Ruckus

Simply Better Wireless.

Ruckus Wireless™ SmartCell Gateway™ 200/ Virtual SmartZone™ High-Scale

Administrator Guide for SmartZone 3.1.1

Part Number 800-70826-001 Rev D
Published February 2016

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Third Party and Open Source Licenses Used in This Product

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by the OpenSymphony Group (http://www.opensymphony.com/).

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

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

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Apache 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or

otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof. "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

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

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

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

Apache 1.1

```
/* ==================================================================
* The Apache Software License, Version 1.1
*
* Copyright (c) 2000 The Apache Software Foundation. All rights
* reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. The end-user documentation included with the redistribution,
* if any, must include the following acknowledgment:
* "This product includes software developed by the
* Apache Software Foundation (http://www.apache.org/)."
* Alternately, this acknowledgment may appear in the software itself,
* if and wherever such third-party acknowledgments normally appear.
*
* 4. The names "Apache" and "Apache Software Foundation" must
* not be used to endorse or promote products derived from this
* software without prior written permission. For written
* permission, please contact apache@apache.org.
*
* 5. Products derived from this software may not be called "Apache",
* nor may "Apache" appear in their name, without prior written
* permission of the Apache Software Foundation.
*
* THIS SOFTWARE IS PROVIDED `AS IS'' AND ANY EXPRESSED OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
```

Object-Graph Navigation Language (OGNL)

Freemarker

Java Beans Activation Framework

1.13. You. (or .Your.) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, .You. includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, .control. means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work;

and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients. rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipient.s rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.6. Larger Works.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN .AS IS. BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as .Participant.) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the

Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY.S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a .commercial item,. as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of .commercial computer software. (as that term is defined at 48 C.F.R. ° 252.227-7014(a)(1)) and commercial computer software documentation. as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdiction.s conflict-of-law provisions.

Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys. fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

NOTICE PURSUANT TO SECTION 9 OF THE COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)

The code released under the CDDL shall be governed by the laws of the State of California (excluding conflict-of-law provisions). Any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California.

JQuery

Copyright (c) 2011 John Resig, http://jquery.com/

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

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

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

OpenSSL

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/* ==
* Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

```
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----------------------
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
** Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
```

Contents

About This Guide

Document Conventions . . . 19
Related Documentation . . . 19
Documentation Feedback . . . 20

1 Navigating the Web Interface

Setting Up the Controller for the First Time . . . 22
Logging On to the Web Interface . . . 22
Web Interface Features . . . 23
  Main Menu . . . 25
  Submenu . . . 26
  Sidebar . . . 26
  Content Area . . . 26
  Miscellaneous Bar . . . 26
Using Widgets on the Dashboard . . . 27
  Widgets That You Can Display . . . 27
    Client Count Summary Widget . . . 28
    AP Status Summary Widget . . . 28
    Domain Summary Widget . . . 29
    System Summary Widget . . . 29
    Data Throughput Summary Widget . . . 30
    Client OS Type Summary Widget . . . 30
  Widget Slots . . . 31
  Adding a Widget . . . 31
  Adding a Widget to a Widget Slot . . . 33
  Displaying a Widget in a Widget Slot . . . 34
  Moving a Widget . . . 35
  Deleting a Widget . . . 35
Changing the Administrator Password . . . 36
Logging Off the Web Interface . . . 37

2 Managing Ruckus Wireless AP Zones

Working with AP Zones . . . 39

Using the Domain Tree and Search Boxes 40
Creating an AP Zone 41
About VLAN Pooling 47
ChannelFly and Background Scanning 48
Benefits of ChannelFly 48
Disadvantages of ChannelFly 49
Background Scanning 49
Creating an AP Zone from a ZoneDirector Backup File 49
Backing Up the ZoneDirector 50
Restoring ZoneDirector Backup to the Controller 51
Cloning an AP Zone from the Domain Tree 53
Cloning an AP Zone from the AP Zone List 53
Viewing Existing AP Zones 55
Viewing the AP Zone Configuration 56
Deleting an AP Zone 57
Working with AP Groups 57
Creating an AP Group 57
Modifying Model Specific Controls 60
Supported LLDP Attributes 61
Configuring the Port Settings of a Particular AP Model 62
Designating an Ethernet Port Type 63
Trunk Ports 64
Access Ports 64
General Ports 64
Configuring Client Admission Control 64
Working with AAA Servers 65
Creating an AAA Server 65
Testing an AAA Server 68
Deleting an AAA Server 68
Working with Hotspot (WISPr) Portals 69
Creating a Hotspot Portal 69
Deleting a Hotspot Portal 72
Working with Guest Access Portals 73
Creating a Guest Access Portal 73
Viewing Guest Access Portals 75
Deleting Guest Access Portals 76
Working with Web Authentication Portals 77
Adding an AAA Server for the Web Authentication Portal 77
Creating a Web Authentication Portal 77

Creating a WLAN for the Web Authentication Portal 79
Working with Hotspot 2.0 Services 81
Working with WLANs and WLAN Groups 82
Creating a WLAN 82
Channel Mode 91
Client Load Balancing 92
Key Points About Client Load Balancing 92
Band Balancing 93
Bypassing Apple CNA 93
Working with WLAN Groups 93
Notes About WLAN Groups 94
Creating a WLAN Group 94
Viewing Existing WLAN Groups 95
Deleting WLAN Groups 95
Working with WLAN Schedules 96
Creating a WLAN Schedule Profile 97
Working with Device Policies 98
Creating a Device Access Policy 98
Viewing Device Access Policies 100
Deleting Device Access Policies 101
Working with L2 Access Control Policies 101
Creating an L2 Access Policy 102
Viewing L2 Access Policies 104
Deleting L2 Access Policies 104
Working with Bonjour Policies 105
Creating a Bonjour Gateway Rule on the AP 105
Applying a Bonjour Policy to an AP 107
Creating a DiffServ Profile 108

3 Managing Global Configuration, AP Tunnel Profiles, Templates, and AP Registration Rules

Managing Global Configuration 110
Creating AP Tunnel Profiles 111
Creating a Ruckus GRE Tunnel Profile 111
Creating a SoftGRE Tunnel Profile 113
Creating an IPsec Profile 114
Working with Zone Templates 118
Creating and Configuring a Zone Template 119
Step 1: Create the Zone Template 119

Step 2: Configure the AP Model-Specific Configuration. 121
Step 3: Configure the AAA Servers of the Zone Template 123
Step 4: Configure the Hotspot (WISPr) Services of the Zone Template 124
Step 5: Configure the Hotspot 2.0 Service of the Zone Template 127
Step 6: Configure the WLAN Service of the Zone Template. 127
Exporting a Zone Template 134
Importing a Zone Template 134
Deleting a Zone Template 135
Working with WLAN Templates. 135
Creating and Configuring a WLAN Template 136
Step 1: Create the WLAN Template 136
Step 2: Configure the AAA Servers for the WLAN Template 137
Step 3: Configure the Hotspot (WISPr) Services of the WLAN Template 139
Step 4: Configure the Hotspot 2.0 Services of the WLAN Template 141
Step 5: Configure the WLAN Services of the WLAN Template. 142
Viewing Existing WLAN Templates 149
Deleting WLAN Templates 149
Working with Registration Rules 150
Creating a Registration Rule. 151
Configuring Registration Rule Priorities. 152
Deleting a Registration Rule 153

4 Working with 3rd Party AP Zones
3rd Party AP Zone Types 155
Adding a 3rd Party AP Zone 155
Viewing Existing 3rd Party AP Zones. 158
Deleting a 3rd Party AP Zone 158

5 Managing Access Points
Overview of Access Point Configuration 159
Viewing Managed Access Points 159
Provisioning and Swapping Access Points 161
Options for Provisioning and Swapping APs. 161
Understanding How Swapping Works 163
Editing AP Configuration 164
Editing Swap Configuration. 166
Moving a Single Access Point to a Different AP Zone 166
Moving Multiple Access Points to a Different AP Zone. 167
Deleting an Access Point 168

6 Configuring Services and Profiles

Configuring the GGSN/PGW Service . . . 169
Configuring Authentication Services . . . 172
Adding an Authentication Service . . . 172
RADIUS Service Options . . . 173
Testing the AAA Server Configuration . . . 175
Viewing RADIUS Services . . . 177
Deleting a RADIUS Service . . . 178
Configuring HLR Services . . . 180
Map Gateway Settings . . . 180
MNC to NDC Mapping . . . 181
Adding MNC to NDC Mapping . . . 181
Viewing MNC to NDC Mapping . . . 183
Deleting MNC to NDC Mappings . . . 184
Configuring Diameter Services . . . 186
Configuring System Wide Settings . . . 186
Configuring Remote Peer Settings . . . 187
Configuring FTP Services . . . 188
Important Notes About FTP Services . . . 190
Configuring Location Services . . . 191
Adding an LBS Server . . . 191
Configuring the Controller to Use the LBS Server . . . 192
Setting an AP Zone to Use an LBS Server . . . 192
Setting an AP Group to Override the LBS Settings of a Zone . . . 193
Configuring an SMS Server . . . 194
Working with Profiles . . . 196
Working with Authentication Profiles . . . 196
Creating an Authentication Profile . . . 196
Viewing Authentication Profiles . . . 198
Deleting Authentication Profiles . . . 199
Working with Accounting Profiles . . . 201
Creating an Accounting Profile . . . 201
Viewing Accounting Profiles . . . 202
Deleting Accounting Profiles . . . 203
Working with Hotspot Profiles . . . 204
Creating a Hotspot Profile . . . 204
Viewing Hotspot Profiles . . . 207
Deleting Hotspot Profiles . . . 208

Working with Network Traffic Profiles 209
Creating a Network Traffic Profile 210
Viewing Network Traffic Profiles 211
Deleting Network Traffic Profiles 212
Applying a Network Traffic Profile to a 3rd Party AP Zone 213
Working with User Traffic Profiles 214
Creating a User Traffic Profile 214
Viewing User Traffic Profiles 216
Deleting Traffic Profiles 216
Working with Forwarding Profiles 217
L2oGRE Profiles 217
Creating an L2oGRE Profile 217
About Keep-Alive Settings 219
Viewing L2oGRE Profiles 220
Deleting an L20GRE Profile 220
L3oGRE Profiles 221
Adding an L3oGRE Profile 221
Viewing L3oGRE Profiles 223
Deleting L30GRE Profiles 223
TTG+PDG Profiles. 224
Adding a TTG+PDG Profile. 224
About DHCP Relay. 226
Viewing TTG+PDG Profiles. 227
Deleting TTG+PDG Profiles 228
PMIPv6 Profiles. 228
Configuring the Global LMA and MAG Options. 228
Creating a PMIPv6 Profile. 229
Viewing PMIPv6 Profiles 229
Deleting PMIPv6 Profiles 229
Mixed Mode Profiles 230
Adding Mixed a Mode Profile 230
Viewing Mixed Mode Profiles 231
Deleting Mixed Mode Profiles 232

7 Configuring the System Settings

Overview of the System Settings. 233
Configuring General System Settings 233
Setting the System Time 234
How APs Synchronize Time with the Controller 234

Configuring the Syslog Server Settings. 235
Event Severity Levels. 236
Default Event Severity to Syslog Priority Mapping 237
Configuring the Northbound Portal Interface 237
Configuring the SMTP Server Settings 238
Configuring the FTP Server Settings. 239
Setting Critical AP Auto Tagging Rules. 240
Configuring Q-in-Q Ether Type. 241
Managing the Global User Agent Black List 242
Enabling and Configuring Node Affinity. 242
Managing the Certificate Store 245
Generating a Certificate Signing Request 246
Importing an SSL Certificate 248
Assigning Certificates to Services 250
Configuring Advanced Gateway Options 251
Configuring Cluster Planes 253
Setting the System IP Mode. 253
Configuring Control Planes. 254
Physical Interface Tab 255
User Defined Interface Tab 257
Static Routes Tab 258
Configuring a Data Plane. 259
Configuring Cluster Redundancy 261
How Cluster Redundancy Works 263
Rehoming Managed APs 264
Configuring Network Management 265
Configuring the SNMPv2 and SNMPv3 Agents 265
Enabling Global SNMP Traps 265
Configuring the SNMPv2 Agent. 266
Configuring the SNMPv3 Agent. 267
Sending SNMP Traps and Email Notifications for Events 269
Enabling or Disabling Notifications for a Single Event. 271
Viewing Enabled Notifications for Events 272
Configuring Event Thresholds. 273
Events with Configurable Thresholds. 274
Controlling Access to the Management Interfaces 275
Configuring Hosted AAA Services. 277
EAP-SIM Configuration 277
EAP-AKA Configuration 279

8 Working with Management Domains

Overview of Management Domains 281
Viewing a List of Management Domains 281
Creating a New Management Domain 282
Deleting a Management Domain 283

9 Managing Administrator Accounts

Overview of Administrator Accounts and Roles 284
Viewing a List of Administrator Accounts, Roles, and RADIUS Servers 284
Creating an Administrator Account 286
Creating a New Administrator Role 287
Editing an Administrator Role 288
Cloning an Existing Administrator Role 289
Adding a RADIUS Server for Administrators 289
About TACACS+ Support 291
Using a Backup RADIUS Server 292
Testing an AAA Server 293
Deleting an Administrator Account, Role, or RADIUS Server 294

10 Managing Mobile Virtual Network Operator Accounts

Overview of Mobile Virtual Network Operator Accounts 296
Viewing a List of MVNOs 296
Creating a New MVNO Account 297
Using a Backup RADIUS Server for Authorizing and Authenticating MVNOs 300
Editing an MVNO Account 300
Deleting an MVNO Account 301

11 Creating and Managing Hotspots

Overview of Hotspot Management 302
Hotspot Terminologies 303
How Hotspot Authentication Works 304
Call Flow for Devices That Use a Web Proxy 308
Devices Using a Static Web Proxy 310
Devices Using a Dynamic Web Proxy 310
User Agent Blacklist 310
Notes on Using iOS Devices to Access the Hotspot 311
Notes on Using Amazon Kindle Fire to Access the Hotspot 312
What You Will Need 313
Hotspot Configuration Options 313

Why Create a User Defined Interface 313
Creating a User Defined Interface. 314
Adding a RADIUS Server to the Controller 316
Adding a RADIUS Accounting Server 316
Creating a Hotspot WLAN 316
Configuring Smart Client Support 316
Configuring the Logon URL. 317
Creating a WLAN. 318
Downloading Captive Portal and Subscriber Portal Logs. 319

12 Monitoring AP Zones, Access Points, and Wireless Clients

Monitoring AP Zones 321
Viewing a Summary of AP Zones 321
Exporting the AP Zone List to CSV. 324
Viewing the Configuration of an AP Zone 325
Viewing All APs That Belong to an AP Zone on Google Maps 326
Monitoring Managed Access Points 328
Viewing a Summary of Access Points 329
Exporting the Access Point List to CSV 331
Viewing the Configuration of an Access Point. 332
Downloading the Support Log from an Access Point 333
Restarting an Access Point Remotely. 334
Running Ping and Traceroute on an Access Point 335
Monitoring Wireless Clients 336
Viewing a Summary of Wireless Clients 336
Exporting the Wireless Client List to CSV 338
Viewing Information About a Wireless Client. 339
Measuring Wireless Network Throughput with SpeedFlex 340

13 Monitoring the System, Alarms, Events, and Administrator Activity

Monitoring the Controller System 342
Viewing the System Cluster Overview 342
Displaying the Chassis View of Cluster Nodes 343
Starting the Cluster Real-time Monitor 344
Monitoring Rogue Access Points 346
Viewing Alarms 347
Using the Search Criteria Section. 349
Exporting the Alarm List to CSV. 350
Clearing Alarms 351

Acknowledging Alarms . . . 351
Viewing Events . . . 351
Using the Search Criteria Section . . . 353
Exporting the Event List to CSV . . . 354
Viewing Administrator Activity . . . 355
Using the Search Criteria Section . . . 357
Exporting the Administrator Activity List to CSV . . . 358

14 Working with Reports

Types of Reports . . . 360
Active TTG Sessions Report . . . 361
Client Number Report . . . 361
Client Number vs Airtime Report . . . 361
Continuously Disconnected APs Report . . . 361
Failed Client Associations Report . . . 361
New Client Associations Report . . . 361
System Resource Utilization Report . . . 362
TX/RX Bytes Report . . . 362
Creating a New Report . . . 362
Step 1: Define the General Report Details . . . 362
Step 2: Define the Resource Filter Criteria . . . 364
Step 3: Define the Time Filter . . . 365
Step 4: Define the Report Generation Schedule . . . 365
Step 5: Enable Email Notifications (Optional) . . . 366
Step 6: Export the Report to an FTP Server (Optional) . . . 366
Step 7: Save the Report . . . 367
Viewing a List of Existing Reports . . . 367
Deleting a Report . . . 367

15 Working with Local, Guest, and Remote Users

Working with Local, Guest, and Remote Users . . . 369
Working with Local Users . . . 369
Creating a Local User Account . . . 370
Editing a Local User Account . . . 371
Working with Guest Users . . . 373

Generating Guest Passes 373
Step 1: Create a Guest Access Portal 373
Step 2: Create a Guest Access WLAN 375
Step 3: Generate a Guest Pass 376
Step 4: Send Guest Passes to Guest Users 379
Printing the Guest Pass 379
Exporting the Guest Pass to CSV 380
Sending the Guest Pass via Email 381
Sending the Guest Pass via SMS 382
Generating Guest Passes from an Imported CSV 383
Viewing the List of Guest Users 386
Deleting Guest Users 386
Creating a Guest Pass Printout Template 387
Working with Remote Users 389
How Onboarding Works 389
Before You Begin 390
Step 1: Create the Onboarding Guest WLAN for Remote Users 391
Step 2: Create a Standard WLAN with Zero-IT Activation Enabled 392
Working with User Roles 394
Creating a User Role 394
Managing Subscription Packages 395
Viewing a List of Subscription Packages 395
Creating a Subscription Package 396
Editing a Subscription Package 397
Deleting a Subscription Package 398

16 Performing Administrative Tasks

Backing Up and Restoring Clusters 399
Creating a Cluster Backup 400
Restoring a Cluster Backup 401
Deleting a Cluster Backup 404
Backing Up and Restoring the Controller’s Network Configuration from an FTP Server . 405
Requirements 405
What Information Is Backed Up 405
Backing Up to an FTP Server 406
Restoring from an FTP Server 408
Backing Up and Restoring System Configuration 413
Creating a System Configuration Backup 414
Exporting the Configuration Backup to an FTP Server Automatically 415

Scheduling a Configuration Backup 416
Downloading a Copy of the Configuration Backup 417
Restoring a System Configuration Backup 418
Deleting a Configuration Backup 419
Resetting a Node to Factory Settings 420
What Happens After Reset to Factory Settings 420
Using the Web Interface 421
Using the CLI 422
Upgrading the Controller 423
Performing the Upgrade 423
Verifying the Upgrade 426
Rolling Back to a Previous Software Version 427
Recovering a Cluster from an Unsuccessful Upgrade 428
If the Controller Has Local Configuration Backup 428
If the Controller Has an FTP Backup 428
Working with Logs 430
Available System Log Types 430
Downloading All Logs 432
Downloading Snapshot Logs Generated from the CLI 434
Managing License Files 435
Uploading a License File 437
Viewing License Details 438
License SKUs 439

A Accessing the Command Line Interface

About the Command Line Interface 440
What You Will Need 440
Step 1: Connect the Administrative Computer to the Controller 441
Step 2: Start and Configure the SSH Client 442
Using an SSH Connection 442
Using a Serial Connection 444
Step 3: Log On to the CLI 447
Changing the Management IP Address from the CLI 448

B Working with the Captive Portal

Overview of the Captive Portal 449
Configuring the Captive Portal 451
Configuring the GGSN/PGW Service 451
Configuring an Authentication Profile 453

Configuring Accounting Profile . . . 457
Configuring TTG+PDG Forwarding Profiles . . . 460
Configuring WISPr (Hotspot) Services of the AP Zone . . . 463
AP Zone WLAN Services & Group . . . 465
Captive Portal Workflows and VSA . . . 468
Successful Captive Portal Authentication . . . 468
Successful GTP Tunnel Establishment . . . 470
Ruckus VSA for Captive Portal . . . 471

C Statistics Files the Controller Exports to an FTP Server

AP Inventory . . . 475
Control Plane Statistics . . . 478
Mobility Zone Inventory . . . 479
Zone Statistics . . . 480
AP Statistics . . . 481
Zone Time Radio Statistics . . . 483
Zone Time WLAN Statistics. . . . 484
AP Time Radio Statistics . . . 486
AP Time WLAN Statistics . . . 487
Control Plane Statistics . . . 488
Data Plane Statistics . . . 494
Data Plane Ethernet Port Statistics . . . 495
AP SoftGRE Tunnel Statistics . . . 496
SoftGRE Gateway Statistics . . . 497
Tenant Time Radio Statistics . . . 498
Tenant Time WLAN Statistics . . . 500
Tenant Zone Statistics . . . 502
Tenant Zone Radio Statistics . . . 504
Tenant Inventory File . . . 506

A Ports to Open for AP-Controller Communication

AP-SCG/SZ/vSZ Communication . . . 1
AP-ZD Communication . . . 3

B SoftGRE Support

Overview of SoftGRE Support . . . 6
Supported Deployment Scenario . . . 6
SoftGRE Packet Format . . . 8
Configuring SoftGRE . . . 9

Creating an AP Zone That Supports SoftGRE 9
Changing the Tunnel Type from SoftGRE. 9
Monitoring SoftGRE 10
Checking the AP Tunnel Type of a Zone 10
Viewing SoftGRE Traffic Statistics of an AP 12
SoftGRE SNMP MIBs 14
SoftGRE Alarms and Events 15
SoftGRE Events 16
SoftGRE Alarms. 17

C Replacing Hardware Components

Installing or Replacing Hard Disk Drives 18
Ordering a Replacement Hard Disk 18
Removing the Front Bezel 19
Removing an HDD Carrier from the Chassis. 20
Installing a Hard Drive in a Carrier. 21
Reinstalling the Front Bezel 23
Replacing PSUs 24
Replacing System Fans 25

D Replacing a Controller Node

Prerequisites. 27
Backing Up and Restoring the Cluster 27
Step 1: Back Up the Cluster from the Web Interface 27
Step 2: Back Up the Cluster from the Controller CLI 28
Step 3: Transfer the Cluster Backup File to an FTP Server 28
Step 4: Restoring the Cluster Backup to the Controller 29
Restoring to a Single Node Environment 29
Restoring to a Multi Node Environment 31
Replacing a Single Node in a Cluster 31
Replacing Multiple Nodes in a Cluster 32
Backing Up and Restoring Configuration. 33
Backed Up Configuration Information 33
Backing Up Configuration 34
Backing Up Configuration from the Web Interface. 34
Backing Up Configuration from the CLI 34
Restoring Configuration 35
Restoring Configuration to a Single Node Environment 35

Restoring Configuration to Multi Node Environment 36
Restoring Configuration to a Single Node in a Cluster. 37
Restoring Configuration to Multiple Nodes in a Cluster 38

E SSID Syntaxes Supported by Ruckus Wireless Products

SCG SSID Syntax 40
1.1. x 40
2.1.x 41
2.5.x 41
ZoneDirector SSID Syntax 42
9.8, 9.7 42
9.6. 43
ZoneFlex AP SSID Syntax. 44
9.8, 9.7, and 9.6 44

Index

About This Guide

This *Administrator Guide* describes how to configure the Ruckus Wireless™ Smart-Cell Gateway™ 200 (SCG-200)/Virtual SmartZone High Scale (vSZ-H) and how to use the web interface to manage access points that are reporting to the SCG-200/ vSZ-H (collectively referred to as “the controller” throughout this guide). This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support website at https://support.ruckuswireless.com/documents.

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
Caution!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
Warning	Information that alerts you to potential personal injury

Related Documentation

In addition to this *Administrator Guide*, each controller documentation set includes the following:

- *Getting Started Guide/Quick Setup Guide*: Provides step-by-step instructions on how to set up and configure the controller out of the box.
- *Online Help*: Provides instructions for performing tasks using the controller web interface. The online help is accessible from the web interface and is searchable.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- Ruckus Wireless SmartCell Gateway 200 Administrator Guide (Release 3.1.1)
- Part number: 800-70500-001
- Page 88

Navigating the Web Interface

1

In this chapter:

- Setting Up the Controller for the First Time
- Logging On to the Web Interface
- Web Interface Features
- Using Widgets on the Dashboard
- Changing the Administrator Password
- Logging Off the Web Interface

NOTE: Before continuing, make sure that you have already set up the controller on the network as described in the *Getting Started Guide* or *Quick Setup Guide* for your controller platform.

CAUTION! Some of the new features (for example, location based services, rogue AP detection, force DHCP, and others) that this guide describes may not be visible on the controller web interface if the AP firmware deployed to the zone you are configuring is earlier than this release. To ensure that you can view and configure all new features that are available in this release, Ruckus Wireless recommends upgrading the AP firmware to the latest version.

Setting Up the Controller for the First Time

For information on how to set up the controller for the first time, including instructions for running and completing the controller's Setup Wizard, see the *Getting Started Guide* or *Quick Setup Guide* for your controller platform.

Logging On to the Web Interface

Before you can log on to the controller web interface, you must have the IP address that you assigned to the Management (Web) interface when you set up the controller on the network using the Setup Wizard. Once you have this IP address, you can access the web interface on any computer that can reach the Management (Web) interface on the IP network.

Follow these steps to log on to the controller web interface.

1. On a computer that is on the same subnet as the Management (Web) interface, start a web browser. Supported web browsers include:
   - Google Chrome 15 (and later) - recommended
   - Microsoft Internet Explorer 9.0
   - Safari 5.1.1 (and later)
   - Mozilla Firefox 8 (and later)
2. In the address bar, type the IP address that you assigned to the Management (Web) interface, and then append a colon and **`8443`** (the controller's management port number) at the end of the address.

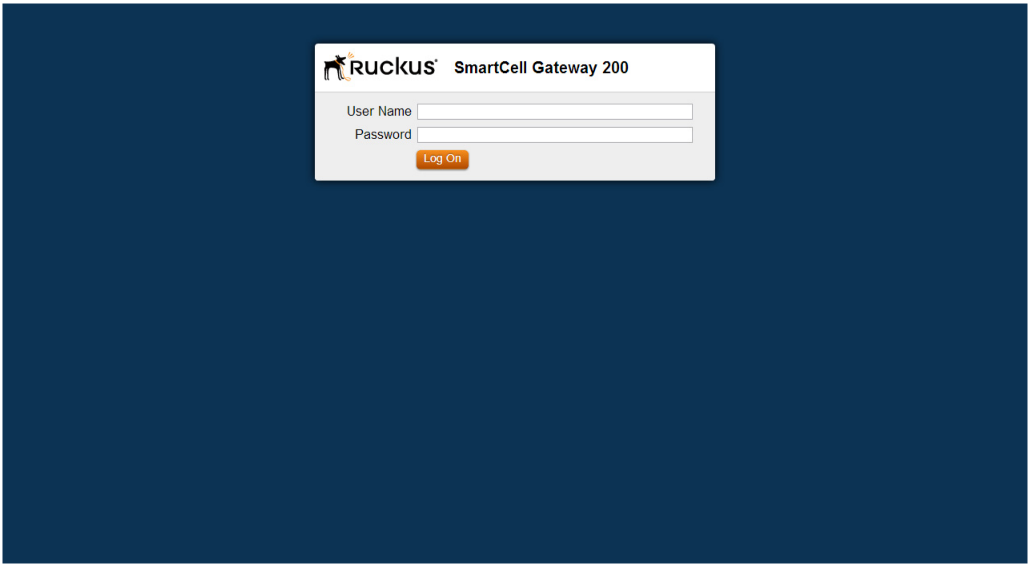
   For example, if the IP address that you assigned to the Management (Web) interface is 10.10.101.1, then you should enter:

   ```
   https://10.10.101.1:8443
   ```

NOTE: The controller web interface requires an HTTPS connection. You must append `https` (not `http`) to the management interface IP address to connect to the web interface. If a browser security warning appears, this is because the default SSL certificate (or security certificate) that the controller is using for HTTPS communication is signed by Ruckus Wireless and is not recognized by most web browsers.

The controller web interface logon page appears.

Figure 1. The controller's logon page



3 Log on to the controller web interface using the following logon details:

- *User Name*: admin
- *Password*: {the password that you set when you ran the Setup Wizard}

4 Click **Log On**.

The web interface refreshes, and then displays the Dashboard, which indicates that you have logged on successfully.

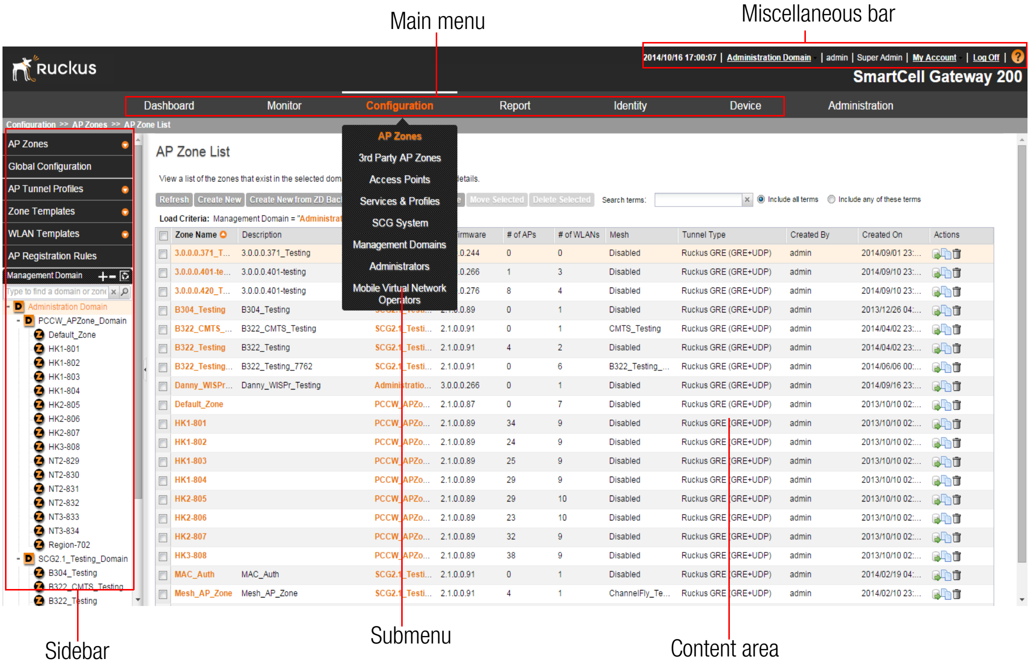
Web Interface Features

The web interface (shown in Figure 2) is the primary interface that you will use to:

- Manage AP zones, access points, and management domains
- Create and manage administrator and mobile virtual network operator accounts
- Monitor AP zones, managed access points, wireless clients
- View alarms, events, and administrator activity
- Generate reports

- Perform administrative tasks, including backing up and restoring system configuration, upgrading the cluster upgrade, downloading support logs, performing system diagnostic tests, viewing the statuses of controller processes, and uploading additional licenses (among others)
- Configure services and profiles for different network elements, packages, and configurations specific to the controller.

Figure 2. The controller web interface features



AP Zone List

View a list of the zones that exist in the selected dom details.

Load Criteria: Management Domain = "Administrat

□	Zone Name	Description		irmware	# of APs	# of WLANs	Mesh	Tunnel Type	Created By	Created On	Actions
□	3.0.0.0.371_T...	3.0.0.0.371_Testing		.0.244	0	0	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/09/01 23:...	
□	3.0.0.0.401-te...	3.0.0.0.401-testing		.0.266	1	3	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/09/10 23:...	
□	3.0.0.0.420_T...	3.0.0.0.401-testing		.0.276	8	4	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/09/10 23:...	
□	B304_Testing	B304_Testing		0.89	0	1	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/12/26 04:...	
□	B322_CMTS_...	B322_CMTS_Testing	SCG2.1_Testi...	2.1.0.0.91	0	1	CMTS_Testing	Ruckus GRE (GRE+UDP)	admin	2014/04/02 23:...	
□	B322_Testing	B322_Testing	SCG2.1_Testi...	2.1.0.0.91	4	2	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/02 23:...	
□	B322_Testing...	B322_Testing_7762	SCG2.1_Testi...	2.1.0.0.91	0	6	B322_Testing_...	Ruckus GRE (GRE+UDP)	admin	2014/06/06 00:...	
□	Danny_WISPr...	Danny_WISPr_Testing	Administratio...	3.0.0.0.266	0	1	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/09/16 23:...	
□	Default_Zone		PCCW_APZo...	2.1.0.0.87	0	7	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK1-801		PCCW_APZo...	2.1.0.0.89	34	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK1-802		PCCW_APZo...	2.1.0.0.89	24	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK1-803		PCCW_APZo...	2.1.0.0.89	25	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK1-804		PCCW_APZo...	2.1.0.0.89	29	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK2-805		PCCW_APZo...	2.1.0.0.89	29	10	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK2-806		PCCW_APZo...	2.1.0.0.89	23	10	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK2-807		PCCW_APZo...	2.1.0.0.89	32	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	HK3-808		PCCW_APZo...	2.1.0.0.89	38	9	Disabled	Ruckus GRE (GRE+UDP)	admin	2013/10/10 02:...	
□	MAC_Auth	MAC_Auth	SCG2.1_Testi...	2.1.0.0.91	0	1	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/02/19 04:...	
□	Mesh_AP_Zone	Mesh_AP_Zone	SCG2.1_Testi...	2.1.0.0.91	4	1	ChannelFly_Te...	Ruckus GRE (GRE+UDP)	admin	2014/02/10 23:...	

The following sections describe the web interface features that are called out in Figure 2:

- Main Menu
- Submenu
- Sidebar
- Content Area
- Miscellaneous Bar

Main Menu

This is the primary navigation menu. The main menu contains six items:

- *Dashboard*: The page that loads after you log on, it provides graphical summary of what is happening on the controller and its managed access points. The Dashboard uses widgets to display graphical summaries of system statuses, access point statuses, client count, management domain statuses, etc. For more information on the Dashboard widgets, see Using Widgets on the Dashboard.
- *Monitor*: Contains options for viewing information about AP zones, access points, wireless clients, system information, alarms, events, and administrator activity.

  For more information, see the following chapters:

  - Monitoring AP Zones, Access Points, and Wireless Clients
  - Monitoring the System, Alarms, Events, and Administrator Activity
- *Configuration*: Contains options for managing AP zones, access points, system settings, management domains, administrator accounts and mobile virtual network administrator accounts.

  For more information, see the following chapters:

  - Managing Ruckus Wireless AP Zones
  - Managing Access Points
  - Configuring Services and Profiles
  - Managing Subscription Packages
  - Configuring the System Settings
  - Working with Management Domains
  - Managing Administrator Accounts
  - Managing Mobile Virtual Network Operator Accounts
- *Report*: Contains options for generating various types of reports, including network tunnel statistics and historical client statistics. For more information, see Working with Reports.
- *Identity*: Contains options for creating and managing profiles and guest passes. For more information, see Working with Local, Guest, and Remote Users.

- *Administration*: Contains options for performing administrative tasks, such as backing up and restoring the database, upgrading the system, downloading log files, and performing diagnostic tests. For more information, see Performing Administrative Tasks.

Submenu

The submenu appears when you hover the mouse pointer over the Main Menu items. The submenu provides options related to the main menu item on which you hovered your mouse pointer. For example, submenu items under the *Configuration* menu include options for configuring AP zones and access points.

Sidebar

The sidebar, located on the left side of the Content Area, provides additional options related to the submenu that you clicked. For example, sidebar items under *Configuration > AP Zones* include AP zone templates and AP registration rules.

On some pages, the sidebar also includes a tree that you can use to filter the information you want to show in the Content Area.

Content Area

This large area displays tables, forms, and information that are relevant to submenu and sidebar items that you clicked.

Miscellaneous Bar

This shows the following information (from left to right):

- *System date and time:* Displays the current system date and time. This is obtained by the controller from the NTP time server that has been configured.
- *Management domain link*: If there is more than one management domain configured on the controller, click *Administration Domain* to display all of the existing management domains, and then click the management domain to which you want to switch the web interface. Refer to the following sections for more information:
  - Creating a new management domain (see Working with Management Domains)
  - Adding an administrator account and assigning a role to the account (see Managing Administrator Accounts)

- *Administrator user name*: Displays the user name of the administrator that is currently logged on.
- *Administrator role*: Displays the administrator role (for example, Super Admin) of the user that is currently logged on.
- *My Account* link*:* Clicking this link displays the following links:
  - *Change Password link*: Click this to change your administrator password. For more information, see Changing the Administrator Password.
  - *Preference*: Click this link to configure the session timeout settings. In *Session Timeout Settings*, type the number of minutes (1 to 1440 minutes) of inactivity after which the administrator will be logged off of the web interface automatically.
- *Log Off link*: Click this to log off the controller web interface. For more information, see Logging Off the Web Interface.
- ?: Click this icon to launch the Online Help, which provides information on how to perform management tasks using the web interface.

Using Widgets on the Dashboard

The dashboard provides a quick summary of what is happening on the controller and its managed access points. It uses widgets to display at-a-glance information about managed access points, AP zones, management domains, client count, domain summary, and system summary, among others.

This section describes the widgets that you can display and how to add, move, and delete widgets from the dashboard.

NOTE: To refresh the information on each widget, click ⟳ (refresh button) in the upper-right corner of the widget.

Widgets That You Can Display

There are six types of dashboard widgets that the controller supports. These include:

- Client Count Summary Widget
- AP Status Summary Widget
- Domain Summary Widget
- System Summary Widget
- Data Throughput Summary Widget

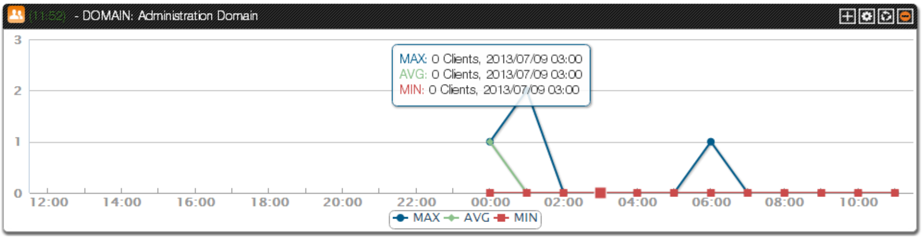
- Client OS Type Summary Widget

Client Count Summary Widget

The client count summary widget displays a graph of the number of wireless clients that are associated with access points that the controller is managing. You can display client count based on the management domain, AP zone, or SSID.

The client count summary widget requires two widget slots.

Figure 3. The client count summary widget

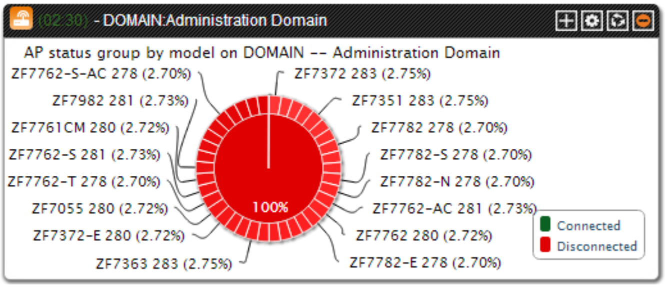

(11:52) - DOMAIN: Administration Domain
MAX: 0 Clients, 2013/07/09 03:00
AVG: 0 Clients, 2013/07/09 03:00
MIN: 0 Clients, 2013/07/09 03:00
3
2
1
0
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
MAX
AVG
MIN

AP Status Summary Widget

The AP status summary widget includes a pie chart that shows the connection status of managed APs that belong to either a management domain or an AP zone. You can configure the pie chart to show access point data based on their connection status, model, and mesh role.

The AP status summary widget requires one widget slot.

Figure 4. The AP status summary widget

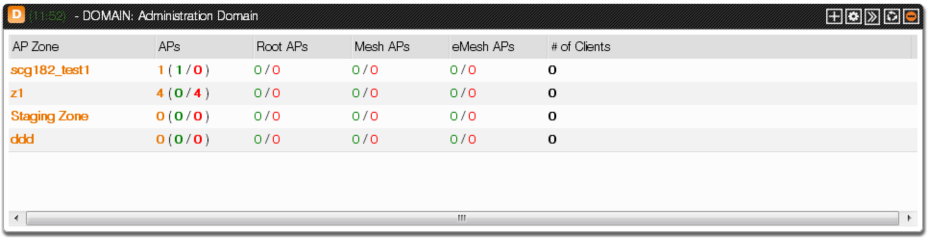


Domain Summary Widget

The domain summary widget displays details about the AP zones and access points that belong to the selected management domain. It shows the AP zones that belong to the management domain, the total number of APs (including their current connection status and mesh status), and current number of clients.

The domain summary widget requires two widget slots.

