop Behavior)	5.0
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework	5.0
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	5.0
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	5.0
RFC 3413	Simple Network Management Protocol (SNMP) Applications	5.0
RFC 3414	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)	5.0
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	5.0
RFC 3416	Version 2 of the Protocol Operations for SNMP	5.0
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMPv3)	5.0
RFC 3418	Management Information Base (MIB) for SNMP [December 2002]	5.0
RFC 3576	Dynamic Authorization Extensions to RADIUS	5.0
RFC 3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	5.0
RFC 3580	IEEE 802.1X RADIUS Guidelines	5.0
RFC 3584	Management Information Base (MIB) for the Simple Network Management Protocol	5.0
RFC 3748	Extensible Authentication Protocol (EAP)	5.0

RFC Number	RFC Name	Release in which Support was Introduced
RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	5.0
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax (with IPv6)	5.0
RFC 4001	Textual Conventions for Internet Network Addresses	5.0
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)	5.0
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)	5.0
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace	5.0
RFC 4137	State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator	5.0
RFC 4186	EAP-SIM	5.0
RFC 4187	EAP-AKA	5.0
RFC 4254	The Secure Shell (SSH) Connection Protocol	5.0
RFC 4282	Network Access Identifier	5.0
RFC 4292	IP Forwarding Table MIB [April 2006]	5.0
RFC 4293	Management Information Base for the Internet Protocol (IP) [April 2006]	5.0
RFC 4346	TLS protocol version 1.1	5.0
RFC 4372	Chargeable User Identity	5.0
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	5.0
RFC 4825	The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)	5.0
RFC 4849	RADIUS Filter Rule Attribute	5.0
RFC 4898	TCP Extended Statistics MIB (TCP-ESTATS)	5.0
RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	5.0
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (PKI Certification)	5.0
RFC 5343	Simple Network Management Protocol (SNMP) Context EngineID Discovery	5.0
RFC 5424	Layered architecture for SYSLOG	5.0
RFC 5590	Transport Subsystem for the Simple Network Management Protocol (SNMP)	5.0
RFC 5591	Transport Security Model for the Simple Network Management Protocol (SNMP)	5.0
RFC 5953	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)	5.0
RFC 6101	The Secure Sockets Layer (SSL) Protocol Version 3.0	5.0
RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format	5.0

RFC Number	RFC Name	Release in which Support was Introduced
RFC 6614	Transport Layer Security (TLS) Encryption for RADIUS	5.1.1
RFC 2818	HTTP Over TLS	5.1.1.3
RFC 4251	The Secure Shell (SSH) Protocol Architecture	5.1.1.3
RFC 4252	The Secure Shell (SSH) Authentication Protocol	5.1.1.3
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol	5.1.1.3
RFC 4254	The Secure Shell (SSH) Connection Protocol	5.1.1.3
RFC 5656	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer	5.1.1.3
RFC 6668	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol	5.1.1.3
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2	5.1.1.3
RFC 3268	Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)	5.1.1.3
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	5.1.1.3
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS	5.1.1.3
RFC 5289	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	5.1.1.3
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	5.1.1.3

Federal Information Processing Standards (FIPS) RFCs

RFC Number	RFC Name	Release in which Support was Introduced
RFC 2737	Entity MIB (Version 2)	5.1.2
RFC 4301	Security Architecture for the Internet Protocol	5.1.1.3
RFC 4303	IP Encapsulating Security Payload (ESP)	5.1.1.3
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPSec	5.1.1.3
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)	5.1.1.3
RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec	5.1.1.3
RFC 4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX	5.1.1.3

IPv6 RFCs

RFC Number	RFC Name	Release in which Support was Introduced
RFC 4862	IPv6 Stateless Address Auto configuration	5.1.2

RFC Number	RFC Name	Release in which Support was Introduced
RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	5.1.1.3
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification	5.1.1.3
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	5.1.1.3
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	5.1.1.3
RFC 1981	Path MTU Discovery for IP version 6	5.1.1.3
RFC 4291	IP Version 6 Addressing Architecture	5.1.1.3
RFC 3879	Deprecating Site Local Addresses	5.1.1.3
RFC 4193	Unique Local IPv6 Unicast Addresses	5.1.1.3
RFC 4007	IPv6 Scoped Address Architecture	5.1.1.3
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	5.1.1.3
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	5.1.1.3
RFC 2462	IPv6 Stateless Address Auto configuration	replaced by RFC 4862
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	5.1.1.3

RFC Compliance Details

This section provides detailed SmartZone compliance information for a subset of the supported RFCs.

Network Access Identifier - RFC 4282

The following table lists the RFC compliance 4282 for the controller based on the network access identifier.

TABLE 3 Network access identifier - RFC 4286

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	Informative
1.1	Terminology	No requirement		No requirement	Informative
1.2	Requirements language	No requirement		No requirement	
1.3	Purpose	No requirement		No requirement	
2	NAI definition	No requirement		No requirement	
2.1	Formal syntax	Fully compliant		Fully compliant	
2.2	NAI length considerations	Fully compliant		Fully compliant	
2.3	Support for username privacy	Non compliant		Non compliant	It is recommended to omit the user name rather than the fixed username.

TABLE 3 Network access identifier - RFC 4286 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
2.4	International character sets	Compliant		Compliant	Does not support bidirectional characters.
2.5	Compatibility with email username	Fully compliant		Fully compliant	
2.6	Compatibility with DNS	Fully compliant		Fully compliant	
2.7	Realm construction	Partially compliant		Partially compliant	Does not support mediating realm.
2.8	Examples	No requirement		No requirement	Informative
3	Security considerations	No requirement		No requirement	
4	IANA considerations	No requirement		No requirement	
Appendix A	Changes from RFC 2486	No requirement		No requirement	Informative

EAP-SIM - RFC 4186

The following table lists the RFC compliance 4186 for the controller based on the EAP-SIM.

TABLE 4 EAP-SIM - RFC 4186

Section Number	Section Title	Controller Proxy Mode		Controller - Hosted AAA Mode	Comment
		AP-Controller	Controller AAA		
1	Introduction	No requirement		No requirement	Descriptive
2	Terms	No requirement		No requirement	Informative
3	Overview	No requirement		No requirement	Informative
4	Operation	No requirement		No requirement	Informative
4.1	Version negotiation	Fully compliant		Fully compliant	
4.2	Identity management	No requirement		No requirement	
4.2.1	Format, generation and usage of peer identities	No requirement		No requirement	
4.2.1.1	General	No requirement		No requirement	Informative
4.2.1.2	Identity privacy support	No requirement		No requirement	Informative
4.2.1.3	Username types in EAP-SIM identities	Fully compliant		Fully compliant	
4.2.1.4	Username decoration	Fully compliant		Not compliant	Only pre-pending string is allowed to decorate the username in non 3GPP proxy mode.
4.2.1.5	NAI realm portion	Not applicable		Not applicable	Requirement for PEER.
4.2.1.6	Format of the permanent username	Not applicable		Fully compliant	Informative
4.2.1.7	Generating pseudonyms and fast reauthentication identities by the server	Not applicable		Compliant	

TABLE 4 EAP-SIM - RFC 4186 (continued)

Section Number	Section Title	Controller Proxy Mode		Controller - Hosted AAA Mode	Comment
		AP-Controller	Controller AAA		
4.2.1.8	Transmitting pseudonyms and fast reauthentication identities to the peer	Fully compliant		Fully compliant	
4.2.1.9	Usage of the pseudonym by the peer	Not applicable		Not applicable	PEER (STA) requirement.
4.2.1.10	Usage of the fast reauthentication Identity by the peer	Not applicable		Not applicable	PEER (STA) requirement.
4.2.2	Communicating the peer identity to the server	No requirement		No requirement	
4.2.2.1	General	Fully compliant		Fully compliant	
4.2.2.2	Fully compliant	Fully compliant		Fully compliant	Fully compliant.
4.2.3	Choice of identity for the EAP-response/identity	Not applicable		Not applicable	Requirement for PEER.
4.2.4	Server operation in the beginning of EAP-SIM exchange	Not applicable		Fully compliant	
4.2.5	Processing of EAP-request/SIM/start by the peer	Not applicable		Not applicable	Requirement for PEER.
4.2.6	Attacks against identity privacy	Not applicable		Not Applicable	Requirement for PEER.
4.2.7	Processing of AT_IDENTITY by the server	Not applicable		Fully compliant	
4.3	Message sequence examples (informative)	No requirement		No requirement	Informative
4.3.1	Full authentication	Fully compliant		Fully compliant	
4.3.2	Fast reauthentication	Fully compliant		Fully compliant	
4.3.3	Fallback to full authentication	Fully compliant		Fully compliant	
4.3.4	Requesting the permanent identity 1	Fully compliant		Fully compliant	
4.3.5	Requesting the permanent identity 2	Fully compliant		Fully compliant	
4.3.6	Three EAP-SIM/start roundtrips	Fully compliant		Fully compliant	
5	Fast reauthentication	No requirement		No requirement	
5.1	General	Not applicable		Fully compliant	
5.2	Comparison to UMTS AKA	No requirement		No requirement	Informative
5.3	Fast reauthentication identity	Not applicable		Fully compliant	
5.4	Fast reauthentication procedure	Not applicable		Fully compliant	
5.5	Fast reauthentication procedure when counter Is too small	Not applicable		Fully compliant	Unable to verify.
6	EAP-SIM notifications	No requirement		No requirement	
6.1	General	No requirement		No requirement	Informative
6.2	Result indications	Not compliant		Not compliant	
6.3	Error cases	No requirement			
6.3.1	Peer operation	Not applicable		Not applicable	Requirement for PEER.
6.3.2	Server operation	Fully compliant		Not compliant	
6.3.3	EAP failure	Fully compliant		Fully compliant	

TABLE 4 EAP-SIM - RFC 4186 (continued)

Section Number	Section Title	Controller Proxy Mode		Controller - Hosted AAA Mode	Comment
		AP-Controller	Controller AAA		
6.3.4	EAP success	Partially compliant		Partially compliant	Does not support AT_RESULT_IND.
7	Key generation	Not applicable		Fully compliant	
8	Message format and protocol extensibility	No requirement		No requirement	
8.1	Message format	Fully compliant		Fully compliant	
8.2	Protocol extensibility	Compliant		Compliant	Supports EAP-SIM version 1.
9	Messages	No requirement		No requirement	
9.1	EAP-request/SIM/start	Fully Compliant		Fully Compliant	Supports EAP-SIM version 1.
9.2	EAP-response/SIM/start	Fully compliant		Fully compliant	Peer operation.
9.3	EAP-request/SIM/challenge	Compliant		Compliant	Does not support AT_RESULT_IND.
9.4	EAP-response/SIM/challenge	Fully compliant		Fully compliant	Peer operation
9.5	EAP-request/SIM/reauthentication	Compliant		Compliant	Does not support AT_RESULT_IND.
9.6	EAP-response/SIM/ reauthentication	Compliant		Compliant	Peer operation. Does not support AT_RESULT_IND.
9.7	EAP response/SIM/client error	Fully compliant		Fully compliant	Peer operation.
9.8	EAP request/SIM/notification	Not compliant		Not compliant	
9.9	EAP response/SIM/notification	Not compliant		Not compliant	
10	Attributes	No requirement		No requirement	Informative
10.1	Table of attributes	No requirement		No requirement	Informative
10.2	AT_VERSION_LIST	Fully compliant		Fully compliant	
10.3	AT_SELECTED_VERSION	Fully compliant		Fully compliant	Peer operation.
10.4	AT_NONCE_MT	Fully compliant		Fully compliant	Peer operation.
10.5	AT_PERMANENT_ID_REQ	Fully compliant		Fully compliant	
10.6	AT_ANY_ID_REQ	Fully compliant		Fully compliant	
10.7	AT_FULLAUTH_ID_REQ	Fully compliant		Fully compliant	
10.8	AT_IDENTITY	Fully compliant		Fully compliant	Peer operation.
10.9	AT_RAND	Not applicable		Fully Compliant	The controller passes the attribute between NAS and AAA server using a proxy mode.
10.10	AT_NEXT_PSEUDONYM	Fully compliant		Compliant	Realm is sent. The controller passes the attribute between NAS and AAA server using a proxy mode.
10.11	AT_NEXT_REAUTH_ID	Fully compliant		Fully compliant	The controller passes the attribute between NAS and AAA server using a proxy mode.