Figure 5. The domain summary widget



D (11:52) - DOMAIN: Administration Domain

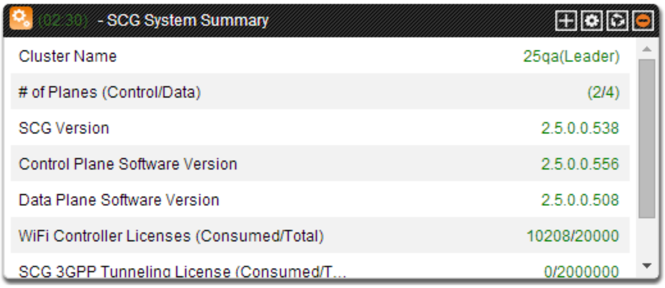
AP Zone	APs	Root APs	Mesh APs	eMesh APs	# of Clients
scg182_test1	1 (1 / 0)	0 / 0	0 / 0	0 / 0	0
z1	4 (0 / 4)	0 / 0	0 / 0	0 / 0	0
Staging Zone	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0
ddd	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0

System Summary Widget

The system summary widget displays information about the controller system, including the name and version of the cluster, the number and software versions of the control planes and data planes that are installed, and the Wi-Fi controller licenses (consumed versus total).

The system summary widget requires one widget slot.

Figure 6. The system summary widget



(02:30) - SCG System Summary

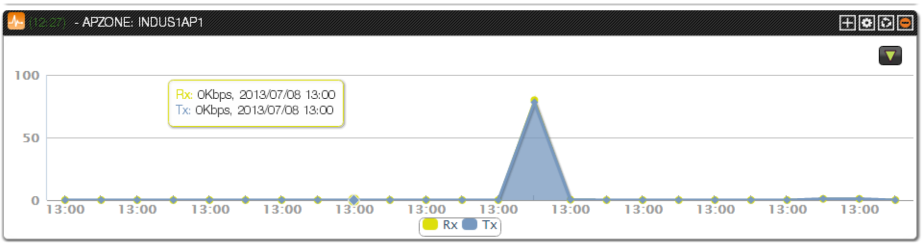
Cluster Name	25qa(Leader)
# of Planes (Control/Data)	(2/4)
SCG Version	2.5.0.0.538
Control Plane Software Version	2.5.0.0.556
Data Plane Software Version	2.5.0.0.508
WiFi Controller Licenses (Consumed/Total)	10208/20000
SCG 3GPP Tunneling License (Consumed/T...	0/2000000

Data Throughput Summary Widget

The data throughput summary widget displays a graph of TX and RX throughputs (in Mbps) based on either AP zone or SSID.

The data throughput summary widget requires two widget slots.

Figure 7. The data throughput summary widget



(12:27) - APZONE: INDUS1AP1

Rx: 0Kbps, 2013/07/08 13:00
Tx: 0Kbps, 2013/07/08 13:00

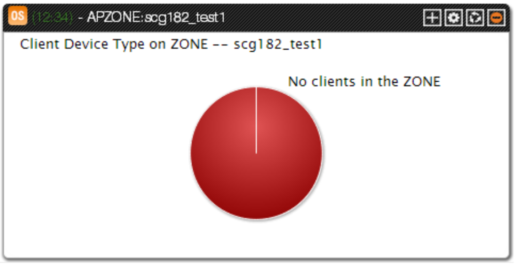
Client OS Type Summary Widget

The client operating system (OS) type summary widget displays a pie chart that shows the types of OS that associated wireless clients are using.

The client OS type summary widget requires one widget slot.

NOTE: The default refresh interval for the Client OS Type Summary widget is 15 minutes. When you add the widget, you can configure this refresh interval to any value between 1 and 30 minutes.

Figure 8. The client OS type summary widget



(12:34) - APZONE:scg182_test1

Client Device Type on ZONE -- scg182_test1

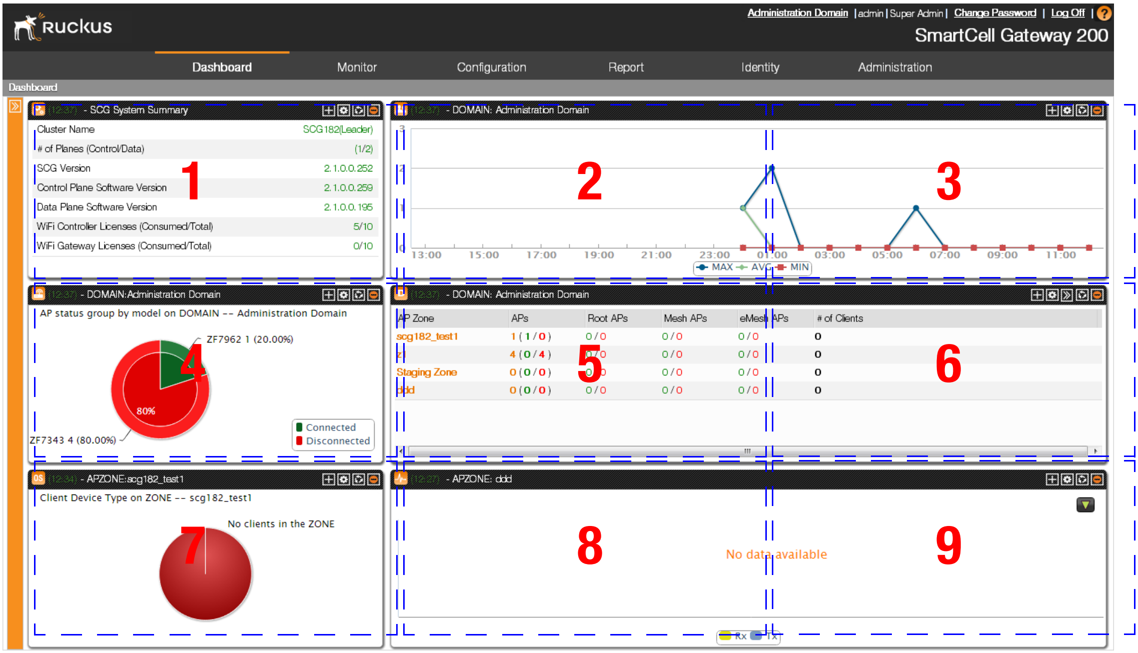
No clients in the ZONE

Widget Slots

The controller provides nine slots on the dashboard for placing widgets. Figure 9 marks these nine slots on the dashboard.

Note that some widgets are wider (for example, the client count summary and data throughput widgets) and require two widget slots. Make sure that there are enough empty slots on the dashboard before you add or move a widget.

Figure 9. There are nine slots for widgets on the dashboard



Cluster Name	SCG182(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	5/10
WiFi Gateway Licenses (Consumed/Total)	0/10

AP Zone	APs	Root APs	Mesh APs	eMesh APs	# of Clients
scg182_test1	1 (1 / 0)	0 / 0	0 / 0	0 / 0	0
z1	4 (0 / 4)	0 / 0	0 / 0	0 / 0	0
Staging Zone	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0
ddd	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0

Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Dashboard
(12:37) - SCG System Summary
(12:37) - DOMAIN: Administration Domain
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
09:00
11:00
MAX
AVG
MIN
(12:37) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
ZF7962 1 (20.00%)
80%
ZF7343 4 (80.00%)
Connected
Disconnected
(12:37) - DOMAIN: Administration Domain
(12:34) - APZONE:scg182_test1
Client Device Type on ZONE -- scg182_test1
No clients in the ZONE
(12:27) - APZONE: ddd
No data available
Rx
Tx
1
2
3
4
5
6
7
8
9

Adding a Widget

Follow these steps to add a widget to the dashboard.

1 Click the » icon in the upper-left corner of the page (below the Ruckus Wireless icon). The icons for adding widgets appear (see Table 1).

Table 1. Icons for adding widgets

Icon	Widget Name
👥	Client count summary widget

Table 1. Icons for adding widgets

Icon	Widget Name
📶	AP status summary widget
D	Domain summary widget
⚙	System summary widget
∿	Data throughput summary widget
OS	Client OS type summary widget

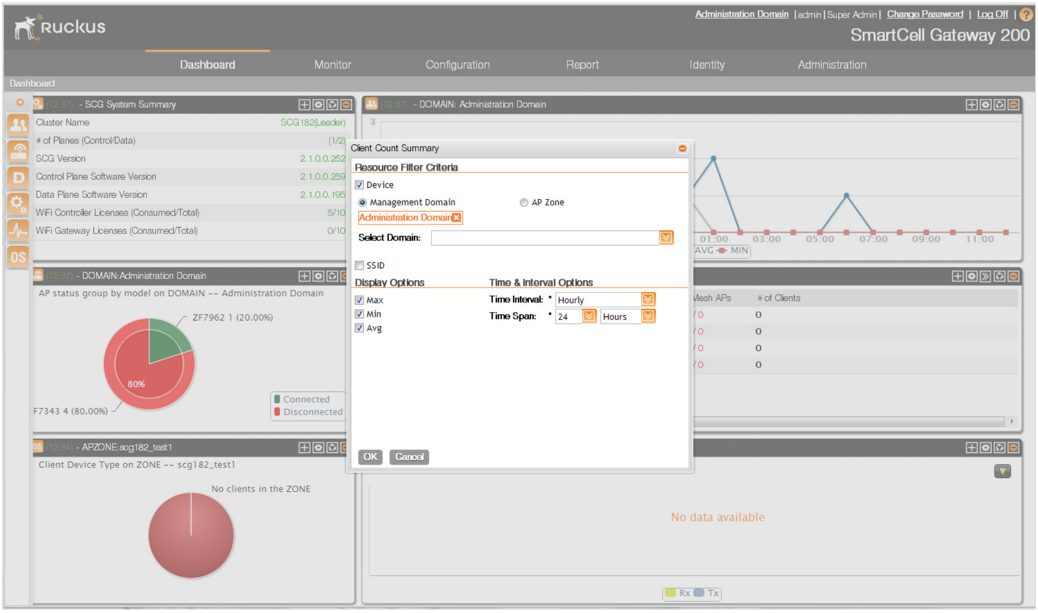
2 Click the icon for the widget that you want to add. A configuration form, which contains widget settings that you can configure, appears.

3 Configure the widget settings.

4 Click **OK**. The page refreshes, and then the widget that you added appears on the dashboard.

You have completed adding a widget. To add another widget, repeat the same procedure.

Figure 10. The configuration form for the Client Count Summary widget


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Dashboard
(12:37) - SCG System Summary
(12:37) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
ZF7962 1 (20.00%)
80%
F7343 4 (80.00%)
Connected
Disconnected
(12:34) - APZONE:scg182_test1
Client Device Type on ZONE -- scg182_test1
No clients in the ZONE
(12:37) - DOMAIN: Administration Domain
01:00
03:00
05:00
07:00
09:00
11:00
AVG
MIN
Mesh APs
# of Clients
No data available
Rx
Tx

Cluster Name	SCG182(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	5/10
WiFi Gateway Licenses (Consumed/Total)	0/10

Client Count Summary

Resource Filter Criteria

☑ Device

● Management Domain ○ AP Zone

Administration Domain ☒

Select Domain:

☐ SSID

Display Options

☑ Max
☑ Min
☑ Avg

Time & Interval Options

Time Interval: * Hourly
Time Span: * 24 Hours

OK Cancel

Adding a Widget to a Widget Slot

A single widget slot can contain multiple widgets of the same size (one-slot widgets versus two-slot widgets). For example, you can add the client count summary widget and data throughput widget (both are two-slot widgets) to the same widget slot.

Follow these steps to add a widget to a widget slot.

1 Locate an existing widget slot to which you want to add a widget.

2 Click the ⊞ icon that is in the upper-right hand corner of the widget slot. A submenu appears and displays the widgets that you can add to the widget slot.

3 Click the name of the widget that you want to add to the widget slot. The widget configuration window appears.

NOTE: You can only add a widget once. If a widget already exists in a different widget slot, you will be unable to add it to another widget slot.

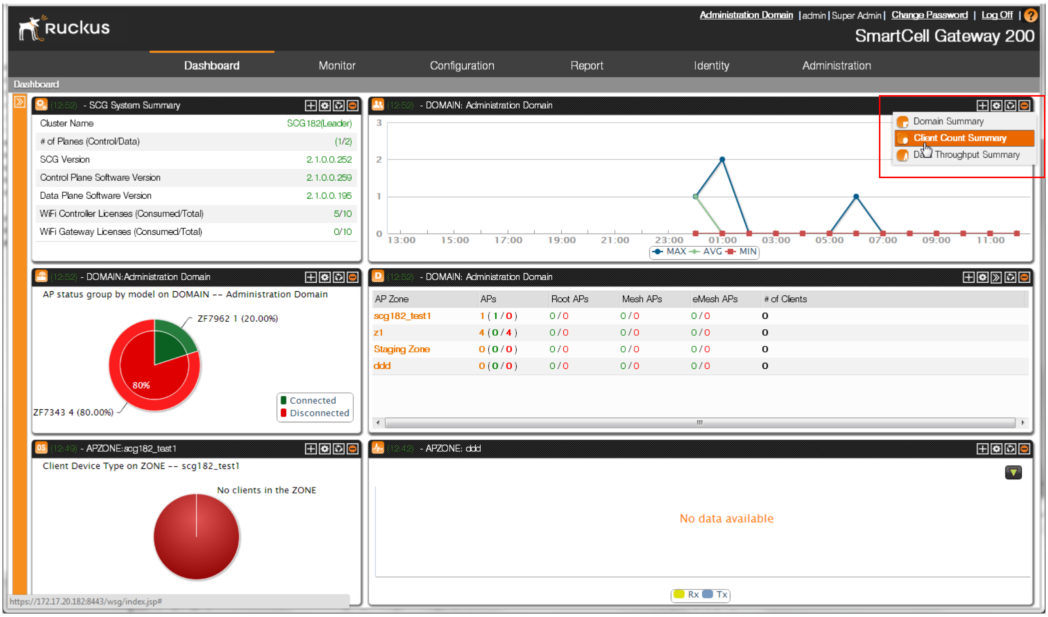
4 Configure the information that you want the widget to display and the interval at which to refresh the information on the widget.

NOTE: The refresh intervals for the client count summary and data throughput summary widgets are non-configurable.

5 Click **OK**. The widget slot refreshes, and then the widget that you added appears.

You have completed adding a widget to a widget slot.

Figure 11. Click the name of the widget that you want to add to the widget slot


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Dashboard
(12:52) - SCG System Summary
(12:52) - DOMAIN: Administration Domain
Domain Summary
Client Count Summary
Data Throughput Summary
3
2
1
0
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
09:00
11:00
MAX
AVG
MIN
(12:52) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
ZF7962 1 (20.00%)
80%
ZF7343 4 (80.00%)
Connected
Disconnected
(12:52) - DOMAIN: Administration Domain
(12:49) - APZONE:scg182_test1
Client Device Type on ZONE -- scg182_test1
No clients in the ZONE
(12:42) - APZONE: ddd
No data available
Rx
Tx
https://172.17.20.182:8443/wsg/index.jsp#

Cluster Name	SCG182(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	5/10
WiFi Gateway Licenses (Consumed/Total)	0/10

AP Zone	APs	Root APs	Mesh APs	eMesh APs	# of Clients
scg182_test1	1 (1 / 0)	0 / 0	0 / 0	0 / 0	0
z1	4 (0 / 4)	0 / 0	0 / 0	0 / 0	0
Staging Zone	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0
ddd	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0

Displaying a Widget in a Widget Slot

A widget slot that contains multiple widgets automatically cycles through the different widgets that have been added to it at one-minute intervals. If you want to view a specific widget in a widget slot, you can manually display it.

Follow these steps to display a widget that belongs to a widget slot manually.

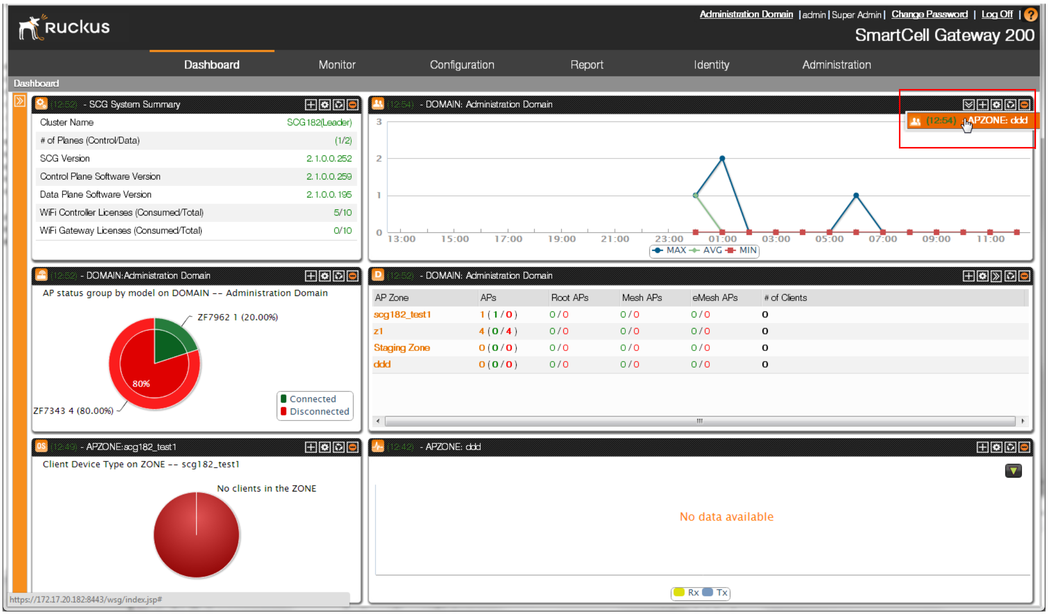
1 Locate the widget slot that contains the widget that you want to display.

2 Click the ▼ icon that is in the upper-right hand corner of the widget slot. A submenu appears and displays the widgets that have been added to the widget slot.

3 Click the name of the widget that you want to display. The widget slot refreshes, and the widget that you clicked appears.

You have completed displaying a widget in a widget slot.

Figure 12. Click the name of the widget that you want to display


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Dashboard
(12:52) - SCG System Summary
(12:54) - DOMAIN: Administration Domain
(12:54) APZONE: ddd
3
2
1
0
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
09:00
11:00
MAX
AVG
MIN
(12:52) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
ZF7962 1 (20.00%)
80%
ZF7343 4 (80.00%)
Connected
Disconnected
(12:52) - DOMAIN: Administration Domain
(12:49) - APZONE:scg182_test1
Client Device Type on ZONE -- scg182_test1
No clients in the ZONE
(12:42) - APZONE: ddd
No data available
Rx
Tx
https://172.17.20.182:8443/wsg/index.jsp#

Cluster Name	SCG182(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	5/10
WiFi Gateway Licenses (Consumed/Total)	0/10

AP Zone	APs	Root APs	Mesh APs	eMesh APs	# of Clients
scg182_test1	1 (1 / 0)	0 / 0	0 / 0	0 / 0	0
z1	4 (0 / 4)	0 / 0	0 / 0	0 / 0	0
Staging Zone	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0
ddd	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0

Moving a Widget

Follow these steps to move a widget from one widget slot to another.

1 Make sure that there are sufficient slots for the widget that you want to move.

2 Hover your mouse pointer on the title bar of the widget. The pointer changes into a four-way arrow.

3 Click-and-hold the widget, and then drag it to the empty slot to which you want to move it.

4 Release the widget.

You have completed moving a widget to another slot.

Deleting a Widget

Follow these steps to delete a widget.

1 Locate the widget that you want to delete.

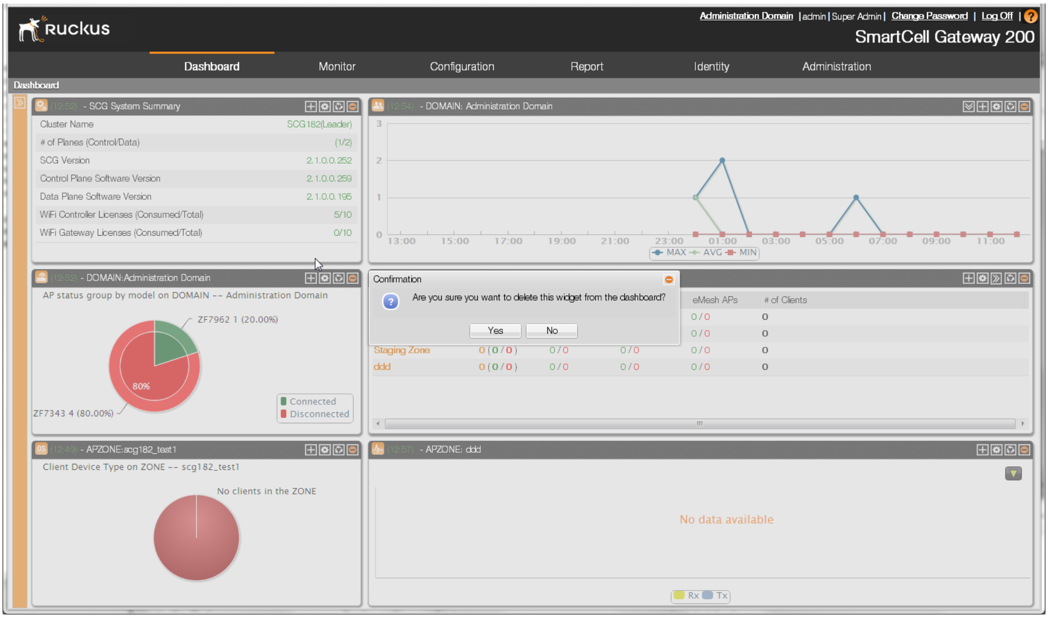
2 Click the ☒ icon that is in the upper-right hand corner of the widget. A confirmation message appears.

3 Click **OK** to confirm.

The dashboard refreshes, and then the widget that you deleted disappears from the page.

Click OK to confirm that you want to delete this widget

Figure 13. Click Yes to delete the widget



(12:52) - SCG System Summary

Cluster Name	SCG182(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	5/10
WiFi Gateway Licenses (Consumed/Total)	0/10

(12:54) - DOMAIN: Administration Domain
3
2
1
0
13:00
15:00
17:00
19:00
21:00
23:00
01:00
03:00
05:00
07:00
09:00
11:00
MAX
AVG
MIN
(12:52) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
ZF7962 1 (20.00%)
80%
ZF7343 4 (80.00%)
Connected
Disconnected

Confirmation

Are you sure you want to delete this widget from the dashboard?

Yes No

				eMesh APs	# of Clients
				0 / 0	0
				0 / 0	0
Staging Zone	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0
ddd	0 (0 / 0)	0 / 0	0 / 0	0 / 0	0

(12:49) - APZONE:scg182_test1
Client Device Type on ZONE -- scg182_test1
No clients in the ZONE
(12:57) - APZONE: ddd
No data available
Rx
Tx

Changing the Administrator Password

Follow these steps to change the administrator password.

1 On the *Miscellaneous Bar*, click **Change Password**. The *Change Password* form appears.

2 In *Old Password*, type your current password.

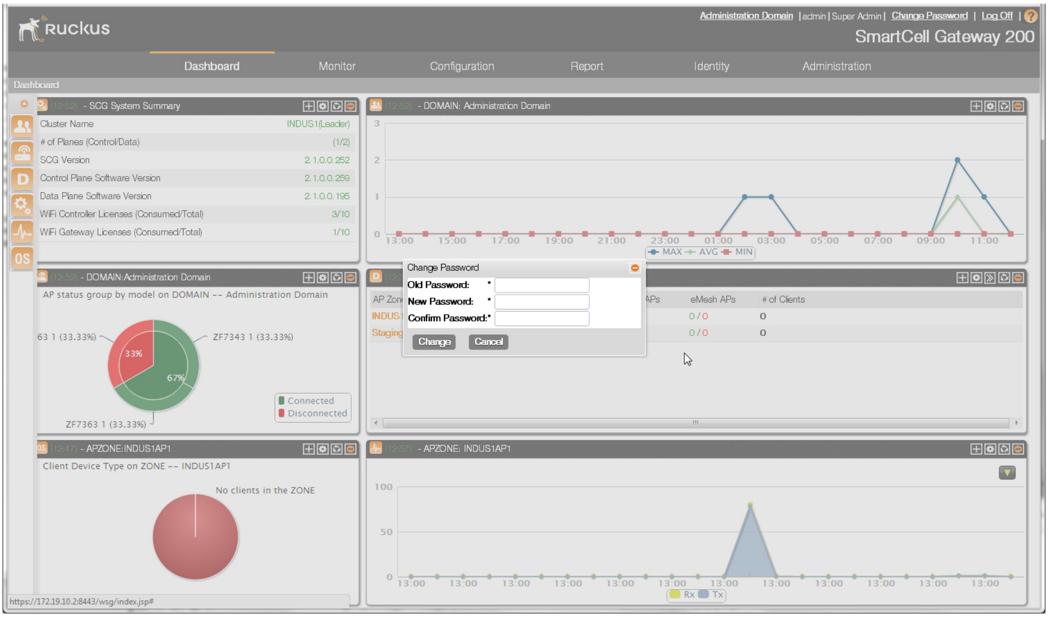
3 In *New Password*, type the new password that you want to use.

4 In *Confirm Password*, retype the new password above.

5 Click **Change**.

You have completed changing your administrator password. The next time you log on to the controller, remember to use your new administrator password.

Figure 14. The Change Password form


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off |
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Dashboard
(12:52) - SCG System Summary
(12:52) - DOMAIN: Administration Domain
MAX AVG MIN
(12:52) - DOMAIN:Administration Domain
AP status group by model on DOMAIN -- Administration Domain
63 1 (33.33%)
ZF7343 1 (33.33%)
ZF7363 1 (33.33%)
33%
67%
Connected
Disconnected
AP Zone
APs
eMesh APs
# of Clients
INDUS1
Staging
(12:47) - APZONE:INDUS1AP1
Client Device Type on ZONE -- INDUS1AP1
No clients in the ZONE
(12:57) - APZONE: INDUS1AP1
Rx
Tx
https://172.19.10.2:8443/wsg/index.jsp#

Cluster Name	INDUS1(Leader)
# of Planes (Control/Data)	(1/2)
SCG Version	2.1.0.0.252
Control Plane Software Version	2.1.0.0.259
Data Plane Software Version	2.1.0.0.195
WiFi Controller Licenses (Consumed/Total)	3/10
WiFi Gateway Licenses (Consumed/Total)	1/10

Change Password

Old Password: *
New Password: *
Confirm Password:*

Change Cancel

Logging Off the Web Interface

Follow these steps to log off the web interface.

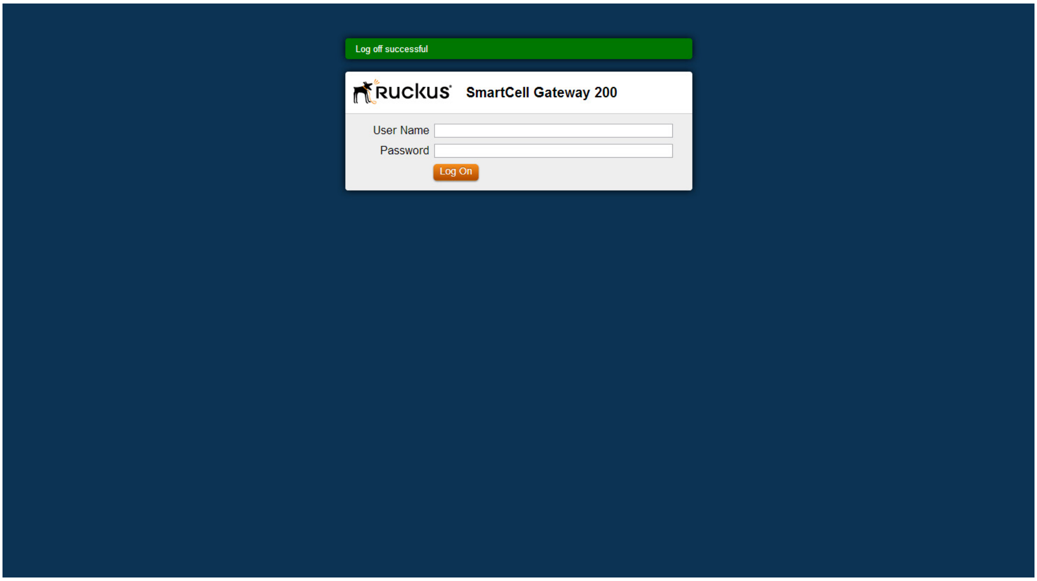
1 On the *Miscellaneous Bar*, click **Log Off**. A confirmation message appears.

2 Click **Yes**. The controller logs you off the web interface. The logon page appears with the following message above the Ruckus Wireless logo:

```
Log off successful
```

You have completed logging off the web interface.

Figure 15. The message "Log off successful" indicates that you have successfully logged off the web interface



Log off successful

Managing Ruckus Wireless AP Zones

2

In this chapter:

- Working with AP Zones
- Working with AP Groups
- Working with AAA Servers
- Working with Hotspot (WISPr) Portals
- Working with Guest Access Portals
- Working with Web Authentication Portals
- Working with Hotspot 2.0 Services
- Working with WLANs and WLAN Groups
- Working with WLAN Schedules
- Working with Device Policies
- Working with L2 Access Control Policies
- Working with Bonjour Policies

Working with AP Zones

An AP zone functions as a way of grouping Ruckus Wireless APs and applying a particular set of settings (including WLANs and their settings) to these groups of Ruckus Wireless APs. Each AP zone can include up to six WLAN services.

By default, an AP zone named *Staging Zone* exists. Any AP that registers with the controller that is not assigned a specific zone is automatically assigned to the Staging Zone. This section describes how to use AP zones to manage devices.

NOTE: When an AP is assigned or moved to the Staging Zone, the cluster name becomes its user name and password after the AP shows up-to-date state. If you need to log on to the AP, use the cluster name for the user name and password.

NOTE: Before creating an AP zone, Ruckus Wireless recommends that you first set the default country code on the *Global Configuration* page. This will help ensure that each new AP zone will use the correct country code. For information on how to set the default country code, see Managing Global Configuration.

This section covers:

- Using the Domain Tree and Search Boxes
- Creating an AP Zone
- Creating an AP Zone from a ZoneDirector Backup File
- Cloning an AP Zone from the Domain Tree
- Cloning an AP Zone from the AP Zone List
- Viewing Existing AP Zones
- Viewing the AP Zone Configuration
- Deleting an AP Zone

Using the Domain Tree and Search Boxes

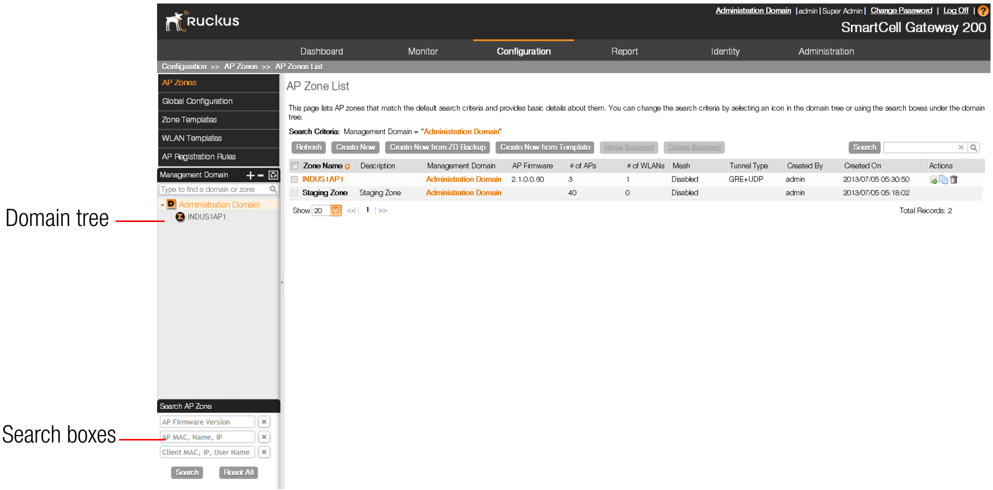
Clicking *Configuration* > *AP Zones* on the main menu displays a sidebar on the left side of the page, which includes the domain tree and search boxes.

The domain tree displays the management domains (D) and AP zones (Z) that are under *Administration Domain*. Clicking a domain icon in the tree displays the AP zones that belong to it in the content area. Clicking an AP zone icon, on the other hand, displays detailed information about the AP zone, including its general information, AAA server configuration, and hotspot configuration.

Below the domain tree are search boxes that you can use to search for AP zones, access points, and wireless clients. Each search box is labeled with the search parameters that it accepts. For example, you can type an AP firmware version number in the first search box.

NOTE The search criteria are case-sensitive.

Figure 16. The domain tree and search boxes



AP Zone List

This page lists AP zones that match the default search criteria and provides basic details about them. You can change the search criteria by selecting an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Management Domain = "Administration Domain"

□	Zone Name	Description	Management Domain	AP Firmware	# of APs	# of WLANs	Mesh	Tunnel Type	Created By	Created On	Actions
□	INDUS1AP1		Administration Domain	2.1.0.0.60	3	1	Disabled	GRE+UDP	admin	2013/07/05 05:30:50	
□	Staging Zone	Staging Zone	Administration Domain		40	0	Disabled		admin	2013/07/05 05:18:02	

Total Records: 2

Creating an AP Zone

NOTE: If you are planning to use SoftGRE tunneling for this AP zone, you must first create a SoftGRE tunnel profile before creating the AP zone. For instructions on how to create a SoftGRE tunnel profile, see Creating a SoftGRE Tunnel Profile.

Follow these steps to create an AP zone.

1. Click *Configuration* > *AP Zones*.
2. Click **Create New**. The form for creating a new AP zone appears.
3. Configure *General Options*.
    - *Zone Name*: Type a name that you want to assign to this new zone.
    - *Description*: Type a description for this new zone. This is an optional field.
    - *AP Firmware*: Select the AP firmware version that you want the AP zone to use. By default, the latest AP firmware available on the controller is selected.

- *Country Code*: Select the country in which you are operating the access points. Different countries and regions maintain different rules that govern which channels can be used for wireless communications. Setting the country code to the proper regulatory region helps ensure that the wireless network does not violate local and national regulatory restrictions.
- *Location*: Type a location name (for example, Ruckus Wireless HQ) for this AP zone.
- *Location Additional Information*: Type additional information about the AP zone (for example, 350 W Java Dr, Sunnyvale, CA 94089, United States).
- *GPS Coordinates*: Type the longitude and latitude coordinates for the AP zone's location.
- *AP Admin Logon*: Specify the user name and password that administrators can use to log on directly to the managed access point's native web interface. The following boxes are provided:
    - *Logon ID*: Type the admin user name.
    - *Password*: Type the admin password.
- *Time Zone*: Select the time zone that you want APs that belong to this zone to use. Options include:
    - *System defined*: Click this option, and then select a time zone from the list.
    - User defined: Click this option, and then configure a custom time zone by setting the time zone abbreviation and GMT offset and configuring daylight saving time support.
- *AP IP Mode*: Select the IP addressing mode that you want APs (that belong to this zone) to use. Options include:
    - **IPv4 Only**
    - **IPv6 Only**

4 Configure *Mesh Options*.

- *Enable*: Select the **Enable mesh networking in this zone** check box if you want managed devices that belong to this zone to be able to form a mesh network automatically. When this check box is selected, the following two options are visible:
    - *Mesh Name (ESSID)*: Type a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller generates.

- *Mesh Passphrase*: Type a passphrase that contains at least 8 characters. This passphrase will be used by the controller to secure the traffic between mesh APs. Alternatively, click do nothing to accept the passphrase that the controller has generated. To generate a new random passphrase with 64 characters or more, click **Generate**.

5 Configure *Radio Options*.

- *Channelization*: Select the channel widths for Radio b/g/n (2.4GHz) and Radio a/n/ac (5GHz). Options include 20, 40, and 80.
- *Channel*: Select the channel numbers to use for *Radio b/g/n (2.4GHz)* and *Radio a/n (5GHz)*. Select **Auto** to automatically assign a radio channel or select a specific channel number to manually assign it to a radio.
- *Tx Power Adjustment*: Select the preferred TX power for each radio, if you want to manually configure the transmit power on the 2.4GHz and 5GHz radios. By default, TX power is set to **Full** on both the 2.4GHz and 5GHz radios.

6 Configure *AP GRE Tunnel Options*.

- *Tunnel Type*: Select a protocol to use for tunneling WLAN traffic back to the controller. Options include **Ruckus GRE**, **SoftGRE**, and **SoftGRE IPSec**.
- *Tunnel Profile*: Select the tunnel profile that you want to use. If you want to use Ruckus GRE tunneling for this AP zone, you can use the default tunnel profile or you can select a profile that you created. If you want to use SoftGRE tunneling, you must first create a SoftGRE tunnel profile.

NOTE: Instructions for creating a Ruckus GRE and SoftGRE tunnel profiles are provided in Creating AP Tunnel Profiles.

7 Configure *Syslog Options*.

- To send events related to APs in this zone to an external syslog server, select the **Enable external syslog server for APs in this zone** check box. Additional options appear below.
- *Server Address*: Type the IP address of the syslog server on the network.

NOTE: The IP address format that you enter here will depend on the AP IP mode that you selected earlier in this procedure. If you selected **IPv4 Only**, enter an IPv4 address. If you selected **IPv6 Only**, enter an IPv6 address.

- *Port*: Type the syslog port number on the server.

- *Facility*: Select the facility level that will be used by the syslog message. Options include Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7.
- *Priority*: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**.

8 Configure *Advanced Options*.

- *Channel Mode*: If you want to allow outdoor APs that belong to this zone to use wireless channels that are regulated as indoor-use only, select the **Allow indoor channels** check box. For more information, see Channel Mode.
- *Background Scanning*: If you want APs to evaluate radio channel usage automatically, enable and configure the background scanning settings on both the 2.4GHz and 5GHz radios. By default, background scanning is enabled on both radios and is configured to run every 20 seconds.
- *Auto Channel Selection*: You can adjust the AP channel to 2.4 GHz or 5 GHz frequencies by selecting the appropriate check-box. Further, you can automatically adjust the AP to optimize performance by choosing one of the following:
  - Background Scanning
  - ChannelFly
- *Smart Monitor*: To disable the WLANs of an AP (that belongs to this zone) whenever the AP uplink or Internet connection becomes unavailable, select the **Enable** check box. And then, configure the following options:
  - *Health Check Interval*: Set the interval (between 5 and 60 seconds) at which the AP will check its uplink connection. The default value is 10 seconds.
  - *Health Check Retry Threshold*: Set the number of times (between 1 and 10 times) that the AP will check its uplink connection. If the AP is unable to detect the uplink after the configured number of retries, the AP will disable its WLANs. The default value is 3 retries.

NOTE: When the AP disables its WLANs, the AP creates a log for the event. When the AP's uplink is restored, it sends the event log (which contains the timestamp when the WLANs were disabled, and then enabled) to the controller.

- *VLAN Pooling*: Select the **Allow VLAN Pooling overlapping** check box to enable VLAN pooling. For more information, see About VLAN Pooling.
- *Rogue AP Detection*: Select the **Report rogue access points** check box to enable rogue device detection in logs and email alarm event notifications.
  - **Report all rogue devices***:* Send alerts for all rogue AP events.
  - **Report only malicious rogue devices of type**: Select which event types to report. Events include SSID spoofing, same network, and MAC spoofing.
  - **Protect the network from malicious rogue access points**: Select this check box to automatically protect your network from network connected rogue APs, SSID-spoofing APs and MAC-spoofing APs. When one of these rogue APs is detected (and this check box is enabled), the Ruckus Wireless AP automatically begins sending broadcast de-authentication messages spoofing the rogue's BSSID (MAC) to prevent wireless clients from connecting to the malicious rogue AP. This option is disabled by default.
- *Client Load Balancing*: Improve WLAN performance by enabling load balancing. Load balancing spreads the wireless client load between nearby access points, so that one AP does not get overloaded while another sites idle. Load balancing must be enabled on a per-radio basis. To enable load balancing, select the **Enable loading balancing on [2.4GHz or 5GHz]** check box, and then set or accept the default *Adjacent Radio Threshold* (50dB for the 2.4GHz radio and 43dB for the 5GHz radio).
- *Band Balancing*: Client band balancing between the 2.4GHz and 5GHz radio bands is disabled by default on all WLANs. To enable band balancing for this WLAN, select the **Enable band balancing on radios by distributing the clients on 2.4GHz and 5GHz bands** check box, and then set the percentages of client load that will be distributed between the 2.4GHz and 5Ghz bands. For more information, see Band Balancing.
- *Location Based Service*: To enable LBS service for this AP zone, select the **Enable LBS Service** check box, and then select an LBS server to use from the drop-down list. For information on how to add an LBS server to the controller, see Configuring Location Services.
- *Client Admission Control*: Set the load thresholds on the AP at which it will stop accepting new clients. See Configuring Client Admission Control.

- *AP Reboot Timeout*: Set the time after which the AP will reboot automatically when it is unable to reach the default gateway or the control interface.
    - *Reboot AP if it cannot reach default gateway after [ ] minutes*: The default timeout is 30 minutes.
    - *Reboot AP if it cannot reach the controller after [ ]*: The default timeout is 2 hours.