TABLE 4 EAP-SIM - RFC 4186 (continued)

Section Number	Section Title	Controller Proxy Mode		Controller - Hosted AAA Mode	Comment
		AP-Controller	Controller AAA		
10.12	AT_IV, AT_ENCR_DATA, and AT_PADDING	Fully compliant		Fully compliant	The controller passes the attribute between NAS and AAA server using a proxy mode.
10.13	AT_RESULT_IND	Not compliant		Not compliant	
10.14	AT_MAC	Fully compliant		Full compliant	The controller passes the attribute between NAS and AAA server using a proxy mode.
10.15	AT_COUNTER	Not applicable		Fully compliant	
10.16	AT_COUNTER_TOO_SMALL	Not applicable		Fully compliant	Peer operation
10.17	AT_NONCE_S	Not applicable		Fully compliant	
10.18	AT_NOTIFICATION	Not compliant		Not compliant	
10.19	AT_CLIENT_ERROR_CODE	Fully compliant		Fully compliant	
11	IANA considerations	No requirement		No requirement	
12	Security considerations	No requirement		No requirement	
12.1	A3 and A8 algorithms	Not applicable		Fully compliant	
12.2	Identity protection	Fully compliant	Not compliant	Compliant	RADIUS messages are sent to the controller using the SSH tunnel. A secure connection is not available since the controller and AAA server are both assumed to be in operator core. The controller supports pseudonym based authentication.
12.3	Mutual authentication and triplet exposure	Not applicable	Not compliant	Not compliant	Communication between the controller and AAA is unsecured.
12.4	Flooding the authentication center	Not compliant		Not compliant	
12.5	Key derivation	Not applicable		Fully compliant	
12.6	Cryptographic separation of keys and session independence	Not applicable		Fully compliant	
12.7	Dictionary attacks	Fully compliant		Fully compliant	
12.8	Credentials reuse	No requirement		No requirement	
12.9	Integrity and replay protection, and confidentiality	Fully compliant		Fully compliant	
12.10	Negotiation attacks	Fully compliant		Fully compliant	
12.11	Protected result indications	Not compliant		Not compliant	
12.12	Man-in-the-middle attacks	Fully compliant	Not compliant	Not compliant	
12.13	Generating random numbers	Not applicable		Fully compliant	
13	Security claims	Not applicable		Fully compliant	
Appendix A	Test vectors	No requirement		No requirement	Informative

TABLE 4 EAP-SIM - RFC 4186 (continued)

Section Number	Section Title	Controller Proxy Mode		Controller - Hosted AAA Mode	Comment
		AP-Controller	Controller AAA		
A.1	EAP-request/identity	No requirement		No requirement	Informative
A.2	EAP-response/identity	No requirement		No requirement	Informative
A.3	EAP-request/SIM/start	No requirement		No requirement	Informative
A.4	EAP-response/SIM/start	No requirement		No requirement	Informative
A.5	EAP-request/SIM/challenge	No requirement		No requirement	Informative
A.6	EAP-response/SIM/challenge	No requirement		No requirement	Informative
A.7	EAP success	No requirement		No requirement	Informative
A.8	Fast reauthentication	No requirement		No requirement	Informative
A.9	EAP-request/SIM/re-authentication	No requirement		No requirement	Informative
A.10	EAP-response/SIM/re-authentication	No requirement		No requirement	Informative
Appendix B	Pseudo-random number generator	No requirement		No requirement	Informative

EAP-AKA - RFC 4187

The following table lists the RFC compliance 4187 for the controller based on the EAP-AKA.

TABLE 5 EAP-AKA - RFC 4187

Section Number	Section Title	Controller as Proxy		Controller - Hosted AAA Mode	Comment
		Ruckus AP	Controller		
1	Introduction and motivation	No requirement		No requirement	Informative
2	Terms and conventions used in this document	No requirement		No requirement	Informative
3	Protocol overview	Fully compliant		Fully compliant	
4	Operation	No requirement		No requirement	
4.1	Identity management	No requirement		No requirement	
4.1.1	Format, generation and usage of peer identities	No requirement		No requirement	
4.1.1.1	General	No requirement		No requirement	Informative
4.1.1.2	Identity privacy support	Fully compliant		Fully compliant	
4.1.1.3	Username types in EAP-AKA identities	Fully compliant		Fully compliant	
4.1.1.4	Username decoration	Fully compliant	Not applicable	Fully compliant	
4.1.1.5	NAI realm portion	Fully compliant		Fully compliant	
4.1.1.6	Format of the permanent username	Fully compliant		Fully compliant	
4.1.1.7	Generating pseudonyms and fast reauthentication identities by the server	Fully compliant		Fully compliant	
4.1.1.8	Transmitting pseudonyms and fast reauthentication identities to the peer	Fully compliant		Fully compliant	
4.1.1.9	Usage of the pseudonym by the peer	Fully compliant		Fully compliant	

TABLE 5 EAP-AKA - RFC 4187 (continued)

Section Number	Section Title	Controller as Proxy		Controller - Hosted AAA Mode	Comment
		Ruckus AP	Controller		
4.1.1.10	Usage of the fast reauthentication identity by the peer	Fully compliant		Fully compliant	
4.1.2	Communicating the peer identity to the server	No applicable		No applicable	Requirement for PEER
4.1.2.1	General	Fully compliant		Fully compliant	
4.1.2.2	Relying on EAP-response/identity discouraged	Fully compliant		Fully compliant	
4.1.3	Choice of identity for the EAP-response/ identity	Not applicable		Not applicable	Requirement for PEER
4.1.4	Server operation in the beginning of EAP-AKA exchange	Fully compliant		Fully compliant	
4.1.5	Processing of EAP-request/AKA-identity by the peer	Not applicable		Not applicable	Requirement for PEER
4.1.6	Attacks against identity privacy	Not applicable		Not applicable	Requirement for PEER
4.1.7	Processing of AT_IDENTITY by the server	Fully compliant		Fully compliant	
4.2	Message sequence examples (informative)	No requirement		No requirement	Informative
4.2.1	Usage of AT_ANY_ID_REQ	No requirement		No requirement	Informative
4.2.2	Fallback on full authentication	No requirement		No requirement	Informative
4.2.3	Requesting the permanent identity 1	No requirement		No requirement	Informative
4.2.4	Requesting the permanent identity 2	No requirement		No requirement	Informative
4.2.5	Three EAP/AKA-identity round trips	No requirement		No requirement	Informative
5	Fast reauthentication	No requirement		No requirement	
5.1	General	Fully compliant		Fully compliant	
5.2	Comparison to AKA	No requirement		No requirement	Informative
5.3	Fast reauthentication identity	Fully compliant		Fully compliant	
5.4	Fast reauthentication procedure	Fully compliant		Fully compliant	
5.5	Fast reauthentication procedure when the counter is too small	No requirement		No requirement	
6	EAP-AKA notifications	No requirement		No requirement	
6.1	General	Non-compliant		Non-compliant	
6.2	Result indications	Non-compliant		Non-compliant	
6.3	Error cases	No requirement		No requirement	
6.3.1	Peer operation	Not applicable		Not applicable	
6.3.2	Server operation				Needs to be verified
6.3.3	EAP failure	Compliant		Compliant	Does not support AT_NOTIFICATION
6.3.4	EAP success			Compliant	Does not support AT_RESULT_IND and AT_NOTIFICATION
7	Key generation	Fully compliant		Fully compliant	
8	Message format and protocol extensibility	No requirement		No requirement	

TABLE 5 EAP-AKA - RFC 4187 (continued)

Section Number	Section Title	Controller as Proxy		Controller - Hosted AAA Mode	Comment
		Ruckus AP	Controller		
8.1	Message format	Fully compliant		Fully compliant	
8.2	Protocol extensibility				
9	Messages	No requirement		No requirement	Informative
9.1	EAP-request/AKA-identity	Fully compliant		Fully compliant	
9.2	EAP-response/AKA-identity	Not applicable		Not applicable	Requirement for PEER
9.3	EAP-request/AKA-challenge	Compliant		Compliant	Does not support AT_RESULT_IND
9.4	EAP-response/AKA-challenge	Not applicable		Not applicable	Requirement for PEER
9.5	EAP-response/AKA-authentication-reject	Not applicable		Not applicable	Requirement for PEER
9.6	EAP-response/AKA-synchronization-failure	Not applicable		Not applicable	Requirement for PEER
9.7	EAP-request/AKA-reauthentication	Fully compliant		Fully compliant	AT_CHECKCODE is not verified
9.8	EAP-response/AKA-reauthentication	Not applicable		Not applicable	Requirement for PEER
9.9	EAP-response/AKA-client-error	Not applicable		Not applicable	Requirement for PEER
9.10	EAP-request/AKA-notification	Non compliant		Non compliant	Does not support AT_NOTIFICATION
9.11	EAP-response/AKA-notification	Not applicable		Not applicable	Requirement for PEER
10	Attributes	No requirement		No requirement	
10.1	Table of attributes	No requirement		No requirement	Informative
10.2	AT_PERMANENT_ID_REQ	Fully compliant		Fully compliant	
10.3	AT_ANY_ID_REQ	Fully compliant		Fully compliant	
10.4	AT_FULLAUTH_ID_REQ	Fully compliant		Fully compliant	
10.5	AT_IDENTITY	Fully compliant		Fully compliant	
10.6	AT_RAND	Fully compliant		Fully compliant	
10.7	AT_AUTN	Fully compliant		Fully compliant	
10.8	AT_RES	Fully compliant		Fully compliant	
10.9	AT_AUTS	Fully compliant		Fully compliant	
10.10	AT_NEXT_PSEUDONYM	Fully compliant		Fully compliant	
10.11	AT_NEXT_REAUTH_ID	Fully compliant		Fully compliant	
10.12	AT_IV, AT_ENCR_DATA, and AT_PADDING	Fully compliant		Fully compliant	
10.13	AT_CHECKCODE	Fully compliant		Fully compliant	AT_CHECKCODE is not verified
10.14	AT_RESULT_IND	Non compliant		Non compliant	
10.15	AT_MAC	Fully compliant		Fully compliant	
10.16	AT_COUNTER	Fully compliant		Fully compliant	
10.17	AT_COUNTER_TOO_SMALL				

TABLE 5 EAP-AKA - RFC 4187 (continued)

Section Number	Section Title	Controller as Proxy		Controller - Hosted AAA Mode	Comment
		Ruckus AP	Controller		
10.18	AT_NONCE_S	Fully compliant		Fully compliant	
10.19	AT_NOTIFICATION	Non compliant		Non compliant	
10.20	AT_CLIENT_ERROR_CODE	Fully compliant		Fully compliant	
11	IANA and protocol numbering considerations	Compliant		Compliant	Does not support AT_RESULT_IND & AT_NOTIFICATION
12	Security considerations	No requirement		No requirement	
12.1	Identity protection	Fully compliant		Fully compliant	
12.2	Mutual authentication	Fully compliant		Fully compliant	Not verified
12.3	Flooding the authentication center	Non compliant		Non compliant	Does not support rate limiting
12.4	Key derivation	No requirement		No requirement	Informative
12.5	Brute force and dictionary attacks	No requirement		No requirement	Informative
12.6	Protection, replay protection, and confidentiality	Fully compliant		Fully compliant	
12.7	Negotiation attacks	No requirement		No requirement	Informative
12.8	Protected result indications	Non compliant		Non compliant	
12.9	Man-in-the-middle attacks	Fully compliant		Fully compliant	Not verified
12.10	Generating random numbers	Fully compliant		Fully compliant	Not verified
13	Security claims	No requirement		No requirement	Informative
Appendix A	Pseudo random number generator	No requirement		No requirement	Informative

RADIUS Support for EAP - RFC 3579

The following table lists the RFC compliance 3579 for the controller based on the EAP.