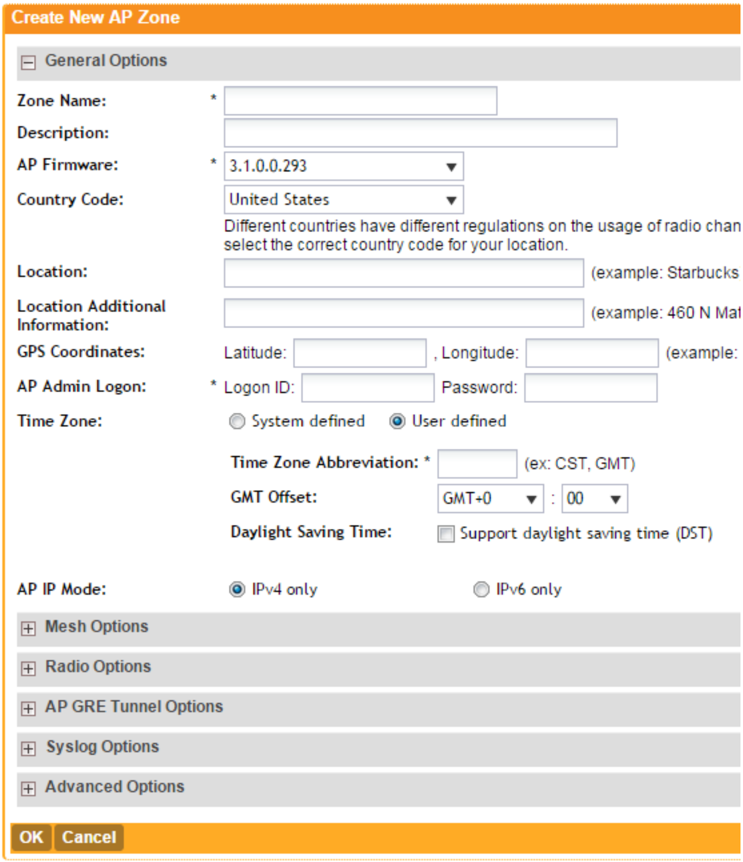
9 Click **OK** to finish creating your first AP zone. When the controller completes creating the AP zone, the following confirmation message appears:

```
AP zone created successfully. Do you want to view the
configuration details?
```

10 Click **Yes** to view the AP zone details, or click **No** to close the confirmation message and return to the AP zone list.

You have completed creating your first AP zone. You can create additional AP zones as needed.

Figure 17. The Create New AP Zone form



Create New AP Zone

⊟ General Options

Zone Name:	*	
Description:		
AP Firmware:	*	3.1.0.0.293 ▼
Country Code:		United States ▼ Different countries have different regulations on the usage of radio chan select the correct country code for your location.
Location:		(example: Starbucks
Location Additional Information:		(example: 460 N Mat
GPS Coordinates:		Latitude: , Longitude: (example:
AP Admin Logon:	*	Logon ID: Password:
Time Zone:		○ System defined ● User defined
		Time Zone Abbreviation: * (ex: CST, GMT)
		GMT Offset: GMT+0 ▼ : 00 ▼
		Daylight Saving Time: □ Support daylight saving time (DST)
AP IP Mode:		● IPv4 only ○ IPv6 only

⊞ Mesh Options

⊞ Radio Options

⊞ AP GRE Tunnel Options

⊞ Syslog Options

⊞ Advanced Options

About VLAN Pooling

When Wi-Fi is deployed in a high density environment (such as a stadium) or in a university campus to provide access for students, the number of IP addresses required for client devices can easily run into several thousands. Allocating a single large subnet results in a high probability of degraded performance due to factors like broadcast/multicast traffic.

To address this problem, VLAN pooling provides a method by which administrators can deploy pools of multiple VLANs from which clients are assigned, thereby automatically segmenting large groups of clients into smaller subgroups, even when connected to the same SSID.

As the client device joins the Wi-Fi network, the VLAN is assigned based on a hash of the client’s MAC address (by default), or via round-robin or least-used VLAN assignment.

ChannelFly and Background Scanning

SmartZone controllers offer the ChannelFly and Background Scanning automatic channel selection methods for spectrum utilization and performance optimization. While Background Scanning must be enabled for rogue AP detection, AP location detection and radio power adjustment, either can be used for automatic channel optimization.

The main difference between ChannelFly and Background Scanning is that ChannelFly determines the optimal channel based on real-time statistical analysis of actual throughput measurements, while Background Scanning uses channel measurement and other techniques to estimate the impact of interference on Wi-Fi capacity based on progressive scans of all available channels.

NOTE: If you enable ChannelFly, Background Scanning can still be used for adjusting radio power and rogue detection while ChannelFly manages the channel assignment. Both cannot be used at the same time for channel management.

Benefits of ChannelFly

With ChannelFly, the AP intelligently samples different channels while using them for service. ChannelFly assesses channel capacity every 15 seconds and changes channel when, based on historical data, a different channel is likely to offer higher capacity than the current channel. Each AP makes channel decisions based on this historical data and maintains an internal log of channel performance individually.

When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and Ruckus mesh nodes in the 2.4 GHz and/or 5 GHz bands.

Initially (in the first 30-60 minutes) there will be more frequent channel changes as ChannelFly learns the environment. However, once an AP has learned about the environment and which channels are most likely to offer the best throughput potential, channel changes will occur less frequently unless a large measured drop in throughput occurs.

ChannelFly can react to large measured drops in throughput capacity in as little as 15 seconds, while smaller drops in capacity may take longer to react to.

Disadvantages of ChannelFly

Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause significant connectivity issues during the initial capacity assessment stage.

You can enable/disable ChannelFly per band. If you have 2.4 GHz clients that do not support 802.11h, Ruckus recommends disabling ChannelFly for 2.4 GHz but leaving it enabled for the 5 GHz band.

Background Scanning

Using Background Scanning, SmartZone controllers regularly samples the activity in all Access Points to assess RF usage, to detect rogue APs and to determine which APs are near each other for mesh optimization. These scans sample one channel at a time in each AP so as not to interfere with network use. This information is then applied in AP Monitoring and other controller monitoring features. You can, if you prefer, customize the automatic scanning of RF activity, deactivate it if you feel it's not helpful, or adjust the frequency, if you want scans at greater or fewer intervals.

NOTE: Background Scanning must be enabled for SmartZone controllers to detect rogue APs on the network.

Creating an AP Zone from a ZoneDirector Backup File

If your organization was previously using Ruckus Wireless ZoneDirector to manage access points on the network and you are in the process of migrating to the controller, you can easily migrate access point management to the controller by creating an AP zone from the ZoneDirector backup file.

When you import a ZoneDirector backup file to the controller, note that only access points that are already approved to join ZoneDirector will be migrated to the controller. Access points that do not have the *Approved* status will be ignored.

Additionally, if an access point that already exists in the controller also exists in the ZoneDirector backup file, the access point will be transferred automatically from its current AP zone to the new AP zone.

NOTE: : Release 3.1.1 supports ZoneDirector backups from releases 9.10 and 9.9 whereas release 3.1 supports backups from releases 9.9 and 9.8.

This section covers:

- Backing Up the ZoneDirector
- Restoring ZoneDirector Backup to the Controller

NOTE: The controller supports RADIUS for AAA management. If a WLAN or hotspot in the ZoneDirector backup file is configured to use a non-RADIUS AAA server (for example, Active Directory, LDAP, or local database), that WLAN or hotspot will not be migrated to the controller.

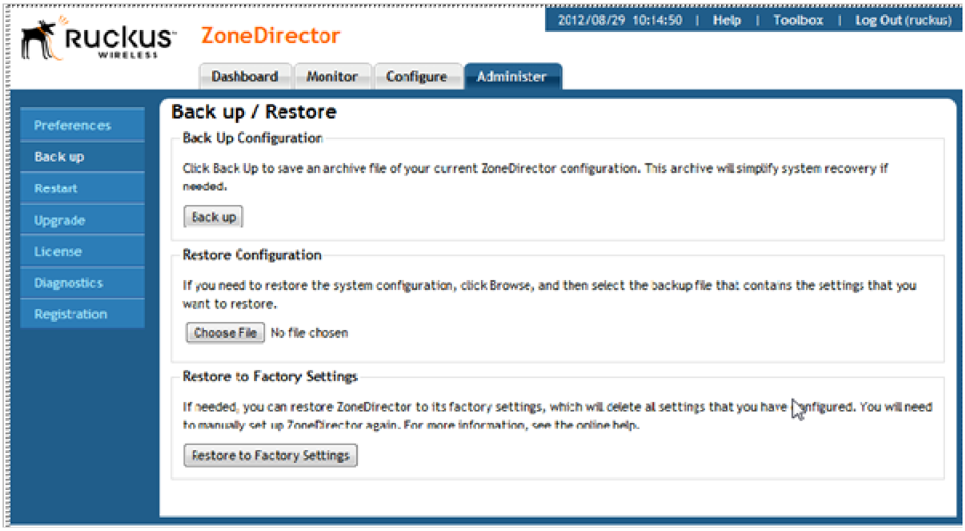
Backing Up the ZoneDirector

Follow these steps to create a ZoneDirector backup.

1. Go to *Administer* > *Back up*.
2. In the *Backup Configuration* section, click **Back Up**. The *File Download* dialog box appears.
3. Click **Save**. The *Save As* dialog box appears.
4. Type a name for the backup file, and then select a location where you want to save it.
5. Verify that the file name ends with .bak extension.
6. Click **Save**. The *Download Complete* dialog box appears.
7. Click **Close**.

You have completed backing up ZoneDirector.

Figure 18. The ZoneDirector backup page



Back up / Restore

Back Up Configuration

Click Back Up to save an archive file of your current ZoneDirector configuration. This archive will simplify system recovery if needed.

Restore Configuration

If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore.

Restore to Factory Settings

If needed, you can restore ZoneDirector to its factory settings, which will delete all settings that you have configured. You will need to manually set up ZoneDirector again. For more information, see the online help.

Restoring ZoneDirector Backup to the Controller

Follow these steps to restore the ZoneDirector backup to the controller.

1 Copy the ZoneDirector backup file to a location (local computer or network) that you can access from the controller web interface.

2 Log on to the controller web interface, and then go to *Configuration* > *AP Zones*. The *AP Zone List* page appears.

3 Click **Create New from ZD Backup**. The *Create New AP Zone from ZD Backup File* dialog box appears.

4 In *AP Firmware*, select the firmware that you want the new zone to use.

5 In *AP Admin Logon ID*, set the user name that administrators can use to log on directly to the managed access points' native web interface.

6 In *AP Admin Password*, set the password for the AP administrator logon ID.

NOTE: The password must be at least eight characters and must consist of at least one number, one letter, and one special character (for example, !, #, $, %, &, or ?).

7 In *ZoneDirector Backup File*, click **Browse**, and then go to the location where you copied the backup file.

8 Select the backup file (with .bak extension), and then click **Open**.

9 Click **Apply.** A progress bar appears as the controller imports the ZoneDirector backup file and creates an AP zone. When the process is complete, the following confirmation message appears:

```
AP zone created successfully. Do you want to view the zone
configuration details?
```

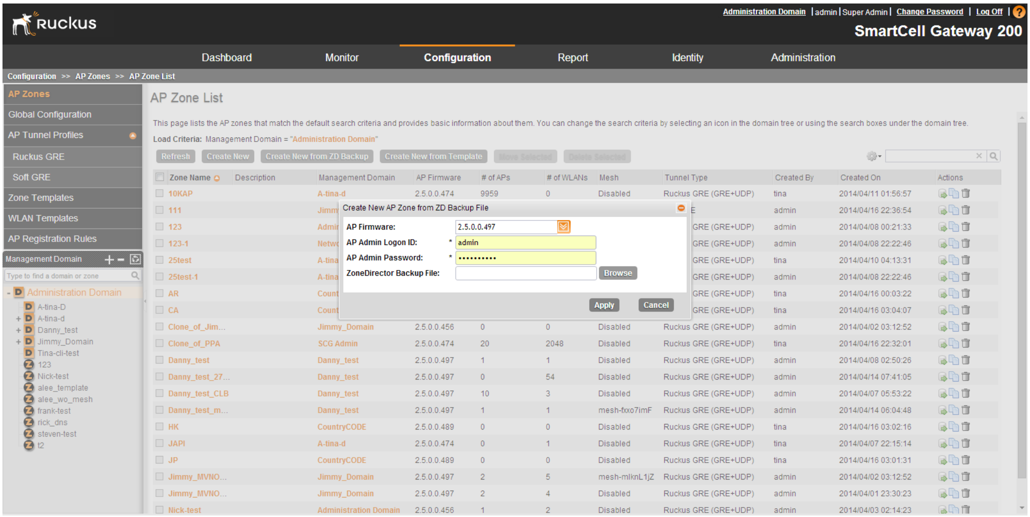
10 Click **Yes** to view the zone configuration, or click **No** to close the confirmation message and stay on the current page.

11 Verify that an AP zone that uses the system name of the ZoneDirector that you backed up appears in the AP zone list. For example, if the ZoneDirector system name is “ZDMain”, look for an AP zone named `ZDMain`. This is the AP zone that you created from the ZoneDirector backup file.

You have completed creating a new AP zone from a ZoneDirector backup file.

NOTE: There are a few minor features that the controller supports but ZoneDirector does not (and vice versa). Because of these differences in features, migrated AP zones and access points may not have some of the features that they had previously. For more information on what features are available in AP zones and access pointed after migration, see ZoneDirector to SmartCell Gateway Migration: Features Matrix.

Figure 19. The Create New AP Zone from ZD Backup File dialog box



AP Zone List

This page lists the AP zones that match the default search criteria and provides basic information about them. You can change the search criteria by selecting an icon in the domain tree or using the search boxes under the domain tree.

Load Criteria: Management Domain = "Administration Domain"

Zone Name	Description	Management Domain	AP Firmware	# of APs	# of WLANs	Mesh	Tunnel Type	Created By	Created On	Actions
10KAP		A-tina-d	2.5.0.0.474	9959	0	Disabled	Ruckus GRE (GRE+UDP)	tina	2014/04/11 01:56:57	
111		Jimm					E	admin	2014/04/16 22:36:54	
123		Admir					GRE (GRE+UDP)	admin	2014/04/08 00:21:33	
123-1		Netw					GRE (GRE+UDP)	admin	2014/04/08 22:22:46	
25test		A-tina					GRE (GRE+UDP)	tina	2014/04/10 04:13:31	
25test-1		A-tina					GRE (GRE+UDP)	admin	2014/04/08 22:22:46	
AR		Count					GRE (GRE+UDP)	tina	2014/04/16 00:03:22	
CA		Count					GRE (GRE+UDP)	tina	2014/04/16 03:04:07	
Clone_of_Jim...		Jimmy_Domain	2.5.0.0.456	0	0	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/02 03:12:52	
Clone_of_PPA		SCG Admin	2.5.0.0.474	20	2048	Disabled	Ruckus GRE (GRE+UDP)	tina	2014/04/16 22:32:01	
Danny_test		Danny_test	2.5.0.0.497	1	1	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/08 02:50:26	
Danny_test_27...		Danny_test	2.5.0.0.497	0	54	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/14 07:41:05	
Danny_test_CLB		Danny_test	2.5.0.0.497	10	3	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/07 05:53:22	
Danny_test_m...		Danny_test	2.5.0.0.497	1	1	mesh-fxxo7imF	Ruckus GRE (GRE+UDP)	admin	2014/04/14 06:04:48	
HK		CountryCODE	2.5.0.0.489	0	0	Disabled	Ruckus GRE (GRE+UDP)	tina	2014/04/16 03:02:16	
JAPI		A-tina-d	2.5.0.0.474	0	1	Disabled	Ruckus GRE (GRE+UDP)	tina	2014/04/07 22:15:14	
JP		CountryCODE	2.5.0.0.489	0	0	Disabled	Ruckus GRE (GRE+UDP)	tina	2014/04/16 03:01:31	
Jimmy_MVNO...		Jimmy_Domain	2.5.0.0.497	2	5	mesh-mlknL1jZ	Ruckus GRE (GRE+UDP)	admin	2014/04/02 03:12:52	
Jimmy_MVNO...		Jimmy_Domain	2.5.0.0.497	2	4	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/01 23:30:23	
Nick-test		Administration Domain	2.5.0.0.456	1	2	Disabled	Ruckus GRE (GRE+UDP)	admin	2014/04/03 02:14:23	

Create New AP Zone from ZD Backup File

AP Firmware: 2.5.0.0.497
AP Admin Logon ID: * admin
AP Admin Password: * ••••••••••
ZoneDirector Backup File:

Cloning an AP Zone from the Domain Tree

Cloning an AP zone enables you to copy the configuration of an existing zone and save it as a new zone. If you need to create an AP zone with configuration settings that are similar to an existing AP zone, cloning that existing AP zone would be the easiest way to do it.

Follow these steps to clone an AP zone.

1 Go to *Configuration* > *AP Zones*.

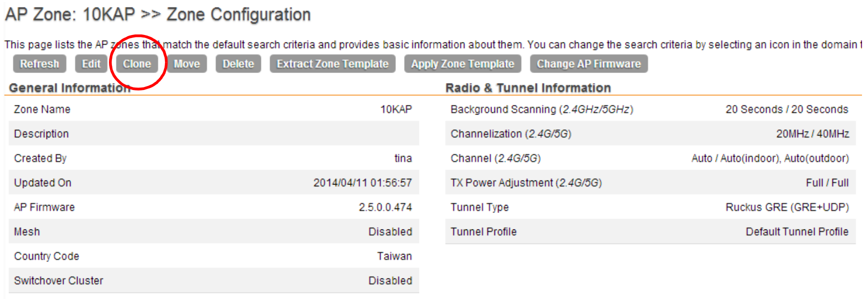
2 In the domain tree, find the AP zone that you want to clone.

3 Click **Clone**. A form appears and prompts you for the name that you want to assign to the cloned zone. The default name is *Clone of {Original Zone Name}*.

4 Edit the AP zone name or leave it as is.

5 Click **OK** to finish cloning the AP zone.

Figure 20. Click the Clone button to save the AP zone as a new zone



AP Zone: 10KAP >> Zone Configuration

This page lists the AP zones that match the default search criteria and provides basic information about them. You can change the search criteria by selecting an icon in the domain t

General Information

Zone Name	10KAP
Description	
Created By	tina
Updated On	2014/04/11 01:56:57
AP Firmware	2.5.0.0.474
Mesh	Disabled
Country Code	Taiwan
Switchover Cluster	Disabled

Radio & Tunnel Information

Background Scanning (*2.4GHz/5GHz*)	20 Seconds / 20 Seconds
Channelization (*2.4G/5G*)	20MHz / 40MHz
Channel (*2.4G/5G*)	Auto / Auto(indoor), Auto(outdoor)
TX Power Adjustment (*2.4G/5G*)	Full / Full
Tunnel Type	Ruckus GRE (GRE+UDP)
Tunnel Profile	Default Tunnel Profile

Cloning an AP Zone from the AP Zone List

Another method to save an existing AP zone as a new zone is by cloning it from the *AP Zone List* page. Follow these steps to clone an AP zone from the *AP Zone List* page.

1 Go to *Configuration* > *AP Zones*.

2 On the *AP Zones List* page, find the AP zone that you want to clone.

3 Click the action icon 🗐 that is in the same row as the AP zone name.

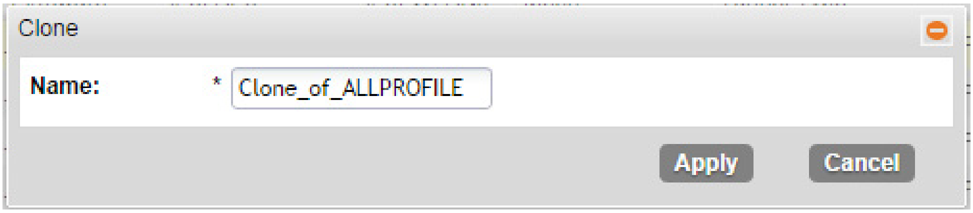
4 A form appears and prompts you for the name that you want to assign to the cloned zone. The default name is *Clone_of_{Original Zone Name}*.

5 Edit the AP zone name or leave it as is.

6 Click **Apply**. The page refreshes, and then the AP zone that you cloned appears in the *AP Zone List*.

You have completed cloning an AP zone from the AP zone list.

Figure 21. A form prompts you for the name that you want to assign to the cloned zone



Name: * Clone_of_ALLPROFILE

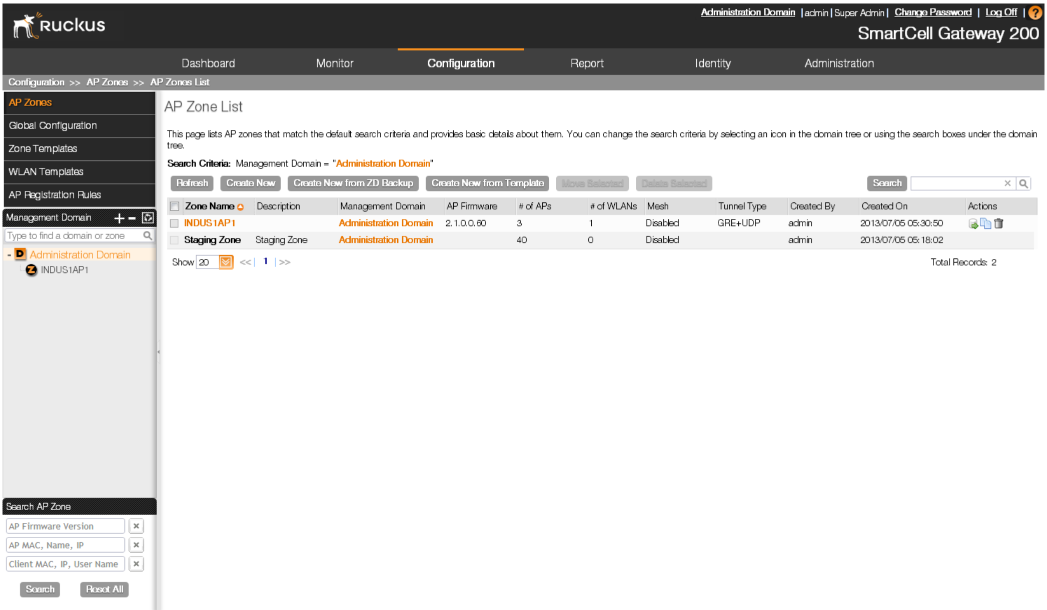
Viewing Existing AP Zones

Follow these steps to view a list of existing AP zones.

1. Go to *Configuration* > *AP Zones*. The *AP Zone List* page appears and displays a list of existing AP zones.
2. To view the configuration of a specific zone, locate the zone whose details you want to view on the *AP Zone List* page.
3. Under the *Zone Name* column, click the AP zone name.

The page refreshes and displays the AP zone configuration page.

Figure 22. The AP Zone List page



This page lists AP zones that match the default search criteria and provides basic details about them. You can change the search criteria by selecting an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Management Domain = "Administration Domain"

□	Zone Name	Description	Management Domain	AP Firmware	# of APs	# of WLANs	Mesh	Tunnel Type	Created By	Created On	Actions
□	INDUS1AP1		Administration Domain	2.1.0.0.60	3	1	Disabled	GRE+UDP	admin	2013/07/05 05:30:50	
□	Staging Zone	Staging Zone	Administration Domain		40	0	Disabled		admin	2013/07/05 05:18:02	

Total Records: 2

Viewing the AP Zone Configuration

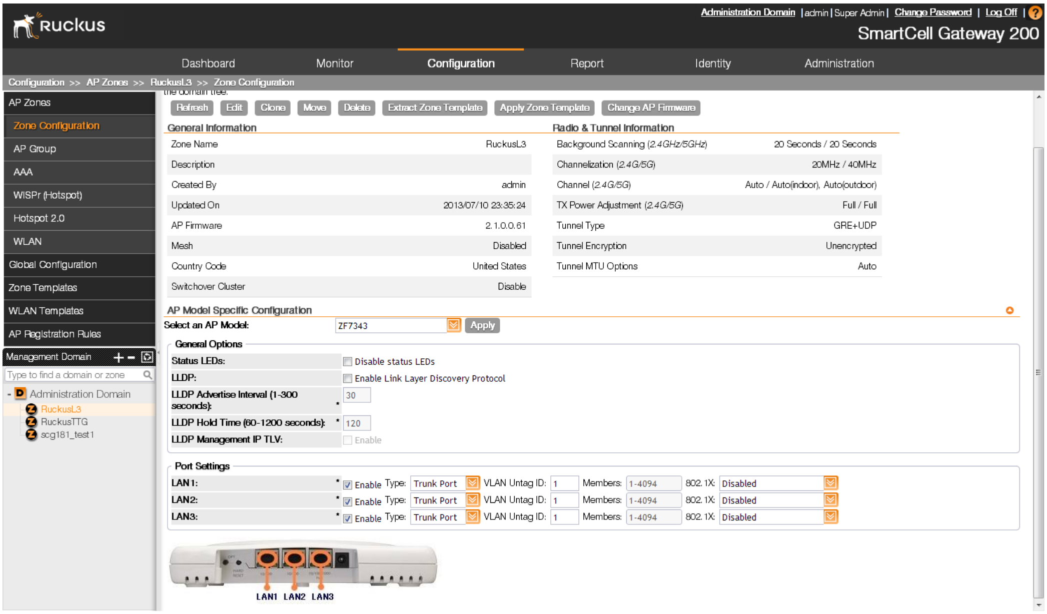
Follow these steps to view a summary of the AP zone configuration.

1 Go to *Configuration* > *AP Zones*.

2 On the *AP Zone List* page, click the name of the AP zone that you want to view.

The *Zone Configuration* page for the AP zone appears and displays as summary of the AP zone configuration.

Figure 23. The Zone Configuration page displays a summary of the zone settings



General Information

Zone Name	RuckusL3
Description	
Created By	admin
Updated On	2013/07/10 23:35:24
AP Firmware	2.1.0.0.61
Mesh	Disabled
Country Code	United States
Switchover Cluster	Disable

Radio & Tunnel Information

Background Scanning (*2.4GHz/5GHz*)	20 Seconds / 20 Seconds
Channelization (*2.4G/5G*)	20MHz / 40MHz
Channel (*2.4G/5G*)	Auto / Auto(indoor), Auto(outdoor)
TX Power Adjustment (*2.4G/5G*)	Full / Full
Tunnel Type	GRE+UDP
Tunnel Encryption	Unencrypted
Tunnel MTU Options	Auto

AP Model Specific Configuration

Select an AP Model: ZF7343

General Options

Status LEDs:	☐ Disable status LEDs
LLDP:	☐ Enable Link Layer Discovery Protocol
LLDP Advertise Interval (1-300 seconds): *	30
LLDP Hold Time (60-1200 seconds): *	120
LLDP Management IP TLV:	☐ Enable

Port Settings

LAN1: *	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled
LAN2: *	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled
LAN3: *	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled

The following buttons and options also appear on the page:

- **Edit**: Click to edit the AP zone configuration.
- **Clone**: Click to clone this AP zone.
- **Move**: Click to move this AP zone from its current management domain to another.
- **Delete**: Click to delete this AP zone.

If you want to override the AP zone settings for specific AP models, configure the *AP Model-Specific Configuration* section at the bottom of the page (see Modifying Model Specific Controls for more information).

Deleting an AP Zone

Deleting an AP zone that contains managed devices will automatically move those devices to the Staging Zone (default zone). Before deleting an AP zone, Ruckus Wireless recommends moving devices that belong to that zone to another zone.

Follow these steps to delete an AP zone.

1 Go to *Configuration* > *AP Zones*.

2 In the domain tree, select the AP zone that you want to delete.

3 Click the **Delete Selected** button. A confirmation message appears.

4 Click **OK** to finish deleting the AP zone.

You have completed deleting an AP zone service.

NOTE Ensure that all the AP's associated to that zone needs to be deleted before deleting the AP Zone.

Working with AP Groups

AP (access point) groups can be used to define configuration options and apply them to groups of APs at once, without having to modify each AP's settings individually.

For each group, administrators can create a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

AP groups are similar to WLAN groups (see Working with WLAN Groups for more information). While WLAN groups can be used to specify which WLAN services are served by which APs, AP groups are used for more specific fine-tuning of how the APs themselves behave.

NOTE: AP group configuration settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Tx Power Adjustment at **Auto** in the AP group configuration page, then go to the individual AP configuration page (*Configuration* > *Access Points* > *Edit [AP MAC address]*) and set the Tx Power setting to a lower setting.

Creating an AP Group

Follow these steps to create an AP group.

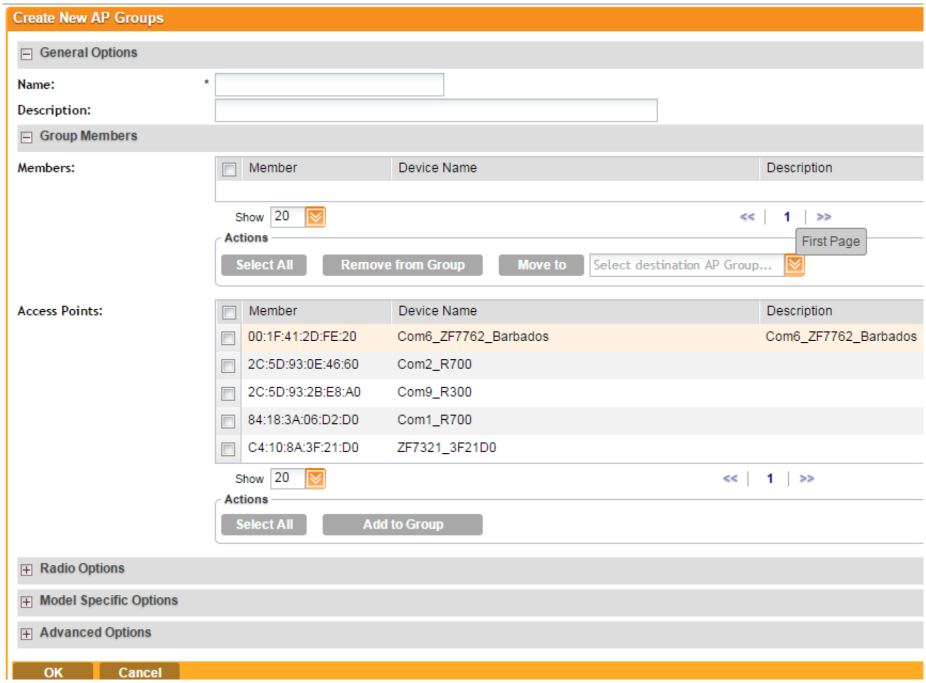
1. Go to *Configuration* > *AP Zones*.
2. On the *AP Zone List page*, click the AP zone name within which you want to create the AP group. The page refreshes, and the AP Zone submenu appears on the sidebar.
3. On the sidebar, click *AP Groups*.
4. Click **Create New**. The *Create New AP Groups* form appears.
5. In *General Settings*, configure the following:
   - *Name*: Type a name for this AP group.
   - *Description*: Type a description for this AP group.
6. In *Group Members*, configure the following:
   - *Members*: When you are creating a new AP group, this section will be empty. This will be populated after you select the access points that you want to belong to this AP group.
   - *Access Points*: This section shows all the access points that currently belong to the AP zone. Select the check boxes before the *Member* column (which shows the AP MAC addresses) of each AP that you want to add to the AP group, and then click **Add to Group**. The APs you selected appear under the *Members* section.
7. In *Radio Options*, select the **Override zone config** check box for the AP zone settings that you want to override, and then configure the following for both the 2.4GHz and 5GHz radios:
   - *Channelization*: Select Auto, 20MHz or 40MHz channel width for either the 2.4GHz or 5GHz radio.
   - *Channel*: Select Auto or manually assign a channel for the 2.4GHz or 5GHz radio.
   - *TX Power*: Set the transmit power on all 2.4GHz or 5GHz radios (default is Auto).
   - *WLAN Group*: Specify to which WLAN group this AP group belongs.
8. In *Model Specific Options*, configure LED, LLDP, and port settings of all APs of each specific model that are members of the AP group. See Modifying Model Specific Controls.
9. In *Advanced Options*, select the **Override zone config** check boxes for the settings that you want to override, and then configure them.

- *Location Based Service*: To disable the LBS service for this AP group, clear the **Enable LBS service** check box. To use a different LBS server for this AP group, select the **Enable LBS service** check box, and then select the LBS server that you want to use from the drop-down list.
- *Auto Channel Selection*: You can adjust the AP channel to 2.4 GHz or 5 GHz frequencies by selecting the appropriate check-box. Further, you can automatically adjust the AP to optimize performance by choosing one of the following:
  - Background Scanning
  - ChannelFly
- *Client Admission Control*: Set the load thresholds on the AP at which it will stop accepting new clients. See Configuring Client Admission Control.

10 Click **OK**.

You have completed creating an AP group.

Figure 24. The Create New AP Group form



Create New AP Groups

⊟ General Options

Name: *

Description:

⊟ Group Members

Members:

□	Member	Device Name	Description

Access Points:

□	Member	Device Name	Description
□	00:1F:41:2D:FE:20	Com6_ZF7762_Barbados	Com6_ZF7762_Barbados
□	2C:5D:93:0E:46:60	Com2_R700	
□	2C:5D:93:2B:E8:A0	Com9_R300	
□	84:18:3A:06:D2:D0	Com1_R700	
□	C4:10:8A:3F:21:D0	ZF7321_3F21D0	

⊞ Radio Options

⊞ Model Specific Options

⊞ Advanced Options

Modifying Model Specific Controls

The following settings can be applied to all APs of a particular model that are members of the AP group:

- *Internal Heater*: Enable internal heaters (specific AP models only).

NOTE: For the internal heater to be operational, ZoneFlex 7762 APs must be powered by the supplied PoE injector and its associated power adapter or a standard 802.3at PSE. For the PoE Out port to be operational, ZoneFlex 7762 APs must be powered by the supplied PoE injector and its associated power adapter.

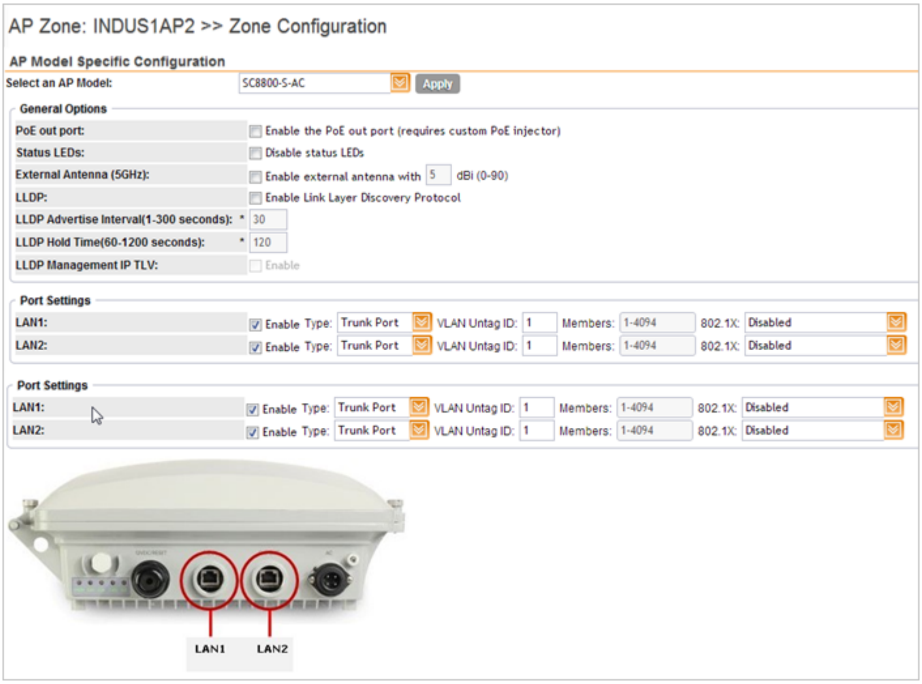
- *PoE Out Ports*: Enable PoE out ports (specific ZoneFlex AP models only).

NOTE: If the controller country code is set to United Kingdom, an additional “Enable 5.8 GHz Channels” option will be available for outdoor 11n/11ac APs. Enabling this option allows the use of restricted C-band channels. These channels are disabled by default and should only be enabled by customers with a valid license to operate on these restricted channels.

- *Status LEDs*: When managed by the controller, you can disable the external LEDs on certain ZoneFlex models, such as the 7300 series APs. This can be useful if your APs are installed in a public location and you do not want to draw attention to them.
- *External Antenna*: External antenna configuration is available for the 5 GHz radio on the ZoneFlex 7762, and for the 2.4 and 5 GHz radios on the 7782-E APs. Once enabled, enter a gain value in the range of 0 to 90dBi.
- *Radio Band*: (ZoneFlex 7441 and 7321 only) Select 2.4 GHz or 5 GHz radio band for the 7441/7321 APs.
- *LLDP*: To enable the AP model to advertise its identity and capabilities on the local network via LLDP, select the **Enable Link Layer Discovery Protocol** check box. For a list of attributes that APs advertise using LLDP, see Supported LLDP Attributes.
  - *Advertise Interval (1-300 seconds)*: Set the interval (in seconds) at which the AP model will send out LLDP information. The default value is 30 seconds.
  - *Hold Time (60-1200 seconds)*: Set the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.

  - *Management IP TLV*: To include the management IP address TLV in the LLDP information that the AP model sends out, select **Enable** check box.
- *Port Settings*: For information on how to configure the port settings, see Configuring the Port Settings of a Particular AP Model.

Figure 25. The AP Model-Specific Configuration section



AP Zone: INDUS1AP2 >> Zone Configuration

AP Model Specific Configuration

Select an AP Model: SC8800-S-AC Apply

General Options

PoE out port:	□ Enable the PoE out port (requires custom PoE injector)
Status LEDs:	□ Disable status LEDs
External Antenna (5GHz):	□ Enable external antenna with 5 dBi (0-90)
LLDP:	□ Enable Link Layer Discovery Protocol
LLDP Advertise Interval(1-300 seconds): *	30
LLDP Hold Time(60-1200 seconds): *	120
LLDP Management IP TLV:	□ Enable

Port Settings

LAN1:	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled
LAN2:	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled

Port Settings

LAN1:	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled
LAN2:	☑ Enable	Type: Trunk Port	VLAN Untag ID: 1	Members: 1-4094	802.1X: Disabled

Supported LLDP Attributes

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device (for example, a Ruckus Wireless AP) to advertise its identity and capabilities on the local network.

LLDP information is sent by devices from each of their interfaces at a fixed interval (default is 30 seconds), in the form of an Ethernet frame. Each LLDP Ethernet frame contains a sequence of type-length-value (TLV) structures starting with Chassis ID, Port ID and Time to Live (TTL) TLV. Table 2 lists the LLDP attributes supported by the controller.

Table 2. LLDP attributes supported by the controller

Attribute (TLV)	**Description**
Chassis ID	Indicates the MAC address of the AP's br0 interface
Port ID	Identifies the port from which the LLDP packet was sent
Time to Live	Same as *LLDP Hold Time*. Indicates the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.
System Name	Indicates the name assigned to the AP. The default name of Ruckus Wireless APs is RuckusAP.
System Description	Indicates the AP model plus software version
System Capabilities	Indicates the AP's capabilities (Bridge, WLAN AP, Router, Docsis), and which capabilities are enabled
Management Address	Indicates the management IP address of the AP
Port Description	Indicates the description of the port in alphanumeric format

Configuring the Port Settings of a Particular AP Model

Use *Port Settings* in the *AP Model-Specific Configuration* section to configure the Ethernet ports of a particular AP model.

Follow these steps to configure the port settings of a certain AP model.

1. All ports are enabled by default (the **Enable** check boxes are all selected). To disable a particular port entirely, clear the **Enable** check box next to the port name (LAN1, LAN2, etc.)

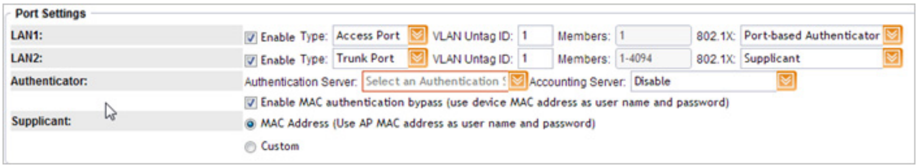
2. For any enabled ports, you can choose whether the port will be used as a Trunk Port, Access Port, or General Port.

   The following restrictions apply:

   - All APs must be configured with at least one Trunk Port.
   - For single port APs, the single LAN port must be a trunk port and is therefore not configurable.

- For ZoneFlex 7025/7055, the LAN5/Uplink port on the rear of the AP is defined as a Trunk Port and is not configurable. The four front-facing LAN ports are configurable.
- For all other APs, you can configure each port individually as either a Trunk Port, Access Port, or General Port. See Designating an Ethernet Port Type for more information.

Figure 26. The Port Settings section



Port Settings

LAN1: ☑ Enable Type: Access Port VLAN Untag ID: 1 Members: 1 802.1X: Port-based Authenticator

LAN2: ☑ Enable Type: Trunk Port VLAN Untag ID: 1 Members: 1-4094 802.1X: Supplicant

Authenticator: Authentication Server: Select an Authentication S Accounting Server: Disable

☑ Enable MAC authentication bypass (use device MAC address as user name and password)

Supplicant: ● MAC Address (Use AP MAC address as user name and password)

○ Custom

Designating an Ethernet Port Type

Ethernet ports can be configured as one of the following port types:

- Trunk Ports
- Access Ports
- General Ports

Trunk links are required to pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned.

For most ZoneFlex APs, you can set which ports you want to be your Access, Trunk and General Ports from the controller web interface, as long as at least one port on each AP is designated as a Trunk Port.

By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for ZoneFlex 7025, whose front ports are enabled as Access Ports by default). If configured as an Access Port, all untagged ingress traffic is the configured Untag VLAN, and all egress traffic is untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN.
- Redefine the native VLAN on this Trunk Port to match your network configuration.

Trunk Ports

Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk Port is a member of all the VLANs that exist on the AP/switch and carries traffic for all those VLANs between switches.

Access Ports

All Access Ports are set to Untag VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. To remove ports from the native VLAN and assign them to specific VLANs, select Access Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094).

The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

Table 3. Access Ports with VLANs configured

VLAN Settings	Incoming Traffic (from Client)	Outgoing Traffic (to Client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN (VLAN 1).	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

General Ports

General ports are user-specified ports that can have any combination of up to 20 VLAN IDs assigned. Enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

Configuring Client Admission Control

Client admission control allows APs to adaptively allow or deny the association of clients based on the potential throughput of the currently associated clients. This helps prevent APs from becoming overloaded with clients and improves user experience for wireless users.

As an administrator, you can help maintain a positive user experience for wireless users on the network by configuring the following client admission control settings:

- Minimum client count

- Maximum radio load
- Minimum client throughput

Client admission control is implemented on a per radio basis and is currently only supported on 802.11n APs.

Working with AAA Servers

This section provides information on add and manage AAA servers that the controller can use to authenticate users.

- Creating an AAA Server
- Testing an AAA Server
- Deleting an AAA Server

Creating an AAA Server

Follow these steps to create a RADIUS or RADIUS Accounting server (if you have one on the network) for the AP zone.

1. Click *Configuration* > *AP Zones* > *Zone Name ({AP Zone Name})* > *AAA*. For example, if you want to create an AAA server for an AP zone named `ap-zone-1`, click *Configuration* > *AP Zones* > *Zone Name (ap-zone-1)* > *AAA*.
2. Click **Create New**. The form for creating a new zone RADIUS server appears.
3. Configure *General Options*.
   - *Name*: Type a name for the AAA server that you are adding.
   - *Description*: Type a brief description for the AAA server.
   - *Type*: Select the type of AAA server that you have on the network. Options include:
     - RADIUS
     - RADIUS Accounting
     - Active Directory
     - LDAP
   - *Backup RADIUS*: Select the **Enable backup RADIUS server** check box if a secondary RADIUS server exists on the network. Configure the settings in Step 5.
4. In the *Primary Server* section, configure the settings of the primary RADIUS server.

- *IP Address*: Type the IP address of the AAA server.

NOTE: The format of the IP address that you need to enter here depends on the AP IP mode that you selected when you created the AP zone (see Creating an AP Zone). If you selected **IPv4 Only**, enter an IPv4 address. If you selected **IPv6 Only**, enter an IPv6 address.

- *Port*: Type the port number of the AAA server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

5 In the *Secondary Server* section, configure the settings of the secondary RADIUS server.

NOTE: The *Secondary Server* section is only visible if you selected the **Enable backup RADIUS server** check box earlier.

- *IP Address*: Type the IP address of the secondary AAA server.

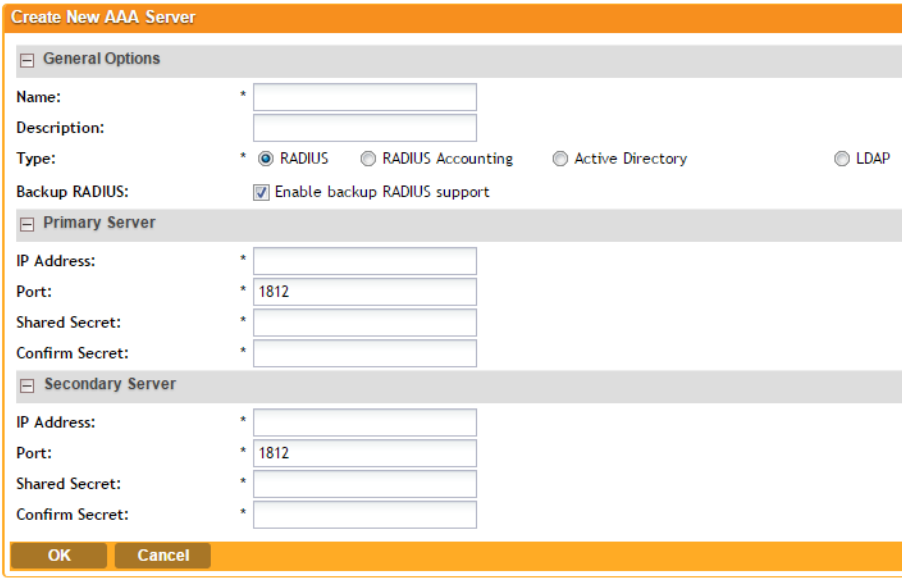
NOTE: The format of the IP address that you need to enter here depends on the AP IP mode that you selected when you created the AP zone (see Creating an AP Zone). If you selected **IPv4 Only**, enter an IPv4 address. If you selected **IPv6 Only**, enter an IPv6 address.

- *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

6 Click **Create New**.

You have completed creating an AAA server for the AP zone.

Figure 27. The Create New AAA Server form



Create New AAA Server

General Options

Name: *

Description:

Type: * ● RADIUS ○ RADIUS Accounting ○ Active Directory ○ LDAP

Backup RADIUS: ☑ Enable backup RADIUS support

Primary Server

IP Address: *

Port: * 1812

Shared Secret: *

Confirm Secret: *

Secondary Server

IP Address: *

Port: * 1812

Shared Secret: *

Confirm Secret: *

Testing an AAA Server

Follow these steps to test if an AAA server that you have created in the controller is functioning.

1 On the *AAA Servers* page, click **Test AAA**. The *Test AAA Servers* form appears.

2 In *Name*, select the name of the AAA server that you want to test.

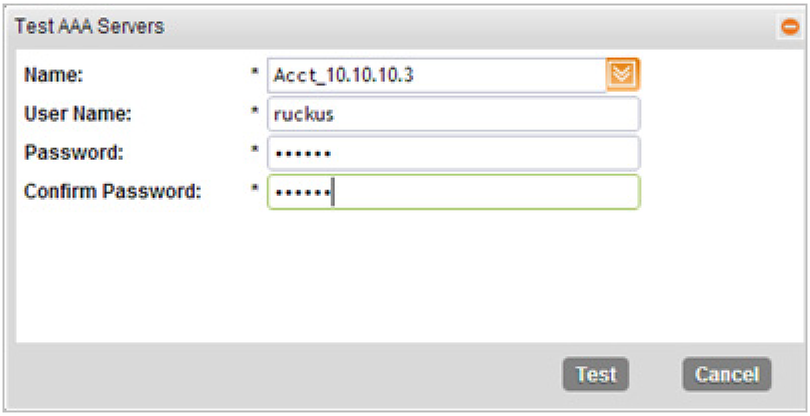
3 In *User Name*, type the user name for your AAA server account.

4 In *Password*, type your AAA server password.

5 In *Confirm Password*, retype the password above.

6 Click **Test**.

Figure 28. Testing an AAA server



Test AAA Servers

Name: * Acct_10.10.10.3

User Name: * ruckus

Password: * ••••••

Confirm Password: * ••••••

Deleting an AAA Server

You can delete a single or multiple AAA servers simultaneously.

- To delete a single AAA server, follow these steps:
  - a Go to the *AAA Servers* page for a specific AP zone.
  - b From the list of existing AAA servers, locate the service that you want to delete.
  - c Under the *Actions* column, click the icon 🗑 that is in the same row as the AAA server. A confirmation message appears.
  - d Click **Yes**. The page refreshes and the AAA server that you deleted disappears from the list.
- To delete multiple AAA servers simultaneously, follow these steps:

a. Go to the *AAA Services* page for a specific AP zone.

b. From the list of existing AAA servers, locate the services that you want to delete.

c. Select the check boxes before the servers that you want delete.

d. Click **Delete Selected**. A confirmation message appears.

Click **Yes**. The page refreshes and the AAA servers that you deleted disappears from the list.

Working with Hotspot (WISPr) Portals

NOTE: If you do not want to provide a hotspot portal to users, skip this section.

NOTE: This section describes the basic settings that you need to configure to include a hotspot service in the zone template. If you need more information about hotspots, including third party prerequisites, see Creating and Managing Hotspots.

Creating a Hotspot Portal

Follow these steps to configure the hotspot service of the zone template.

1. Click *Configuration* > *AP Zones*.
2. On the *AP Zone List* page, click the AP zone for which you want to create a hotspot service.
3. On the sidebar, click **Hotspot (WISPr)**. The *Hotspot (WISPr) Portal* page appears.
4. Click **Create New**. The form for creating a new hotspot portal appears.
5. In the *General Options* section, configure the following options:
   - *Name*: Type a name for the hotspot portal.
   - *Description*: Type a description for the hotspot portal.
6. In the *Redirection* section, configure the following options:
   - *Smart Client Support*: Select one of the following options:
     - **None**: Select this option to disable Smart Client support on the hotspot portal.
     - **Enable**: Selection this option to enable Smart Client support.

- **Only Smart Client Allowed**: Select this option to allow only Smart Clients to connect to the hotspot portal.

  For more information, see Configuring Smart Client Support.

- *Logon URL*: Type the URL of the subscriber portal (the page where hotspot users can log in to access the service). For more information, see Configuring the Logon URL.
- *Start Page*: Set where users will be redirected after they log in successfully:
  - **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
  - **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).

7. In the *User Session* section, configure the following options:
   - *Session Timeout*: Set a time limit (in minutes) after which users will be disconnected from the hotspot portal and will be required to log on again.
   - *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot portal without having to log on again.
8. In the *Location Informatio*n section, configure the following options:
   - *Location ID*: Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
     - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
     - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
     - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
     - network

     The following is an example of what the Location ID entry should look like: isocc=us,cc=1,ac=408,network=RuckusWireless
   - *Location Name*: Type the name of the location of the hotspot portal.
9. In *Walled Garden*, click **Create New** to add a walled garden. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account.

   In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:

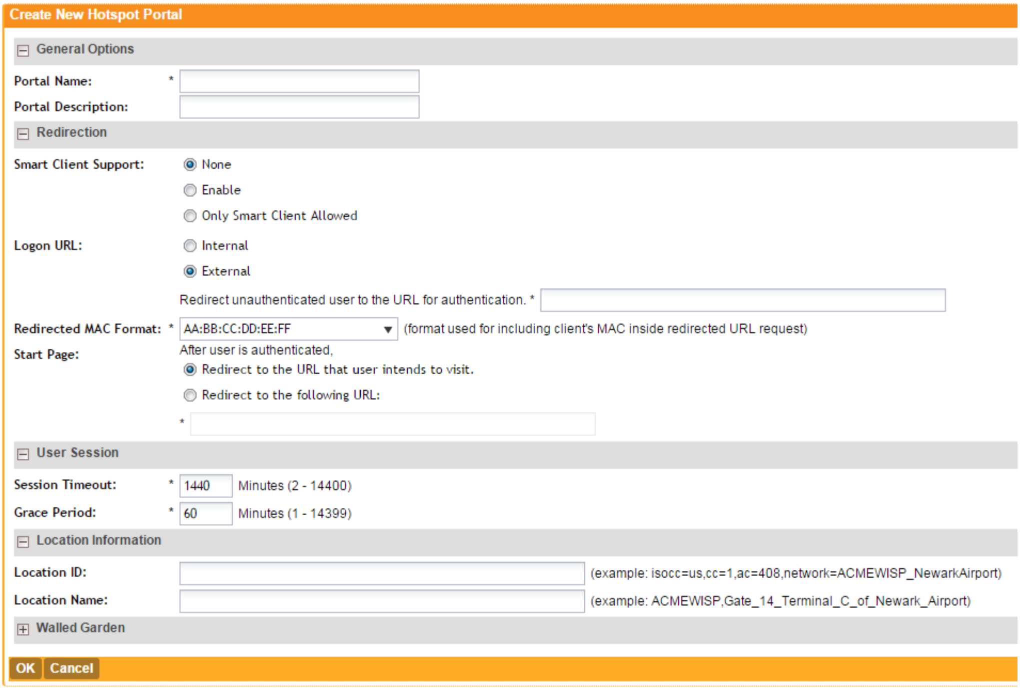
- IP address (for example, 10.11.12.13)
- IP range (for example, 10.11.12.13-10.11.12.15)
- Classless Inter-Domain Routing or CIDR (for example, 10.11.12.100/28)
- IP address and mask (for example, 10.11.12.13 255.255.255.0)
- Exact website address (for example, www.ruckuswireless.com)
- Website address with regular expression (for example, *.ruckuswireless.com, *.com, *)

After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to re-authenticate when they navigate through the page.

10 Click **Create New**.

You have completed configuring a hotspot portal of the AP zone. For additional steps that you need to perform to ensure that the hotspot portal works, see Creating and Managing Hotspots.

Figure 29. The Create New Hotspot Portal form



Create New Hotspot Portal

⊟ General Options

Portal Name: *

Portal Description:

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication. *

Redirected MAC Format: * AA:BB:CC:DD:EE:FF ▼ (format used for including client's MAC inside redirected URL request)

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit.
○ Redirect to the following URL:
*

⊟ User Session

Session Timeout: * 1440 Minutes (2 - 14400)

Grace Period: * 60 Minutes (1 - 14399)

⊟ Location Information

Location ID: (example: isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)

Location Name: (example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

⊞ Walled Garden

OK Cancel

Deleting a Hotspot Portal

You can delete a single or multiple hotspot portals simultaneously.

- To delete a single hotspot portal, follow these steps:
  - a Go to the *Hotspot (WISPr)* page for a specific AP zone.
  - b From the list of existing hotspot portals, locate the portal that you want to delete.
  - c Under the *Actions* column, click the icon 🗑 that is in the same row as the hotspot portal. A confirmation message appears.
  - d Click **Yes**. The page refreshes and the hotspot portal that you deleted disappears from the list.
- To delete multiple hotspot portals simultaneously, follow these steps:
  - a Go to the *Hotspot (WISPr)* page for a specific AP zone.
  - b From the list of existing hotspot portals, locate the hotspots that you want to delete.

c Select the check boxes before the hotspots that you want delete.

d Click **Delete Selected**. A confirmation message appears.

e Click **Yes**. The page refreshes and the hotspot portals that you deleted disappear from the list.

Working with Guest Access Portals

Using the controller's guest access features, you can provide visitors to your organization limited access to a guest WLAN with configurable guest policies, or given the option to self-activate their devices to an internal WLAN using Zero-IT activation via the bring your own device (BYOD) onboarding portal (or both).

The following sections describe how to configure guest WLANs and access policies that control guest use of your network.

- Creating a Guest Access Portal
- Viewing Guest Access Portals
- Deleting Guest Access Portals

Creating a Guest Access Portal

Each guest WLAN must be associated with a guest access portal, which defines the behavior of the guest WLAN interface. Follow these steps to create a guest access portal.

1 Click *Configuration* > *AP Zones*.

2 On the *AP Zone List* page, click the AP zone for which you want to create a guest access portal. The *Guest Access Portal* page appears.

3 Click **Create New**. The *Create New Guest Access Portal* form appears.

4 In *General Options*, configure the following:

- *Portal Name*: Type a name for the guest access portal that you are creating.
- *Portal Description*: Type a short description of the guest access portal.
- *Language*: Select the display language to use for the buttons on the guest access logon page.

5 In *Redirection*, select where to redirect the user after successfully completing authentication.

- **Redirect to the URL that the user intends to visit**: Allows the guest user to continue to their destination without redirection.

- **Redirect to the following URL**: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.

6 In *Guest Access*, configure the following options:

- *Guest Pass SMS Gateway*: You can deliver the guest pass to the user using Short Message Service (SMS). But first you need to configure an SMS server (see Configuring an SMS Server). If you previously configured an SMS server, you can select it here or you can click **Disabled**.
- *Terms And Conditions*: To require users to read and accept your terms and conditions prior to use of the guest hotspot, select the **Show Terms And Conditions** check box. The box below, which contains the default *Terms of Use* text, becomes editable. Edit the text or leave it unchanged to use the default text.
- *Web Portal Logo*: By default, the guest hotspot logon page displays the Ruckus Wireless logo. To use your own logo, click the **Upload** button, select your logo (recommended size is 138 x 40 pixels, maximum file size is 20KB), and then click **Upload**.
- *Web Portal Title*: Type your own guest hotspot welcome text or accept the default welcome text (“Welcome to the Guest Access login page”).

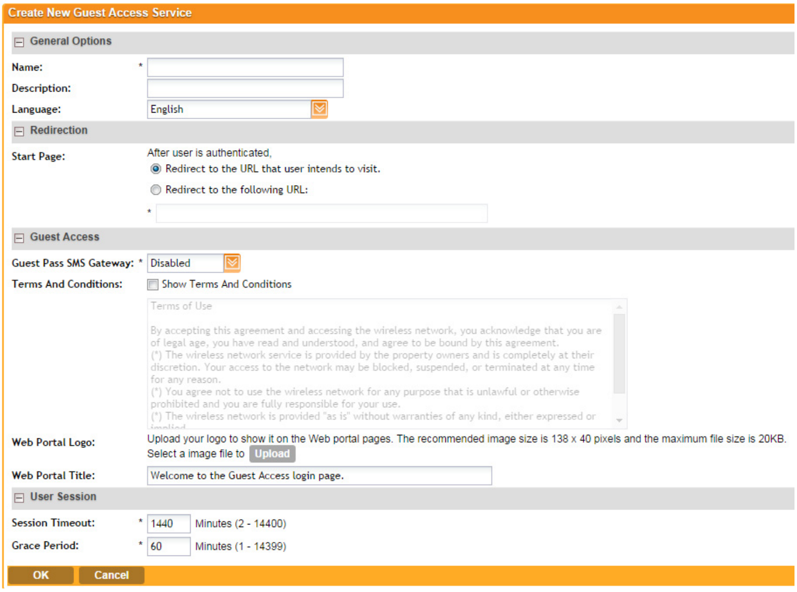
7 In *User Session*, configure the following:

- *Session Timeout*: Specify a time limit after which users will be disconnected and required to log on again.
- *Grace Period*: Set the time period during which clients will not need to re-authenticate after getting disconnected from the hotspot. Enter a number (in minutes) between 1 and 14399.

8 Click **OK**.

You have completed creating a guest access portal.

Figure 30. Creating a guest access portal



Create New Guest Access Service

⊟ **General Options**

Name: *

Description:

Language: English

⊟ **Redirection**

Start Page: After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL: *

⊟ **Guest Access**

Guest Pass SMS Gateway: * Disabled

Terms And Conditions: □ Show Terms And Conditions

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
(*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.
(*) The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

Web Portal Logo: Upload your logo to show it on the Web portal pages. The recommended image size is 138 x 40 pixels and the maximum file size is 20KB.
Select a image file to Upload

Web Portal Title: Welcome to the Guest Access login page.

⊟ **User Session**

Session Timeout: * 1440 Minutes (2 - 14400)

Grace Period: * 60 Minutes (1 - 14399)

Viewing Guest Access Portals

Follow these steps to view a list of existing guest access portals.

1 Click *Configuration* > *AP Zones*.

2 On the *AP Zone List* page, click the AP zone for which you are created the guest access portals.

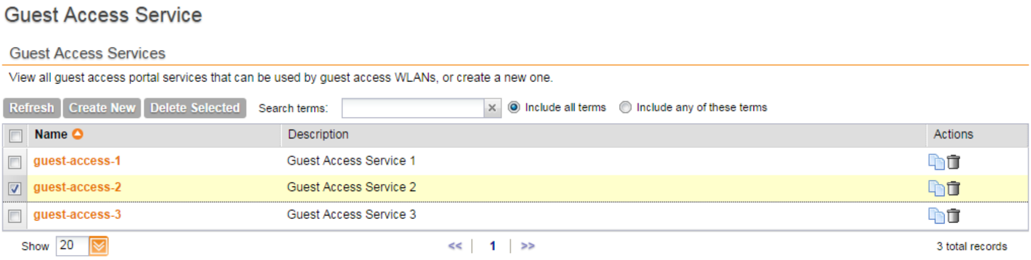
3 On the sidebar, click **Guest Access**. The *Guest Access Portal* page appears and displays all existing guest access portals and their basic settings are shown, including the following:

- Name
- Description
- Actions (that you can perform)

4 To view or update the settings of a guest access portal, click the guest access portal name.

You have completed viewing the existing guest access portals.

Figure 31. Viewing guest access portals



Guest Access Service

Guest Access Services

View all guest access portal services that can be used by guest access WLANs, or create a new one.

□	Name	Description	Actions
□	guest-access-1	Guest Access Service 1	
☑	guest-access-2	Guest Access Service 2	
□	guest-access-3	Guest Access Service 3	

Show 20   << | 1 | >>   3 total records

Deleting Guest Access Portals

Follow these steps to delete guest access portals.

1 On the *AP Zone List* page, click the AP zone for which you created the guest access portal.

2 On the sidebar, click **Guest Access**. The *Guest Access Portal* page appears.

3 Locate the service or services that you want to delete.

4 Select the check boxes (first column) for the services that you want to delete.

5 Click **Delete Selected**.

The services that you selected disappear from the list. You have completed deleting guest access portals.

NOTE: If you are deleting a single guest access portal, you can also click the 🗑 icon (under the *Actions* column) that is in the same row as the service that you want to delete.

Working with Web Authentication Portals

A web authentication portal (also known as a “captive portal”) redirects users to a logon web page the first time they connect to a WLAN, and requires them to log on before granting access to use the WLAN.

Creating and configuring a web authentication portal requires the following steps:

- Adding an AAA Server for the Web Authentication Portal
- Creating a Web Authentication Portal
- Creating a WLAN for the Web Authentication Portal

Adding an AAA Server for the Web Authentication Portal

Add an AAA server that the web authentication portal can use to authenticate users. For instructions on how to add an AAA server to the controller, see Creating an AAA Server.

Creating a Web Authentication Portal

Follow these steps to create a web authentication portal.

1 Go to *Configuration* > *AP Zones*.

2 Click the AP zone for which you want to create a web authentication portal.

1 On the *AP Zones* submenu, click **Web Authentication**. The *Web Authentication Portal* page appears.

2 Click **Create New**. The *Create New Web Authentication Portal* form appears.

3 In *General Options*, configure the following options:

   - *Portal Name*: Type a name for the web authentication portal that you are creating.
   - *Portal Description*: Type a brief description of the portal.
   - *Language*: Select the display language that you want to use on the web authentication portal.

4 In *Redirection*, select where to redirect the user after successfully completing authentication.

   - **Redirect to the URL that the user intends to visit**: Allows the guest user to continue to their destination without redirection.

- **Redirect to the following URL**: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.

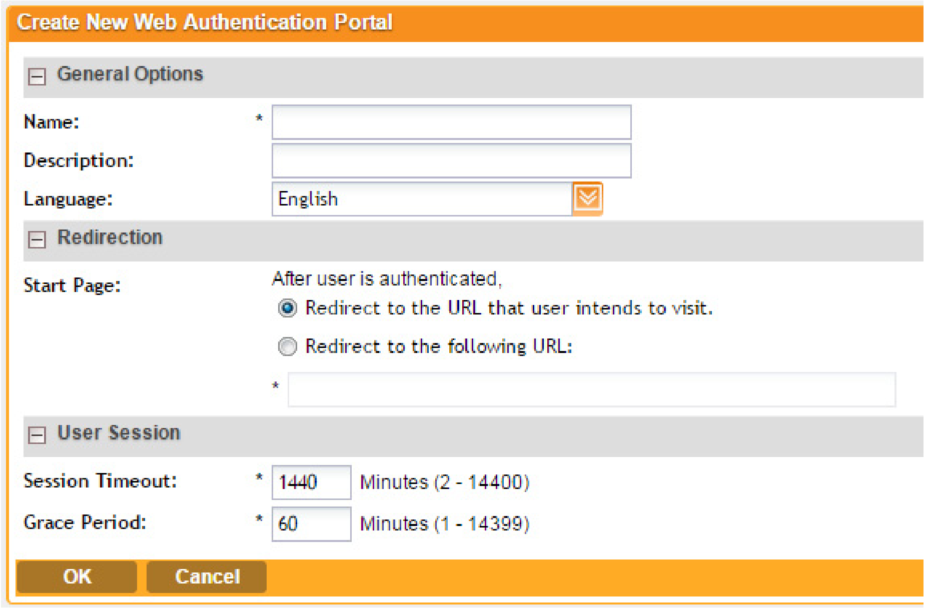
5 In *User Session*, configure the following:

- *Session Timeout*: Set the time (in minutes) after which inactive users will be disconnected and required to log in again.
- *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log on again.

6 Click **OK**.

You have completed creating a web authentication portal.

Figure 32. The Create New Web Authentication Portal page



Create New Web Authentication Portal

⊟ General Options

Name: *

Description:

Language: English

⊟ Redirection

Start Page: After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL:

*

⊟ User Session

Session Timeout: * 1440 Minutes (2 - 14400)

Grace Period: * 60 Minutes (1 - 14399)

Creating a WLAN for the Web Authentication Portal

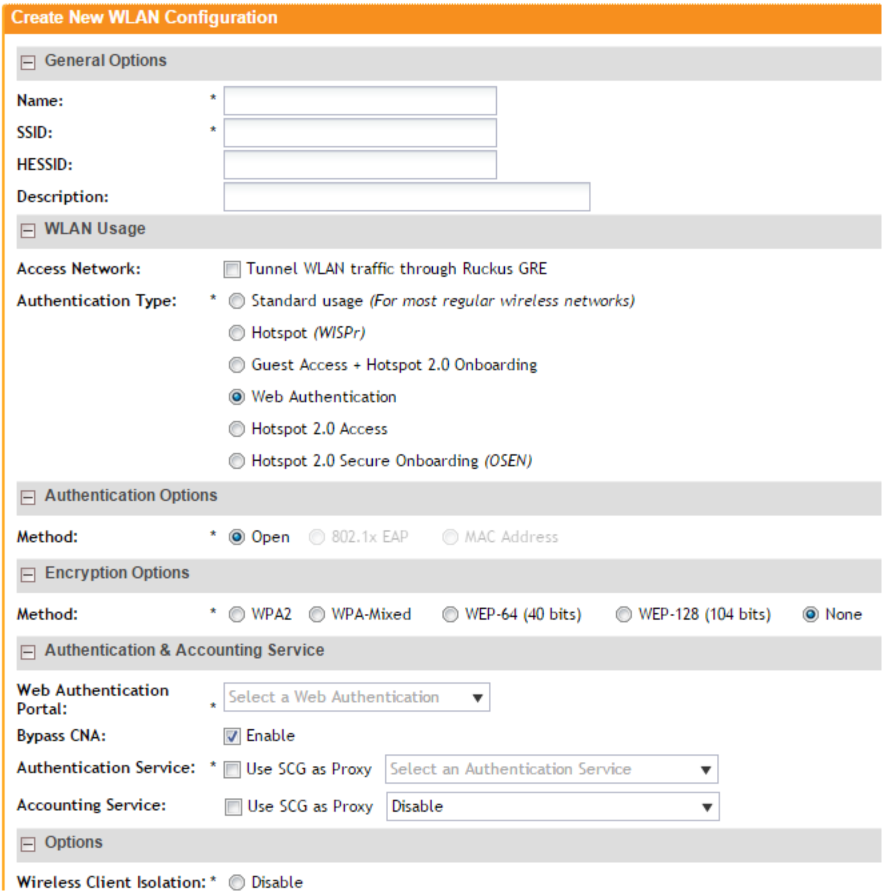
Follow these steps to create a WLAN that you can use for a web authentication portal.

1. Go to *Configuration* > *AP Zones* > *WLANs*.
2. In the *WLAN Configuration* section, click **Create New**.
3. In *General Options*, configure the following:
   - Name
   - SSID
   - Description
4. In *Authentication Type*, click **Web Authentication**.
5. In *Authentication & Accounting Server*, select the RADIUS and/or RADIUS Accounting server that you created earlier in Adding an AAA Server for the Web Authentication Portal.
6. In *Web Authentication*, select the web authentication portal that you created earlier in Creating a Web Authentication Portal. This service contains, among others, the start page where users will be redirected when they associate with this WLAN.
7. Configure the remaining WLAN options as desired. For information on these options, see Creating a WLAN.
8. Click **OK**.

You have completed creating a WLAN for web authentication.

After you create a WLAN that will be used for web authentication, you must then provide all users with the URL to your logon page. After they discover the WLAN on their wireless device or laptop, they open their browser, connect to the logon page and enter the required login information.

Figure 33. Creating a WLAN to provide web authentication



Create New WLAN Configuration

⊟ General Options

Name:	*	
SSID:	*	
HESSID:		
Description:		

⊟ WLAN Usage

Access Network:		□ Tunnel WLAN traffic through Ruckus GRE
Authentication Type:	*	○ Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access + Hotspot 2.0 Onboarding ● Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Secure Onboarding *(OSEN)*

⊟ Authentication Options

Method:	*	● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method:	*	○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

⊟ Authentication & Accounting Service

Web Authentication Portal:	*	Select a Web Authentication ▼
Bypass CNA:		☑ Enable
Authentication Service:	*	□ Use SCG as Proxy Select an Authentication Service ▼
Accounting Service:		□ Use SCG as Proxy Disable ▼

⊟ Options

Wireless Client Isolation:	*	○ Disable

Working with Hotspot 2.0 Services

Hotspot 2.0 is a newer Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol. Hotspot 2.0 aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association. This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.

The Hotspot 2.0 implementation on the controller complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specifications.

See the *Hotspot 2.0 Reference Guide* for this release for information on configuring Hotspot 2.0 services, including:

- Working with Hotspot 2.0 operator profiles
- Working with Hotspot 2.0 identity providers
- Creating a Hotspot 2.0 online signup portal

Working with WLANs and WLAN Groups

- Creating a WLAN
- Working with WLAN Groups

Creating a WLAN

Follow these steps to create a WLAN for an AP zone.

1. Click *Configuration* > *AP Zones*.
2. On the *AP Zone List* page, click the AP zone for which you want to create a WLAN service.
3. On the sidebar, click **WLAN**. The *WLAN Configuration* page appears.
4. In the *WLAN Configuration* section, click **Create New**. The form for creating a new WLAN service appears.
5. In the *General Options* section, configure the following options.
   - *Name/SSID*: Type a short name (two to 32 alphanumeric characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the SSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same controller) while still being able to manage the different WLANs independently.
   - *HESSID*: Type the homogenous extended service set identifier (HESSID). The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value must be identical to one of the BSSIDs in the homogeneous ESS.
   - *Description*: Type a brief description of the qualifications/purpose for this WLAN (for example, Engineering or Voice).
6. In *WLAN Usage*, configure the following:
   - In *Access Network*, select the **Tunnel WLAN traffic through Ruckus GRE** check box if you want to tunnel the traffic from this WLAN back to the controller. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the controller.

- In *Core Network Type* (only visible if you selected the **Tunnel WLAN traffic through Ruckus GRE** check box), select one of the following core network types:
    - Bridge
    - L3oGRE
    - L2oGRE
    - TTG+PDG
    - PMIPv6
    - Mixed Tunnel Mode
- In *Authentication Type*, click one of the following options:
    - **Standard usage (For most regular wireless networks)**: This is a regular WLAN suitable for most wireless networks.
    - **Hotspot (WISPr)**: Click this option if you want to use a hotspot portal that you previously created. For instructions on how to create a hotspot service, see Working with Hotspot (WISPr) Portals.
    - **Guest Access + Hotspot 2.0 Onboarding**: Click this option if you want guest users to use this WLAN and offer Hotspot 2.0 service to guest users. After you complete creating this WLAN for guest access, you can start generating guest passes (see Working with Guest Users).

NOTE: For more information about Hotspot 2.0 online signup, see the *Hotspot 2.0 Reference Guide* for this release.

-
    - **Web Authentication**: Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect. See Working with Web Authentication Portals.
    - **Hotspot 2.0**: Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See Working with Hotspot 2.0 Services.
    - **Hotspot 2.0 Secure Onboarding (OSEN)**: Click this option if you want to use this WLAN for Hotspot 2.0 OSEN. See the *Hotspot 2.0 Reference Guide* for this release for more information.

7. In *Authentication Options*, click the authentication method by which users will be authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.

- **Open (Default)**: No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
- **802.1x EAP**: A very secure authentication/encryption method that requires a back-end authentication server, such as a RADIUS server. Your choice mostly depends on the types of authentication the client devices support and your local network authentication environment.
- **MAC Address**: Authenticate clients by MAC address. MAC address authentication requires a RADIUS server and uses the client MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
    - *MAC Authentication*: The default password is the device's MAC address. If you want to set your own authentication password, select the **Use user defined text as authentication password (default is device MAC address)** check box, and then type the password in the box provided.
    - *MAC Address Format*: Select the MAC address format that you want APs to use when sending authentication requests to the RADIUS server. Select one of the following supported MAC address formats:
        - `aabbccddeeff` (Default format. For example, 0010a42319c0)
        - `AA-BB-CC-DD-EE-FF`
        - `AA:BB:CC:DD:EE:FF`
        - `AABBCCDDEEFF`
        - `aa-bb-cc-dd-ee-ff`
        - `aa:bb:cc:dd:ee:ff`

8 In *Encryption Options*, select an encryption method to use. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.

- **WPA2**: Enhanced WPA encryption using stronger TKIP or AES encryption algorithm.
- **WPA-Mixed**: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **WEP-64 (40 bits)**: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.

- **WEP-128 (104 bits)**: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- **None**: No encryption; traffic is sent in clear text.

CAUTION! If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

9 In *Hotspot Portal*, configure the following options.

NOTE: This section only appears if you clicked **Hotspot (WISPr)** in *WLAN Usage > Authentication Type*.

- *Hotspot (WISPr) Portal*: Select the hotspot that you want this WLAN to use. This option appears only when **Hotspot (WISPr)** is selected as the WLAN usage type. This hotspot portal may be the hotspot that you created in Creating a Hotspot Portal.
- *Bypass CNA*: Select the **Enable** check box if you want to bypass the Apple CNA feature on iOS and OS X devices that connect to this WLAN. See Bypassing Apple CNA for more information.
- *Authentication Service*: Select the authentication server that you want to use for this WLAN. Options include **Local DB**, **Always Accept**, and any AAA servers that you previously added (see Working with AAA Servers). Additionally, if you want the controller to proxy authentication messages to the AAA server, select the **Use the Controller as Proxy** check box.
- *Accounting Service*: Select the RADIUS Accounting server that you want to use for this WLAN. You must have added a RADIUS Accounting server previously (see Working with AAA Servers). Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.

10 In *Guest Access Portal*, configure the following options:

NOTE: This section only appears if you clicked **Guest Access + Hotspot 2.0 Onboarding** in *WLAN Usage > Authentication Type*.

- *Guest Access Portal*: Select the guest access portal that you created earlier for this onboarding WLAN.

- *Bypass CNA*: Select the **Enable** check box if you want to bypass the Apple CNA feature on iOS and OS X devices that connect to this WLAN. See Bypassing Apple CNA for more information.
- *Guest Authentication*: Select **Guest** to require users to enter their guest credentials, or select **Always Accept** to allow users without guest credentials to authentication.
- *Guest Accounting*: Select the RADIUS Accounting server that you want to use for this WLAN. You must have added a RADIUS Accounting server previously (see Working with AAA Servers). Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.

11 In the *Online Signup/Onboarding Service* section, configure the following options:

NOTE: This section only appears if you clicked **Guest Access + Hotspot 2.0 Onboarding** in *WLAN Usage > Authentication Type*.

- *Hotspot 2.0 Signup*: Select the **Hotspot 2.0 devices** check box to enable support for Hotspot 2.0 devices. See the *Hotspot 2.0 Reference Guide* for this release for more information.
- *Zero-IT Onboarding*: Select the **Non-Hotspot 2.0 devices (i.e., legacy devices) and Hotspot Rel 1 devices** check box. See Working with Remote Users for more information.
- *Onboarding Portal*: Select the portal signup profile that you want this guest WLAN to use.
- *Authentication Services*: Select the authentication server that you previously added to the controller.

12 In the Authentication & Accounting Service section, configure the following options:

- *Web Authentication Portal*: Select the web authentication portal that you created previously. See Working with Web Authentication Portals for more information.
- *Bypass CNA*: Select the **Enable** check box if you want to bypass the Apple CNA feature on iOS and OS X devices that connect to this WLAN. See Bypassing Apple CNA for more information.

- *Authentication Service*: Select the authentication server that you want to use for this WLAN. Options include **Local DB**, **Always Accept**, and any AAA servers that you previously added (see Working with AAA Servers). Additionally, if you want the controller to proxy authentication messages to the AAA server, select the **Use the Controller as Proxy** check box.
- *Accounting Service*: Select the RADIUS Accounting server that you want to use for this WLAN. You must have added a RADIUS Accounting server previously (see Working with AAA Servers). Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.

13 In *Options*, configure the following options:

- *Wireless Client Isolation*: Wireless client isolation enables subnet restrictions for connected clients. Click **Enable** if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is **Disable**.
- *Priority*: Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to “Low.” By default, all WLANs are set to high priority.

14 In *RADIUS Options*, click + (plus sign) to display the options, and then configure the following:

- NAS ID: Select how to the RADIUS server will identify the AP:
  - WLAN BSSID
  - AP MAC
  - User-defined
- *NAS Request Timeout*: Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *NAS Max Number of Retries*: Type the number of failed connection attempts after which the controller will fail over to the backup RADIUS server.
- *NAS Reconnect Primary*: If the controller fails over to the backup RADIUS server, this is the interval (in minutes) at which the controller will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID*: Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

15 In *Advanced Options*, configure the following options:

- *User Traffic Profile:* If you want this WLAN to use a user traffic profile that you previously created, select it from the drop-down menu. Otherwise, select **System Default**. For more information, see Working with User Traffic Profiles.
- *L2 Access Control*: If you want this WLAN to use an L2 access control policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with L2 Access Control Policies.
- *Device Policy*: If you want this WLAN to use a device policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with Device Policies.
- *Access VLAN*: By default, all wireless clients associated with APs that the controller is managing are segmented into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2-4094) in the box.
- *Hide SSID*: Select this check box if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.
- *Client Load Balancing*: To disable client load balancing on this WLAN, select the **Do not perform client load balancing for this WLAN service check** box. For more information, see Client Load Balancing.
- *Proxy ARP*: Select this check box to enable proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP request and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified.
- *Max Clients*: This option limits the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage.
- *802.11d*: Select this check box to enable this standard on this WLAN. 802.11d provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. Click this option if you are operating in one of these additional regulatory domains.

- *Force DHCP*: Enable this option to force clients to obtain a valid IP address from DHCP within the specified number of seconds. This prevents clients configured with a static IP address from connecting to the WLAN. Additionally, if a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
- *DHCP Option 82*: Select the **Enable DHCP Option 82** check box to enable this feature. When this feature is enabled and an AP receives a DHCP request from a wireless client, the AP will encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.
- *Client TX/RX Statistics*: Select the **Ignore statistics from unauthorized clients** check box if you do not want the controller to monitor traffic statistics for unauthorized clients.
- *Inactivity Timeout*: Select this check box and enter a value in seconds (60 to 600) after which idle clients will be disconnected.
- *Client Fingerprinting:* By selecting this check box, the controller will attempt to identify client devices by their operating system, device type and host name, if available. This makes identifying client devices easier on the Dashboard, Monitor and Client Details pages.
- *OFDM Only*: Select the check box to force clients associated with this WLAN to use only Orthogonal Frequency Division Multiplexing (OFDM) to transmit data. OFDM-only allows the client to increase management frame transmission speed from CCK rates to OFDM rates. This feature is implemented per WLAN and only affects the 2.4GHz radio.
- *BSS Min Rate*: Select this check box to set the bss rates of management frames from default rates (CCK rates for 2.4G or OFDM rate – 6Mbps for 5G] to the desired rates. By default, BSS Min Rate is disabled.

NOTE OFDM-only takes higher priority than BSS-minrate. However, OFDM-only relies on BSS-minrate to adjust its rate for management frames.

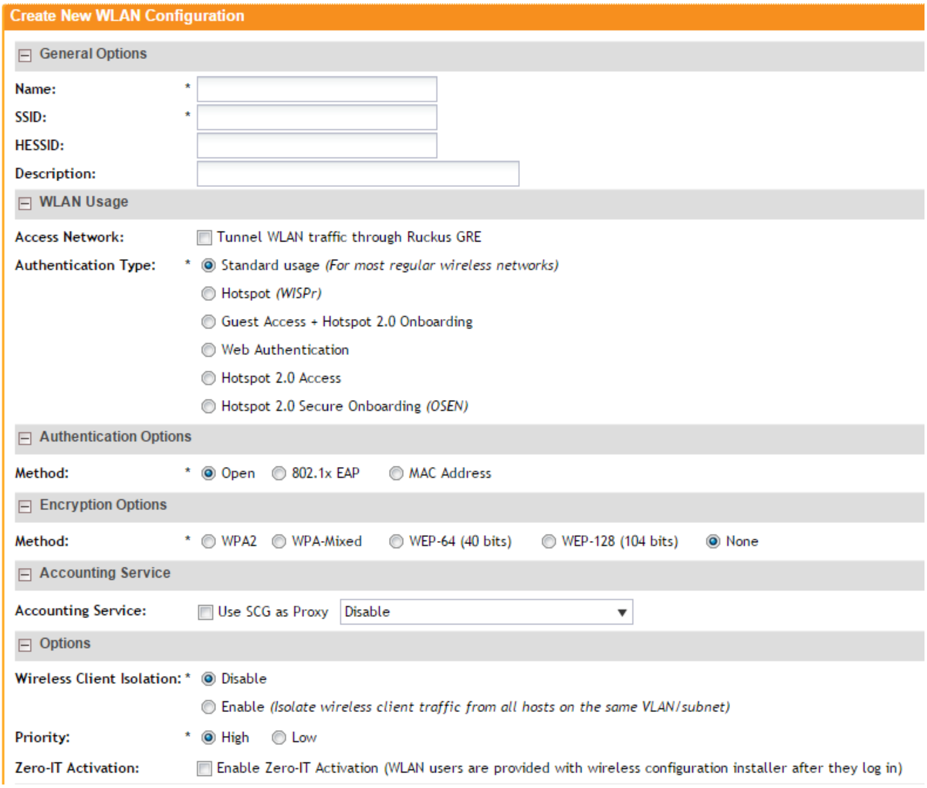
- *Mgmt Tx Rate*: To set the maximum transmit rate for management frame, select a value (in Mbps) from the drop-down list.