TABLE 6 RADIUS Support for EAP - RFC 3579

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	
1.1	Specification of requirement	No requirement		No requirement	
1.2	Terminology	No requirement		No requirement	
2	RADIUS support for EAP	Compliant		Compliant	
2.1	Protocol overview	Partially compliant		Partially compliant	
2.2	Invalid packets	Partially compliant		Partially compliant	EAP-NAK and DOS attack is not supported
2.3	Retransmission	Not applicable		Not applicable	
2.4	Fragmentation	Fully compliant		Fully compliant	
2.5	Alternative uses	Not applicable		Not applicable	
2.6	Usage guidelines	Compliant		Compliant	

TABLE 6 RADIUS Support for EAP - RFC 3579 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
2.6.1	Identifier space	Compliant		Compliant	
2.6.2	Role reversal	Not applicable		Not applicable	
2.6.3	Conflicting messages	Compliant		Compliant	
2.6.4	Priority	Compliant		Compliant	
2.6.5	Displayable messages	Compliant		Compliant	
3	Attributes	Fully compliant		Fully compliant	
3.1	EAP message	Fully compliant		Fully compliant	
3.2	Message authenticator	Compliant		Compliant	
3.3	Table of attributes	Fully compliant		Fully compliant	
4.1	Security requirements	No requirement		No requirement	
4.2	Security protocol	Not applicable		Not applicable	IPSec is not used
4.3	Security Issues	Partially compliant		Partially compliant	
4.3.1	Privacy Issues	Not applicable		Not applicable	
4.3.2	Spoofing and hijacking	Partially compliant		Partially compliant	
4.3.3	Dictionary attacks	Not applicable		Not applicable	
4.3.4	Known plain text attacks	Not applicable		Not applicable	
4.3.5	Replay attacks	Not applicable		Not applicable	
4.3.6	Negotiation attacks	Not applicable		Not applicable	
4.3.7	Impersonation	No requirement		No requirement	
4.3.8	Man in the middle attacks	Not applicable		Not applicable	
4.3.9	Separation of authenticator and authentication server	Partially compliant		Partially compliant	
4.3.10	Multiple databases	No requirement		No requirement	
5	IANA considerations	No requirement		No requirement	
6	References	No requirement		No requirement	
6.1	Normative references	No requirement		No requirement	
6.2	Informative references	No requirement		No requirement	

EAP - RFC 3748

The following table lists the RFC compliance 3748 for the controller based on the EAP.

TABLE 7 EAP - RFC 3748

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	
1.1	Specification of requirements	No requirement		No requirement	
1.2	Terminology	No requirement		No requirement	
1.3	Applicability	No requirement		No requirement	

TABLE 7 EAP - RFC 3748 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
2	Extensible authentication protocol (EAP)	Fully compliant		Fully compliant	
2.1	Support for sequences	Fully compliant		Fully compliant	
2.2	EAP multiplexing model	No requirement		No requirement	
2.3	Pass through behavior	Compliant		Compliant	Controller does not support EAP. Fails for AAA RADIUS server and Diameter server
2.4	Peer-to-Peer operation	Compliant	Not applicable	compliant	Controller supports EAP-TLS in proxy mode
3	Lower layer behavior	No requirement		No requirement	
3.1	Lower layer requirements	Not applicable		Not applicable	
3.2	EAP usage within PPP	Not applicable		Not applicable	
3.2.	PPP configuration option format	Fully compliant		Fully compliant	
3.3	EAP usage within IEEE 802	Compliant		Compliant	
3.4	Lower layer indications	Not applicable		Not applicable	
4	EAP packet format	Fully compliant		Fully compliant	
4.1	Request and response	Compliant		Compliant	Code, identifier, length, type and data
4.2	Success and failure	Fully compliant		Fully compliant	
4.3	Retransmission behavior	Compliant		Compliant	
5	Initial EAP request/response types	Compliant		Compliant	
5.1	Identity	Compliant		Compliant	Piggyback
5.2	Notification	No requirement		No requirement	Notification is optional as mentioned in the RFC
5.3	NAK	Not applicable		Not applicable	
5.3.1	Legacy NAK	Not applicable		Not applicable	
5.3.2	Expanded NAK	Not applicable		Not applicable	
5.4	MD5-challenge	Compliant		Compliant	NAK and expanded NAK
5.5	One-Time Password (OTP)	Not applicable		Not applicable	
5.6	Generic Token Card (GTC)	Not applicable		Not applicable	Not applicable
5.7	Expanded types	Not applicable		Not applicable	
5.8	Experimental	Not applicable		Not applicable	Not applicable
6	IANA considerations	No requirement		No requirement	
6.1	Packet codes	Fully compliant		Fully compliant	
6.2	Method types	No requirement		No requirement	

TABLE 7 EAP - RFC 3748 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
7	Security considerations	No requirement		No requirement	
7.1	Threat model	No requirement		No requirement	
7.2	Security claims	No requirement		No requirement	
7.2.1	Security claims terminology for EAP methods	No requirement		No requirement	
7.3	Identity protection	Compliant		Compliant	
7.4	Man-in-the-middle attacks	No requirement		No requirement	
7.5	Packet modification attacks	Not applicable		Not applicable	
7.6	Dictionary attacks	Not applicable		Not applicable	
7.7	Connection to an untrusted network	Not applicable		Not applicable	
7.8	Negotiation attacks	Not applicable		Not applicable	
7.9	Implementation idiosyncrasies	Not applicable		Not applicable	
7.10	Key derivation	Compliant		Compliant	
7.11	Weak cipher suites	Not applicable		Not applicable	
7.12	Link layer	Not applicable		Not applicable	
7.13	Separation of authenticator and backend authentication server	Not applicable	Compliant	Not applicable	
7.14	Clear text passwords	Not applicable		Not applicable	
7.15	Channel binding	Not applicable		Not applicable	
7.16	Protected result indications	No requirement		No requirement	
8	Acknowledgments	No requirement		No requirement	
9	References	No requirement		No requirement	
9.1	Normative references	No requirement		No requirement	
9.2	Informative references	No requirement		No requirement	

RADIUS - RFC 2865

The following table lists the RFC compliance 2865 for the controller based on the RADIUS.

TABLE 8 RADIUS as per RFC 2865

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	Informative
1.1	Specification of requirement	No requirement		No requirement	Informative
1.2	Terminology	No requirement		No requirement	Informative
2	Operation	Fully compliant		Fully compliant	
2.1	Challenge/response	Fully compliant		Fully compliant	

TABLE 8 RADIUS as per RFC 2865 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
2.2	Interoperation with PAP and CHAP	No requirement		No requirement	
2.3	Proxy	Fully compliant	Not applicable	Fully compliant	
2.4	Why UDP?	No requirement		No requirement	Informative
2.5	Retransmission hints	No requirement		No requirement	Informative
2.6	Keep-Alive considered harmful	No requirement		No requirement	Informative
3	Packet format	Fully compliant		Fully compliant	
4	Packet types	Fully compliant		Fully compliant	
4.1	Access request	Partial compliant		Compliant	User password and CHAP password is not implemented.
4.2	Access accept	Fully compliant		Fully compliant	
4.3	Access reject	Fully compliant		Not applicable	
4.4	Access challenge	Fully compliant		Fully compliant	
5	Attributes	Partial compliant		Partial compliant	
5.1	User name	Fully compliant		Fully compliant	
5.2	User password	Not applicable		Not applicable	
5.3	CHAP password	Not applicable		Not applicable	
5.4	NAS-IP address	Fully compliant		Fully compliant	
5.5	NAS port	Fully compliant		Fully compliant	
5.6	Service type	Compliant		Compliant	Framed and authorize (5176) is used.
5.7	Framed protocol	Not applicable		Not applicable	
5.8	Framed-IP address	Not applicable		Not applicable	
5.9	Framed-IP netmask	Not applicable		Not applicable	
5.10	Framed routing	Not applicable		Not applicable	
5.11	Filter Id	Not applicable		Not applicable	
5.12	Framed MTU	Compliant		Compliant	Used only in request.
5.13	Framed compression	Not applicable		Not applicable	
5.14	Login-IP-Host	Not applicable		Not applicable	
5.15	Login-Service	Not applicable		Not applicable	
5.16	Login-TCP-Port	Not applicable		Not applicable	
5.17	Unassigned	Not applicable		Not applicable	
5.18	Reply message	Partial compliant		Not applicable	Used only in reject.
5.19	Callback number	Not applicable		Not applicable	
5.20	Callback Id	Not applicable		Not applicable	
5.21	Unassigned)	Not applicable		Not applicable	
5.22	Framed route	Not applicable		Not applicable	
5.23	Framed-IPX-network	Not applicable		Not applicable	

TABLE 8 RADIUS as per RFC 2865 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
5.24	State	Partial compliant		Partial compliant	Access request sent by AP is not present.
5.25	Class	Not applicable		Not applicable	
5.26	Vendor specific	Fully compliant		Fully compliant	
5.27	Session timeout	Fully compliant		Not applicable	
5.28	Idle timeout	Fully compliant		Not applicable	
5.29	Termination-action	Not applicable		Not applicable	
5.30	Called-Station-Id	Fully compliant		Fully compliant	
5.31	Calling-Station-Id	Fully compliant		Fully compliant	
5.32	NAS identifier	Fully compliant		Fully compliant	
5.33	Proxy state	Fully compliant	Not applicable	Not applicable	
5.34	Login-LAT-Service	Not applicable		Not applicable	
5.35	Login-LAT-Node	Not applicable		Not applicable	
5.36	Login-LAT-Group	Not applicable		Not applicable	
5.37	Framed-AppleTalk-link	Not applicable		Not applicable	
5.38	Framed-AppleTalk-network	Not applicable		Not applicable	
5.39	Framed-AppleTalk-zone	Not applicable		Not applicable	
5.40	CHAP challenge	Not applicable		Not applicable	
5.41	NAS port type	Compliant		Compliant	
5.42	Port limit	Not applicable		Not applicable	
5.43	Login-LAT-Port	Not applicable		Not applicable	
5.44	Table of attributes	Partial compliant		Partial compliant	
6	IANA considerations	No requirement		No requirement	

RADIUS - RFC 4372

The following table lists the RFC compliance 4372 for the controller based on the dynamic authorization extension to remote authentication dial in user service (RADIUS).