- *Service Schedule*: Use the Service Schedule tool to control which hours of the day, or days of the week to enable/disable WLAN service. Options include:
  - **Always On**: Click this enable this WLAN at all times.
  - **Always Off**: Click this option to disable the WLAN service at all times.
  - **Specific**: Click this to set specific hours during which this WLAN will be enabled. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Click on a day of the week to enable/disable this WLAN for the entire day. Colored cells indicate WLAN enabled. Click and drag to select specific times of day. You can also disable a WLAN temporarily for testing purposes, for example.
- *Band Balancing*: To disable band balancing on this WLAN, select the **Do not perform band balancing for this WLAN service** check box. For more information, see Band Balancing.

16 Click **OK** at the bottom of the form.

You have completed creating and configuring a WLAN service of the AP zone.

Figure 34. Top half of the Create New WLAN Configuration form



Create New WLAN Configuration

⊟ General Options

Name:	*	
SSID:	*	
HESSID:		
Description:		

⊟ WLAN Usage

Access Network:		□ Tunnel WLAN traffic through Ruckus GRE
Authentication Type:	*	● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access + Hotspot 2.0 Onboarding ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Secure Onboarding *(OSEN)*

⊟ Authentication Options

Method:	*	● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method:	*	○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

⊟ Accounting Service

Accounting Service:		□ Use SCG as Proxy Disable ▼

⊟ Options

Wireless Client Isolation:	*	● Disable ○ Enable *(Isolate wireless client traffic from all hosts on the same VLAN/subnet)*
Priority:	*	● High ○ Low
Zero-IT Activation:		□ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in)

Channel Mode

Some countries restrict certain 5GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15GHz to 5.25GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7761-CM and 7731) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment (such as a warehouse), the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or the controller web interface.

Client Load Balancing

Enabling load balancing can improve WLAN performance by helping to spread the wireless client load between nearby access points, so that one AP does not get overloaded while another sits idle. The load balancing feature can be controlled from within the controller web interface to balance the number of clients per radio on adjacent APs.

"Adjacent APs" are determined by the controller at startup by measuring the RSSI during channel scans. After startup, the controller uses subsequent scans to update the list of adjacent radios periodically and when a new AP sends its first scan report. When an AP leaves, the controller immediately updates the list of adjacent radios and refreshes the client limits at each affected AP.

Once the controller is aware of which APs are adjacent to each other, it begins managing the client load by sending the configured client limits to the APs. These limits are "soft values" that can be exceeded in several scenarios, including:

1. When a client's signal is so weak that it may not be able to support a link with another AP
2. When a client's signal is so strong that it really belongs on this AP.

The APs maintain these configured client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.

Key Points About Client Load Balancing

Before you enable load balancing, keep the following considerations in mind:

- The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- The process does not require any time-critical interaction between APs and the controller.
- Provides control of adjacent AP distance with safeguards against abandoning clients.
- Can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.
- Background scanning must be enabled on the WLAN for load balancing to work.

Band Balancing

Band balancing balances the client load on radios by distributing clients between the 2.4GHz and 5GHz radios. This feature is enabled by default and set to a target of 25% of clients connecting to the 2.4GHz band. To balance the load on a radio, the AP encourages dual-band clients to connect to the 5GHz band when the configured percentage threshold is reached.

Bypassing Apple CNA

Some Apple iOS and OS X clients include a feature called Captive Network Assistant (CNA), which allows clients to connect to an open captive portal WLAN without displaying the logon page.

When a client connects to a wireless network, the CNA feature launches a pre-browser login utility and it sends a request to a success page on the Apple website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

The controller provides an option to work around the Apple CNA feature if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) logon must be performed by opening a browser to any unauthenticated page (HTTP) to get redirected to the logon page.

Working with WLAN Groups

A WLAN group is a way of specifying which APs or AP groups provide which WLAN services. If your wireless network covers a large physical environment (for example, multi-floor or multi-building office) and you want to provide different WLAN services to different areas of your environment, you can use WLAN groups to do this.

For example, if your wireless network covers three building floors (1st floor to 3rd floor) and you need to provide wireless access to visitors on the 1st floor, you can do the following:

1. Create a WLAN service (for example, “Guest Only Service”) that provides guest-level access only.
2. Create a WLAN group (for example, “Guest Only Group”), and then assign “Guest Only Service” (WLAN service) to “Guest Only Group” (WLAN group).

3 Assign APs on the 1st Floor (where visitors need wireless access) to your "Guest Only Group".

Any wireless client that associates with APs assigned to the "Guest Only Group" will get the guest-level access privileges defined in your "Guest Only Service." APs on the 2nd and 3rd floors can remain assigned to the default WLAN Group and provide normal-level access.

Notes About WLAN Groups

Before you start using WLAN groups to provision WLAN settings to APs or AP groups, take note of the following important notes:

- Creating WLAN groups is optional. If you do not need to provide different WLAN services to different areas in your environment, you do not need to create a WLAN group.
- A default WLAN group called "default" exists. The first 27 WLANs that you create are automatically assigned to this default WLAN group.
- A WLAN group can include a maximum of 27 member WLANs. For dual radio APs, each radio can be assigned to only one WLAN group (single radio APs can be assigned to only one WLAN group).

Creating a WLAN Group

Follow these steps to create a WLAN group.

1. Go to *Configuration > AP Zones*.
2. Click the AP zone for which you want to create a device access policy.
3. In the *AP Zones* submenu, click **WLAN**. The *WLAN Services & Groups* page appears.
4. Look for the *WLAN Group Configuration* section.
5. Click **Create New**.
6. In *Group Name*, type a descriptive name that you want to assign to this WLAN group. For example, if this WLAN will contain WLANs that are designated for guest users, you can name this as Guest WLAN Group.
7. In *Description* (optional), type some notes or comments about this group.
8. Under *WLAN List*, select the check boxes for the WLANs that you want to be part of this WLAN group. The VLAN Override and NAS-ID columns for the selected WLANs become active.

9 In the VLAN override settings, choose whether to override the VLAN configured for each member WLAN. Available options include:

- No Change: Click this option if you want the WLAN to keep the same VLAN tag (default: 1).
- Tag: Click this option to override the VLAN configured for the WLAN service.

10 In the NAS-ID settings, choose whether to override the NAS-ID configured for each member WLAN. Available options include:

- No Change: Click this option if you want the WLAN to keep the same NAS-ID tag.
- User-defined: Click this option to override the NAS-ID that has been assigned to this WLAN service.

11 Click Create New. The Create New form disappears and the WLAN group that you created appears in the table under WLAN Groups.

You may now assign this WLAN group to an AP or AP group.

Viewing Existing WLAN Groups

Follow these steps to view a list of existing WLAN groups.

1 Go to *Configuration > AP Zones*.

2 Click the AP zone for which you want to create a device access policy.

3 In the *AP Zones* submenu, click **WLAN**. The *WLAN Services & Groups* page appears.

4 Look for the *WLAN Group Configuration* section. All existing WLAN groups and their basic settings are shown, including the:

- WLAN group name
- Description
- Actions (that you can perform)

To view WLANs that belong to a particular WLAN group, click the WLAN group name.

You have completed viewing existing WLAN groups.

Deleting WLAN Groups

Follow these steps to delete WLAN groups.

1 Go to *Configuration > AP Zones*.

2 Click the AP zone for which you want to create a device access policy.

3. In the *AP Zones* submenu, click **WLAN**. The *WLAN Services & Groups* page appears.
4. Scroll down to the *WLAN Group Configuration* section.
5. Locate the WLAN group or groups that you want to delete.
6. Select the check boxes (first column) for the WLAN groups that you want to delete.
7. Click **Delete Selected**.

The WLAN groups that you selected disappear from the list. You have completed deleting WLAN groups.

NOTE: If you are deleting a single WLAN group, you can also click the 🗑 icon (under the *Actions* column) that is in the same row as the WLAN group that you want to delete.

Working with WLAN Schedules

A WLAN schedule profile specifies the hours of the day or week during which a WLAN service will be enabled or disabled. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Create a WLAN schedule profile, and then when you configure a WLAN, select the schedule profile to enable or disable the WLAN service during those hours/days.

NOTE: This feature will not work properly if the system does not have the correct time. To ensure that the system always maintains the correct time, configure an NTP server and point the system to the NTP server's IP address, as described in Setting the System Time.

NOTE: WLAN service schedule times should be configured based on your browser's current time zone. If your browser and the target AP/WLAN are in different time zones, configure the on/off times according to the desired schedule according to your local browser. For example, if you wanted a WLAN in Los Angeles to turn on at 9 AM and your browser was set to New York time, configure the WLAN service schedule to enable the WLAN at noon. When configuring the service schedule, all times are based on your browser's time zone setting.

Creating a WLAN Schedule Profile

Follow these steps to create a WLAN schedule profile.

1 Go to *Configuration > AP Zones*.

2 On the *AP Zones* submenu, click **WLAN Scheduler**.

3 Click *Create New*. The *Create New WLAN Schedule Table* form appears.

4 Set a WLAN schedule.

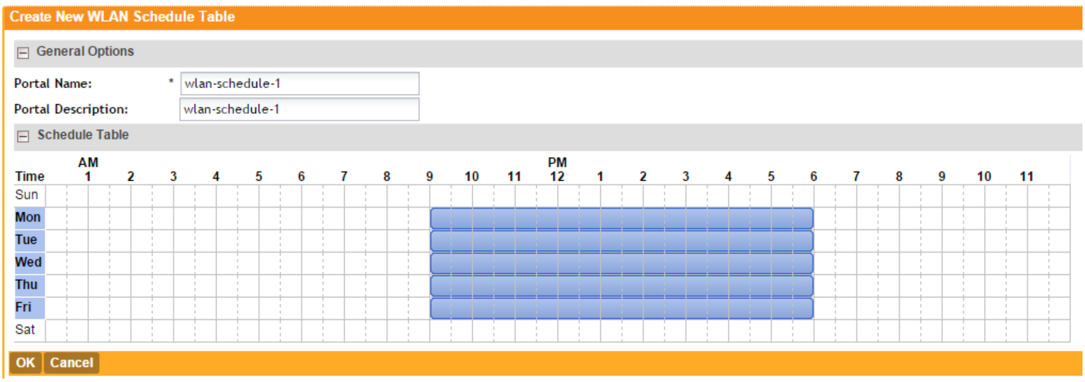
- To enable or disable the WLAN for an entire day, click the day of the week under the Time column.
- To enable or disable the WLAN for specific hour of a specific day, click the squares in the table. A single square represents 30 minutes (two-15 minute blocks).

Blue-colored cells indicate the hours when the WLAN is enabled. Clear (or white) cells indicate the hours when the WLAN is disabled.

5 Click **Create New**. The page refreshes, and then the schedule you created appears in the WLAN Scheduler section.

You have completed creating a WLAN schedule. This WLAN schedule will now appear as an option when you set the WLAN service schedule to **Specific** (see Figure 36)

Figure 35. Creating a WLAN schedule



Create New WLAN Schedule Table

⊟ General Options

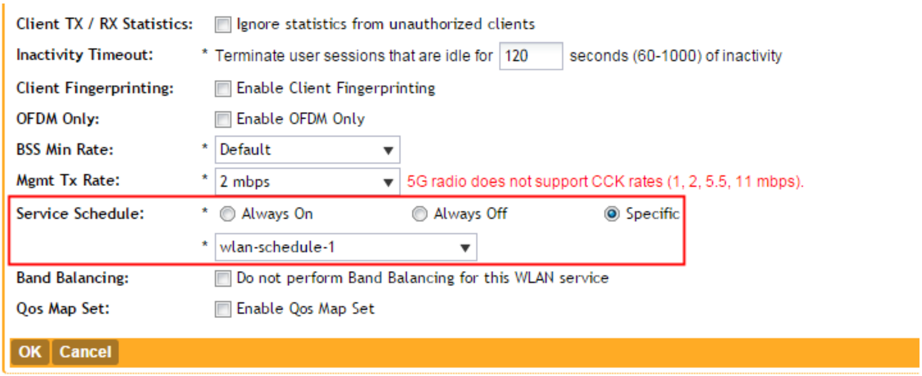
Portal Name: * wlan-schedule-1

Portal Description: wlan-schedule-1

⊟ Schedule Table

		AM											PM											
Time		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sun																								
Mon										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Tue										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Wed										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Thu										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Fri										▨	▨	▨	▨	▨	▨	▨	▨	▨						
Sat																								

Figure 36. The WLAN schedule appears as an option when you set the WLAN service schedule to “Specific”



Client TX / RX Statistics: □ Ignore statistics from unauthorized clients

Inactivity Timeout: * Terminate user sessions that are idle for 120 seconds (60-1000) of inactivity

Client Fingerprinting: □ Enable Client Fingerprinting

OFDM Only: □ Enable OFDM Only

BSS Min Rate: * Default ▼

Mgmt Tx Rate: * 2 mbps ▼ 5G radio does not support CCK rates (1, 2, 5.5, 11 mbps).

Service Schedule: * ○ Always On ○ Always Off ● Specific
* wlan-schedule-1 ▼

Band Balancing: □ Do not perform Band Balancing for this WLAN service

Qos Map Set: □ Enable Qos Map Set

Working with Device Policies

In response to the growing numbers of personally owned mobile devices such as smart phones and tablets being brought into the network, IT departments are requiring more sophisticated control over how devices connect, what types of devices can connect, and what they are allowed to do once connected.

Using device access policies, the system can identify the type of client attempting to connect, and perform control actions such as permit/deny, rate limiting, and VLAN tagging based on the device type.

Once a device access policy has been created, you can apply the policy to any WLANs or WLAN groups for which you want to control access by device type. You could, for example, allow only Apple OS devices on one WLAN and only Linux devices on another.

Creating a Device Access Policy

Follow these steps to create a device access policy.

1 Go to *Configuration* > *AP Zones*.

2 Click the AP zone for which you want to create a device access policy.

3 On the *AP Zones* submenu, click **Device Policy**.

4 Click **Create New**.

5 In *Name*, type a name for this policy.

6 In *Description*, type a short description for this policy.

7 In *Default Access*, click either **Allow** or **Block**. This is the default action that the system will take if no rules are matched.

8 In the *Rules* section, click **Create New**. The *Create New Device Policy Rules* form appears.

9 Configure the rule settings:

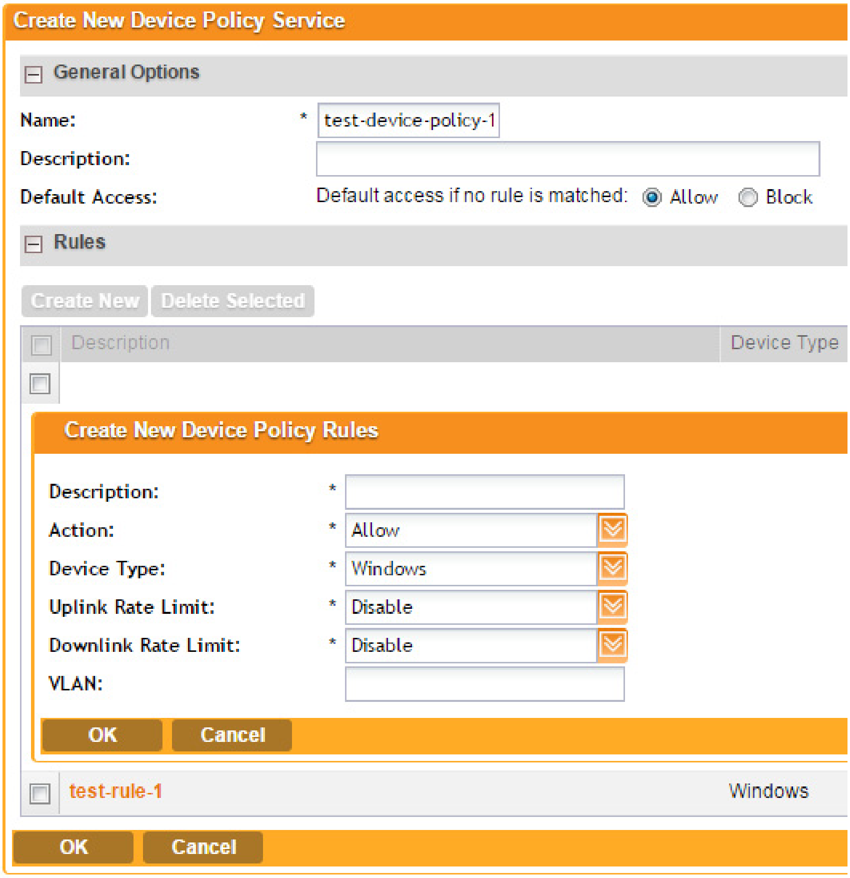
- *Description*: Type a description for this rule.
- *Action*: Select either **Allow** or **Block**. This is the action that the system will take if the client matches any of the attributes in the rule.
- *Device Type*: Select from any of the supported client types.
- *Uplink Rate*: Select the uplink rate limit for this client type, or select Disable.
- *Downlink Rate*: Select the download rate limit for this client type, or select Disable.
- *VLAN*: Segment this client type into a specified VLAN (1~4094; if no value is entered, this policy does not impact device VLAN assignment).

10 To add a new rule, click **Create New** again, and then repeat Step 9.

11 When you finish creating all the rules that you want to add to the policy, click **OK** at the bottom of the form. The page refreshes, and then the policy that you created appears under the *Device Policy Services* section.

You have completed creating a device access policy.

Figure 37. The Create New Device Policy Service form



Create New Device Policy Service

⊟ General Options

Name: * test-device-policy-1

Description:

Default Access: Default access if no rule is matched: ● Allow ○ Block

⊟ Rules

□	Description	Device Type
□		

Create New Device Policy Rules

Description: *

Action: * Allow

Device Type: * Windows

Uplink Rate Limit: * Disable

Downlink Rate Limit: * Disable

VLAN:

□	test-rule-1	Windows

Viewing Device Access Policies

Follow these steps to view a list of existing device access policies.

1 Go to *Configuration* > *AP Zones*.

2 Click the AP zone for which you want to view existing device access policies.

3 On the *AP Zones* submenu, click **Device Policy**.

The *Device Policy Services* page appears and lists all existing device access policies and their basic settings are shown, including the:

- Name
- Description

- Default access (allow or block)
- Actions (that you can perform)

To view or update policy settings, click the policy name.

You have completed viewing device access policies.

Deleting Device Access Policies

Follow these steps to delete device access policies.

1. Go to *Configuration* > *AP Zones*.
2. Click the AP zone for which you want to create a device access policy.
3. On the *AP Zones* submenu, click **Device Policy**.
4. Locate the policy or policies that you want to delete.
5. Select the check boxes (first column) for the policies that you want to delete.
6. Click Delete Selected.

The policies that you selected disappear from the list. You have completed deleting device access policies.

NOTE: If you are deleting a single policy, you can also click the 🗑 icon (under the *Actions* column) that is in the same row as the policy that you want to delete.

Working with L2 Access Control Policies

Another method to control access to the network is by defining Layer 2/MAC address access control lists (ACLs), which can then be applied to one or more WLANs or WLAN groups. L2 ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. MAC addresses that are in the deny list are blocked at the AP.

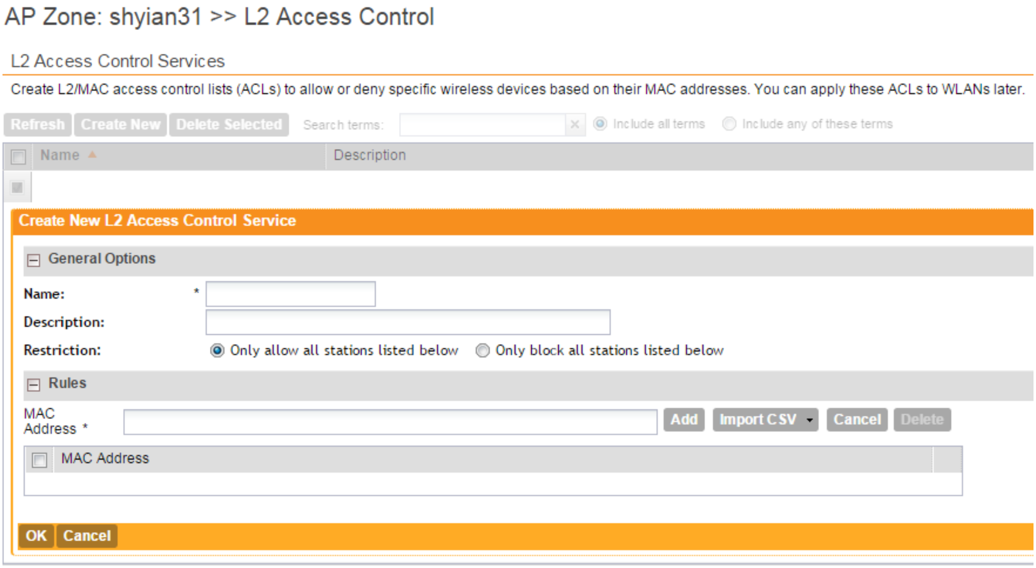
Creating an L2 Access Policy

Follow these steps to create an L2 access policy.

1. Go to *Configuration > AP Zones*.
2. Click the AP zone for which you want to create an L2 ACL.
3. On the *AP Zones* submenu, click **L2 Access Control**.
4. Click **Create New**. The *Create New L2 Access Control Service* form appears.
5. In *Name*, type a name for this policy.
6. In *Description*, type a short description for this policy.
7. In *Restriction*, select the default action that the controller will take if no rules are matched. Available options include:
    - **Only allow all stations listed below**
    - **Only block all stations listed below**
8. In *MAC Address* (under the *Rules* section), type the MAC address to which this L2 access policy applies.
9. Click **Add**.
10. To add another MAC address, repeat steps 8 to 9.
11. When you have finished adding all the MAC addresses that you need to add, click **OK**. The page refreshes, and then the L2 access policy that you created appears in the *L2 Access Control Services* section.

You have completed creating an L2 access policy.

Figure 38. The Create New L2 Access Control Services form



AP Zone: shyian31 >> L2 Access Control

L2 Access Control Services

Create L2/MAC access control lists (ACLs) to allow or deny specific wireless devices based on their MAC addresses. You can apply these ACLs to WLANs later.

Create New L2 Access Control Service

General Options

Name: *	
Description:	
Restriction:	● Only allow all stations listed below ○ Only block all stations listed below

Rules

MAC Address *

Viewing L2 Access Policies

Follow these steps to view a list of existing L2 access profiles.

1. Go to *Configuration* > *AP Zones*.
2. Click the AP zone for which you want to view existing L2 ACLs.
3. On the *AP Zones* submenu, click **L2 Access Control**.
4. Look for the *L2 Access Control Services* section. All existing L2 access policies and their basic settings are shown, including the:
   - Name
   - Description
   - Default access (allow or block)
   - Actions (that you can perform)
5. To view or change the MAC addresses have been defined in a particular L2 access policy, click the profile name.

You have completed viewing existing L2 access policies.

Deleting L2 Access Policies

Follow these steps to delete L2 access policies.

1. Go to *Configuration* > *AP Zones*.
2. Click the AP zone from which you want to delete L2 ACLs.
3. On the *AP Zones* submenu, click **L2 Access Control**.
4. In the *L2 Access Control Services* section, locate the policy or policies that you want to delete.
5. Select the check boxes (first column) for the policies that you want to delete.
6. Click **Delete Selected**.

The policies that you selected disappear from the list. You have completed deleting L2 access policies.

NOTE: If you are deleting a single policy, you can also click the 🗑 icon (under the *Actions* column) that is in the same row as the policy that you want to delete.

Working with Bonjour Policies

Bonjour™ is Apple's implementation of a zero-configuration networking protocol for Apple devices over IP. It allows OS X and iOS devices to locate other devices such as printers, file servers and other clients on the same broadcast domain and use the services offered without any network configuration required.

Multicast applications such as Bonjour require special consideration when being deployed over wireless networks. Bonjour only works within a single broadcast domain, which is usually a small area. This is by design to prevent flooding a large network with multicast traffic. However, in some situations, a user may want to offer Bonjour services from one VLAN to another.

The controller's Bonjour gateway feature addresses this requirement by providing an mDNS proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from/to which VLANs.

In order for the Bonjour Gateway to function, the following network configuration requirements must be met:

1. The target networks must be segmented into VLANs.
2. VLANs must be mapped to different SSIDs.
3. The controller must be connected to a VLAN trunk port.

Additionally, if the VLANs to be bridged by the gateway are on separate subnets, the network has to be configured to route traffic between them.

Creating a Bonjour Gateway Rule on the AP

Using the Bonjour gateway feature, Bonjour bridging service is performed on a designated AP rather than on the controller. Offloading the Bonjour policy to an AP is necessary if a Layer 3 switch or router exists between the controller and the APs. The controller identifies a single AP that meets the memory/processor requirements (this feature is only supported on certain APs), and delivers a set of service rules - a Bonjour policy - to the AP to perform the VLAN bridging.

NOTE: This feature is only supported on the following access points: R700, R300, 7982, 7372/52, 7055, 7782/81, SC-8800 series.

Here are the requirements and limitations of the Bonjour gateway feature:

- Bonjour policy deployment to an AP takes effect after the AP joins the controller.

- Some APs of one local area link must be on one subnet. The switch interfaces connected to these APs in a local area link to must be configured in VLAN-trunk mode. Only by doing so can the designated AP can receive all the multicast Bonjour protocol packets from other VLANs.
- Dynamic VLANs are not supported.
- Some AP models are incompatible with this feature due to memory requirements.

Follow these steps to create rules for an AP that will bridge Bonjour services across VLANs.

1 Go to *Configuration > AP Zones*.

2 On the *AP Zone List* page, click the zone name for which you want to configure the Bonjour gateway.

3 On the *AP Zones* sidebar, click **Bonjour Policy**.

4 Click **Create New** to create a Bonjour gateway policy. The *Create Bonjour Policy* form appears.

5 In *Name*, type a name for the policy.

6 In *Description*, type a description for the policy.

7 In the *Rules* section, click **Create New** to create a rule.

8 Configure the following options:

   - *Bridge Service*: Select the Bonjour service from the list.
   - *From VLAN*: Select the VLAN from which the Bonjour service will be advertised.
   - *To VLAN*: Select the VLAN to which the service should be made available.
   - *Notes*: Add optional notes for this rule.

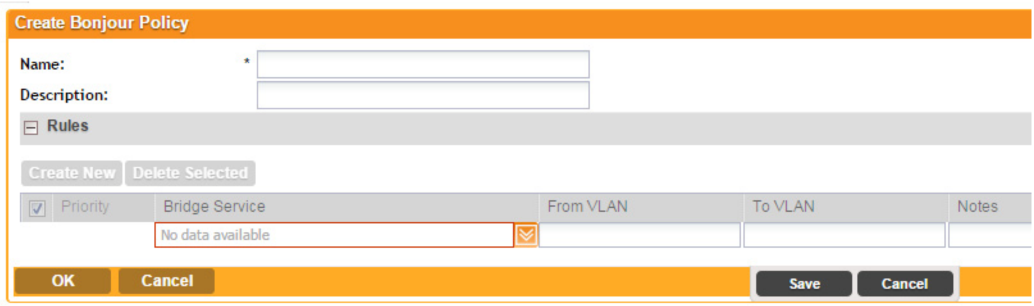
9 Click **Save** to save the rule. To create another rule, repeat steps 7 to 9.

10 After you finish creating all rules that you require, click **OK** to close the *Create Bonjour Policy* form.

11 Select the **Enable Bonjour gateway on the AP** check box.

You have completed creating a Bonjour gateway policy.

Figure 39. The Create Bonjour Policy form



Applying a Bonjour Policy to an AP

Once you have created a Bonjour policy for an AP, you will need to designate the AP that will be responsible for implementing this policy.

Follow these steps to apply a Bonjour policy to an AP.

1 Go to *Configuration* > *Access Points*.

2 From the list of APs, click the MAC address of the AP to which you want to apply the Bonjour policy. The *Edit AP [{MAC address}]* form appears.

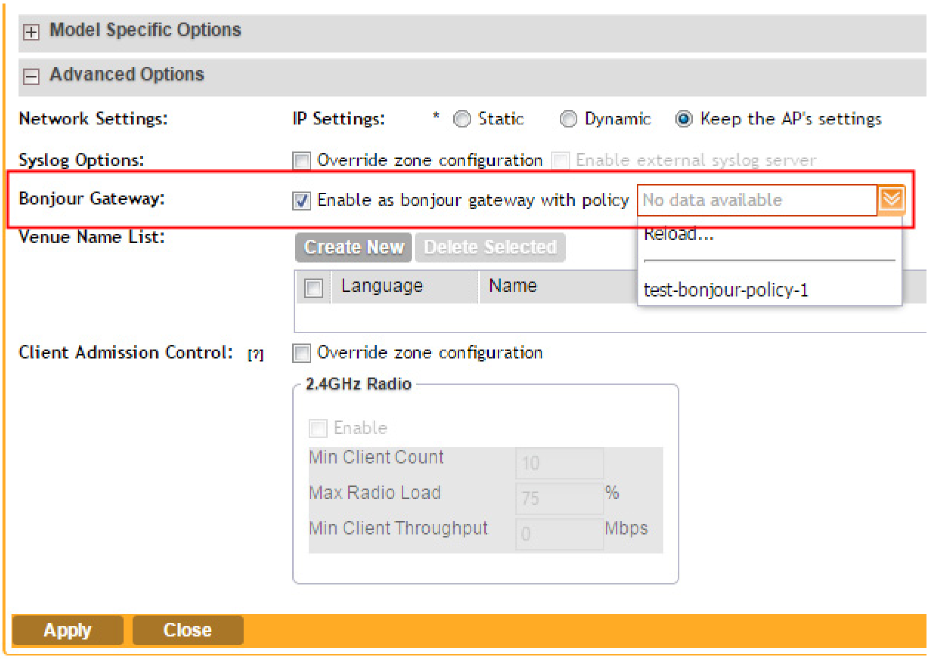
3 Scroll down to the *Advanced Options* section, and then locate the *Bonjour Gateway* option.

4 Select the **Enable as bonjour gateway with policy** check box, and then select the Bonjour policy that you want to apply to the AP (see Figure 40).

5 Click **Apply**.

You have completed applying a Bonjour gateway policy to an AP.

Figure 40. Select the Bonjour policy that you created earlier



⊞ Model Specific Options

⊟ Advanced Options

Network Settings: IP Settings: * ○ Static ○ Dynamic ● Keep the AP's settings

Syslog Options: □ Override zone configuration □ Enable external syslog server

Bonjour Gateway: ☑ Enable as bonjour gateway with policy No data available

Reload...

test-bonjour-policy-1

Venue Name List:

□	Language	Name

Client Admission Control: [?] □ Override zone configuration

2.4GHz Radio

□ Enable

Min Client Count 10

Max Radio Load 75 %

Min Client Throughput 0 Mbps

Creating a DiffServ Profile

If you need to configure the type of traffic (ToS) bit settings for the access side traffic from Ruckus Wireless APs, follow these steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to Ruckus GRE and SoftGRE traffic.

1. Click *AP Zones* > *Zone Name ({AP Zone Name})* > *DiffServ*. For example, if you want to create a DiffServ profile for an AP zone named “ap-zone-1,” click *AP Zones* > *Zone Name (ap-zone-1)* > *DiffServ*. The *DiffServ Profiles* page appears.
2. Click **Create New**. The form for creating a new DiffServ profile appears.
3. In *Name*, type a name for the DiffServ profile that you are creating.
4. In *Description*, type a brief description for the DiffServ profile.
5. In *Tunnel DiffServ*, configure the following options.
    - *Set Uplink DiffServ*: Select the check box if you want to set the Differentiated Services field for uplink user traffic from Ruckus Wireless APs towards either the controller or a third party gateway via SoftGRE. Configure the desired value to be set by the Ruckus Wireless AP.

- *Set Downlink DiffServ*: Select the check box if you want to set the Differentiated Services field for downlink user traffic from the controller towards the AP, and then configure the desired value to be set by the Ruckus Wireless AP.

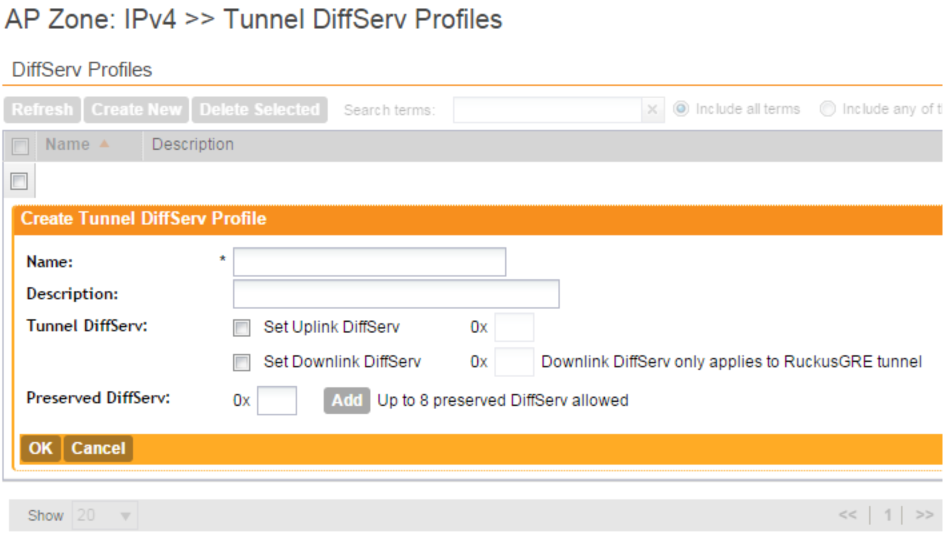
6 In *Preserved DiffServ*, configure up to eight (8) entries in the preserved DiffServ list. The *Preserved DiffServ* list allows the preservation of values that have been already marked in incoming packets either in uplink or downlink traffic.

7 Click **OK**. The page refreshes, and then the DiffServ profile you created appears on the page.

You have completed creating a DiffServ profile.

NOTE: Control DSCP can be configured from the controller's CLI.

Figure 41. The Create Tunnel DiffServ Profile form



AP Zone: IPv4 >> Tunnel DiffServ Profiles

DiffServ Profiles

Name: *

Description:

Tunnel DiffServ: □ Set Uplink DiffServ 0x

□ Set Downlink DiffServ 0x Downlink DiffServ only applies to RuckusGRE tunnel

Preserved DiffServ: 0x Add Up to 8 preserved DiffServ allowed

Managing Global Configuration, AP Tunnel Profiles, Templates, and AP Registration Rules

3

Managing Global Configuration

Global configuration refers to the country code and the port number that is used for tunneling GRE + UDP traffic. These settings are applied across all AP zones and the managed devices that belong to each AP zone.

Different countries have different regulations on the usage of radio channels. To ensure that the controller is using an authorized radio channel, select the correct country code for your location. If you change the country code now, this change will only be applied to new zones and the APs that will be assigned to them. Existing zones and the APs that belong to them will retain the country code that was configured previously.

Follow these steps to set the global configuration.

1. Go to *Configuration > AP Zones*.
2. On the sidebar, click **Global Configuration**.
3. In *Default Country Code for New Zone*, select the correct country code for the geographical location where the managed devices (or APs) are deployed. Selecting the correct country code will ensure that managed devices use an authorized radio channel.

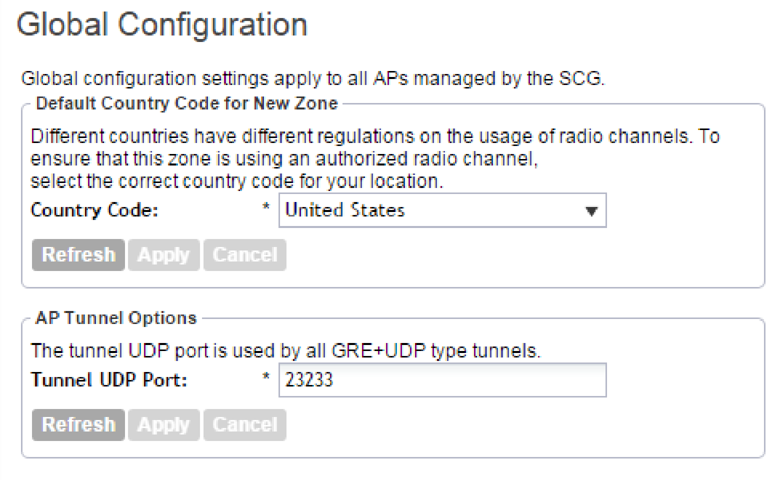
   After you select a new country code, the **Apply** and **Cancel** buttons become active.
4. Click **Apply** to save the country code.
5. In *AP GRE Tunnel Options*, type the port number that you want the controller to use for tunneling GRE and UDP traffic from managed devices. The default tunnel port number is 23233.

CAUTION! Make sure that you open this port number on the network firewall to ensure that a GRE tunnel can be established successfully.

After you type the new tunnel port number, the **Apply** and **Cancel** buttons become active.

6 Click **Apply** to save the tunnel port number.

Figure 42. The AP Zone Global Configuration page



Global Configuration

Global configuration settings apply to all APs managed by the SCG.

Default Country Code for New Zone

Different countries have different regulations on the usage of radio channels. To ensure that this zone is using an authorized radio channel, select the correct country code for your location.

Country Code: * United States

AP Tunnel Options

The tunnel UDP port is used by all GRE+UDP type tunnels.

Tunnel UDP Port: * 23233

Creating AP Tunnel Profiles

This section describes the procedures for creating Ruckus GRE, SoftGRE, and IPsec tunnel profiles.

- Creating a Ruckus GRE Tunnel Profile
- Creating a SoftGRE Tunnel Profile
- Creating an IPsec Profile

Creating a Ruckus GRE Tunnel Profile

Follow these steps to create a Ruckus GRE tunnel profile.

1 Go to *Configuration* > *AP Zones*.

2 On the sidebar, click *AP Tunnel Profiles* > *Ruckus GRE*. The *Ruckus GRE* page appears.

3 Click **Create New**. The *Create Ruckus GRE Profile* form appears.

4 Configure the following options:

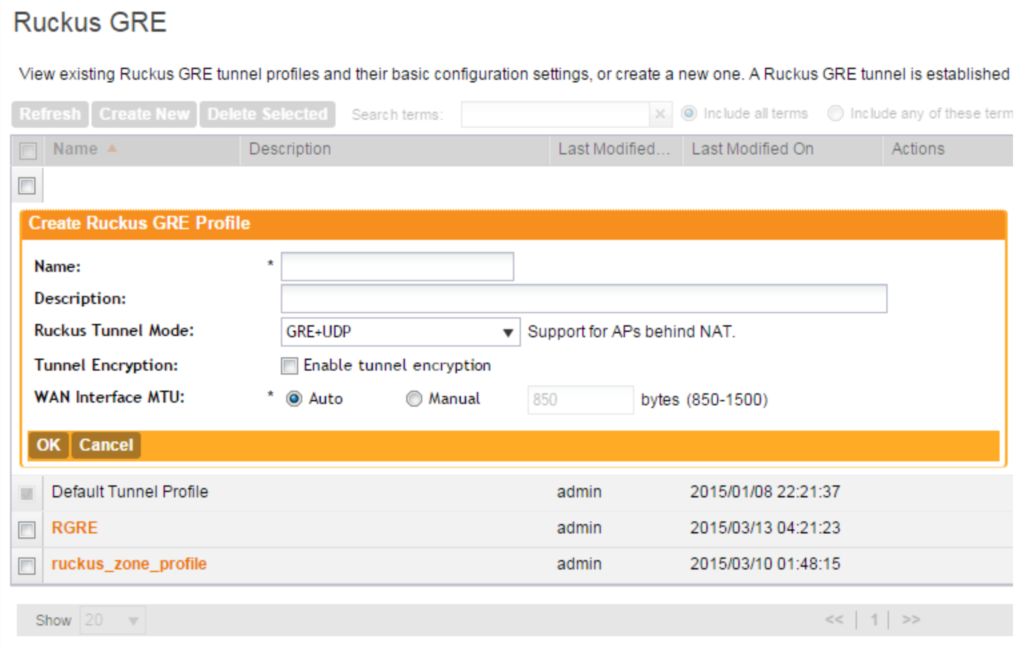
   - *Name*: Type a name for the profile that you are creating.
   - *Description*: Type a short description of the profile.

- *Ruckus Tunnel Mode*: Select a protocol to use for tunneling WLAN traffic back to the controller:
  - **GRE + UDP**: Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the controller.
  - **GRE**: Select this option to tunnel regular WLAN traffic only.
- *Tunnel Encryption*: Select the **Enable tunnel encryption** check box if you want managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the controller. By default, when WLAN traffic is tunneled to the controller, only the management traffic is encrypted; data traffic is unencrypted.
- *WAN Interface MTU*: Set the maximum transmission unit (MTU) for the tunnel to either Auto (default) or a specific size (850 to 1500 bytes). MTU is the size of the largest protocol data unit that can be passed on the controller network.

5 Click **Create New**.

You have completed creating a Ruckus GRE tunnel profile.

Figure 43. Creating a Ruckus GRE tunnel profile



Ruckus GRE

View existing Ruckus GRE tunnel profiles and their basic configuration settings, or create a new one. A Ruckus GRE tunnel is established

Create Ruckus GRE Profile

Name: *
Description:
Ruckus Tunnel Mode: GRE+UDP ▾ Support for APs behind NAT.
Tunnel Encryption: □ Enable tunnel encryption
WAN Interface MTU: * ● Auto ○ Manual 850 bytes (850-1500)

	Name	Description	Last Modified...	Last Modified On	Actions
□	Default Tunnel Profile		admin	2015/01/08 22:21:37	
□	RGRE		admin	2015/03/13 04:21:23	
□	ruckus_zone_profile		admin	2015/03/10 01:48:15	

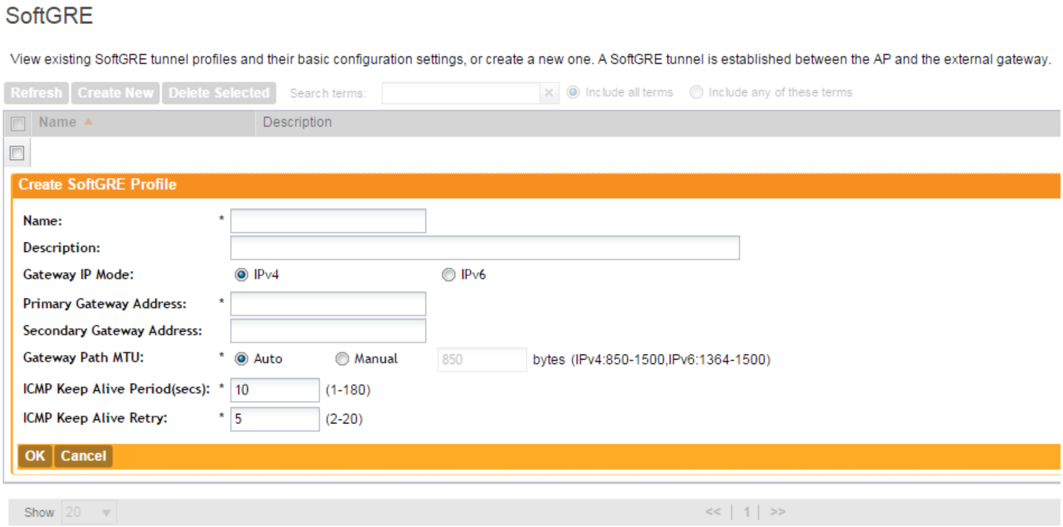
Creating a SoftGRE Tunnel Profile

CAUTION! A SoftGRE tunnel does not support APs that are behind a NAT server.

Follow these steps to create a SoftGRE tunnel profile.

1. Go to *Configuration* > *AP Zones*.
2. On the sidebar, click *AP Tunnel Profiles* > *SoftGRE*. The *SoftGRE* page appears.
3. Click **Create New**. The *Create SoftGRE Profile* form appears.
4. Configure the following options:
   - *Name*: Type a name for the profile that you are creating.
   - *Description*: Type a short description of the profile.
   - *Gateway IP Mode*: Click the IP addressing mode that the gateway is using. Options include:
     - **IPv4**
     - **IPv6**
   - *Primary Gateway Address*: Type the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
   - Secondary Gateway Address: If you have a secondary gateway server on the network, type its IP address or FQDN in the box provided. If the controller is unable to reach the primary gateway server, it will automatically attempt to reach the secondary gateway address that you specify here.
   - *Gateway Path MTU*: Set the maximum transmission unit (MTU) for the gateway path. Options include **Auto** (default) and **Manual** (range is 850 to 1500 bytes).
   - *ICMP Keep Alive Period*: Type the time interval (in seconds) at which APs send a keepalive message to the active third party WLAN gateway. The range is 1 to 180 seconds and the default value is 10 seconds.
   - *ICMP Keep Alive Retry*: Type the number of keepalive attempts that APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is 2 to 10 retries and the default value is 5 retries.
5. Click **Create New**.

Figure 44. Creating a SoftGRE profile



SoftGRE

View existing SoftGRE tunnel profiles and their basic configuration settings, or create a new one. A SoftGRE tunnel is established between the AP and the external gateway.

Name:	*		
Description:			
Gateway IP Mode:		● IPv4	○ IPv6
Primary Gateway Address:	*		
Secondary Gateway Address:			
Gateway Path MTU:	*	● Auto ○ Manual	850 bytes (IPv4:850-1500,IPv6:1364-1500)
ICMP Keep Alive Period(secs):	*	10	(1-180)
ICMP Keep Alive Retry:	*	5	(2-20)

Creating an IPsec Profile

Follow these steps to create an IPsec profile that APs can use when the AP tunnel settings are set to SoftGRE + IPsec.

1. Go to *Configuration > AP Zones*.
2. On the sidebar, click *AP Tunnel Profiles > IPsec*. The *IPsec* page appears.
3. Click **Create New**. The *Create IPSec Profile* form appears.
4. In *General Options*, configure the following:
   - *Name*: Type name for the IPSec profile that you are creating.
   - *Description*: Type a description for this profile.
   - *Security Gateway*: Type the IP address or FQDN of the IPSec server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
5. In *Authentication*, configure the following:
   - *Type*: Click **Preshared Key** to use PSK for authentication or click **Certificate** to use an X.509 certificate on the certificate authority (CA) or registration authority (RA) server. The controller uses the CMPv2 protocol to obtain the signed certificate from the CA/RA server.

- *Preshared Key*: If you clicked **Preshared Key** in *Type*, type the PSK in this box. The PSK must be eight to 128 ASCII characters in length.

6 In *Security Association*, configure the following:

- *IKE Proposal Type*: Click **Default** to use the default Internet Key Exchange (IKE) security association (SA) proposal type or click **Specific** to manually configure the IKE SA proposal. If you clicked **Specific**, you will need to configure the following settings:
  - *Encryption Algorithm*: Options include 3DES, AES128, AES192, and AES256.
  - *Integrity Algorithm*: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512.
  - *Pseudo-Random Function*: Options include Use integrity ALG, PRF-MD5, PRF-SHA1, PRF-AES-XCBC, PRF-AES-CMAC, PRF-SHA256, and PRF-SHA384.
  - *DH Group*: Options for Diffie-Hellman groups for IKE include modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.
- *ESP Proposal Type*: Click **Default** to use the default Encapsulating Security Payload (ESP) SA proposal type or click **Specific** to manually configure the ESP proposal. If you clicked **Specific**, you will need to configure the following settings:
  - *Encryption Algorithm*: Options include 3DES, AES128, AES192, AES256, and NONE.
  - *Integrity Algorithm*: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512
  - *DH Group*: Options for Diffie-Hellman groups for ESP include None, modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.

7 In *Rekey Options*, configure the following:

- *Internet Key Exchange*: To set time interval at which the IKE key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable IKE rekey, select the **Disable** check box.
- *Encapsulating Security Payload*: To set time interval at which the ESP key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable ESP rekey, select the **Disable** check box.

8 In *Certificate Management Protocol*, configure the following:

- *DHCP Option 43 Sub Code for CA/RA Address*: Set the DHCP Option 43 subcode that will be used to discover the address of the CA/RA server on the network. The default subcode is 8.
- *CA/RA Address*: Type the IP address or FQDN of the CA/RA server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
- *Server Path*: Type the path to the X.509 certificate on the CA/RA server.
- *DHCP Option 43 Sub Code for Subject Name of CA/RA*: Set the DHCP Option 43 subcode that will be used to discover the subject name of the CA/RA server on the network. The default subcode is 5.
- *Subject Name of CA/RA*: Type an ASCII string that represents the subject name of the CA/RA server.

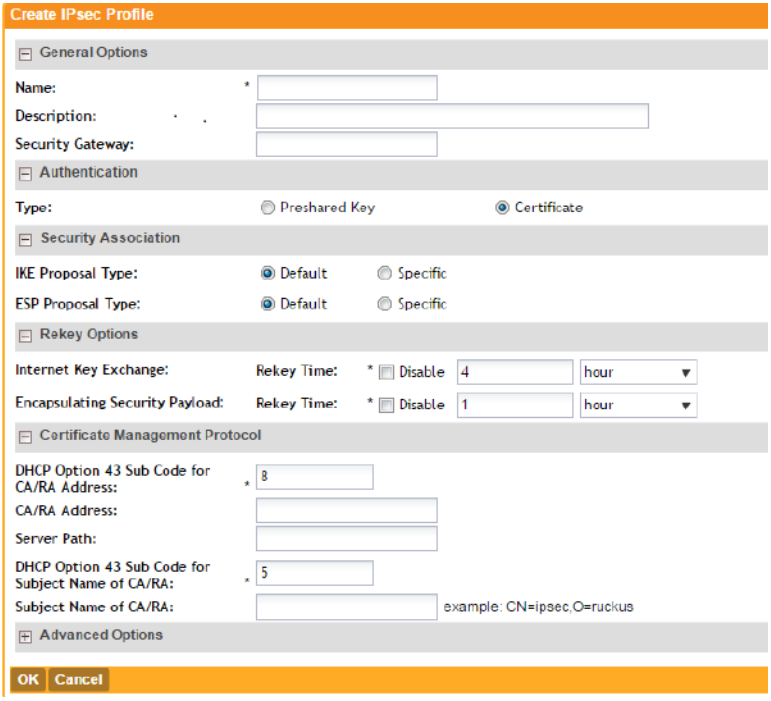
9 In *Advanced Options*, configure the following:

- *DHCP Option 43 Sub Code for Security Gateway*: Set the DHCP Option 43 subcode that will be used to discover the address of the security gateway on the network. The default subcode is 7.
- *Retry Limit*: Set the number of times that the controller will attempt to discover the address of the security gateway. The default retry count is 5. Accepted values are 0 (disable) to 16.
- *Replay Window*: Set the ESP replay window (in packets). The default size is 32 packets. Accepted values are 0 (disable) to 32 packets.
- *IP Compression*: To enable IP Payload Compression Protocol (IPComp) compression before encryption, click **Enable**. The default value is **Disable**.
- *Force NAT-T*: To enforce UDP encapsulation of ESP packets, click **Enable**. The default value is **Disable**.
- *Dead Peer Detection*: By default, the IKE protocol runs a health check with remote peer to ensure that it is alive. To disable this health check, click **Disable**.
- *NAT-T Keep Alive Interval*: To set the keep alive interval (in seconds) for NAT traversal, type a value in the box. The default keep alive interval is 20 seconds. Accepted values are 1 to 65536. To disable the keep alive interval, click **Disable**.
- *FailOver Options*: To configure the failover settings when APs are unable to connect, configure the following:

- *Retry Period*: Set the number of days (minimum 3 days) during which APs will keep attempting to connect. To keep try indefinitely, select the **Forever** check box.
- *Retry Interval*: Set the interval (in minutes) between each retry attempt. The default retry interval is 1 minute. Accepted values are from 1 to 30 minutes.
- *Retry Mode*: If you want APs to fall back to the specified primary security gateway, click **Revertive**. If you want APs to maintain connectivity with the security gateway to which they are currently connected, click **Non-revertive**.

10 Click **OK**.

Figure 45. Creating an IPSec profile



Create IPsec Profile

⊟ General Options

Name: *

Description:

Security Gateway:

⊟ Authentication

Type: ○ Preshared Key ● Certificate

⊟ Security Association

IKE Proposal Type: ● Default ○ Specific

ESP Proposal Type: ● Default ○ Specific

⊟ Rekey Options

Internet Key Exchange: Rekey Time: * □ Disable 4 hour ▼

Encapsulating Security Payload: Rekey Time: * □ Disable 1 hour ▼

⊟ Certificate Management Protocol

DHCP Option 43 Sub Code for CA/RA Address: * 8

CA/RA Address:

Server Path:

DHCP Option 43 Sub Code for Subject Name of CA/RA: * 5

Subject Name of CA/RA: example: CN=ipsec,O=ruckus

⊞ Advanced Options

Working with Zone Templates

A zone template contains configuration settings (radio, AP GRE tunnel, channel mode, and background scanning) that you can apply to all access points that belong to a particular AP zone. Applying a zone template to an AP zone will overwrite all settings on all access points that belong that the AP zone.

This section describes the following topics:

- Creating and Configuring a Zone Template
- Exporting a Zone Template
- Importing a Zone Template
- Deleting a Zone Template

Creating and Configuring a Zone Template

Creating a zone template requires that you create the template and configure the services that will be deployed with the template. Follow these steps to create and configure a zone template.

Step 1: Create the Zone Template

Step 2: Configure the AP Model-Specific Configuration

Step 3: Configure the AAA Servers of the Zone Template

Step 4: Configure the Hotspot (WISPr) Services of the Zone Template

Step 5: Configure the Hotspot 2.0 Service of the Zone Template

Step 6: Configure the WLAN Service of the Zone Template

Step 1: Create the Zone Template

Follow these steps to create a zone template.

1 Click *Configuration > AP Zones*.

2 On the sidebar, click **Zone Templates**. The *Zone Templates* page appears.

3 Click the **Create New** button. The *Create New Zone Template* form appears.

4 Configure *General Options*.

   a In *Template Name*, type a name for the zone template that you are creating.

   b In *Description*, type a description for this template.

   c In *Template Firmware*, select the controller firmware version to which to apply this template.

   d In *Country Code*, select the correct code for the country in which you are operating the controller network. Different countries and regions maintain different rules that govern which channels can be used for wireless communications. Selecting the correct country code will ensure that APs that are part of the controller network do not violate local and national regulatory restrictions.

   e In *AP Admin Logon*, configure the following options:

   - **Logon ID**: Set the administrator user name.
   - **Password**: Set the administrator password.

   Any administrator can use this user name and password combination to log on directly to the managed access point's native web interface.

f. In *Syslog Options,* if you have a syslog server on the network and you want the controller to send syslog data to it, select the **Enable external server for APs in this zone** check box.

5. Configure *Radio Options*.

   a. In the *Radio Options b/g/n (2.4GHz)* section, configure the following options:

      - *Channelization*: Select the channel width. Options include 20MHz, 40MHz, or 80MHz**.**
      - *Channel*: Select **Auto** or manually assign a channel for the 2.4GHz radio.
      - *TX Power Adjustment*: Manually set the transmit power on all 2.4GHz radios (default is Full).

   b. In *Radio Options a/n (5GHz)*, configure the following options:

      - *Channelization*: Select **20MHz** or **40MHz** channel width.
      - *Channel*: Select **Auto** or manually assign a channel for the 5GHz radio.
      - *TX Power Adjustment*: Manually set the transmit power on all 5GHz radios (default is Full).

6. Configure *AP GRE Tunnel Options*.

   a. *Tunnel Type*: Select an option for tunneling WLAN traffic back to the controller:

      - Ruckus GRE
      - SoftGRE
      - SofteGRE + IPSec

   b. *Tunnel Encryption*: Select the **Enable tunnel encryption** check box if you want managed APs to decrypt 802.11 packets, and then use an AES-encrypted tunnel to send them to the controller. When WLAN traffic is tunneled to the controller, only the management traffic is encrypted while data traffic is unencrypted by default.

   - *Tunnel MTU Options*: Manually set the maximum transmission unit (MTU) or use **Auto** (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.

7. Configure *Advanced Options*.

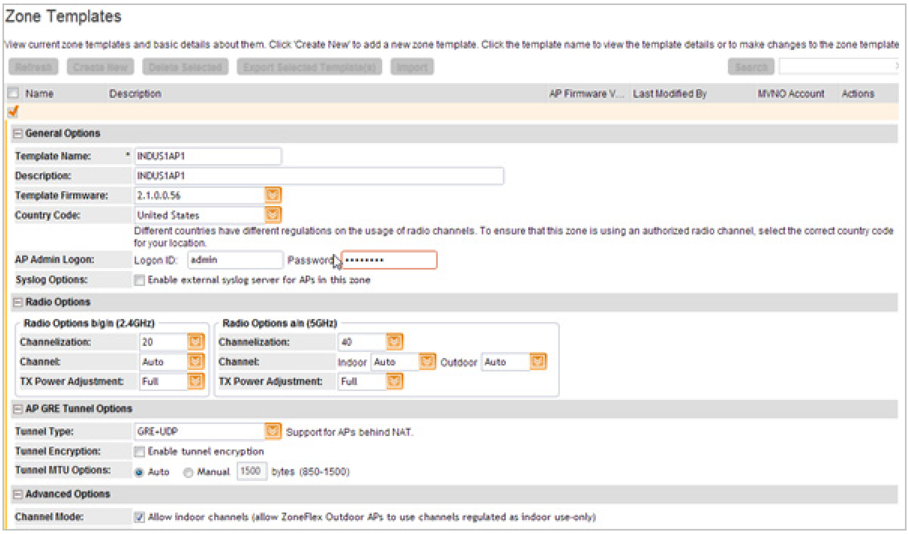
   - *Channel Mode*: Select the **Allow indoor channels** check box if you want to allow ZoneFlex outdoor APs to use indoor-use only channels. For more information on channel mode, see Channel Mode.

- *Background Scanning*: If you want APs to automatically evaluate radio channel usage, enable and configure the background scanning settings on both the 2.4GHz and 5GHz radios. By default, background scanning is enabled on both radios and set to run every 20 seconds.

8 Click **Create New** to create the zone template.

9 Continue to Step 2: Configure the AP Model-Specific Configuration.

Figure 46. The Create New Zone Template form



Zone Templates

View current zone templates and basic details about them. Click 'Create New' to add a new zone template. Click the template name to view the template details or to make changes to the zone template

General Options

Template Name: * INDUS1AP1

Description: INDUS1AP1

Template Firmware: 2.1.0.0.56

Country Code: United States

Different countries have different regulations on the usage of radio channels. To ensure that this zone is using an authorized radio channel, select the correct country code for your location.

AP Admin Logon: Logon ID: admin Password: ••••••••

Syslog Options: □ Enable external syslog server for APs in this zone

Radio Options

Radio Options b/g/n (2.4GHz)

Channelization: 20

Channel: Auto

TX Power Adjustment: Full

Radio Options a/n (5GHz)

Channelization: 40

Channel: Indoor Auto Outdoor Auto

TX Power Adjustment: Full

AP GRE Tunnel Options

Tunnel Type: GRE+UDP Support for APs behind NAT.

Tunnel Encryption: □ Enable tunnel encryption

Tunnel MTU Options: ● Auto ○ Manual 1500 bytes (850-1500)

Advanced Options

Channel Mode: ☑ Allow indoor channels (allow ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

Step 2: Configure the AP Model-Specific Configuration

Follow these steps to configure the AP model-specific configuration of the zone template.

1 Click *Configuration* > *AP Zones*.

2 On the sidebar, click **Zone Templates**. The *Zone Templates* page appears.

3 Click the name of the zone template for which you want to configure AP model-specific settings.

4 On the sidebar, click **AP Model-Specific Configuration**.

5 In *Select an AP Model*, select the AP model that you want to configure, and then click **Apply** to display the configuration option for the selected AP model.

6 In *General Options*, configure the following options (depending on the selected AP model, some of the options listed below may not be visible):

- *PoE out port*: To enable the PoE out port on the AP model, select the **Enable the PoE out port (requires custom PoE injector)** check box.
- *Status LEDs*: To disable the external status LEDs on the AP model, select the **Disable status LEDs** check box. This can be useful if your APs are installed in a public location and you do not want to draw attention to them.
- *External Antenna (2.4GHz)*: To enable the external 2.4GHz antenna on the AP model, select the **Enable external antenna with [x] dBi** (0-90) check box, and then a value for the dBi.
- *External Antenna (5GHz)*: To enable the external 5GHz antenna on the AP model, select the **Enable external antenna with [x] dBi** (0-90) check box, and then a value for the dBi.
- *LLDP*: To enable the AP model to advertise its identity and capabilities on the local network via LLDP, select the **Enable Link Layer Discovery Protocol** check box. For a list of attributes that APs advertise using LLDP, see Supported LLDP Attributes.
- *LLDP Advertise Interval (1-300 seconds)*: Set the interval (in seconds) at which the AP model will send out LLDP information. The default value is 30 seconds.
- *LLDP Hold Time (60-1200 seconds)*: Set the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.
- *LLDP Management IP TLV*: To include the management IP address TLV in the LLDP information that the AP model sends out, select **Enable** check box.
- *Port Settings*: For information on how to configure the port settings, see Configuring the Port Settings of a Particular AP Model.

7 Continue to Step 3: Configure the AAA Servers of the Zone Template.

Step 3: Configure the AAA Servers of the Zone Template

Follow these steps to configure the AAA servers that the zone template will use.

1. Click *Configuration* > *AP Zones*.
2. On the sidebar, click **Zone Templates**. The *Zone Templates* page appears.
3. Click the name of the zone template for which you want to configure an AAA server.
4. On the sidebar, click **AAA**.
5. Click **Create New**. The form for creating a new RADIUS server appears.
6. Configure *General Options*.
   - *Name*: Type a name for the AAA server that you are adding.
   - *Type*: Select the type of AAA server that you have on the network. Options include:
     - RADIUS
     - RADIUS Accounting
     - Active Directory
     - LDAP
   - *Backup RADIUS*: Select the **Enable backup RADIUS server** check box if a secondary RADIUS server exists on the network. Configure the settings in Step 8.
7. In the *Primary Server* section, configure the settings of the primary RADIUS server.
   - *IP Address*: Type the IP address of the AAA server.
   - *Port*: Type the port number of the AAA server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
   - *Shared Secret*: Type the AAA shared secret.
   - *Confirm Secret*: Retype the shared secret to confirm.
8. In the *Secondary Server* section, configure the settings of the secondary RADIUS server.

NOTE: The *Secondary Server* section is only visible if you selected the **Enable backup RADIUS server** check box earlier.

- *IP Address*: Type the IP address of the secondary AAA server.

- *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

9. Click **Create New** to create the AAA server for the zone template.
10. Continue to Step 4: Configure the Hotspot (WISPr) Services of the Zone Template.

Step 4: Configure the Hotspot (WISPr) Services of the Zone Template

NOTE: If you do not need to provide a hotspot portal to users, skip this section.

NOTE: This section describes the basic settings that you need to configure to include a hotspot portal in the zone template. If you need more information about hotspots, including third party prerequisites, see Creating and Managing Hotspots.

Follow these steps to configure the hotspot settings for the zone template.

1. Click *Configuration* > *AP Zones*.
2. On the sidebar, click **Zone Templates**. The *Zone Templates* page appears.
3. Click the name of the zone template for which you want to configure a hotspot portal.
4. On the sidebar, click **Hotspot (WISPr)**.
5. Click **Create New**. The form for creating a new hotspot portal appears.
6. In the *General Options* section, configure the following options:
   - *Name*: Type a name for the hotspot portal.
   - *Description*: Type a description for the hotspot portal.
7. In the *Redirection* section, configure the following options:
   - *Smart Client Support*: Select one of the following options:
     - **None**: Select this option to disable Smart Client support on the hotspot portal.
     - **Enable**: Selection this option to enable Smart Client support.
     - **Only Smart Client Allowed**: Select this option to allow only Smart Clients to connect to the hotspot portal.

For more information, see Configuring Smart Client Support.

- In *Logon URL*, type the URL of the subscriber portal (the page where hotspot users can log on to access the hotspot portal). For more information, see Configuring the Logon URL.
- In *Start Page*, set where users will be redirected after they log in successfully:
  - **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
  - **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).

8 In the *User Session* section, configure the following options:

- *Session Timeout*: Set a time limit (in minutes) after which users will be disconnected from the hotspot portal and will be required to log on again.
- *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot portal without having to log on again.

9 In the *Location Informatio*n section, configure the following options:

- *Location ID*: Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
  - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
  - network

  The following is an example of what the Location ID entry should look like: isocc=us,cc=1,ac=408,network=RuckusWireless
- *Location Name*: Type the name of the location of the hotspot portal.

10 In *Walled Garden*, click **Create New** to add a walled garden. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account.

In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:

- IP address (for example, 10.11.12.13)

- Exact website address (for example, www.ruckuswireless.com)
- Website address with regular expression (for example, *.ruckuswireless.com, *.com, *)

After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to re-authenticate when they navigate through the page.

11 Click **Create New** to create the hotspot portal of the zone template.

12 Continue to Step 5: Configure the Hotspot 2.0 Service of the Zone Template.

NOTE: For additional steps that you need to perform to ensure that the WISPr hotspot portal works, see Creating and Managing Hotspots.

Step 5: Configure the Hotspot 2.0 Service of the Zone Template

To configure a Hotspot 2.0 service, you will need to create and configure at least one service provider profile and one operator profile. Refer to the *Hotspot 2.0 Reference Guide* for this release for more information.

Step 6: Configure the WLAN Service of the Zone Template

Follow these steps to create and configure a WLAN service of an AP zone.

1. Click *Configuration > AP Zones*.
2. On the sidebar, click **Zone Templates**. The *Zone Templates* page appears.
3. Click the name of the zone template for which you want to create a WLAN service. The *Zone Configuration* page appears.
4. On the sidebar, click **WLAN**.
5. Under the *WLAN Configuration* section, click **Create New**. The form for creating a new WLAN service appears.
6. In the *General Options* section, configure the following options.
   - *Name/SSID*: Type a short name (two to 32 alphanumeric characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the SSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same controller) while still being able to manage the different WLANs independently.
   - *HESSID* (optional): Type the homogenous extended service set identifier (SSID). The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value must be identical to one of the BSSIDs in the homogeneous ESS.
   - *Description*: Type a brief description of the qualifications/purpose for this WLAN (for example, Engineering or Voice).
7. In *WLAN Usage*, configure the following:
   - In *Access Network*, select the **Tunnel WLAN traffic through Ruckus GRE** check box if you want to tunnel the traffic from this WLAN back to the controller. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted

wireless connection (for example, VoIP devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the controller.

- In *Core Network Type* (only visible if you selected the **Tunnel WLAN traffic through Ruckus GRE** check box), select one of the following core network types:
    - Bridge
    - L3oGRE
    - L2oGRE
    - TTG+PDG
    - PMIPv6
    - Mixed Tunnel Mode
- In *Authentication Type*, click one of the following options:
    - **Standard usage (For most regular wireless networks)**: This is a regular WLAN suitable for most wireless networks.
    - **Hotspot (WISPr)**: Click this option if you want to use a hotspot portal that you previously created. For instructions on how to create a hotspot portal, see Working with Hotspot (WISPr) Portals.
    - **Guest Access + Hotspot 2.0 Onboarding**: Click this option if you want guest users to use this WLAN. After you complete creating this WLAN for guest access, you can start generating guest passes. See Working with Guest Users.
    - **Web Authentication**: Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect. See Working with Web Authentication Portals.
    - **Hotspot 2.0**: Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See Working with Hotspot 2.0 Services.

8. In *Authentication Options*, click the authentication method by which users will be authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.

    - **Open (Default)**: No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.

- **802.1x EAP**: A very secure authentication/encryption method that requires a back-end authentication server, such as a RADIUS server. Your choice mostly depends on the types of authentication the client devices support and your local network authentication environment.
- **MAC Address**: Authenticate clients by MAC address. MAC address authentication requires a RADIUS server and uses the MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
  - Use user defined text as authentication password (default is device MAC address)
  - Set device MAC address in 802.1x format 00-10-A4-23-19-C0. (The default is 0010a42319c0).

9 In *Method* under *Encryption Options*, select an encryption method to use. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.

- **WPA**: Standard Wi-Fi Protected Access with either TKIP or AES encryption.
- **WPA2**: Enhanced WPA encryption using stronger TKIP or AES encryption algorithm.
- **WPA-Mixed**: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **WEP-64**: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.
- **WEP-128**: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- **None**: No encryption; traffic is sent in clear text.

CAUTION! If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

10 In *Authentication & Accounting Service*, configure the following options:

- **Authentication Service**: This option appears only when 802.1x EAP is selected as the authentication method. Select the authentication server that you want to use for this WLAN. Only AAA servers that you previously added appear here.
- **Accounting Service**: Select the RADIUS Accounting server that you want to use as a proxy for the controller from the drop-down list, You must have added a RADIUS Accounting server previously (see Step 3: Configure the AAA Servers of the Zone Template).

11 In *Hotspot (WISPr) Portal*, select the hotspot that you want this WLAN to use. This option appears only when Hotspot (WISPr) is selected as the WLAN usage type. This hotspot portal may be the hotspot that you created in Step 5: Configure the Hotspot 2.0 Service of the Zone Template. Additionally, if you added a RADIUS accounting server to the controller earlier, you can enable RADIUS proxy accounting by selecting the Enable RADIUS Accounting Proxy check box.

12 In *Options*, configure the following options:

- *Wireless Client Isolation*: Wireless client isolation enables subnet restrictions for connected clients. Click **Enable** if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is **Disable**.
- *Priority*: Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to "Low." By default, all WLANs are set to high priority.

13 In *RADIUS Options*, click + (plus sign) to display the options, and then configure the following:

- *RADIUS NAS ID*: Select how to the RADIUS server will identify the AP:
  - WLAN BSSID
  - AP MAC
  - User-defined
- RADIUS NAS Request Timeout: Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *RADIUS NAS Max Number of Retries*: Type the number of failed connection attempts after which the controller will fail over to the backup RADIUS server.

- *RADIUS NAS Reconnect Primary*: If the controller fails over to the backup RADIUS server, this is the interval (in minutes) at which the controller will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID*: Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

14 In *Advanced Options*, configure the following options:

- *User Traffic Profile:* If you want this WLAN to use a user traffic profile that you previously created, select it from the drop-down menu. Otherwise, select **System Default**. For more information, see Working with User Traffic Profiles.
- *L2 Access Control*: If you want this WLAN to use an L2 access control policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with Device Policies.
- *Device Policy*: If you want this WLAN to use a device policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with Device Policies.
- *Access VLAN*: By default, all wireless clients associated with APs that the controller is managing are segmented into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2-4094) in the box.
  - *Enable VLAN Pooling*: If you want to automatically segment large groups of clients (that may or may not be connected to the same SSID) into multiple smaller subgroups using multiple VLANs, select this check box. See About VLAN Pooling for more information.
- *Hide SSID*: Click this option if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.
- *Client Load Balancing*: Improve WLAN performance by enabling load balancing. Load balancing spreads the wireless client load between nearby access points, so that one AP does not get overloaded while another sites idle. Load balancing must be enabled on a per-radio basis. To enable load balancing, select the **Enable loading balancing on [2.4GHz or 5GHz]** check box, and then set or accept the default *Adjacent Radio Threshold* (50dB for the 2.4GHz radio and 43dB for the 5GHz radio).

- *Proxy ARP*: When enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (e.g., ARP request and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified.
- *Max Clients*: This option limits the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage.
- *802.11d*: This standard provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. Click this option if you are operating in one of these additional regulatory domains.
- *DHCP Option 82*: Select the **Enable DHCP Option 82** check box to enable this feature. When this feature is enabled and an AP receives a DHCP request from a wireless client, the AP will encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.
- *Client TX/RX Statistics*: Select the **Ignore statistics from unauthorized clients** check box if you do not want the controller to monitor traffic statistics for unauthorized clients.
- *Inactivity Timeout*: Select the check box and enter a value in seconds (60 to 600) after which idle clients will be disconnected.
- *Client Fingerprinting:* By selecting this check box, the controller will attempt to identify client devices by their operating system, device type and host name, if available. This makes identifying client devices easier on the Dashboard, Monitor and Client Details pages.
- *OFDM Only*: Select the check box to force clients associated with this WLAN to use only Orthogonal Frequency Division Multiplexing (OFDM) to transmit data. OFDM-only allows the client to increase management frame transmission speed from CCK rates to OFDM rates. This feature is implemented per WLAN and only affects the 2.4GHz radio.

- *BSS Min Rate*: Select this check box to set the bss rates of management frames from default rates (CCK rates for 2.4G or OFDM rate – 6Mbps for 5G] to the desired rates. By default, BSS Min Rate is disabled.

NOTE OFDM-only takes higher priority than BSS-minrate. However, OFDM-only relies on BSS-minrate to adjust its rate for management frames.

- *Mgmt Tx Rate*: To set the maximum transmit rate for management frame, select a value (in Mbps) from the drop-down list.
- *DiffServ Profile*: To apply a DiffServ profile to this WLAN service, select a profile that you previously created. See Creating a DiffServ Profile for more information.
- *Service Schedule*: Use the Service Schedule tool to control which hours of the day, or days of the week to enable/disable WLAN service. Options include:
  - **Always On**: Click to enable this WLAN at all times.
  - **Always Off**: Click to disable the WLAN service at all times.
  - **Specific**: Click to set specific hours during which this WLAN will be enabled. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Click on a day of the week to enable/disable this WLAN for the entire day. Colored cells indicate WLAN enabled. Click and drag to select specific times of day. You can also disable a WLAN temporarily for testing purposes, for example.
- *Band Balancing*: To disable band balancing on this WLAN, select the **Do not perform band balancing for this WLAN service** check box. For more information, see Band Balancing.

15 Click **Create New**.

You have completed creating and configuring a zone template.

Exporting a Zone Template

If you are planning to create a zone template with settings that are similar to an existing template, you can simply export the existing zone template, import it as a new template, and then edit the settings. You can save time by doing this, instead of creating a new zone template from scratch.

Follow these steps to export a zone template.

1. Go to *Configuration > AP Zones*.
2. On the sidebar, click **Zone Templates**.
3. Locate the zone template that you want to export.
4. Click the 💾 icon that is in the same row as the zone template that you want to export.
5. Alternatively, select the check box before the zone template name, and then click Export Selected Template(s)
6. Your web browser downloads the zone template from the controller.
7. Go to the default download folder that you have configured for your web browser, and then verify that the zone template file (with `.bak` extension) exists.

You have completed exporting a zone template.

Importing a Zone Template

Follow these steps to import a zone template.

1. Copy the zone template file (with .bak extension) to a computer or network location that you can access from the controller web interface.
2. If you are importing the zone template into the same controller, rename the zone template from which you created the file. If you do not rename the original zone template, the controller will detect that a duplicate zone template exists and the import process will be unsuccessful.
3. To edit a zone template, click the template name on the *Zone Templates* page. When the *Edit Zone Template* form appears, edit the template name, and then click **Apply**.
4. Go to *Configuration > AP Zones*.
5. On the sidebar, click **Zone Templates**.
6. Click **Import**. The *Importing Zone Template* form appears.
7. Click **Browse**, and then browse to the location where you saved the zone template file.

8 Select the file, and then click **Open**.

9 On the *Importing Zone Template* form, click **Apply**. A progress bar appears as the controller imports the zone template file.

When the process is complete, the page refreshes, to reflect the zone template that you imported on the list of zone templates. To edit the zone template, click the template name, and then make the changes that you want.

You have completed importing a zone template.

Deleting a Zone Template

Follow these steps to delete a zone template.

1 Locate the zone template that you want to delete.

2 Click the 🗑 icon that is in the same row as the zone template that you want to delete.

3 Alternatively, select the check box before the zone template name, and then click **Delete selected**.

   The following confirmation message appears:

   ```
   Are you sure you want to delete the selected row?
   ```

4 Click **Yes**. The page refreshes, and then zone template that you deleted disappears from the list.

You have completed deleting a zone template.

Working with WLAN Templates

A WLAN template contains configuration settings (AAA server, hotspot, and WLAN settings) that you can apply to all access points that belong to a particular AP zone.

Unlike zone templates, however, WLAN templates will only overwrite the configuration of access points that have the same WLAN name that is defined in the WLAN template. For example, if an access point has two WLANs named Ruckus1 and Ruckus2, and then you apply a WLAN template that contains settings for a WLAN named Ruckus1, the settings of Ruckus1 on the access point (and any other access point that belongs to the same AP zone) will be overwritten by the settings from the WLAN template. The settings of the Ruckus2 WLAN, however, will remain the same.

This section covers:

- Creating and Configuring a WLAN Template
- Viewing Existing WLAN Templates

- Deleting WLAN Templates

Creating and Configuring a WLAN Template

Creating a WLAN template requires that you create the template and configure the services that will be deployed with the template.

Follow these steps to create a WLAN template.

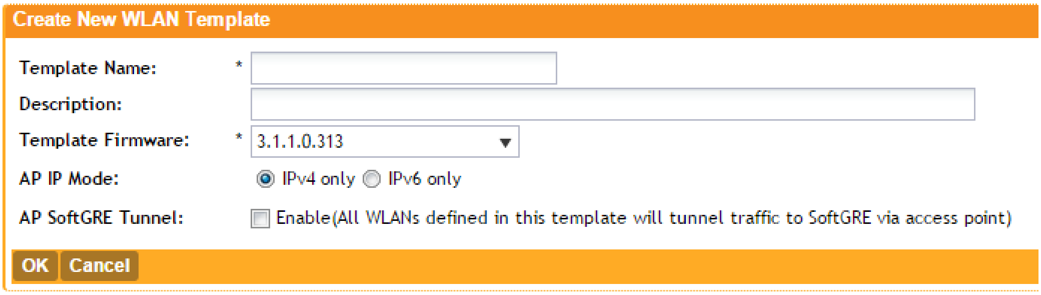
- Step 1: Create the WLAN Template
- Step 2: Configure the AAA Servers for the WLAN Template
- Step 3: Configure the Hotspot (WISPr) Services of the WLAN Template
- Step 4: Configure the Hotspot 2.0 Services of the WLAN Template
- Step 5: Configure the WLAN Services of the WLAN Template

Step 1: Create the WLAN Template

Follow these steps to create a WLAN template.

1. Go to *Configuration > AP Zones*.
2. On the sidebar, click **WLAN Templates**.
3. On the *WLAN Templates* page, click **Create New**. The *Create New WLAN Template* form appears.
4. In *Template Name*, type a name for the WLAN template that you are creating.
5. In *Description*, type a description for this template.
6. In *Template Firmware*, select the controller firmware version to which to apply this template.
7. In *AP IP Mode*, select the IP addressing mode that you want APs (to which this template will applied) to use. Options include:
   - IPv4 Only
   - IPv6 Only
8. In *AP SoftGRE Tunnel*, select the **Enable** check box if you want all WLANs created from this template to tunnel traffic to SoftGRE through the AP.
9. Click **Create New** at the bottom of the form.
10. Continue to Step 2: Configure the AAA Servers for the WLAN Template.

Figure 47. The form for creating a WLAN template



Create New WLAN Template

Template Name:	*	
Description:		
Template Firmware:	*	3.1.1.0.313 ▼
AP IP Mode:		● IPv4 only ○ IPv6 only
AP SoftGRE Tunnel:		□ Enable(All WLANs defined in this template will tunnel traffic to SoftGRE via access point)

Step 2: Configure the AAA Servers for the WLAN Template

Follow these steps to create and configure an AAA server for the WLAN template.

1. Click *Configuration > AP Zones*.
2. On the sidebar, click **WLAN Templates**. The *WLAN Templates* page appears.
3. Click the name of the WLAN template for which you want to create an AAA server.
4. On the sidebar, click **AAA**. The *AAA Servers* page appears.
5. Click **Create New**. The *Create New Zone RADIUS Server* form appears.
6. Configure *General Options*.
   - *Name*: Type a name for the AAA server that you are adding.
   - *Type*: Select the type of AAA server that you have on the network. Options include:
     - RADIUS
     - RADIUS Accounting
     - Active Directory
     - LDAP
   - *Backup RADIUS*: Select the **Enable backup RADIUS server** check box if a secondary RADIUS server exists on the network. Configure the settings in Step 8.
7. In the *Primary Server* section, configure the settings of the primary RADIUS server.
   - *IP Address*: Type the IP address of the AAA server.
   - *Port*: Type the port number of the AAA server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.

- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

8 In the *Secondary Server* section, configure the settings of the secondary RADIUS server.

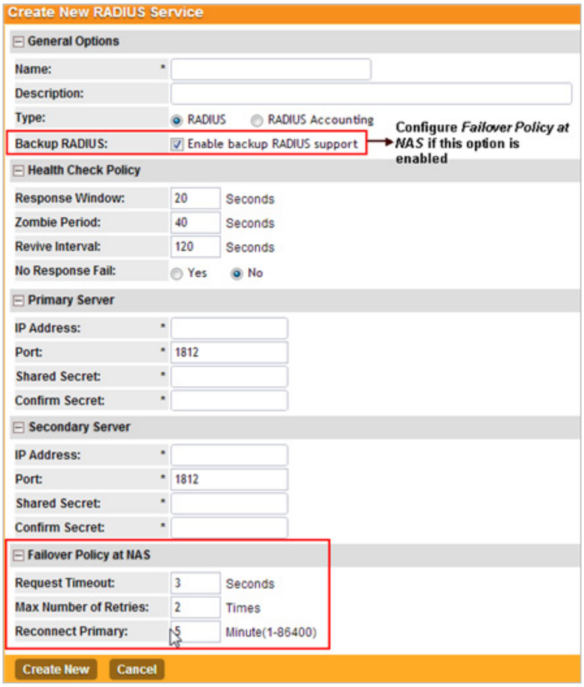
NOTE: The *Secondary Server* section is only visible if you selected the **Enable backup RADIUS server** check box earlier.