TABLE 9 RADIUS - RFC 4372

Section Number	Section Title	Compliance	Comment
1.	Introduction	No requirement	
1.1	Motivation	No requirement	
1.2	Terminology	No requirement	
2	Operation	No requirement	
2.1.	Chargeable User Identify (CUI) attribute	Compliant	
2.2	CUI attribute	Compliant	
3	Attribute table	Compliant	
4	Diameter considerations	Not applicable	

TABLE 9 RADIUS - RFC 4372 (continued)

Section Number	Section Title	Compliance	Comment
5	IANA considerations	No requirement	
6	Security considerations	Compliant	
7	Acknowledgments	No requirement	
8	References	No requirement	
8.1	Normative references	No requirement	
8.2	Informative references	No requirement	

RADIUS - RFC 5176

The following table lists the RFC compliance 5176 for the controller based on the dynamic authorization extensions to remote authentication dial in user service (RADIUS).

TABLE 10 RADIUS - RFC 5176

Section Number	Section Title	TTG	Non TTG	Comment
1.	Introduction	No requirement		
1.1	Applicability	No requirement		
1.2	Requirements language	No requirement		
1.3	Terminology	No requirement		
2	Overview	No requirement		
2.1.	Disconnect Messages (DM)	Compliant		No acct terminate cause in DM-ACK. (disconnect message acknowledgment)
2.2	Change of Authorization Messages (CoA)	Compliant		
2.3	Packet format	Compliant		Messages from DAC (Dynamic Authorization Client) need to be assigned to the controller IP address rather than the NAS IP address.
3	Attributes	Compliant		Does not support IPv6.
3.1.	Proxy state	Compliant		
3.2	Authorize only	Partially compliant		Ruckus AP does not support CoA service type authorize only.
3.3	State	Compliant		
3.4	Message authenticator	Compliant		
3.5	Error cause	Compliant		Error cause attribute values 201, 202, 406, 502, 504, 507 and 508 are not supported in this release.
3.6	Table of attributes	Compliant		
4	Diameter considerations	Not applicable		
5	IANA considerations	No requirement		
6	Security considerations	No requirement		
6.1	Authorization issues	Compliant		
6.2	IPsec usage guidelines	Non-compliant		This feature is not supported.

TABLE 10 RADIUS - RFC 5176 (continued)

Section Number	Section Title	TTG	Non TTG	Comment
6.3	Replay protection	Partially compliant		The event timestamp attribute is not included in CoA. DM request checks for duplication of controller initiated CoA/DM.
7	Example traces	No requirement		
8	References	No requirement		
8.1	Normative references	No requirement		
8.2	Informative references	No requirement		
9	Acknowledgments	No requirement		

RADIUS Extension - RFC 2869

The following table lists the RFC compliance 2869 for the controller based on the RADIUS extension.

TABLE 11 RADIUS Extension - RFC 2869

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	Information
1.1	Specification of requirements	No requirement		No requirement	Information
1.2	Terminology	No requirement		No requirement	Information
2	Operation	No requirement		No requirement	Information
2.1	RADIUS support for interim accounting updates	Compliant		Compliant	Supports accounting interim.
2.2	RADIUS support for Apple remote access protocol	Not applicable		Not applicable	
2.3	RADIUS support for EAP (Extensible Authentication Protocol)	Fully compliant		Fully compliant	Supports EAP inside RADIUS.
2.3.1	Protocol overview	Fully compliant		Fully compliant	The controller acts as both proxy and AAA server.
2.3.2	Retransmission	Compliant		Compliant	Session timeout is present only in **accept message.**
2.3.3	Fragmentation	Fully compliant		Fully compliant	
2.3.4	Examples	Not applicable		Not applicable	Does not support EAP-PPP.
2.3.5	Alternative uses	Not Applicable		Not Applicable	Does not support encapsulated EAP.
3	Packet format	Compliant		Compliant	
4	Packet type	Compliant		Compliant	
5	Attributes	Partially compliant		Partially compliant	The controller does not use all the listed attributes.
5.1	Acct-Input-Gigawords				
5.2	Acct-Output-Gigawords				

TABLE 11 RADIUS Extension - RFC 2869 (continued)

Section Number	Section Title	Controller as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
5.3	Event timestamp	Not applicable		Not applicable	
5.4	ARAP password	Not applicable		Not applicable	
5.5	ARAP features	Not applicable		Not applicable	
5.5	ARAP-zone-access	Not applicable		Not applicable	
5.7	ARAP security	Not applicable		Not applicable	
5.8	ARAP security-data	Not applicable		Not applicable	
5.9	Password retry	Not applicable		Not applicable	
5.10	Prompt	Not applicable		Not applicable	
5.11	Connect info	Fully compliant		Fully compliant	
5.12	Configuration token	No requirement		No requirement	Does not support this attribute.
5.13	EAP message	Fully compliant		Fully compliant	
5.14	Message authenticator	Fully compliant		Fully compliant	
5.15	ARAP challenge-response	No requirement		No requirement	
5.16	Acct-interim-interval	Fully compliant		No requirement	Configuration is available in the controller web user interface.
5.17	NAS-Port-ID	No requirement		No requirement	
5.18	Framed pool	No requirement		No requirement	
5.19	Table of attributes	Partially compliant		Partially compliant	The listed attributes are compliant
6	IANA considerations	No requirement		No requirement	
7	Security considerations	No requirement		No requirement	
7.1	Message authenticator security	Fully compliant		Fully compliant	
7.2	EAP security	Not applicable		Not applicable	
8	References	No requirement		No requirement	
9	Acknowledgments	No requirement		No requirement	
10	Chair's address	No requirement		No requirement	
11	Author's address	No requirement		No requirement	
12	Full copyright statement	No requirement		No requirement	

RADIUS Accounting - RFC 2866

The following table lists the RFC compliance 2866 for the controller based on the RADIUS accounting.

TABLE 12 RADIUS Accounting - RFC 2866

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the Controller)		TTG Support (Controller generated accounting packets)	Comments
		Ruckus AP	Controller		
1	Introduction	No requirement		No requirement	Informative

TABLE 12 RADIUS Accounting - RFC 2866 (continued)

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the Controller)		TTG Support (Controller generated accounting packets)	Comments
		Ruckus AP	Controller		
1.1	Specification of requirement	No requirement		No requirement	Informative
1.2	Terminology	No requirement		No requirement	Informative
2	Operation	Compliant	Fully compliant	Fully compliant	Accounting packets initiated from Ruckus AP's for PDG does not have a secondary server option.
2.1	Proxy	Not applicable	Fully compliant	Fully compliant	
3	Packet format	Fully compliant		Fully compliant	
4	Packet type	Fully compliant		Fully compliant	
4.1	Accounting request	Fully compliant		Fully compliant	For TTG, NAS port type is set to 0 (ASYNC) and no NAS port. For PDG, NAS port type is set to as (19), wireless 802.11.
4.2	Accounting response	Fully compliant		Fully compliant	
5	Attributes	Fully compliant		Fully compliant	
5.1	Acct – Status Type	Fully compliant	Compliant	Compliant	Accounting on/off Proxy is not supported for TTG Calls as controller has other mechanisms to handle the same.
5.2	Acct – Delay- Time	Fully compliant		Fully compliant	
5.3	Acct – Input – Octates	Non compliant		Non compliant	The attribute is present in interim message. The RFC recommends that the attribute is present in **stop**.
5.4	Acct – Output – Octates	Non compliant		Non compliant	The attribute is present in interim message. The RFC recommends that the attribute is present in **stop**.
5.5	Acct-Session-Id	Fully compliant		Fully compliant	For TTG, the case value is assigned by GGSN/PGW.
5.5	Acct-Authentic	Compliant		Not applicable	Only RADIUS is used.
5.7	Acct-Session-Time	Non compliant		Non compliant	The attribute is present in interim message. The RFC recommends that the attribute is present in **stop**.
5.8	Acct-Input-Packets	Non compliant		Non compliant	The attribute is present in interim message. The RFC recommends that the attribute is present in **stop**.
5.9	Acct-Output-Packets	Non compliant		Non compliant	The attribute is present in interim message. The RFC recommends that the attribute is present in **stop**.

TABLE 12 RADIUS Accounting - RFC 2866 (continued)

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the Controller)		TTG Support (Controller generated accounting packets)	Comments
		Ruckus AP	Controller		
5.10	Acct-Terminate-Cause	Compliant		Compliant	Only a few causes have been implemented.
5.11	Acct-Multi-Session-Id	Fully compliant		Not applicable	
5.12	Acct-Link-Count	Fully compliant		Not applicable	
5.13	Table of attributes	Compliant		Compliant	
6	IANA considerations	No requirement		No requirement	
7	Security considerations	No requirement		No requirement	
8	Change log	No requirement		No requirement	
9	References	No requirement		No requirement	
10	Acknowledgments	No requirement		No requirement	
11	Chair's address	No requirement		No requirement	
12	Author's address	No requirement		No requirement	
13	Full copyright statement	No requirement		No requirement	

Lightweight Directory Access Protocol (LDAP) - RFC 4511

The following table lists the RFC compliance 4511 for controller based on the Lightweight Directory Access Protocol (LDAP).

TABLE 13 LDAP Compliance- RFC 4511

Section Number	Section Title	Proxy Requirement	Comments
1	Introduction	No requirement	
2	Conventions	No requirement	
3	Protocol model	No requirement	
4	Element of protocol	No requirement	
4.1	Common elements	No requirement	
4.2	Bind operations	Compliant	
4.3	Unbind operation	Compliant	
4.4	Unsolicited notification	Not compliant	
4.5	Search operation	Compliant	
4.6	Modify operation	Not compliant	
4.7	Add operation	Not compliant	
4.8	Delete operation	Not compliant	
4.9	Modify DN operation	Not compliant	
4.10	Compare operation	Not compliant	
4.11	Abandon operation	Not compliant	
4.12	Extended operation	Not compliant	
4.13	Intermediate response message	Not compliant	
4.14	Start TLS operation	Not compliant	
5	Protocol encoding	Compliant	

TABLE 13 LDAP Compliance- RFC 4511 (continued)

Section Number	Section Title	Proxy Requirement	Comments
5.2	Transmission Control Protocol (TCP)	Compliant	
5.3	Termination of the LDAP session	Compliant	Unbind
6	Security considerations	Compliant	Simple authentication
7	Acknowledgments	No requirement	
8	Normative references	No requirement	
9	Informative references	No requirement	

CoA and DM to support RFC 5176 in Proxy Mode

Change of Authorization (CoA) and Disconnect Message (DM) attributes that support RFC 5176 in Proxy Mode are documented.

The following sections contain information about:

- Compliance Table
- CoA message attributes
- Disconnect message attributes
- Error cause

TABLE 14 Compliance table for CoA/DM

Section	Section Title	CoA /DM message from Radius server processed by Controller	Comments
1	Introduction	No requirement	Informative
1.1	Applicability	No requirement	Informative
1.2	Requirements Language	No requirement	Informative
1.3	Terminology	No requirement	Informative
2	Overview	Fully Compliant	Commonly implemented features of Disconnect and Change-of-Authorization
2.1	Disconnect Messages(DMs)	Fully Compliant	
2.2	Change-of-Authorization(CoA) Messages	Compliant	
2.3	Packet Format	Compliant	
3	Attributes	Compliant	NAS identification attributes and session identification attributes are supported.
3.1	Proxy State	Non-compliant	
3.2	Authorize Only	Non-compliant	
3.3	State	Partially compliant	Attribute is present in the CoA message.
3.4	Message-Authenticator	Fully compliant	
3.5	Error-Cause	Partially compliant	Only a few causes are handled.
3.6	T able of Attributes	Partially compliant	Few attributes are not supported. If it is received the controller-RAC ignores it.
4	Diameter Considerations	Non-compliant	
5	IANA Considerations	No requirement	Informative
6	Security Considerations	Non-compliant	
6.1	Authorization Issues	Non-compliant	
6.2	IPsec Usage Guidelines	Non-compliant	

TABLE 14 Compliance table for CoA/DM (continued)

Section	Section Title	CoA /DM message from Radius server processed by Controller	Comments
6.3	Replay Protection	Non-compliant	
7	Example Traces	No requirement	Informative
8	References	No requirement	Informative
8.1	Normative References	No requirement	Informative
8.2	Informative References	No requirement	Informative
9	Acknowledgments	No requirement	Informative
	Appendix A	No requirement	Informative

CoA Message Attributes

The following table lists the CoA message attributes.