- *IP Address*: Type the IP address of the secondary AAA server.
- *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

9 Click **Create New** to create the AAA server for the WLAN template.

10 Continue to Step 3: Configure the Hotspot (WISPr) Services of the WLAN Template.

Figure 48. The Create New RADIUS Server form



Create New RADIUS Service

⊟ General Options

Name: *	
Description:	
Type:	● RADIUS ○ RADIUS Accounting
Backup RADIUS:	☑ Enable backup RADIUS support

Configure *Failover Policy at NAS* if this option is enabled

⊟ Health Check Policy

Response Window:	20 Seconds
Zombie Period:	40 Seconds
Revive Interval:	120 Seconds
No Response Fail:	○ Yes ● No

⊟ Primary Server

IP Address: *	
Port: *	1812
Shared Secret: *	
Confirm Secret: *	

⊟ Secondary Server

IP Address: *	
Port: *	1812
Shared Secret: *	
Confirm Secret: *	

⊟ Failover Policy at NAS

Request Timeout:	3 Seconds
Max Number of Retries:	2 Times
Reconnect Primary:	5 Minute(1-86400)

Step 3: Configure the Hotspot (WISPr) Services of the WLAN Template

NOTE: If you are not providing a hotspot portal to users, skip this section.

NOTE: This section describes the basic settings that you need to configure to include a hotspot portal in the zone template. If you need more information about hotspots, including third party prerequisites, see Creating and Managing Hotspots.

Follow these steps to configure the hotspot settings of the WLAN template.

1 Click *Configuration* > *AP Zones*.

2 On the sidebar, click **WLAN Templates**. The *WLAN Templates* page appears.

3 Click the name of the WLAN template for which you want to create a hotspot portal.

4 On the sidebar, click **Hotspot (WISPr)**. The *Hotspot (WISPr) Portal* page appears.

5 Click **Create New**. The *Create New Hotspot Portal* form appears.

6 In the *General Options* section, configure the following options:

- *Name*: Type a name for the hotspot portal.
- *Description*: Type a description for the hotspot portal.

7 In the *Redirection* section, configure the following options:

- *Smart Client Support*: Select one of the following options:
  - **None**: Select this option to disable Smart Client support on the hotspot portal.
  - **Enable**: Selection this option to enable Smart Client support.
  - **Only Smart Client Allowed**: Select this option to allow only Smart Clients to connect to the hotspot portal.

  For more information, see Configuring Smart Client Support.
- In *Logon URL*, type the URL of the subscriber portal (the page where hotspot users can log in to access the hotspot portal). For more information, see Configuring the Logon URL.
- In *Start Page*, set where users will be redirected after they log in successfully:
  - **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
  - **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).

8 In the *User Session* section, configure the following options:

- *Session Timeout*: Set a time limit (in minutes) after which users will be disconnected from the hotspot portal and will be required to log on again.
- *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot portal without having to log on again.

9 In the *Location Information* section, configure the following options:

- *Location ID*: Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
  - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.

  - network

  The following is an example of what the Location ID entry should look like: isocc=us,cc=1,ac=408,network=RuckusWireless

- *Location Name*: Type the name of the location of the hotspot portal.

10 In *Walled Garden*, click **Create New** to add a walled garden. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account.

In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:

- IP address (for example, 10.11.12.13)
- Exact website address (for example, www.ruckuswireless.com)
- Website address with regular expression (for example, *.ruckuswireless.com, *.com, *)

After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to re-authenticate when they navigate through the page.

11 Click **Create New** to create the hotspot portal of the WLAN template.

12 Continue to Step 4: Configure the Hotspot 2.0 Services of the WLAN Template.

Step 4: Configure the Hotspot 2.0 Services of the WLAN Template

To configure a Hotspot 2.0 service, you will need to create and configure at least one service provider profile and one operator profile. See *Hotspot 2.0 Reference Guide* for this release for information on how to configure Hotspot 2.0 services using a WLAN template.

Step 5: Configure the WLAN Services of the WLAN Template

Follow these steps to create and configure a WLAN service of a WLAN template.

1. Click *Configuration > AP Zones.*
2. On the sidebar, click **WLAN Templates**. The *WLAN Templates* page appears.
3. Click the name of the WLAN template for which you want to create a WLAN service.
4. On the sidebar, click **WLAN**.
5. Click **Create New**. The form for creating a new WLAN service appears.
6. In the *General Options* section, configure the following options.
   - *Name/SSID*: Type a short name (two to 32 alphanumeric characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the SSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same controller) while still being able to manage the different WLANs independently.
   - *HESSID*: Type the homogenous extended service set identifier (HESSID). The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value must be identical to one of the BSSIDs in the homogeneous ESS.
   - *Description*: Type a brief description of the qualifications/purpose for this WLAN (for example, Engineering or Voice).
7. In *WLAN Usage*, configure the following:
   - In *Access Network*, select the **Tunnel WLAN traffic through Ruckus GRE** check box if you want to tunnel the traffic from this WLAN back to the controller. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the controller.
   - In *Authentication Type*, click one of the following options:
     - **Standard usage (For most regular wireless networks)**: This is a regular WLAN suitable for most wireless networks.

    - **Hotspot (WISPr)**: Click this option if you want to use a hotspot portal that you previously created. For instructions on how to create a hotspot portal, see Working with Hotspot (WISPr) Portals.
    - **Guest Access + Hotspot 2.0 Onboarding**: Click this option if you want guest users to use this WLAN. After you complete creating this WLAN for guest access, you can start generating guest passes. See Working with Guest Users.
    - **Web Authentication**: Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect. See Working with Web Authentication Portals.
    - **Hotspot 2.0**: Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See Working with Hotspot 2.0 Services.

8. In *Authentication Options*, click the authentication method by which users will be authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.
    - **Open (Default)**: No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
    - **802.1x EAP**: A very secure authentication/encryption method that requires a back-end authentication server, such as a RADIUS server. Your choice mostly depends on the types of authentication the client devices support and your local network authentication environment.
    - **MAC Address**: Authenticate clients by MAC address. MAC address authentication requires a RADIUS server and uses the MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
        - Use user defined text as authentication password (default is device MAC address)
        - Set device MAC address in 802.1x format 00-10-A4-23-19-C0. (The default is 0010a42319c0).
9. In *Method* under *Encryption Options*, select an encryption method to use. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.
    - **WPA**: Standard Wi-Fi Protected Access with either TKIP or AES encryption.

- **WPA2**: Enhanced WPA encryption using stronger TKIP or AES encryption algorithm.
- **WPA-Mixed**: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **WEP-64**: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.
- **WEP-128**: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- **None**: No encryption; traffic is sent in clear text.

CAUTION! If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

10 In *Authentication & Accounting Service*, configure the following options:

- **Authentication Service**: This option appears only when 802.1x EAP is selected as the authentication method. Select the authentication server that you want to use for this WLAN. Only AAA servers that you previously added appear here.
- **Accounting Service**: Select the RADIUS Accounting server that you want to use as a proxy for the controller from the drop-down list, You must have added a RADIUS Accounting server previously (see Step 2: Configure the AAA Servers for the WLAN Template).

11 In *Hotspot (WISPr) Portal*, select the hotspot that you want this WLAN to use. This option appears only when Hotspot (WISPr) is selected as the WLAN usage type. This hotspot portal may be the hotspot that you created in Step 3: Configure the Hotspot (WISPr) Services of the WLAN Template. Additionally, if you added a RADIUS accounting server to the controller earlier, you can enable RADIUS proxy accounting by selecting the Enable RADIUS Accounting Proxy check box.

12 In *Options*, configure the following options:

- *Wireless Client Isolation*: Wireless client isolation enables subnet restrictions for connected clients. Click **Enable** if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is **Disable**.

- *Priority*: Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to "Low." By default, all WLANs are set to high priority.

13 In *RADIUS Options*, click + (plus sign) to display the options, and then configure the following:

- *RADIUS NAS ID*: Select how to the RADIUS server will identify the AP:
  - WLAN BSSID
  - AP MAC
  - User-defined
- *RADIUS NAS Request Timeout*: Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *RADIUS NAS Max Number of Retries*: Type the number of failed connection attempts after which the controller will fail over to the backup RADIUS server.
- *RADIUS NAS Reconnect Primary*: If the controller fails over to the backup RADIUS server, this is the interval (in minutes) at which the controller will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID*: Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

14 In *Advanced Options*, click + (plus sign) to display the options, and then configure the following options:

- *User Traffic Profile:* If you want this WLAN to use a user traffic profile that you previously created, select it from the drop-down menu. Otherwise, select **System Default**. For more information, see Working with User Traffic Profiles.
- *L2 Access Control*: If you want this WLAN to use an L2 access control policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with L2 Access Control Policies.
- *Device Policy*: If you want this WLAN to use a device policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**. For more information, see Working with Device Policies.

- *Access VLAN*: By default, all wireless clients associated with APs that the controller is managing are segmented into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2-4094) in the box.
  - *Enable VLAN Pooling*: If you want to automatically segment large groups of clients (that may or may not be connected to the same SSID) into multiple smaller subgroups using multiple VLANs, select this check box. See About VLAN Pooling for more information.
- *Hide SSID*: Select this check box if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.
- *Client Load Balancing*: To disable client load balancing on this WLAN, select the **Do not perform client load balancing for this WLAN service check** box. For more information, see Client Load Balancing.
- *Proxy ARP*: Select this check box to enable proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP request and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified.
- *Max Clients*: This option limits the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage.
- *802.11d*: Select this check box to enable this standard on this WLAN. 802.11d provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. Click this option if you are operating in one of these additional regulatory domains.
- *Force DHCP*: Enable this option to force clients to obtain a valid IP address from DHCP within the specified number of seconds. This prevents clients configured with a static IP address from connecting to the WLAN. Additionally, if a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.

- *DHCP Option 82*: Select the **Enable DHCP Option 82** check box to enable this feature. When this feature is enabled and an AP receives a DHCP request from a wireless client, the AP will encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.
- *Client TX/RX Statistics*: Select the **Ignore statistics from unauthorized clients** check box if you do not want the controller to monitor traffic statistics for unauthorized clients.
- *Inactivity Timeout*: Select this check box and enter a value in seconds (60 to 600) after which idle clients will be disconnected.
- *Client Fingerprinting:* By selecting this check box, the controller will attempt to identify client devices by their operating system, device type and host name, if available. This makes identifying client devices easier on the Dashboard, Monitor and Client Details pages.
- *OFDM Only*: Select the check box to force clients associated with this WLAN to use only Orthogonal Frequency Division Multiplexing (OFDM) to transmit data. OFDM-only allows the client to increase management frame transmission speed from CCK rates to OFDM rates. This feature is implemented per WLAN and only affects the 2.4GHz radio.
- *BSS Min Rate*: Select this check box to set the bss rates of management frames from default rates (CCK rates for 2.4G or OFDM rate – 6Mbps for 5G] to the desired rates. By default, BSS Min Rate is disabled.

NOTE OFDM-only takes higher priority than BSS-minrate. However, OFDM-only relies on BSS-minrate to adjust its rate for management frames.

- *Mgmt Tx Rate*: To set the maximum transmit rate for management frame, select a value (in Mbps) from the drop-down list.
- *Service Schedule*: Use the Service Schedule tool to control which hours of the day, or days of the week to enable/disable WLAN service. Options include:
  - **Always On**: Click this enable this WLAN at all times.
  - **Always Off**: Click this option to disable the WLAN service at all times.

- **Specific**: Click this to set specific hours during which this WLAN will be enabled. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Click on a day of the week to enable/disable this WLAN for the entire day. Colored cells indicate WLAN enabled. Click and drag to select specific times of day. You can also disable a WLAN temporarily for testing purposes, for example.

- *Band Balancing*: To disable band balancing on this WLAN, select the **Do not perform band balancing for this WLAN service** check box. For more information, see Band Balancing.

15 Click **OK** at the bottom of the form.

You have completed creating and configuring a WLAN template.

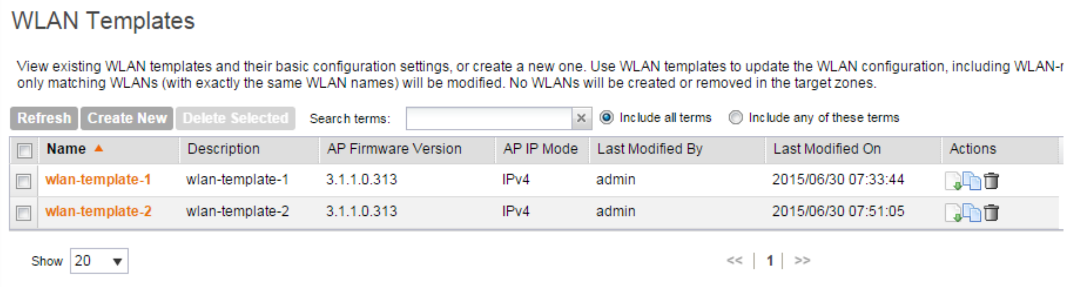
Viewing Existing WLAN Templates

Follow these steps to view the list of WLAN templates created.

1 Click *Configuration* > *AP Zones*.

2 On the sidebar, click **WLAN Templates**. The *WLAN Templates* page appears and displays the details of WLAN templates that have been configured on the controller.

Figure 49. List view of WLAN templates



WLAN Templates

View existing WLAN templates and their basic configuration settings, or create a new one. Use WLAN templates to update the WLAN configuration, including WLAN-r
only matching WLANs (with exactly the same WLAN names) will be modified. No WLANs will be created or removed in the target zones.

Search terms: ● Include all terms ○ Include any of these terms

□	Name ▲	Description	AP Firmware Version	AP IP Mode	Last Modified By	Last Modified On	Actions
□	wlan-template-1	wlan-template-1	3.1.1.0.313	IPv4	admin	2015/06/30 07:33:44	
□	wlan-template-2	wlan-template-2	3.1.1.0.313	IPv4	admin	2015/06/30 07:51:05	

Show 20 ▼ << | 1 | >>

Deleting WLAN Templates

You can delete a single or multiple WLAN templates simultaneously. Follow these steps to delete a single or multiple WLAN templates.

1 Go to *Configuration* > *AP Zones*.

2 On the sidebar, click **WLAN Templates**. The *WLAN Templates* page appears.

To delete a single WLAN template, follow these steps:

a From the list of existing WLAN templates, locate the template that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the WLAN template. A confirmation message appears.

c Click **Yes**. The page refreshes and the WLAN template that you deleted disappears from the list.

To delete multiple WLAN templates simultaneously, follow these steps:

a From the list of existing WLAN templates, locate the templates that you want to delete.

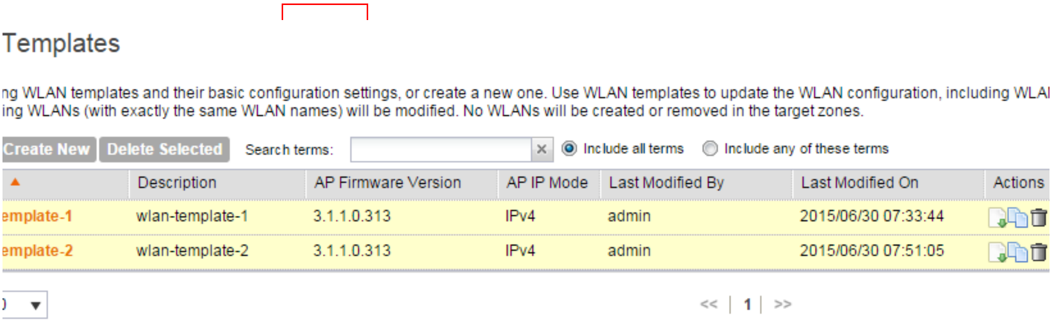
b Select the check boxes before the templates that you want delete.

c Click **Delete Selected**. A confirmation message appears.

d Click **Yes**. The page refreshes and the AAA servers that you deleted disappears from the list.

You have completed deleting single or multiple WLAN templates.

Figure 50. Deleting multiple WLAN templates simultaneously



Templates

ng WLAN templates and their basic configuration settings, or create a new one. Use WLAN templates to update the WLAN configuration, including WLAI
ing WLANs (with exactly the same WLAN names) will be modified. No WLANs will be created or removed in the target zones.

Create New | Delete Selected | Search terms: ● Include all terms ○ Include any of these terms

▲	Description	AP Firmware Version	AP IP Mode	Last Modified By	Last Modified On	Actions
emplate-1	wlan-template-1	3.1.1.0.313	IPv4	admin	2015/06/30 07:33:44	
emplate-2	wlan-template-2	3.1.1.0.313	IPv4	admin	2015/06/30 07:51:05	

<< | 1 | >>

Working with Registration Rules

Registration rules enable the controller to assign an AP to an AP zone automatically based on the rule that the AP matches.

This section describes the following tasks:

- Creating a Registration Rule
- Configuring Registration Rule Priorities
- Deleting a Registration Rule

NOTE: A registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected on disconnected state and whether it belongs to the Staging Zone or any other zone), the controller will assign the AP to its last known AP zone.

Creating a Registration Rule

Follow these steps to create a registration rule.

1 Go to *Configuration > AP Zones*.

2 On the sidebar, click **AP Registration Rules**. The AP Registration Rules page appears.

3 Click **Create New**. The *AP Registration Rule* form appears.

4 In *Rule Description*, type a name that you want to assign to this rule.

5 In *Rule Type*, click the basis upon which you want to create the rule. Options include:

NOTE: The format of the IP address or addresses that you need to enter here depends on the AP IP mode that you selected when you created the AP zone to which this rule will be assigned. If you selected **IPv4 Only**, enter an IPv4 address. If you selected **IPv6 Only**, enter an IPv6 address.

- **IP Address Range**: If you select this option, enter the From (starting) and To (ending) IP address that you want to use.
- **Subnet**: If you select this option, enter the IP address and subnet mask pair to use for matching.
- **GPS Coordinates**: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.
- **Provision Tag**: If the access points that are joining the controller have been configured with provision tags, click the **Provision Tag** option, and then type a tag name in the **Provision Tag** box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

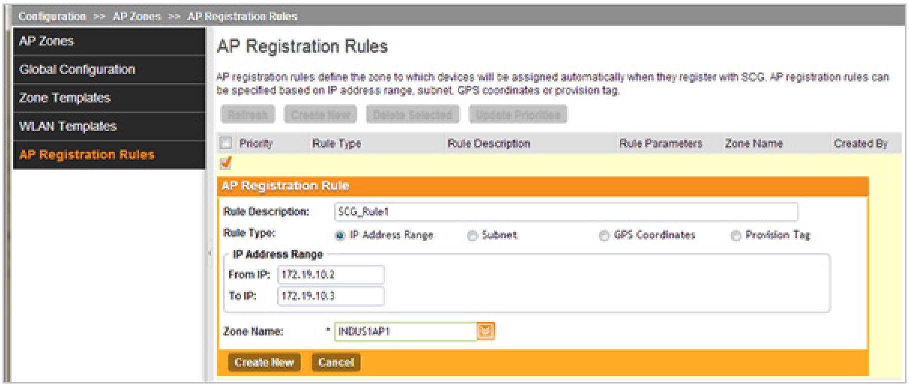
NOTE: Provision tags can be configured on a per-AP basis from the access point's command line interface.

6 In *Zone Name*, click the down arrow to display available AP zones, and then click the AP zone to which APs that match this rule will be assigned.

- Click **Create New**. A progress bar appears as the controller saves the AP registration rule.

When the process is complete, the page refreshes, and then registration rule that you created appears on the *AP Registration Rules* page.

Figure 51. Creating an AP registration rule



AP Registration Rules

AP registration rules define the zone to which devices will be assigned automatically when they register with SCG. AP registration rules can be specified based on IP address range, subnet, GPS coordinates or provision tag.

AP Registration Rule

Rule Description: SCG_Rule1

Rule Type: ● IP Address Range ○ Subnet ○ GPS Coordinates ○ Provision Tag

IP Address Range

From IP: 172.19.10.2

To IP: 172.19.10.3

Zone Name: * INDUS1AP1

To create another registration rule, repeat the preceding steps. You can create as many registration rules as you need to manage the APs on the network.

Configuring Registration Rule Priorities

The controller applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority). If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the controller assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the registration rule priorities.

1 Go to *Configuration* > *AP Zones*.

2 On the sidebar, click **AP Registration Rules**. The *AP Registration Rules* page appears and displays the rules that you have created.

3 Change the priority of each registration rule as required.

4 To give a rule higher priority, move it up the table by clicking the ⬆ (up-arrow) icon that is in the same row as the rule name.

5 To give a rule lower priority, move it down the table by clicking the ⬇ (down-arrow) icon that is in the same row as the rule name.

When you finish configuring the rule priority, click **Update Priorities** to save your changes.

Deleting a Registration Rule

Follow these steps to delete a registration rule.

1. On the *AP Registration Rules* page, select the check box that is in the same row as the registration rule that you want to delete.
2. Click 🗑 (trash bin icon). A confirmation message appears.
3. Click **Yes** to confirm that you want to delete the registration rule.

The *AP Registration Rules* page refreshes, and then the registration rule that you deleted disappears from the list.

Working with 3rd Party AP Zones 4

The controller connects to 3rd party AP zones the same way as it does to Ruckus Wireless AP zones. The controller receives RADIUS messages directly from 3rd party APs and supports multiple 3rd party AP zones. It connects to 3rd party AP's using QinQ for data traffic. Access network interface to APs from the controller via QinQ contains UE MAC. 3rd party APs are managed by 3rd party AP controller where the controller acts as a wireless access gateway (WAG).

APs are grouped under 3rd party AP zones based on Access C-VLAN and S-VLAN range. Each 3rd party AP zone is identified by a list of IP addresses, ranges, and subnets used by the APs for sending RADIUS traffic to the controller. A 3rd party AP zone ID" is generated internally for each zone. Each 3rd party AP zone is associated with a single "3rd party AP zone".

Supported authentication and accounting procedures are the same as Ruckus Wireless APs.

This section covers:

- 3rd Party AP Zone Types
- Adding a 3rd Party AP Zone
- Viewing Existing 3rd Party AP Zones
- Deleting a 3rd Party AP Zone

3rd Party AP Zone Types

The following configuration combinations determine the type of 3rd party AP zone.

1. Access network type (L2oGRE, Q-in-Q L2)
2. Core network type (TTG+PDG, Bridge)
3. Authentication method (Open, 802.1X, WISPr)

The following table lists the configuration combinations.

Table 4. Configuration combinations and requirements

Access (Southbound)	Core (Northbound)	Authentication	Requirements
Q-in-Q L2	TTG+PDG	802.1X	You need to configure: • Authentication and Accounting Services • User Traffic Profile - TTG+PDG • Core network VLAN Options • Access Network Q-in-Q VLAN Tags • RADIUS Client Options
Q-in-Q L2	Bridge	• Hotspot (WISPr) • Open	You need to configure: • User Traffic Profile - forwarding profile is required • Core Network VLAN Options • Access Network Q-in-Q VLAN Tags

Adding a 3rd Party AP Zone

Follow these steps to add a 3rd Party AP zone service.

1. Go to *Configuration > 3rd Party AP Zones*. This section displays the details of 3rd Party AP Zones servers that have been configured on the controller.
2. Click **Create New**.
3. In *Name*, type a name for the 3rd party AP zone that you are creating.
4. In *Description*, type a brief description of the service that you are creating. This is an optional field.
5. In *Access Network*, select either **QinQ Layer 2** (default) or **L2oGRE**.
6. In *Core Network*, select either **Bridge** or **TTG+PDG** (default).

7 In *Authentication Service Type*, select either **Open** (default) or **Hotspot (WISPr)**.

8 In Access Network Traffic Profile, there should be at least one network traffic profile should be specified for each 3rd Party AP Zone. When a new 3rd party AP zone is created, the default network traffic profile specified for the zone is SCG Factory Default network. This is in case the administrator has not specified any other profile.

9 In *User Traffic Profile,* there should be at least one user traffic profile specified for each 3rd party AP zone.

10 In *Core Network VLAN Options*, configure the following options:

- If the core network is Bridge and the access network is Q-in-Q Layer 2:
  - Select the **Enable the Core Network VLAN Type**.
  - Set *Core Network VLAN Mapping Type* to **Strip Access S-VLAN, preserve Access V-LAN.**
- If the core network is TTG+PDG and the access network is Q-in-Q Layer 2:
  - Select the **Enable the Core Network VLAN Type**.
  - Set *Core Network VLAN Mapping Type* to **Strip Access S-VLAN, preserve Access V-LAN**.
- If the core network is Bridge and the access network is L2oGRE:
  - Ensure that the **Enable the Core Network VLAN Type** is not selected.
  - Set *Core Network VLAN Mapping Type* to **Preserve Access VLAN**.
- If core network is Bridge and the access network is L2oGRE:
  - Select the **Enable the Core Network VLAN Type**.
  - Set *Core Network VLAN Mapping Type* to **Add Fixed SVLAN, Preserve Access VLAN as C-VLAN**.

11 In Access Network Q-in-Q VLAN tags configuration is required when access network type is Q-in-Q L2. Access network Q-in-Q VLAN tags configuration defines a list of Q-in-Q tags. These VLAN tags are used to identify the 3rd Party AP Zone for the UE traffic. The controller does not allow duplicate C-VLAN tags within the same zone or across the zones.

- Access Network Source IPs configuration is required when access network type is L2oGRE. Access network IP addresses configuration defines a list of IP ranges. These IP ranges identify the 3rd Party AP Zone for the UE traffic. The controller does not allow overlapping IP ranges within the same zone or across the zones.

12 RADIUS client options needs to be configured if the core network type is TTG+PDG and authentication type is 802.1X. RADIUS client default secret is required. The IP ranges should not be overlapping within the same zone or across zones. The share secret for each IP range is not required.

13 Click **Create New**.

You have completed adding a new 3rd party AP zone service.

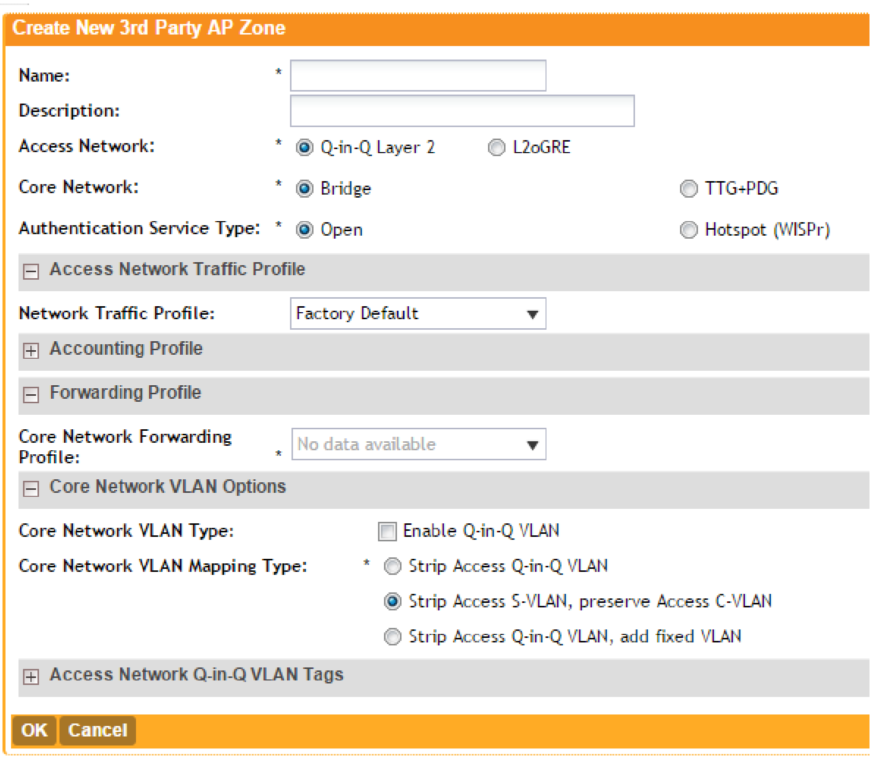


Figure 52. The Create New 3rd Party AP Zone form

Create New 3rd Party AP Zone

Name: *

Description:

Access Network: * ● Q-in-Q Layer 2 ○ L2oGRE

Core Network: * ● Bridge ○ TTG+PDG

Authentication Service Type: * ● Open ○ Hotspot (WISPr)

⊟ Access Network Traffic Profile

Network Traffic Profile: Factory Default ▼

⊞ Accounting Profile

⊟ Forwarding Profile

Core Network Forwarding Profile: * No data available ▼

⊟ Core Network VLAN Options

Core Network VLAN Type: □ Enable Q-in-Q VLAN

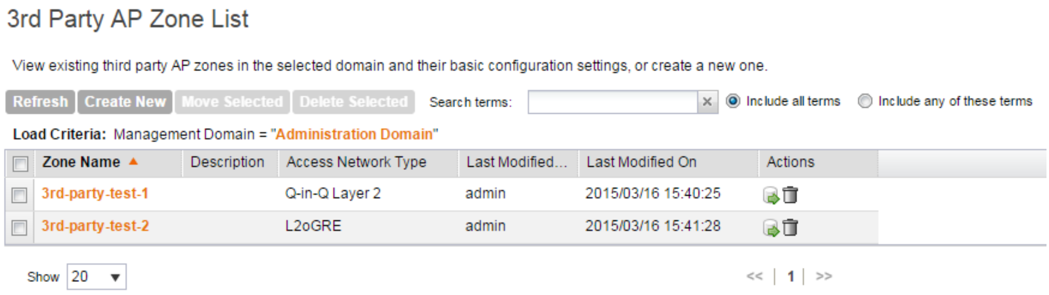
Core Network VLAN Mapping Type: * ○ Strip Access Q-in-Q VLAN
● Strip Access S-VLAN, preserve Access C-VLAN
○ Strip Access Q-in-Q VLAN, add fixed VLAN

⊞ Access Network Q-in-Q VLAN Tags

Viewing Existing 3rd Party AP Zones

To view a list of 3rd party AP zones that have been created, go to *Configuration > 3rd Party AP Zones*. The 3rd party AP zones that have been configured on the controller appear on the list.

Figure 53. A list of existing 3rd party AP zones appears



3rd Party AP Zone List

View existing third party AP zones in the selected domain and their basic configuration settings, or create a new one.

Load Criteria: Management Domain = "Administration Domain"

□	Zone Name ▲	Description	Access Network Type	Last Modified...	Last Modified On	Actions
□	3rd-party-test-1		Q-in-Q Layer 2	admin	2015/03/16 15:40:25	
□	3rd-party-test-2		L2oGRE	admin	2015/03/16 15:41:28	

Deleting a 3rd Party AP Zone

Follow these steps to delete a 3rd party AP zone.

1 In the *3rd Party AP Zone* section, locate the AP zone that you want to delete.

2 Under the *Actions* column, click the icon 🗑 that is in the same row as the zone name. A confirmation message appears.

3 Click **Yes**.

4 The page refreshes, and the AP zone that you deleted disappears from the *3rd Party Zone List* page.

You have completed deleting a 3rd party AP zone.

Managing Access Points

5

In this chapter:

- Overview of Access Point Configuration
- Viewing Managed Access Points
- Provisioning and Swapping Access Points
- Editing AP Configuration
- Editing Swap Configuration
- Moving a Single Access Point to a Different AP Zone
- Moving Multiple Access Points to a Different AP Zone
- Deleting an Access Point

Overview of Access Point Configuration

Once you have created registration rules and the AP zones to which joining access points can be assigned automatically, access points will be able to join or register with the controller automatically. After an access point registers successfully with the controller, you can update its configuration by following the steps described in this section.

Viewing Managed Access Points

After an access point registers successfully with the controller, it appears on the Access Points page, along with other managed access points. Follow these steps to view a list of managed access points.

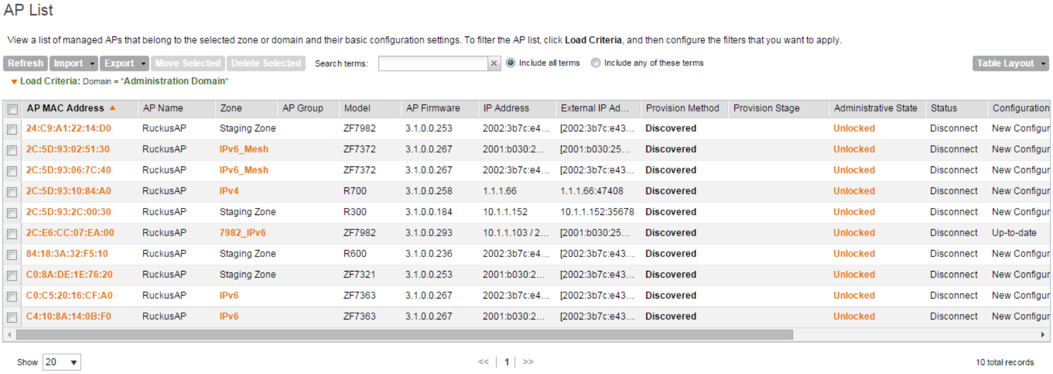
1. Go to *Configuration* > *Access Points*. A list of access points that are being managed by the controller appears on the Access Points in Management Domain page. These are all the access points that belong to all management domains.
2. The list of managed access points displays details about each access point, including its:
   - AP MAC address
   - AP name

- Zone (AP zone)
- Model (AP model)
- AP firmware
- IP address (internal IP address)
- External IP address
- Provision Method
- Provision State
- Administrative Status
- Status
- Configuration Status
- Registered On (date the access point joined the controller network)
- Registration Details
- Registration State
- Actions (actions that you can perform)

NOTE: By default, the *Access Points* page displays 20 access points per page (although you have the option to display up to 250 access points per page). If the controller is managing more than 20 access points, the pagination links at the bottom of the page are active. Click these pagination links to view the succeeding pages on which the remaining access points are listed.

3 To view access points that belong to a particular administration domain, click the name of the administration domain in the domain tree (on the sidebar). The page refreshes, and then displays all access points that belong to that management domain.

Figure 54. Viewing a list of managed access points



AP List

View a list of managed APs that belong to the selected zone or domain and their basic configuration settings. To filter the AP list, click **Load Criteria**, and then configure the filters that you want to apply.

▾ **Load Criteria:** Domain = "Administration Domain"

□	AP MAC Address ▲	AP Name	Zone	AP Group	Model	AP Firmware	IP Address	External IP Ad...	Provision Method	Provision Stage	Administrative State	Status	Configuration
□	24:C9:A1:22:14:D0	RuckusAP	Staging Zone		ZF7982	3.1.0.0.253	2002:3b7c:e4...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur
□	2C:5D:93:02:51:30	RuckusAP	IPv6_Mesh		ZF7372	3.1.0.0.267	2001:b030:2...	[2001:b030:25...	Discovered		Unlocked	Disconnect	New Configur
□	2C:5D:93:06:7C:40	RuckusAP	IPv6_Mesh		ZF7372	3.1.0.0.267	2002:3b7c:e4...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur
□	2C:5D:93:10:84:A0	RuckusAP	IPv4		R700	3.1.0.0.258	1.1.1.66	1.1.1.66:47408	Discovered		Unlocked	Disconnect	New Configur
□	2C:5D:93:2C:00:30	RuckusAP	Staging Zone		R300	3.1.0.0.184	10.1.1.152	10.1.1.152:35678	Discovered		Unlocked	Disconnect	New Configur
□	2C:E6:CC:07:EA:00	RuckusAP	7982_IPv6		ZF7982	3.1.0.0.293	10.1.1.103 / 2...	[2001:b030:25...	Discovered		Unlocked	Disconnect	Up-to-date
□	84:18:3A:32:F5:10	RuckusAP	Staging Zone		R600	3.1.0.0.236	2002:3b7c:e4...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur
□	C0:8A:DE:1E:76:20	RuckusAP	Staging Zone		ZF7321	3.1.0.0.253	2001:b030:2...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur
□	C0:C5:20:16:CF:A0	RuckusAP	IPv6		ZF7363	3.1.0.0.267	2002:3b7c:e4...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur
□	C4:10:8A:14:0B:F0	RuckusAP	IPv6		ZF7363	3.1.0.0.267	2001:b030:2...	[2002:3b7c:e43...	Discovered		Unlocked	Disconnect	New Configur

Provisioning and Swapping Access Points

The controller supports the provisioning and swapping of access points. As an administrator you can:

- Upload a file containing list of AP and the pre-provisioned configuration data for each AP. The controller processes the file and provides details on regarding the import results (including a list of failed APs and failure reasons).
- Modify or delete pre-provisioning data if AP does not connect to the controller
- Monitor the status and stage of the pre-provisioned APs
- Manually lock or unlock APs
- Upload a file containing list of AP pairs for swapping. The controller processes the file and provide the detailed import result (including a list of failed APs and failure reasons).
- Manually enter the AP swap pair
- Delete the swap configuration if AP fails to contact the controller
- Monitor the status and stage of the swapping AP pairs
- Manually swap the APs

Options for Provisioning and Swapping APs

Use the following buttons on the *AP List* page to perform the AP provisioning and swapping.

- **Import Batch Provisioning APs**: Click this button to import the provisioning file. The controller displays the import results. Any errors that occur during the import process will be listed by the controller.
- **Export All Batch Provisioning APs**: Click this button to download a CSV file that lists all APs that have been provisioned. The exported CSV contains the following information:
  - AP MAC Address
  - Zone Name
  - Model
  - AP Name
  - Description
  - Location
  - GPS Coordinates
  - Logon ID
  - Password
  - Administrative State
  - IP Address
  - Network Mask
  - Gateway
  - Primary DNS
  - Secondary DNS

NOTE: The exported CSV file for all batch provisioned APs only contains pre-provisioned APs. It does not contain swapping APs or auto discovered APs.

NOTE: If no APs have been pre-provisioned, you will still be able to export the CSV file but it will be empty (except for the column titles).

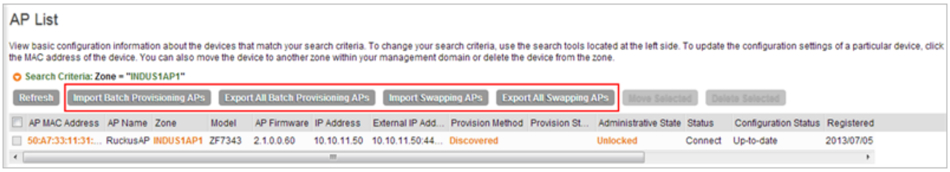
- **Import Swapping APs**: Manually trigger the swapping of two APs by clicking the swap action in the row. You can also edit the pre-provision configuration only if the AP does not connect to the controller. Click the AP MAC address to bring up the configuration edit form, and then select **Pre-provision Configuration**.
- **Export All Batch Swapping APs**: Click this button to download a CSV file that lists all APs that have been swapped. The exported CSV contains the following information:

- Swap In AP MAC
- Swap In AP Model
- Swap Out AP MAC

NOTE: The exported CSV file for batch swapping APs only contains swapping APs. It does not contain pre-provisioned APs or auto discovered APs.

- **Delete Selected**: To delete multiple pre-provisioned APs simultaneously, select the check boxes before the AP MAC addresses, and then click **Delete Selected**. To delete a single pre-provisioned AP, click the 🗑 icon that is in the same row as the AP MAC address. If the AP has not contacted the controller, the AP record disappears from the table. If the AP comes up later, the controller treats it as a discovered AP. If the AP is connected to the controller, the delete operation is similar to the AP delete operation.

Figure 55. Options for provisioning and swapping APs



AP List

View basic configuration information about the devices that match your search criteria. To change your search criteria, use the search tools located at the left side. To update the configuration settings of a particular device, click the MAC address of the device. You can also move the device to another zone within your management domain or delete the device from the zone.

Search Criteria: Zone = "INDUS1AP1"

□	AP MAC Address	AP Name	Zone	Model	AP Firmware	IP Address	External IP Add...	Provision Method	Provision St...	Administrative State	Status	Configuration Status	Registered
□	50:A7:33:11:31:...	RuckusAP	INDUS1AP1	ZF7343	2.1.0.0.60	10.10.11.50	10.10.11.50:44...	Discovered		Unlocked	Connect	Up-to-date	2013/07/05

Understanding How Swapping Works

The following table lists how the controller handles swapping by detailing each stage. For example, you have entered swap configuration as *Swap In: A* and *Swap out: B*.

Table 5. AP swapping stages

Stage	State A	Stage A	State B	Stage B
1. Enter data	Swapping	Not Registered	Approved	Waiting for swap in AP registration
2. AP register	Swapping	Waiting for swapping in	Approved	Waiting for swapping out
3. User swap	Approved	Swapped in	Swapping	Swapped out
4: Second swap	Swapping	Swapped out and waiting for swapping in	Approved	Swapped in and waiting for swapping out

Editing AP Configuration

Follow these steps to update the configuration of a managed access point.