TABLE 15 CoA Message Attributes

No	CoA Message Attribute	State	Comment
1	User-Name	Supported	Validated by RAC if present in CoA request
4	NAS-IP-A ddress	Supported	Validated by RAC if present in CoA request
5	NAS-Port	Supported	Validated by RAC if present in CoA request
6	Service-Type	Ignored	Not validated and ignored by RAC (ACK is sent)
7	Framed-Protocol	Ignored	Not validated and ignored by RAC (ACK is sent)
8	Framed-IP-Address	Supported	Validated by RAC if present in CoA request
9	Framed-IP-Netmask	Ignored	Not validated and ignored by RAC (ACK is sent)
10	Framed-Routing	Ignored	Not validated and ignored by RAC (ACK is sent)
11	Filter-ID	Supported	Validated by RAC if present in CoA request
12	Framed-MTU	Ignored	Not validated and ignored by RAC (ACK is sent)
13	Framed-Compression	Ignored	Not validated and ignored by RAC (ACK is sent)
14	Login-IP-Host	Ignored	Not validated and ignored by RAC (ACK is sent)
15	Login-Service	Ignored	Not validated and ignored by RAC (ACK is sent)
16	Login-TCP-Port	Ignored	Not validated and ignored by RAC (ACK is sent)
18	Reply-Message	Ignored	Not validated and ignored by RAC (ACK is sent)
19	Call back-Number	Ignored	Not validated and ignored by RAC (ACK is sent)
20	Callback-Id	Ignored	Not validated and ignored by RAC (ACK is sent)
22	Framed-Route	Ignored	Not validated and ignored by RAC (ACK is sent)
23	Framed-IPX-Network	Ignored	Not validated and ignored by RAC (ACK is sent)
24	State	Ignored	Not validated and ignored by RAC (ACK is sent)
25	Class	Supported	Validated by RAC if present in CoA request
26	Vendor-Specific	Not supported	Not supported by RAC (NAK is sent)
27	Session-Timeout	Supported	Validated by RAC if present in CoA request
28	Idle-Timeout	Supported	Validated by RAC if present in CoA request
29	Termination-Action	Ignored	Validated by RAC if present in CoA request
30	Called-Station-Id	Supported	Validated by RAC if present in CoA request
31	Calling-Station-Id	Supported	Validated by RAC if present in CoA request

TABLE 15 CoA Message Attributes (continued)

No	CoA Message Attribute	State	Comment
32	NAS-Identifier	Supported	Validated by RAC if present in CoA request
33	Proxy-State	Ignored	Not validated and ignored by RAC (ACK is sent)
34	Login-LAT-Service	Ignored	Not validated and ignored by RAC (ACK is sent)
35	Login-LAT-Node	Ignored	Not validated and ignored by RAC (ACK is sent)
36	Login-LAT-Group	Ignored	Not validated and ignored by RAC (ACK is sent)
37	Framed-AppleTalk-Link	Ignored	Not validated and ignored by RAC (ACK is sent)
38	Framed-AppleTalk-	Ignored	Not validated and ignored by RAC (ACK is sent)
39	Framed-AppleTalk-Zone	Ignored	Not validated and ignored by RAC (ACK is sent)
44	Acct-Session-ID	Supported	Validated by RAC if present in CoA request
50	Acct-Multi-Session-Id	Supported	Validated by RAC if present in CoA request
55	Event-Timestamp	Ignored	Not validated and ignored by RAC (ACK is sent)
56	Egress-VLANID	Ignored	Not validated and ignored by RAC (ACK is sent)
57	Ingress-Filters	Ignored	Not validated and ignored by RAC (ACK is sent)
58	Egress-VLAN-Name	Ignored	Not validated and ignored by RAC (ACK is sent)
59	User-Priority-Table	Ignored	Not validated and ignored by RAC (ACK is sent)
61	NAS-Port-Type	Not supported	Not supported by RAC (NAK is sent)
62	Port-Limit	Ignored	Not validated and ignored by RAC (ACK is sent)
63	Login-LAT-Port	Ignored	Not validated and ignored by RAC (ACK is sent)
64	Tunnel-Type	Ignored	Not validated and ignored by RAC (ACK is sent)
65	Tunnel-Medium-Type	Ignored	Not validated and ignored by RAC (ACK is sent)
66	Tunnel-Client-Endpoint	Ignored	Not validated and ignored by RAC (ACK is sent)
67	Tunnel-Server-Endpoint	Ignored	Not validated and ignored by RAC (ACK is sent)
69	Tunnel-Password	Ignored	Not validated and ignored by RAC (ACK is sent)
71	ARAP-Features	Ignored	Not validated and ignored by RAC (ACK is sent)
72	ARAP-Zone-Access	Ignored	Not validated and ignored by RAC (ACK is sent)
78	Configuration-Token	Ignored	Not validated and ignored by RAC (ACK is sent)
79	EAP-Message	Ignored	Not validated and ignored by RAC (ACK is sent)
80	Message-Authenticator	Ignored	Not validated and ignored by RAC (ACK is sent)
81	Tunnel-Private-Group-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
82	Tunnel-Assignment-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
83	Tunnel-Preference	Ignored	Not validated and ignored by RAC (ACK is sent)
85	Acct-Interim-Interval	Supported	Validated by RAC if present in CoA request
87	NAS-Port-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
88	Framed-Pool	Ignored	Not validated and ignored by RAC (ACK is sent)
89	Chargeable-User-Identity	Supported	Validated by RAC if present in CoA request
90	Tunnel-Client-Auth-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
91	Tunnel-Server-Auth-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
92	NAS-Filter-Rule	Ignored	Not validated and ignored by RAC (ACK is sent)
94	Originating-Line-Info	Not supported	Not supported by RAC (NAK is sent)
95	NAS-IPv6-Address	Supported	Validated by RAC if present in CoA request
96	Framed-Interface-ID	Supported	Validated by RAC if present in CoA request

TABLE 15 CoA Message Attributes (continued)

No	CoA Message Attribute	State	Comment
97	Framed-IPv6-Prefix	Supported	Validated by RAC if present in CoA request
98	Login-IPv6-Host	Ignored	Not validated and ignored by RAC (ACK is sent)
99	Framed-IPv6-Route	Ignored	Not validated and ignored by RAC (ACK is sent)
100	Framed-IPv6-Pool	Ignored	Not validated and ignored by RAC (ACK is sent)
101	Error-Cause	Not supported	Not supported by RAC (NAK is sent)
123	Delegated-IPv6-Prefix	Ignored	Not validated and ignored by RAC (ACK is sent)

Disconnect Messages Attributes

The following table lists the Disconnect Messages (DM) message attributes.

TABLE 16 DM Attributes

No	CoA Message Attribute	State	Comment
1	User-Name	Supported	Validated by RAC if present in DM request
4	NAS-IP-Address	Supported	Validated by RAC if present in DM request
5	NAS-Port	Supported	Validated by RAC if present in DM request
6	Service-Type	Ignored	Not validated and ignored by RAC (ACK is sent)
8	Framed-IP-Address	Supported	Validated by RAC if present in DM request
18	Reply-Message	Ignored	Not validated and ignored by RAC (ACK is sent)
19	Callback-Number	Ignored	Not validated and ignored by RAC (ACK is sent)
24	State	Not supported	Not validated and ignored by RAC (ACK is sent)
25	Class	Ignored	Not validated and ignored by RAC (ACK is sent)
26	Vendor-Specific	Not supported	Not supported by RAC (NAK is sent)
27	Session-Timeout	Supported	Validated by RAC if present in DM request
30	Called-Station-ID	Supported	Validated by RAC if present in DM request
31	Calling-Station-ID	Supported	Validated by RAC if present in DM request
32	NAS-Identifier	Supported	Validated by RAC if present in DM request
33	Proxy-State	Ignored	Not validated and ignored by RAC (ACK is sent)
44	Acct-Session-ID	Supported	Validated by RAC if present in DM request
49	Acct-Terminate-Cause	Supported	Validated by RAC if present in DM request
50	Acct-Multi-Session-ID	Supported	Validated by RAC if present in CoA request
55	Event-Timestamp	Ignored	Not validated and ignored by RAC (ACK is sent)
61	NAS-Port-Type	Not supported	Not supported by RAC (NAK is sent)
79	EAP-Message	Ignored	Not validated and ignored by RAC (ACK is sent)
80	Message-Authenticator	Ignored	Not validated and ignored by RAC (ACK is sent)
87	NAS-Port-ID	Ignored	Not validated and ignored by RAC (ACK is sent)
89	Chargeable-User-Identity	Supported	Validated by RAC if present in DM request
95	NAS-IPv6-Address	Supported	Validated by RAC if present in DM request
96	Framed-Interface-ID	Supported	Validated by RAC if present in DM request
97	Framed-IPv6-Prefix	Supported	Validated by RAC if present in DM request
101	Error-Cause	Not supported	Not supported by RAC (NAK is sent)

Error Cause

The following table lists the error cause attributes.

TABLE 17 Error Cause

No	Attribute	State	Comments
201	Residual Session Context Removed		
202	Invalid EAP Packet (Ignored)		
401	Unsupported Attribute	Supported	
402	Missing Attribute	Supported	
403	NAS Identification Mismatch	Supported	
404	Invalid Request		
405	Unsupported Service		
406	Unsupported Extension		
407	Invalid Attribute Value		
501	Administratively Prohibited		
502	Request Not Routable (Proxy)		
503	Session Context Not Found	Supported	
504	Session Context Not Removable		
505	Other Proxy Processing Error		
506	Resources Unavailable		
507	Request Initiated		
508	Multiple Session Selection Unsupported		

Controller and 3GPP Compliance Report

Overview

This compliance report lists the 3GPP controller to GPRS Tunneling compliance test report for the controllers. It contains the test topology and compliance matrix support. This document shows the test results for all the supported features.

NOTE
Refer to About This Report on page 9 for conventions used in this report.

NOTE
If the compliance statement is identical for all sections below a certain level, the sub-sections may not be itemized.

3GPP Controller to GPRS Tunneling

The following table lists the 3GPP inter-working of the controller to GPRS tunneling protocols. This is based on 3GPP TS 29.060 compliance aspects.

TABLE 18 3GPP Controller to GPRS Tunneling

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions and abbreviations	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Abbreviations	No requirement	Informative
4	General	Partially compliant	Used from the Wi-Fi offload perspective. The controller acts as SGSN while interacting with GGSN. Does not support RAN, Iu (UTRAN-SGSN) and Gn (SGSN-SGSN) interfaces.
5	Transmission order and bit definitions	Fully compliant	
6	GTP header	Compliant	Does not support NPDU and extension headers. Sequence numbers are present for GTPC but absent for GTPU.
6.1	Extension headers	Not applicable	
6.1.1	PDCP PDU number	Not applicable	
6.1.2	Suspend request	Not applicable	
6.1.3	Suspend response	Not applicable	
6.1.4	MBMS support indication	Not applicable	
7	GTP messages and message formats	No requirement	

TABLE 18 3GPP Controller to GPRS Tunneling (continued)

Section Number	Section Title	Support	Comments
7.1	Message formats	Compliant	
7.1.1	Presence requirements of information elements	No requirement	
7.2	Path management messages	Compliant	Messages exchanged only between the controller (SGSN) and GGSN.
7.2.1	Echo request	Compliant	Does not support private extension.
7.2.2	Echo response	Compliant	Does not support private extension.
7.2.3	Version not supported	Compliant	
7.2.4	Supported extension headers notification	Not applicable	
7.3	Tunnel management messages	No requirement	
7.3.1	Create PDP context request	Compliant	
7.3.2	Create PDP context response	Compliant	
7.3.3	Update PDP context request	Compliant	
7.3.4	Update PDP context response	Compliant	
7.3.5	Delete PDP context request	Compliant	
7.3.6	Delete PDP context response	Compliant	
7.3.7	Error indication	Compliant	The controller (SGSN) handles and deletes the session if the message is initiated by GGSN. The controller (SGSN) does not initiate it.
7.3.8	PDU notification request	Not applicable	
7.3.9	PDU notification response	Not applicable	
7.3.10	PDU notification reject request	Not applicable	
7.3.11	PDU notification reject response	Not applicable	
7.4	Location management messages	Not applicable	
7.5	Mobility management messages	Not applicable	
7.6	Reliable delivery of signaling messages	Compliant	
7.7	Information elements	Compliant	Supported Information elements are provided in this chapter.
7.7.1	Cause	Compliant	
7.7.2	IMSI	Fully compliant	
7.7.3	RAI	Fully compliant	
7.7.4	TLLI	Not applicable	
7.7.5	P-TMSI	Not applicable	
7.7.6	Reordering required	Not applicable	
7.7.7	Authentication triplet	Not applicable	
7.7.8	MAP cause	Not applicable	
7.7.9	P-TMSI signature	Not applicable	
7.7.10	MS validated	Not applicable	
7.7.11	Recovery	Fully compliant	
7.7.12	Selection mode	Not applicable	
7.7.13	Tunnel endpoint identifier date I	Fully compliant	
7.7.14	Tunnel endpoint identifier control plane	Fully compliant	
7.7.15	Tunnel endpoint identifier date I1	Not applicable	

TABLE 18 3GPP Controller to GPRS Tunneling (continued)

Section Number	Section Title	Support	Comments
7.7.16	Teatdown Ind	Fully compliant	
7.7.17	NSAPI	Fully compliant	
7.7.18	RANAP cause	Not applicable	
7.7.19	RAB context	Not applicable	
7.7.20	Radio priority SMS	Not applicable	
7.7.21	Radio priority	Not applicable	
7.7.22	Packet flow Id	Not applicable	
7.7.23	Charging characteristics	Compliant	
7.7.24	Trace reference	Not applicable	
7.7.25	Trace type	Not applicable	
7.7.25A	MS not reachable reason	Not applicable	
7.7.25B	Radio priority LCS	Not applicable	
7.7.26	Charging Id	Not applicable	
7.7.27	End user address	Compliant	
7.7.28	MM context	Not applicable	
7.7.29	PDP context	Not applicable	
7.7.30	Access point name	Fully compliant	
7.7.31	Protocol configuration options	Fully compliant	
7.7.32	GSN address	Fully compliant	
7.7.33	MSISDN	Fully compliant	
7.7.34	QOS profile	Fully compliant	
7.7.35	Authentication quintuplet	Not applicable	
7.7.36	TFT	Not applicable	
7.7.37	Target identification	Not applicable	
7.7.38	UTRAN transparent container	Not applicable	
7.7.39	RAB setup information	Not applicable	
7.7.40	Extension header type list	Not applicable	
7.7.41	Trigger Id	Not applicable	
7.7.42	OMC Identity	Not applicable	
7.7.43	RAN transport container	Not applicable	
7.7.44	Charging gateway address	Compliant	Supports only IPv4.
7.7.45	PDP context prioritization	Not applicable	
7.7.45A	Additional RAB setup information	Not applicable	
7.7.46	Private extension	Not applicable	
7.7.47	SGSN number	Not applicable	
7.7.48	Common flags	Not applicable	
7.7.49	APN restriction	Not applicable	
7.7.50	RAT type	Compliant	
7.7.51	User location information	Not applicable	
7.7.52	MS time zone	Not applicable	
7.7.53	IMEI (SV)	Not applicable	

TABLE 18 3GPP Controller to GPRS Tunneling (continued)

Section Number	Section Title	Support	Comments
7.7.54	CAMEL charging information container	Not applicable	
7.7.55	MBMS UE context	Not applicable	
7.7.56	Temporary mobile group identity	Not applicable	
7.7.57	RIM routing address	Not applicable	
7.7.58	MBMS protocol configuration options	Not applicable	
7.7.59	MBMS session duration	Not applicable	
7.7.60	MBMS service area	Not applicable	
7.7.61	Source RNC PDCP context info	Not applicable	
7.7.62	Additional trace Info	Not applicable	
7.7.63	Hop counter	Not applicable	
7.7.64	Selected PLMN Id	Not applicable	
7.7.65	MBMS session identifier	Not applicable	
7.7.66	MBMS 2G/3G indicator	Not applicable	
7.7.67	Enhanced NSAPI	Not applicable	
7.7.68	Additional MBMS trace info	Not applicable	
7.7.69	MBMS session repetition number	Not applicable	
7.7.70	MBMS time to data transfer	Not applicable	
7.7.71	Void	No requirement	
7.7.72	BSS container	Not applicable	
7.7.73	Cell identification	Not applicable	
7.7.74	PDU numbers	Not applicable	
7.7.75	BSSGP cause	Not applicable	
7.7.76	Required MBMS bearer capabilities	Not applicable	
7.7.77	RIM routing address discriminator	Not applicable	
7.7.78	List of set-up PFCs	Not applicable	
7.7.79	PS handover XID parameters	Not applicable	
7.7.80	Reliable inter RAT handover info	Not applicable	
8	Controlplane (GTP-C)	Compliant	
8.1	Controlplane protocol	Fully compliant	
8.2	Usage of the GTP-C header	Compliant	
9	GTP-U	Fully compliant	
9.1	GTP-U protocol entity	Fully compliant	
9.1.1	Handling of sequence numbers	Not applicable	Does not support sequence numbers.
9.2	GTP-U service access points and primitives	Not applicable	
9.3	Protocol stack	Fully compliant	
9.3.1	Usage of the GTP-U header	Fully compliant	
9.3.1.1	Usage of sequence number	Not applicable	Sequence number is supported only for control plane.
9.4	Tunneling between SGSNs	Not applicable	The controller provides a Wi-Fi offload solution.
9.5	Tunneling between source RNC and target RNC	Not applicable	
9.6	Tunneling between GGSNs	Not applicable	

TABLE 18 3GPP Controller to GPRS Tunneling (continued)

Section Number	Section Title	Support	Comments
10	Path protocols	No requirement	
10.1	UDP/IP	Fully compliant	
10.1.1	UDP header	No requirement	
10.1.1.1	Request messages	Fully compliant	
10.1.1.2	Response messages	Fully compliant	
10.1.1.3	Encapsulated T-PDUs	Fully compliant	
10.1.1.4	Error indication, RAN information Relay, Version not supported and supported extension header notification	Compliant	
10.1.2	IP header	Fully compliant	
10.1.2.1	Request messages and encapsulated T-PDUs	Fully compliant	
10.1.2.2	Response messages	Fully compliant	
10.1.2.3	Error indication, RAN information Relay, Version not supported and supported extension header notification	Compliant	
11	Error handling	No requirement	
11.1	Protocol errors	Compliant	
11.1.1	Different GTP versions	Compliant	Supports GTPv1 and GTPv2. Does not support Fallback.
11.1.2	GTP message too short	Fully compliant	
11.1.3	Unknown GTP signaling message	Fully compliant	
11.1.4	Unexpected GTP signaling message	Fully compliant	
11.1.5	Missing mandatory present information element	Fully compliant	
11.1.6	Invalid length	Fully compliant	
11.1.7	Invalid mandatory information element	Fully compliant	
11.1.8	Invalid optional information element	Fully compliant	
11.1.9	Unknown information element	Fully compliant	
11.1.10	Out of sequence information elements	Fully compliant	
11.1.11	Unexpected information element	Fully compliant	
11.1.12	Repeated information elements	Fully compliant	
11.1.13	Incorrect optional information elements	Fully compliant	
11.2	Path failure	Fully compliant	
11.3	MS detach	Fully compliant	
11.4	Restoration and recovery	Fully compliant	
12	Security provided to GTP communication over Gn and Gp interfaces	Not applicable	Security is provided only for mobility management messages, which is not supported.
13	IP, networking technology used by GTP	No requirement	
13.1	IP version	Fully compliant	Does not support IPv6.
13.2	IP fragmentation	Not applicable	Path MTU is set as less.
13.2.1	MO direction	Not applicable	
13.2.2	MT direction	Not applicable	
13.2.3	Tunneling from old to new SGSN	Not applicable	

TABLE 18 3GPP Controller to GPRS Tunneling (continued)

Section Number	Section Title	Support	Comments
14	GTP parameters	No requirement	
14.1	Timers	Compliant	
14.2	Others	Compliant	

SNMP v3 Compliance

Module Compliance

The following figure shows the module compliance based on RFC 2571.

FIGURE 1 Statement of module compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.6.1	Check system group	FAILED
3.6.2	Check sysORTable	PASSED
3.6.3	Check SNMP group	PASSED
3.9.1	Detect missing object in GROUP	WARNING
3.9.2	Detect missing objects in MIBs	WARNING

Boundary Conditions Compliance

The following figure shows the statement of boundary conditions compliance for RFC 2571.

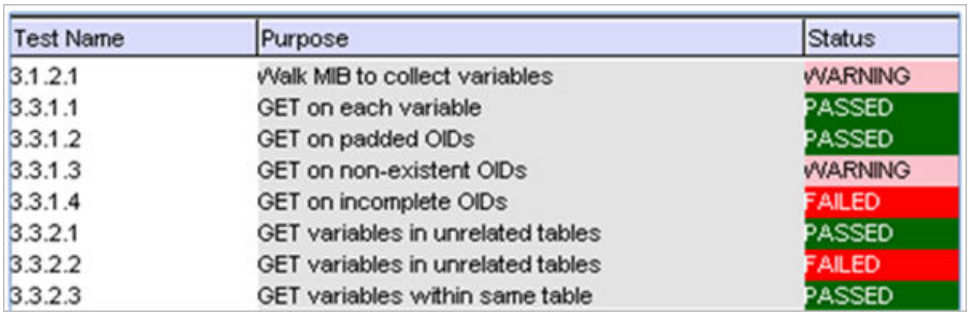
FIGURE 2 Boundary conditions compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.5.1.1	snmpInASNParseErrs	PASSED
3.5.1.2	Request with non-minimal encoding	PASSED
3.5.1.3.1	snmpInASNParseErrs	PASSED
3.5.1.3.2	snmpInBadVersions	PASSED
3.5.1.3.3	Request with 129 sub-ids	PASSED
3.5.1.4	Request with smaller BER length	PASSED
3.5.1.5	Request with larger BER length	PASSED
3.5.1.7	Request with unexpected PDUs	PASSED
3.5.2.1	Request with non-zero errorStatus	PASSED
3.5.2.2	Request with non-zero errorIndex	PASSED
3.5.2.3	Request with zero varbinds	PASSED
3.5.2.4	Request without using NULL	PASSED
3.5.2.5	Request with tooBig varbinds	PASSED
3.5.2.6	Request with MAX and MIN req-ID	PASSED

SNMP GET Compliance

The following figure shows the statement of SNMP set compliance for RFC 2571.

FIGURE 3 SNMP GET compliance

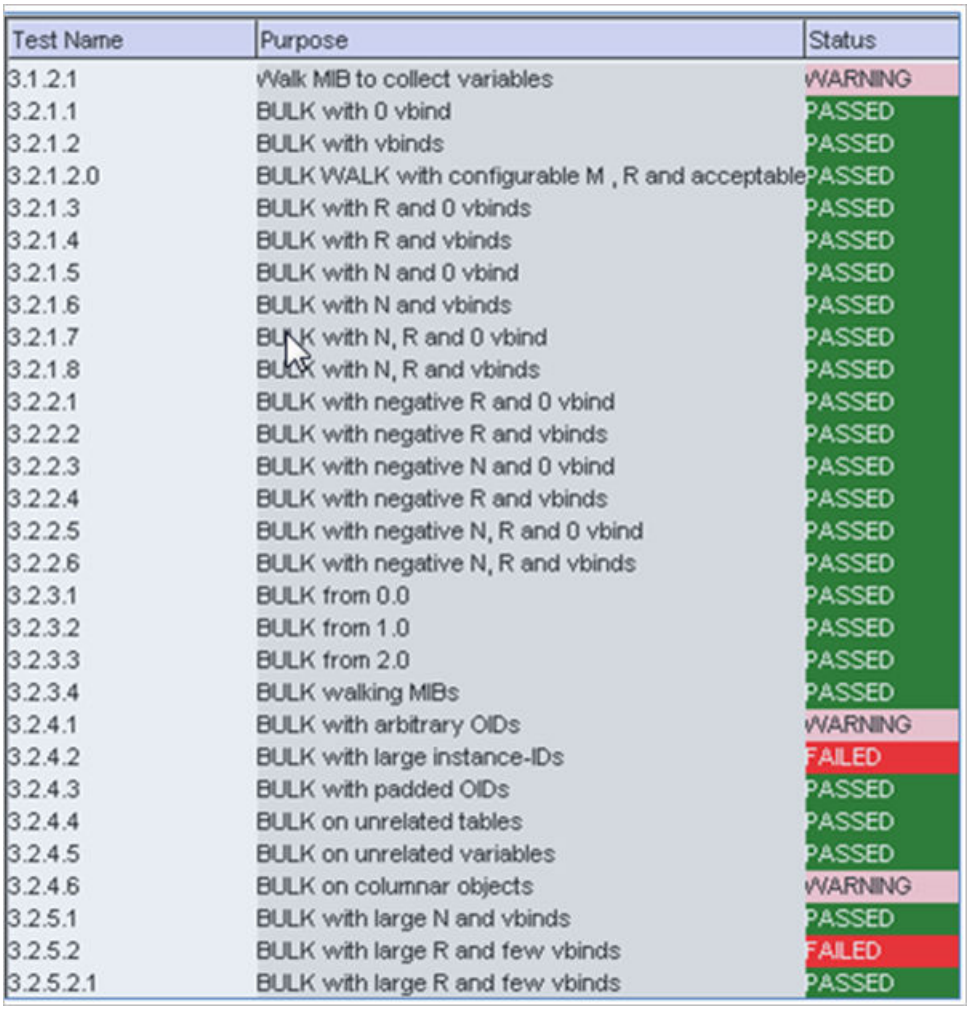


Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.3.1.1	GET on each variable	PASSED
3.3.1.2	GET on padded OIDs	PASSED
3.3.1.3	GET on non-existent OIDs	WARNING
3.3.1.4	GET on incomplete OIDs	FAILED
3.3.2.1	GET variables in unrelated tables	PASSED
3.3.2.2	GET variables in unrelated tables	FAILED
3.3.2.3	GET variables within same table	PASSED

SNMP Bulk Compliance

The following figure shows the statement of SNMP bulk compliance for RFC 2571.

FIGURE 4 SNMP bulk compliance



Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.2.1.1	BULK with 0 vbind	PASSED
3.2.1.2	BULK with vbinds	PASSED
3.2.1.2.0	BULK WALK with configurable M , R and acceptable	PASSED
3.2.1.3	BULK with R and 0 vbinds	PASSED
3.2.1.4	BULK with R and vbinds	PASSED
3.2.1.5	BULK with N and 0 vbind	PASSED
3.2.1.6	BULK with N and vbinds	PASSED
3.2.1.7	BULK with N, R and 0 vbind	PASSED
3.2.1.8	BULK with N, R and vbinds	PASSED
3.2.2.1	BULK with negative R and 0 vbind	PASSED
3.2.2.2	BULK with negative R and vbinds	PASSED
3.2.2.3	BULK with negative N and 0 vbind	PASSED
3.2.2.4	BULK with negative R and vbinds	PASSED
3.2.2.5	BULK with negative N, R and 0 vbind	PASSED
3.2.2.6	BULK with negative N, R and vbinds	PASSED
3.2.3.1	BULK from 0.0	PASSED
3.2.3.2	BULK from 1.0	PASSED
3.2.3.3	BULK from 2.0	PASSED
3.2.3.4	BULK walking MIBs	PASSED
3.2.4.1	BULK with arbitrary OIDs	WARNING
3.2.4.2	BULK with large instance-IDs	FAILED
3.2.4.3	BULK with padded OIDs	PASSED
3.2.4.4	BULK on unrelated tables	PASSED
3.2.4.5	BULK on unrelated variables	PASSED
3.2.4.6	BULK on columnar objects	WARNING
3.2.5.1	BULK with large N and vbinds	PASSED
3.2.5.2	BULK with large R and few vbinds	FAILED
3.2.5.2.1	BULK with large R and few vbinds	PASSED

SNMP Next Compliance

The following figure shows the statement of SNMP next compliance for RFC 2571.

FIGURE 5 SNMP next compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.1.2.3	Walk by column and scalar	never run
3.1.1.1	NEXT request from 0.0	PASSED
3.1.1.2	NEXT request from 1.0	PASSED
3.1.1.3	NEXT request from 2.0	PASSED
3.1.2.2	Walk and check object syntax	FAILED
3.1.3.1	NEXT with arbitrary OIDs	FAILED
3.1.3.2	NEXT with large instance-IDs	FAILED
3.1.3.3	NEXT with padded OIDs	PASSED
3.1.4.1	NEXT on unrelated tables	PASSED
3.1.4.2	NEXT with unrelated variables	PASSED
3.1.4.3	NEXT on columnar objects	PASSED
3.1.5	Check Request-ID correlation	PASSED

SNMP Set Compliance

The following figure shows the statement of SNMP set compliance for RFC 2571.

FIGURE 6 SNMP set compliance

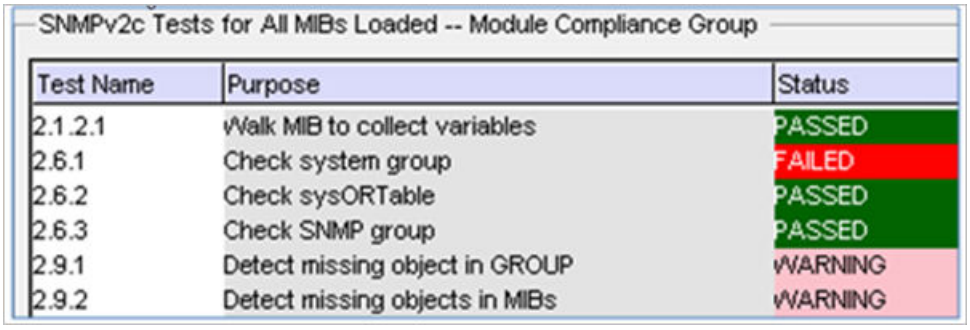
Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.4.1	SET read-write objects	FAILED
3.4.1.1	SET non-existent objects	WARNING
3.4.1.2	SET on incomplete OIDs	FAILED
3.4.1.3	SET read-write & read-create objects atomically	FAILED
3.4.2	SET with invalid syntax	FAILED
3.4.3.1	SET Integer below range	FAILED
3.4.3.1.0	SET Integer with lower/upper value	UNINITIATED
3.4.3.2	SET Integer above range	FAILED
3.4.3.3	SET Integer below enumeration	FAILED
3.4.3.3.0	SET Integer with lower/upper enumeration	UNINITIATED
3.4.3.4	SET Integer above enumeration	FAILED
3.4.4.1	SET non-ASCII NVT string	FAILED
3.4.4.1.0	SET ASCII NVT string	UNINITIATED
3.4.4.2	SET with wrong NVT string	FAILED
3.4.4.3	SET string below SIZE	FAILED
3.4.4.3.0	SET string with upper/lower SIZE	UNINITIATED
3.4.4.4	SET string above SIZE	FAILED
3.4.5.1	SET read-only objects	FAILED

SNMP v2c Compliance

Module Compliance

The following figure shows the module compliance based on RFC 1901.

FIGURE 7 Statement of module compliance



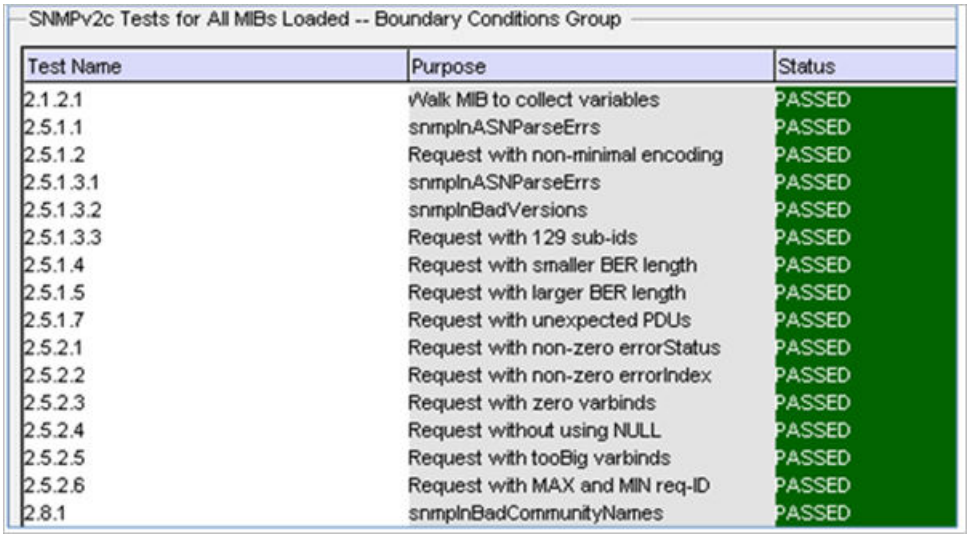
SNMPv2c Tests for All MIBs Loaded -- Module Compliance Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.6.1	Check system group	FAILED
2.6.2	Check sysORTable	PASSED
2.6.3	Check SNMP group	PASSED
2.9.1	Detect missing object in GROUP	WARNING
2.9.2	Detect missing objects in MIBs	WARNING

Boundary Conditions Compliance

The following figure shows the statement of boundary conditions compliance for RFC 1901.

FIGURE 8 Boundary conditions compliance



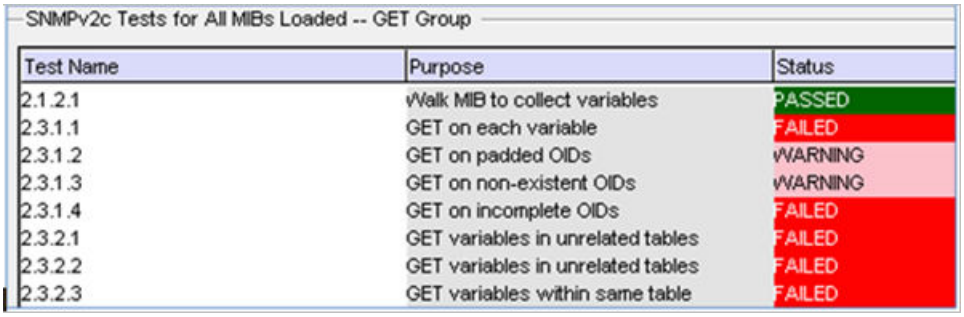
SNMPv2c Tests for All MIBs Loaded -- Boundary Conditions Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.5.1.1	snmpInASNParseErrs	PASSED
2.5.1.2	Request with non-minimal encoding	PASSED
2.5.1.3.1	snmpInASNParseErrs	PASSED
2.5.1.3.2	snmpInBadVersions	PASSED
2.5.1.3.3	Request with 129 sub-ids	PASSED
2.5.1.4	Request with smaller BER length	PASSED
2.5.1.5	Request with larger BER length	PASSED
2.5.1.7	Request with unexpected PDUs	PASSED
2.5.2.1	Request with non-zero errorStatus	PASSED
2.5.2.2	Request with non-zero errorIndex	PASSED
2.5.2.3	Request with zero varbinds	PASSED
2.5.2.4	Request without using NULL	PASSED
2.5.2.5	Request with tooBig varbinds	PASSED
2.5.2.6	Request with MAX and MIN req-ID	PASSED
2.8.1	snmpInBadCommunityNames	PASSED

SNMP GET Compliance

The following figure shows the statement of SNMP GET compliance for RFC 1901.

FIGURE 9 SNMP GET compliance



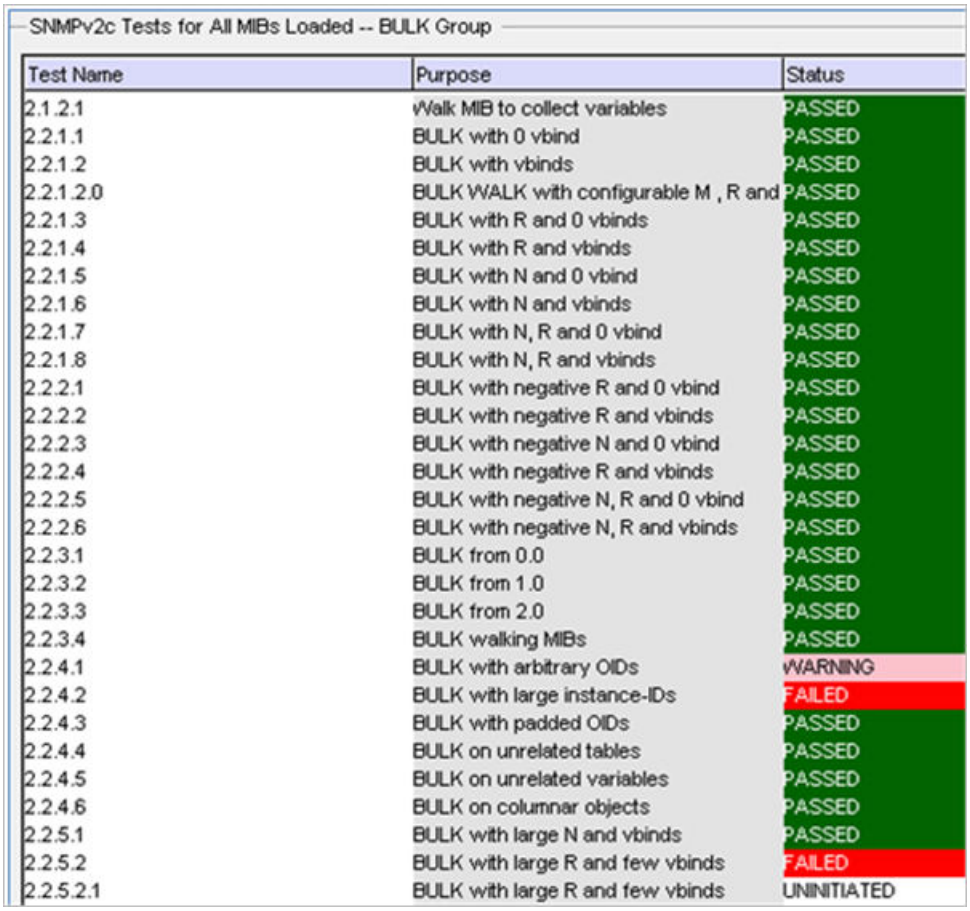
SNMPv2c Tests for All MIBs Loaded -- GET Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.3.1.1	GET on each variable	FAILED
2.3.1.2	GET on padded OIDs	WARNING
2.3.1.3	GET on non-existent OIDs	WARNING
2.3.1.4	GET on incomplete OIDs	FAILED
2.3.2.1	GET variables in unrelated tables	FAILED
2.3.2.2	GET variables in unrelated tables	FAILED
2.3.2.3	GET variables within same table	FAILED

SNMP Bulk Compliance

The following figure shows the statement of SNMP bulk compliance for RFC 1901.

FIGURE 10 SNMP bulk compliance



SNMPv2c Tests for All MIBs Loaded -- BULK Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.2.1.1	BULK with 0 vbind	PASSED
2.2.1.2	BULK with vbinds	PASSED
2.2.1.2.0	BULK WALK with configurable M , R and	PASSED
2.2.1.3	BULK with R and 0 vbinds	PASSED
2.2.1.4	BULK with R and vbinds	PASSED
2.2.1.5	BULK with N and 0 vbind	PASSED
2.2.1.6	BULK with N and vbinds	PASSED
2.2.1.7	BULK with N, R and 0 vbind	PASSED
2.2.1.8	BULK with N, R and vbinds	PASSED
2.2.2.1	BULK with negative R and 0 vbind	PASSED
2.2.2.2	BULK with negative R and vbinds	PASSED
2.2.2.3	BULK with negative N and 0 vbind	PASSED
2.2.2.4	BULK with negative R and vbinds	PASSED
2.2.2.5	BULK with negative N, R and 0 vbind	PASSED
2.2.2.6	BULK with negative N, R and vbinds	PASSED
2.2.3.1	BULK from 0.0	PASSED
2.2.3.2	BULK from 1.0	PASSED
2.2.3.3	BULK from 2.0	PASSED
2.2.3.4	BULK walking MIBs	PASSED
2.2.4.1	BULK with arbitrary OIDs	WARNING
2.2.4.2	BULK with large instance-IDs	FAILED
2.2.4.3	BULK with padded OIDs	PASSED
2.2.4.4	BULK on unrelated tables	PASSED
2.2.4.5	BULK on unrelated variables	PASSED
2.2.4.6	BULK on columnar objects	PASSED
2.2.5.1	BULK with large N and vbinds	PASSED
2.2.5.2	BULK with large R and few vbinds	FAILED
2.2.5.2.1	BULK with large R and few vbinds	UNINITIATED

SNMP Set Compliance

The following figure shows the statement of SNMP set compliance for RFC 1901.

FIGURE 11 SNMP set compliance

SNMPv2c Tests for All MIBs Loaded -- SET Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.4.1	SET read-write objects	FAILED
2.4.1.1	SET non-existent objects	FAILED
2.4.1.2	SET on incomplete OIDs	FAILED
2.4.1.3	SET read-write & read-create objects ato	FAILED
2.4.2	SET with invalid syntax	FAILED
2.4.3.1	SET Integer below range	FAILED
2.4.3.1.0	SET Integer within range	UNINITIATED
2.4.3.2	SET Integer above range	FAILED
2.4.3.3	SET Integer below enumeration	FAILED
2.4.3.3.0	SET Integer with lower/upper enumeratio	UNINITIATED
2.4.3.4	SET Integer above enumeration	FAILED
2.4.4.1	SET non-ASCII NVT string	FAILED
2.4.4.1.0	SET ASCII NVT string	UNINITIATED
2.4.4.2	SET with wrong NVT string	FAILED
2.4.4.3	SET string below SIZE	FAILED
2.4.4.3.0	SET string with upper/lower SIZE	UNINITIATED
2.4.4.4	SET string above SIZE	FAILED
2.4.5.1	SET read-only objects	FAILED
2.4.5.2	SET varbinds order processing	FAILED
2.4.5.3	SET varbinds order processing	FAILED
2.4.6.1	SET varbinds value processing	FAILED
2.4.6.1.0	SET two varbinds with both correct value	UNINITIATED
2.4.6.2	SET varbinds value processing	FAILED
2.4.6.2.0	SET two varbinds with both bad values	UNINITIATED
2.5.1.6	SET with constructed value	FAILED
2.5.1.6.0	SET with primitive value	UNINITIATED

Event Compliance - GTPv1

This compliance is compliant on Virtual SmartZone (vSZ).

Introduction

The following sections are the compliance for 3GPP controller to GPRS Tunneling.

NOTE
This release is compliant with GPP TS Rel6. The following optional informational element from REL7 is added as part of *CREATE PDP REQUEST* - Common Flag IE, which is specified in section 7.7.48 of 3GPP TS 29.060 Rel 7.

Compliance for GTPv1 Section 7.3.6

Messages are sent by the controller (SGSN) using the **delete PDP context response,** which is received by the GGSN. The controller (SGSN) also decodes these messages when GGSN initiates it using the **delete PDP context response**. This is in compliance for section 7.3.6. The following table lists the attributes and the requirement.

NOTE
This compliance is for 3GPP Controller to GPRS Tunneling on page 39.

TABLE 19 Compliance for Section 7.3.6

Attribute (IE)	Requirement	Reference
Cause	Mandatory	7.7.1

Event Compliance - GTPv2-c

This compliance is compliant on Virtual SmartZone (vSZ).

Introduction

This compliance is compliant on Virtual SmartZone (vSZ).

NOTE
This release is compliant to GPP TS Rel6. The following optional informational element from REL7 is added as part of CREATE PDP REQUEST - Common Flag IE, which is specified in section 7.7.48 of 3GPP TS 29.060 Rel 7.

Compliance for GTPv2 Section 7.2.16

Messages are sent by the controller in update bearer response. The following table lists the attributes and the interfaces.

TABLE 20 Compliance for section 7.2.16

Attribute (IE)	Presence	Interface (S2a, S5/S8, Both)	Comments
Cause	M	Both	Cause value
Bearer Context	M	Both	
Recovery	C	Both	This attribute is included when the peer node is contacted for the first time.
PCO	CO	S5/S8	Protocol Configuration Options (PCO), contains the PCO received from PDN GW in create session response.

Bearer Context Attributes for Section 7.2.16

The following table lists the attributes and the interfaces for bearer context.

TABLE 21 Bearer Context content

Attribute (IE)	Presence	Interface (S2a, S5/S8, Both)	Comments
EBI	M	Both	EPS Bearer ID (LBI)
Cause	M	Both	This attribute indicates if the bearer handling was successful. If unsuccessful it gives the reason.
Recovery	C	Both	

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com