1 On the *AP List* page, locate the access point whose configuration you want to update.

2 Click the MAC address of the access point. The AP configuration form appears.

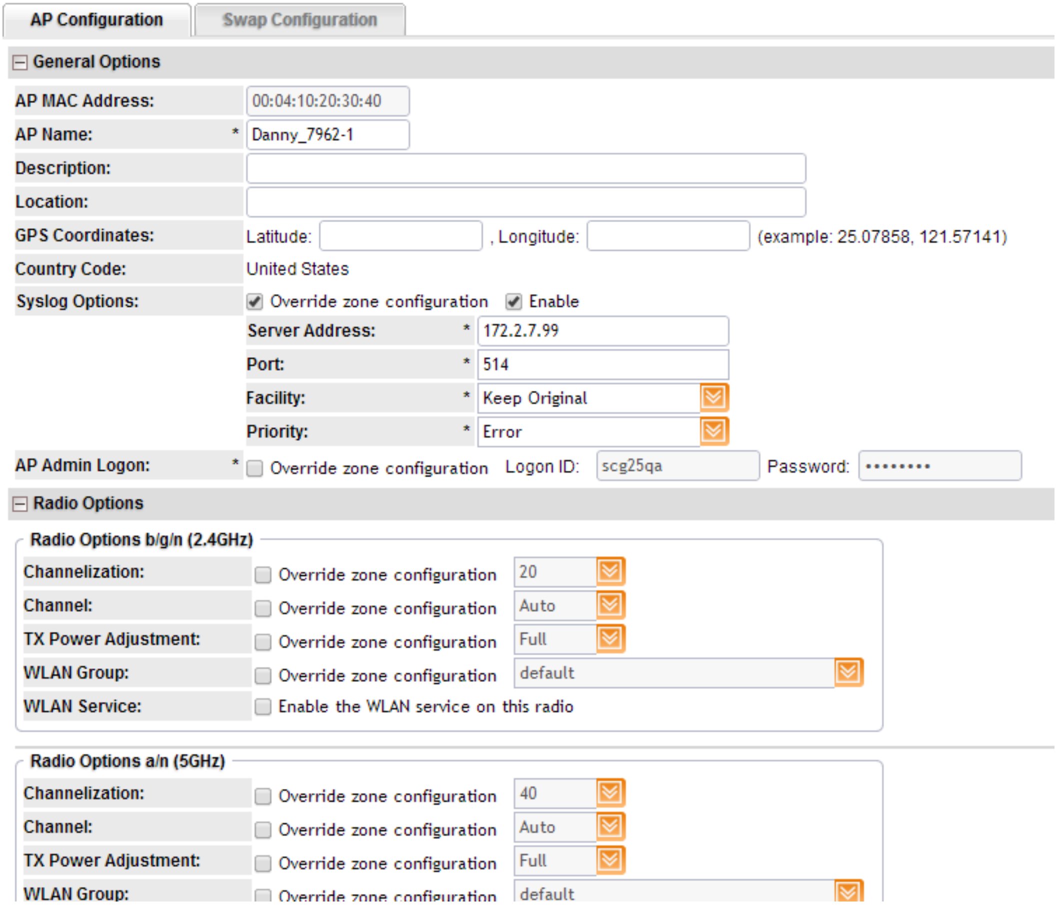
3 Update the access point configuration by modifying the options in the form.

4 Click **OK**.

You have completed editing the AP configuration.

NOTE: The `loc` parameter (which holds the *Location* attribute in the AP configuration) in the controller's Captive Portal redirection to the configured hotspot login portal is encoded using the Hex encoder from the org.apache.commons.codec.binary library. If you have hotspots on the network and you are using an external portal, take note of the encoding mechanism for the `loc` parameter so your external portal can decode it.

Figure 56. The AP Configuration form



AP Configuration | Swap Configuration

⊟ General Options

AP MAC Address:	00:04:10:20:30:40
AP Name: *	Danny_7962-1
Description:	
Location:	
GPS Coordinates:	Latitude: , Longitude: (example: 25.07858, 121.57141)
Country Code:	United States
Syslog Options:	☑ Override zone configuration ☑ Enable
	Server Address: * 172.2.7.99
	Port: * 514
	Facility: * Keep Original
	Priority: * Error
AP Admin Logon: *	□ Override zone configuration Logon ID: scg25qa Password: ••••••••

⊟ Radio Options

Radio Options b/g/n (2.4GHz)

Channelization:	□ Override zone configuration	20
Channel:	□ Override zone configuration	Auto
TX Power Adjustment:	□ Override zone configuration	Full
WLAN Group:	□ Override zone configuration	default
WLAN Service:	□ Enable the WLAN service on this radio	

Radio Options a/n (5GHz)

Channelization:	□ Override zone configuration	40
Channel:	□ Override zone configuration	Auto
TX Power Adjustment:	□ Override zone configuration	Full
WLAN Group:	□ Override zone configuration	default

Editing Swap Configuration

The controller supports the swapping or replacement of a managed AP with a new AP of the same model. This feature is useful when you want to avoid service interruption because you need to replace an AP in the field.

By configuring the swap settings, you can easily and automatically export and apply the settings of the old AP to the new AP.

Follow these steps to configure the swap settings of an AP.

1 On the *AP List* page, locate the access point whose swap configuration you want to update.

2 Click the AP MAC address of the access point.

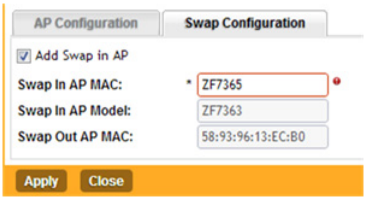
3 Click the **Swap Configuration** tab.

4 Update the access point configuration by modifying the options in the form.

5 Click **OK**.

You have completed editing the swap configuration.

Figure 57. The Swap Configuration form



☑ Add Swap in AP

Swap In AP MAC: * ZF7365

Swap In AP Model: ZF7363

Swap Out AP MAC: 58:93:96:13:EC:B0

Moving a Single Access Point to a Different AP Zone

Follow these steps to move a single access point from its current AP zone to a different one.

NOTE: The AP that you move will inherit the configuration of the new AP zone.

1 On the *AP List* page, locate the access point that you want to move to a different AP zone.

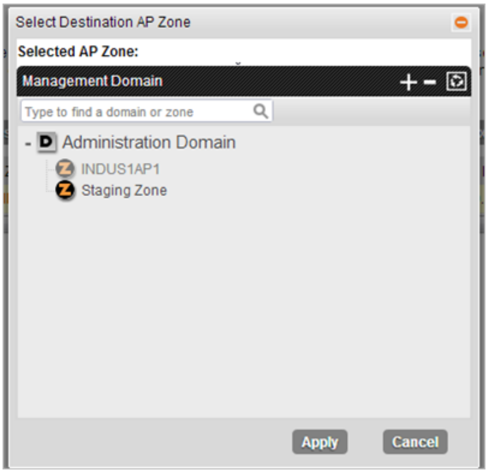
2 Once you locate the access point, click the ➡ icon that is under the *Actions* column. The *Select a Destination AP Zone* form appears.

3 Select the AP zone to which you want to move the access point.

4 Click **OK**.

You have completed moving an access point to a new AP zone.

Figure 58. Selecting and moving an access point



Select Destination AP Zone

Selected AP Zone:

Moving Multiple Access Points to a Different AP Zone

Follow these steps to move multiple access points to a different AP zone simultaneously.

1 On the *AP List* page, locate the access points that you want to move to a different AP zone.

2 Once you locate the access points that you want to move, select the check boxes before their MAC addresses.

3 Click the **Move Selected** button that is above the access points table. The *Select Destination AP Zone* form appears.

4 Select the AP zone to which you want to move the access points.

5 Click **OK**.

You have completed moving the selected access points to a new AP zone.

Deleting an Access Point

Follow these steps to delete an access point that is currently registered with the controller.

1 On the *AP List* page, locate the access point that you want to delete.

2 Once you locate the access point, click the 🗑 icon that is under the *Actions* column. A confirmation message appears.

3 Click **OK**.

The list of managed access points refreshes, and then the access point that you deleted disappears from the list.

NOTE: Wireless clients that are associated with the access point that you deleted will still be able to connect to the network until the next time the access point attempts to rejoin the controller. When these access points attempt to rejoin the controller (through a discovery process), they will be placed in a new AP zone if they match an existing AP registration rule. If they do not match an AP registration rule, they will be placed automatically in the *Staging Zone*, at which point wireless clients associated with these access points will lose network connectivity.

NOTE: After you delete an access point, it could take approximately two minutes before it appears in the Staging Zone again (if the access point does not match an existing AP registration rule). After the access point appears in the Staging Zone, it may continue to broadcast the previous SSID for the next five minutes, after which it will stop.

Configuring Services and Profiles 6

In this chapter:

- Configuring the GGSN/PGW Service
- Configuring Authentication Services
- Configuring HLR Services
- Configuring Diameter Services
- Configuring FTP Services
- Configuring Location Services
- Configuring an SMS Server
- Working with Authentication Profiles
- Working with Accounting Profiles
- Working with Hotspot Profiles
- Working with Network Traffic Profiles
- Working with Forwarding Profiles

Configuring the GGSN/PGW Service

The controller has 3GPP defined Tunnel Terminating Gateway (TTG) functionality, which enables it to act as a gateway between the UE (southbound) and the telecom core (northbound) to tunnel traffic between the UE (user equipment, such as mobile phones). The controller gateway terminates the tunnel, and then transfers the data over to GGSN (Gateway GPRS serving node) implementing the Gn' interface via GTPv1 (Release 6).

The Gn interface is used in controlling the signal between controller and GGSN as well as for tunneling end user data payload within the backbone network between both the nodes.

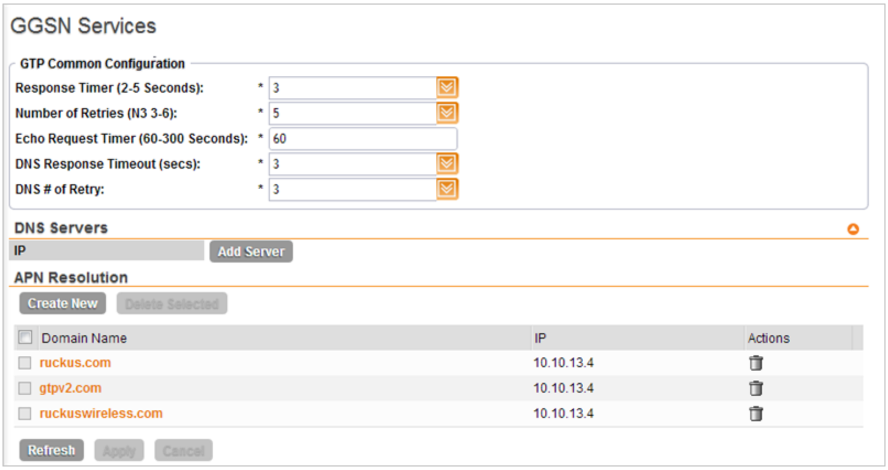
GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between the controller and GGSN. A GTP tunnel is established between the controller and GGSN for a data session initiated from UE.

A GTP tunnel is identified by a pair of IP addresses and a pair of GTP Tunnel End Point Identifiers (TEIDs), where one IP address and TEID is for the SGSN and the other is for GGSN. TEID is a session identifier used by GTP protocol entities in SGSN and GGSN.

GTP separates signaling from payload. Traffic is sorted onto a control plane (GTP-C) for signaling and a user plane (GTP-U) for user data. GTP-C is a tunnel control and management protocol and is used to create, modify and delete tunnels. GTP-U is a tunneling mechanism that provides a service for carrying user data packets.

Clicking *Configuration* > *Services & Profiles* on the main menu displays a sidebar on the left side of the page, which includes *GGSN Services*. Figure 59 shows the GGSN Service configuration page.

Figure 59. The GGSN services configuration page



GGSN Services

GTP Common Configuration

Response Timer (2-5 Seconds): * 3

Number of Retries (N3 3-6): * 5

Echo Request Timer (60-300 Seconds): * 60

DNS Response Timeout (secs): * 3

DNS # of Retry: * 3

DNS Servers

IP

APN Resolution

□ Domain Name	IP	Actions
□ ruckus.com	10.10.13.4	🗑
□ gtpv2.com	10.10.13.4	🗑
□ ruckuswireless.com	10.10.13.4	🗑

Follow these steps to configure the GGSN/PGW service.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar (under *Services*), click **GGSN**.

3 In the *GTP Common Configuration* section, configure the following options:

- *Response Timer*: Define the response expected from GGN server from the drop down list, which ranges from 2 to 5 seconds. The controller will try contacting GGSN during a call establishment.

- *Number of Retries*: Define the number of times that the controller will attempt to contact the GGSN. If all attempts fail, the relevant alarm is raised to confirm the failure of the GGSN path. For example, if the response timer is 3 and the number of retries is 5, it means that for each retry, the controller will attempt to contact the GGSN for 3 seconds.
- *Echo Request Timer*: Define number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure.
- *DNS Response Time*: Specify the maximum time that DNS waits for a response from a signaling request message.
- *DNS # Retry*: specify the maximum number of times that the DNS attempts to send a signaling request.

4 In the *DNS Servers* section, click **Add Server** to add a DNS IP address. If you're adding multiple DNS IP addresses, you can set their priority by clicking the **Move Up** and **Move Down** buttons. DNS servers that are higher up on the list of servers are given higher priority.

5 In the *APN Resolution* section, click **Create New** to define the IP address of the GGSN that should serve the AP. Configure the following options:

- **Domain Name**: Type the GGSN domain name.
- **IP Address**: Type the GGSN IP address.

6 Click **Apply**.

You have completed configuring the GGSN service.

Configuring Authentication Services

An authentication service defines the external authentication server configuration. RADIUS services authenticates profiles to specify external RADIUS services used based on the realm value.

This section covers:

- Adding an Authentication Service
- Testing the AAA Server Configuration
- Viewing RADIUS Services
- Deleting a RADIUS Service

NOTE: If you want to use a primary and secondary RADIUS servers for authenticating administrators, follow the steps in Adding a RADIUS Server for Administrators.

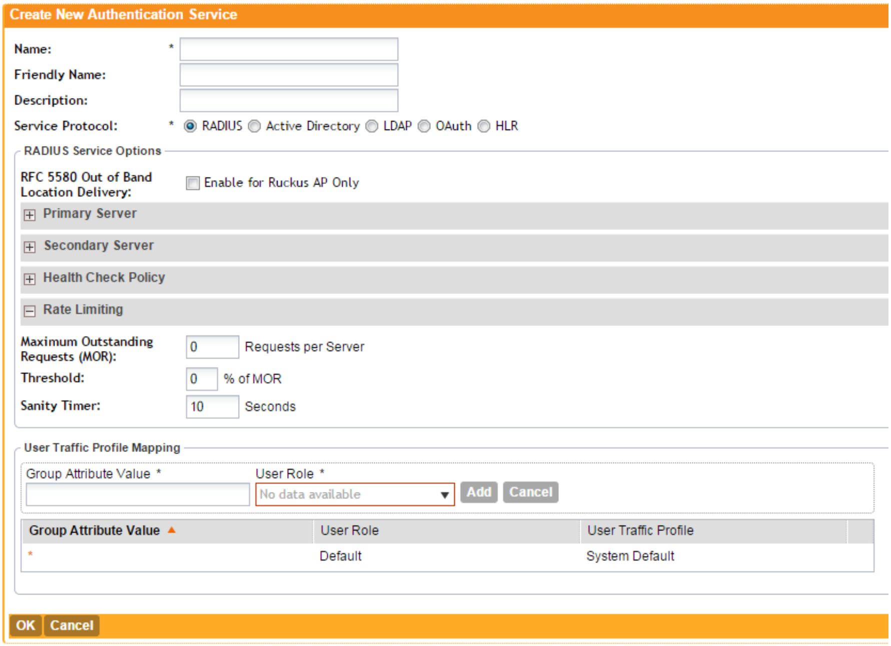
Adding an Authentication Service

Follow these steps to add an authentication service that the controller can use.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar (under *Services*), click **Authentication**. The *Authentication Services* page appears.
3. Click **Create New**. The *Create New Authentication Service* form appears.
4. In *Name*, type a name for the authentication service that you are adding.
5. In *Friendly Name* (optional), type an alternative name that is easy to remember.
6. In *Description* (optional), type a description for the authentication service.
7. In *Type*, select one of the following options:
   - RADIUS (see RADIUS Service Options)
   - Active Directory
   - LDAP
   - OAuth
   - HLR
8. Configure the settings for the authentication service type that you selected.
9. Click **OK**. The page refreshes and the authentication service you have added appears on the list of existing authentication services.

You have completed adding an authentication service to the controller.

Figure 60. The Create New Authentication Service form



Create New Authentication Service

Name: *
Friendly Name:
Description:
Service Protocol: * ● RADIUS ○ Active Directory ○ LDAP ○ OAuth ○ HLR

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: □ Enable for Ruckus AP Only

Maximum Outstanding Requests (MOR): 0 Requests per Server
Threshold: 0 % of MOR
Sanity Timer: 10 Seconds

User Traffic Profile Mapping

Group Attribute Value *
User Role * No data available

Group Attribute Value ▲	User Role	User Traffic Profile
*	Default	System Default

RADIUS Service Options

If you selected RADIUS in Adding an Authentication Service, you need to configure the following options:

- *RFC 5580 Out of Band Location Delivery*: If you want out-of-band location delivery (RFC 5580) to apply only to Ruckus Wireless APs, select the **Enable for Ruckus AP Only** check box.
- *Primary Server*: Configure the primary RADIUS server settings.
    - *IP Address*: Type the IP address of the RADIUS server.
    - *Port*: Type the port number of the RADIUS server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
    - *Shared Secret*: Type the RADIUS shared secret.
    - *Confirm Secret*: Retype the shared secret to confirm.
- *Secondary Server*: If you have a secondary RADIUS server on the network that you want to use as a backup, select the **Enable Secondary Server** check box, and then configure the settings below.

  - *Automatic Fallback Disable*: By default, when a secondary RADIUS server is enabled and the primary RADIUS server becomes unavailable, the secondary server takes over the handling of RADIUS requests. When the primary server becomes available again, it takes back control over RADIUS requests from the secondary server.

    If you want to prevent the primary server from retaking control over RADIUS requests from the secondary server, select the **Automatic Fallback Disable** check box.
  - *IP Address*: Type the IP address of the secondary AAA server.
  - *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
  - *Shared Secret*: Type the AAA shared secret.
  - *Confirm Secret*: Retype the shared secret to confirm.
- *Health Check Policy*: These options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.
  - *Response Window*: Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the “zombie period” (see below). If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server. Note that the zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus ¼ of the configured Zombie Period. The default Response Window is 20 seconds.
  - *Zombie Period*: Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable. An AAA server that is marked “zombie” (inactive or unreachable) will be used for proxying with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server. The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is proxied to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.

- *Revive Interval*: Set the time (in seconds) after which, if no RADIUS messages are proxied to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.
- *No Response Fail*: Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.

CAUTION! To ensure that the RADIUS failover mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For information on configuring the RADIUS NAS request timeout and max number of retries, see Working with WLANs and WLAN Groups. For 3rd party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at 3rd party controller/ AP.

10 *Rate Limiting*: Configure the following options.

- *Maximum Outstanding Requests (MOR)*: Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096.
- *Threshold (% of MOR)*: Set a percentage value of the MOR at which (when reached) the controller will generate an event. For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.
- *Sanity Timer*: Set a timer (in seconds) that will be started whenever a condition that generates an event is reached. This helps prevent conditions that trigger events which occur frequently.

Testing the AAA Server Configuration

The test AAA server holds the information of authentication or accounting server, including the server IP, service port, shared secret and other settings of the current user. If the requested service is successful, the API will display the information.

NOTE: Before you can test the AAA server configuration, you must have created an AAA server. See Adding an Authentication Service for more information.

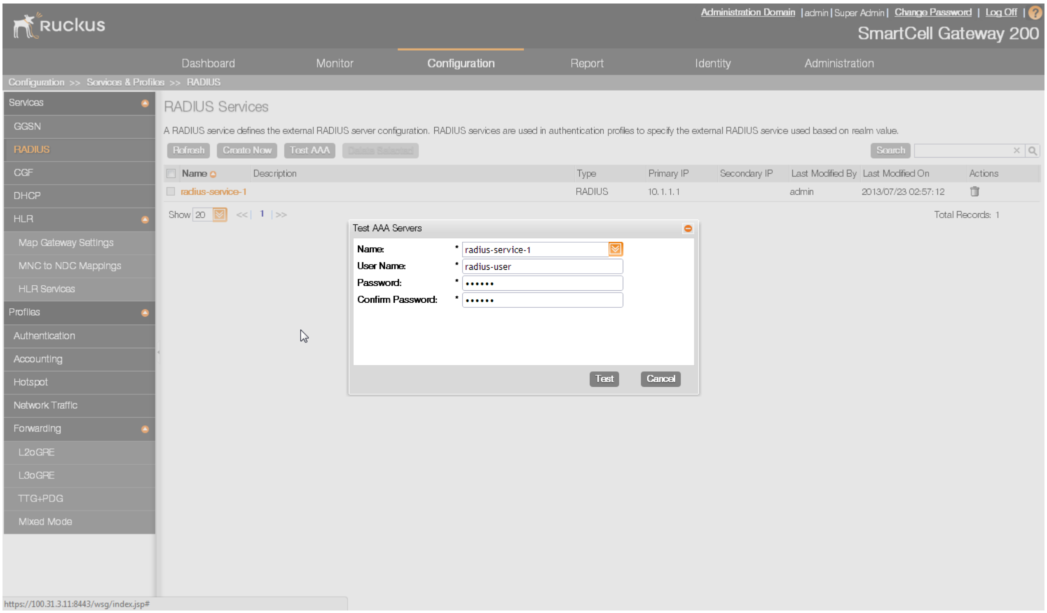
Follow these steps to test the AAA server configuration.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar under *Services*, click **RADIUS**. The *RADIUS Services* page appears.
3. Click **Test AAA**. The *Test AAA Servers* form appears.
4. Configure the options in the *Test AAA Servers* form.
    - *Name*: Select the name of the RADIUS server that you want to test.
    - *User Name*: Type the RADIUS user name that you want to use for testing.
    - *Password*: Type the RADIUS password for the user.
    - *Confirm Password:* Retyped the RADIUS password above.
5. Click **Test**. The message “Please wait...” appears.

If the service request fails, a relevant error message is displayed. Similarly, if the user name or password is incorrect, the error message includes this information along with the server IP address and port. If the server IP address, port, or shared secret is incorrect, the connection to AAA server fails and the error message *“Invalid server setting”* appears and displays the server IP address and port.

If both primary and secondary servers exist, the requested service will be interrupted when controller meets a failure and an error message is displayed.

Figure 61. The Test AAA Servers form



RADIUS Services

A RADIUS service defines the external RADIUS server configuration. RADIUS services are used in authentication profiles to specify the external RADIUS service used based on realm value.

□	Name	Description	Type	Primary IP	Secondary IP	Last Modified By	Last Modified On	Actions
□	radius-service-1		RADIUS	10.1.1.1		admin	2013/07/23 02:57:12	🗑

Total Records: 1

Test AAA Servers

Name:	*	radius-service-1
User Name:	*	radius-user
Password:	*	••••••
Confirm Password:	*	••••••

https://100.31.3.11:8443/wsg/index.jsp#

Viewing RADIUS Services

Follow these steps to view a list of RADIUS servers that have been configured on the controller.

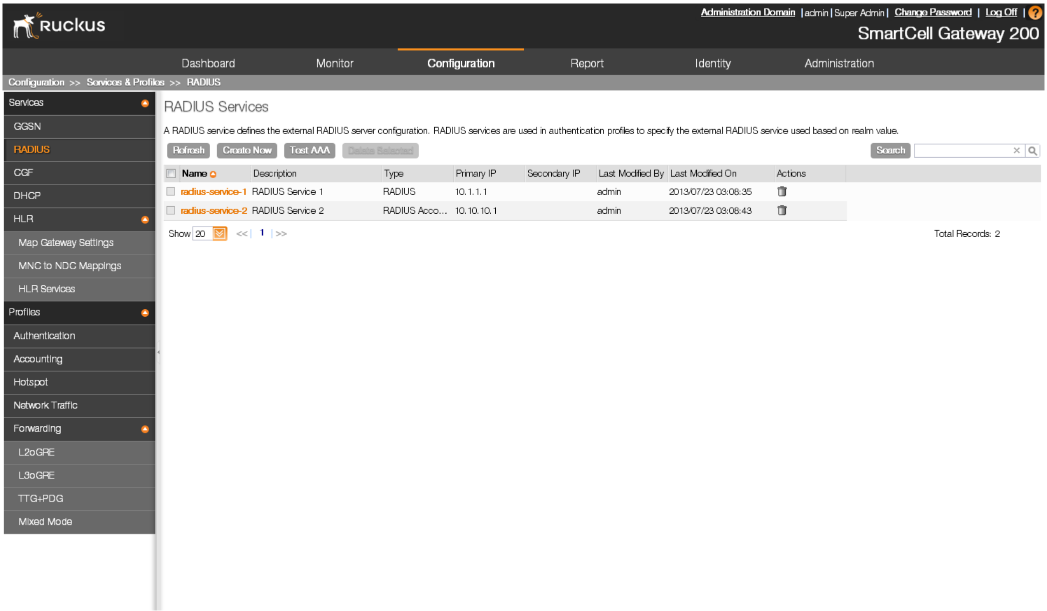
1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Services*, click **RADIUS**. The *RADIUS Services* page appears and displays a list of RADIUS servers that have been configured on the controller. RADIUS details that are shown on the RADIUS services page include:

- Name
- Description
- Type: RADIUS or RADIUS Accounting
- Primary IP
- Secondary IP
- Last Modified By
- Last Modified On
- Actions

You have completed viewing a list of RADIUS services.

Figure 62. Viewing a list of RADIUS services



RADIUS Services

A RADIUS service defines the external RADIUS server configuration. RADIUS services are used in authentication profiles to specify the external RADIUS service used based on realm value.

□	Name	Description	Type	Primary IP	Secondary IP	Last Modified By	Last Modified On	Actions
□	radius-service-1	RADIUS Service 1	RADIUS	10.1.1.1		admin	2013/07/23 03:08:35	🗑
□	radius-service-2	RADIUS Service 2	RADIUS Acco...	10.10.10.1		admin	2013/07/23 03:08:43	🗑

Total Records: 2

Deleting a RADIUS Service

You can delete a single or multiple RADIUS services simultaneously.

- To delete a single RADIUS service, follow these steps:

  a Go to *Configuration* > *Services & Profiles*.

  b On the sidebar under *Services*, click **Authentication**. The *Authentication Services* page appears.

  c From the list of existing authentication servers, locate the RADIUS server that you want to delete.

  d Under the *Actions* column, click the icon 🗑 that is in the same row as the RADIUS service name. A confirmation message appears.

  e Click **Yes**. The page refreshes, and the RADIUS service that you deleted disappears from the view list.

- To delete multiple RADIUS services simultaneously, follow these steps:

  a Go to *Configuration* > *Services & Profiles*.

  b On the sidebar under *Services*, click **RADIUS**. The *RADIUS Services* page appears.

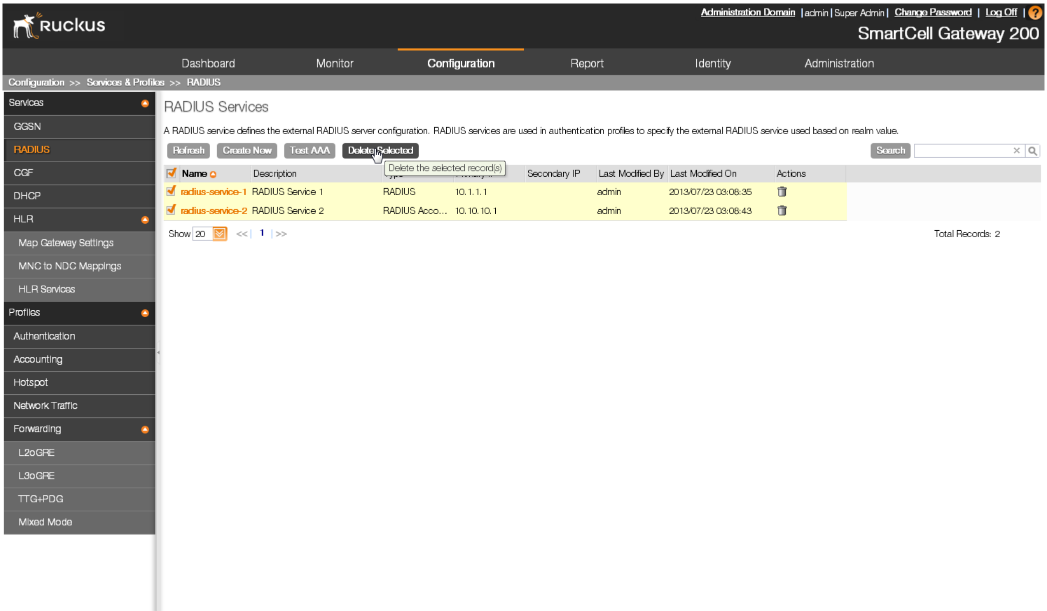
  c From the list of existing RADIUS services, locate the services that you want to delete.

  d Select the check boxes before the services that you want delete.

  e Click **Delete Selected**. A confirmation message appears.

  f Click **Yes**. The page refreshes and the RADIUS services that you deleted disappears from the list.

Figure 63. Deleting multiple RADIUS services simultaneously



RADIUS Services

A RADIUS service defines the external RADIUS server configuration. RADIUS services are used in authentication profiles to specify the external RADIUS service used based on realm value.

☑	Name	Description			Secondary IP	Last Modified By	Last Modified On	Actions
☑	radius-service-1	RADIUS Service 1	RADIUS	10.1.1.1		admin	2013/07/23 03:08:35	🗑
☑	radius-service-2	RADIUS Service 2	RADIUS Acco...	10.10.10.1		admin	2013/07/23 03:08:43	🗑

Show 20 <<| 1 |>>

Total Records: 2

Configuring HLR Services

The controller and multiple Home Location Registers (HLRs) manage a wireless services gateway for performing authentication/ authorization and for unsolicited changes of authorization.

This section covers:

- Map Gateway Settings
- MNC to NDC Mapping

Map Gateway Settings

Configure the MAP gateway settings to set up multiple HLRs for performing authentication and/or authorization and for unsolicited changes of authorization. The MAP gateway is responsible for initiating MAP queries with the UE's home HLR. Since the MAP gateway may interface with multiple HLRs, the route to the home HLR is selected based on the realm information.

The following configuration settings apply to all the HLR services configured on the controller.

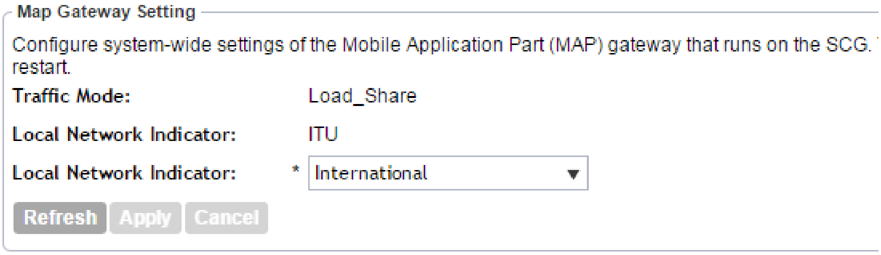
CAUTION! Changes to these settings could cause critical controller processes to restart.

Follow these steps to configure a MAP gateway settings for the HLR service.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar under *Services*, click **HLR**.
3. Click **Map Gateway Settings** on the sidebar under *HLR*.
4. Configure *Map Gateway Settings*.
   - *Traffic Mode*: This setting is always set to **Load_Share** and is not configurable.
   - *Protocol Variant*: This setting is always set to **ITU** and is not configurable.
   - *Local Network Indicator*: Select either **International** or **National**.
5. Click **Apply**.

You have completed configuring the Map Gateway Settings.

Figure 64. The Map Gateway Settings configuration form



Map Gateway Setting

Configure system-wide settings of the Mobile Application Part (MAP) gateway that runs on the SCG.
restart.

Traffic Mode:	Load_Share
Local Network Indicator:	ITU
Local Network Indicator:	* International ▼

MNC to NDC Mapping

The MNC (Mobile Network Code) to NDC (Network Destination Code) mapping information is required for sending and receiving MAP traffic. This information is used by all the HLR services that have been created.

This section covers:

- Adding MNC to NDC Mapping
- Viewing MNC to NDC Mapping
- Deleting MNC to NDC Mappings

Adding MNC to NDC Mapping

Follow these steps to add a new MNC (Mobile Network Code) to NDC (Network Destination Code) mapping.

NOTE: Before you can add an MNC to NDC mapping, you must first enable the Map Gateway. See Map Gateway Settings for more information.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Services*, click **HLR**.

3 Click **MNC to NDC Mappings** on the sidebar under *HLR*. The *MNC to NDC Mapping* page appears.

4 Click **Create New**.

5 Define the MNC to NDC mapping by filling out the following boxes.

- **MCC**: Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.
- **MNC**: Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.

- **NDC**: Type the network destination code digits, which has a maximum length of 5 digits.

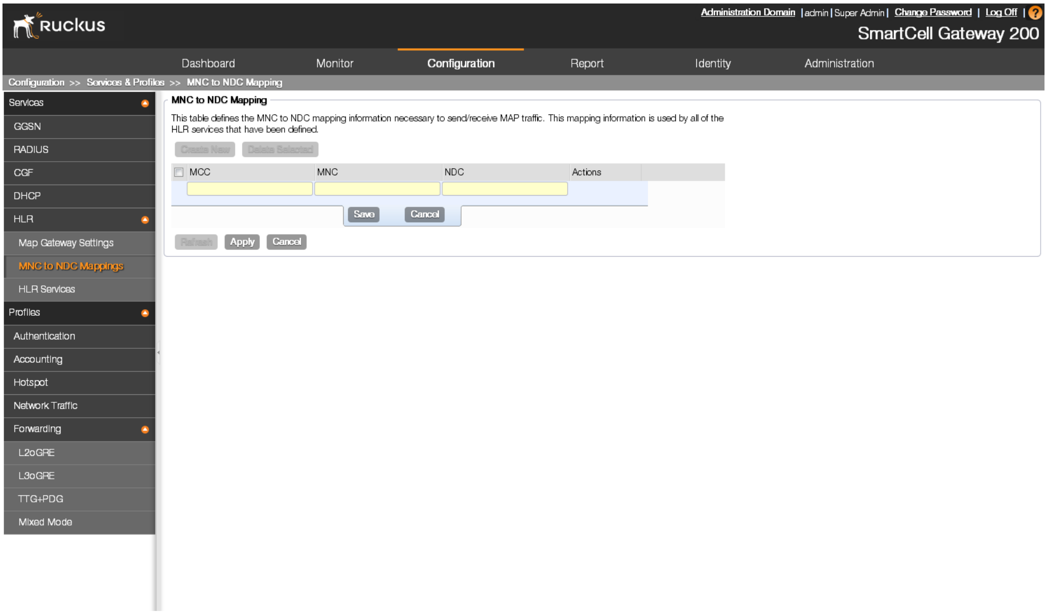
6 Click **Save**.

7 To add another mapping, repeat steps 4 to 6.

8 Click **Apply**.

You have completed adding an MNC to NDC mapping.

Figure 65. Adding an MNC to NDC mapping



MNC to NDC Mapping

This table defines the MNC to NDC mapping information necessary to send/receive MAP traffic. This mapping information is used by all of the HLR services that have been defined.

□	MCC	MNC	NDC	Actions

Viewing MNC to NDC Mapping

Follow these steps to view a list of mapping information.

1 Go to *Configuration* > *Services & Profiles*.

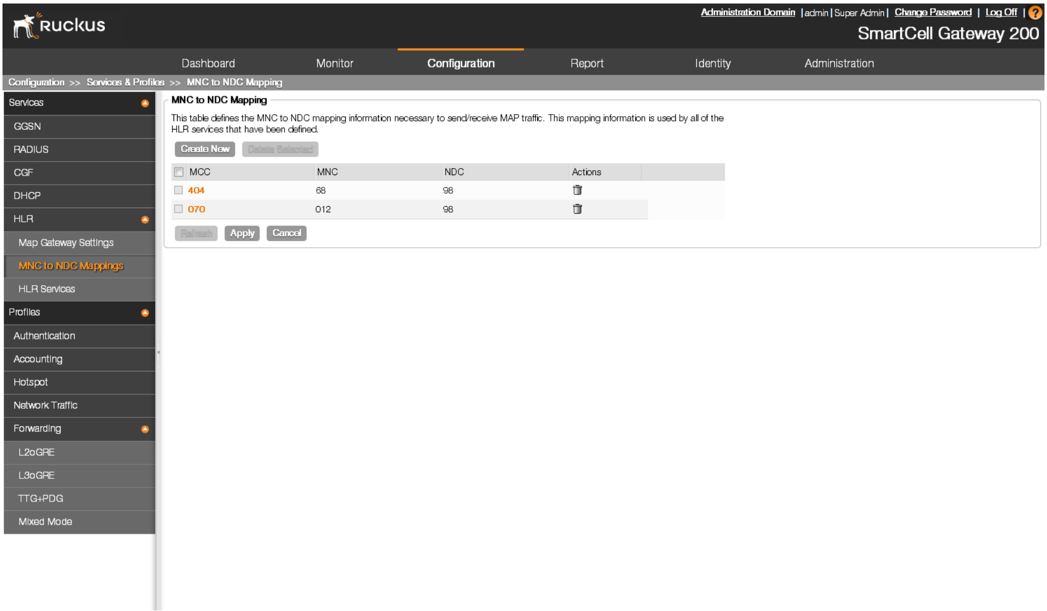
2 On the sidebar under *Services*, click **HLR**.

3 Click **MNC to NDC Mappings** on the sidebar under *HLR*. The *MNC to NDC Mapping* page appears and lists the MNC to NDC mappings that you have created. For each mapping on the list, the following details are displayed:

- MCC
- MNC
- NDC
- Actions: Displays the trash bin icon, which you can click to delete the mapping

You have completed viewing a list of existing MNC to NDC mappings.

Figure 66. The MNC to NDC Mapping page displays the mappings that you have created



This table defines the MNC to NDC mapping information necessary to send/receive MAP traffic. This mapping information is used by all of the HLR services that have been defined.

□ MCC	MNC	NDC	Actions
□ 404	68	98	🗑
□ 070	012	98	🗑

Deleting MNC to NDC Mappings

Follow these steps to delete a single or multiple mappings simultaneously.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Services*, click **HLR**. The *HLR* submenu appears.

3 Click **MNC to NDC Mappings**.

4 Delete a single mapping or multiple mappings.

To delete a single mapping:

a From the list of existing mappings, locate the mapping that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the mapping. A confirmation message appears.

c Click **Yes**. The page refreshes, and the mapping that you deleted disappears from the view list.

To delete multiple mappings simultaneously, follow these steps:

a From the list of existing mappings, locate the mappings that you want to delete.

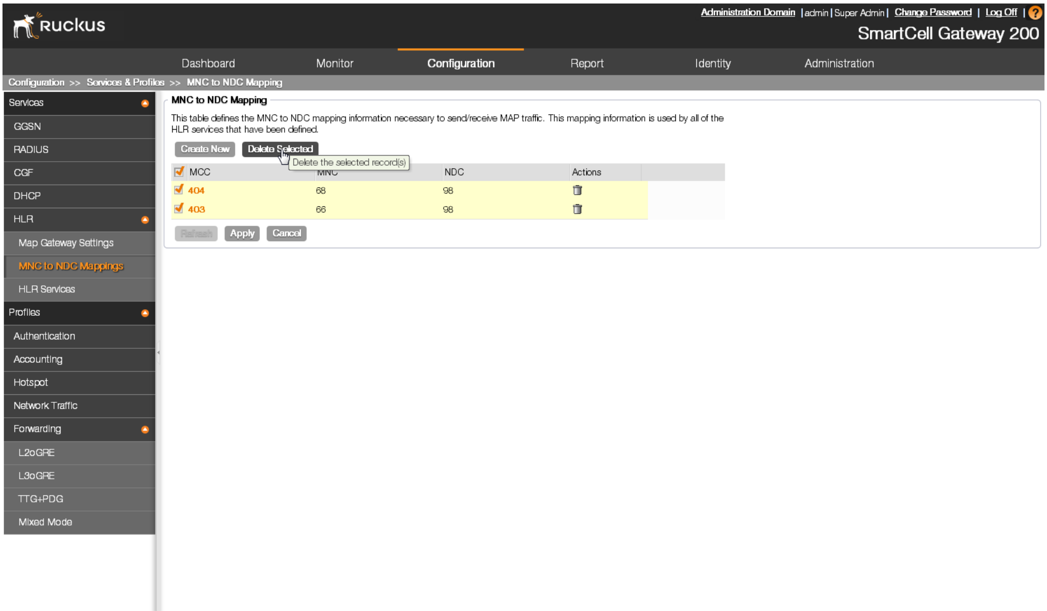
b Select the check boxes before the mappings that you want delete.

c Click **Delete Selected**. A confirmation message appears.

d Click **Yes**. The page refreshes and the mappings that you deleted disappears from the list.

You have completed deleting MNC to NDC mappings.

Figure 67. Deleting multiple MNC to NDC mappings simultaneously



MNC to NDC Mapping

This table defines the MNC to NDC mapping information necessary to send/receive MAP traffic. This mapping information is used by all of the HLR services that have been defined.

☑ MCC	MNC	NDC	Actions
☑ 404	68	98	🗑
☑ 403	66	98	🗑

Configuring Diameter Services

The controller supports the 3GPP STa interface for EAP-SIM to authenticate and authorize subscribers.

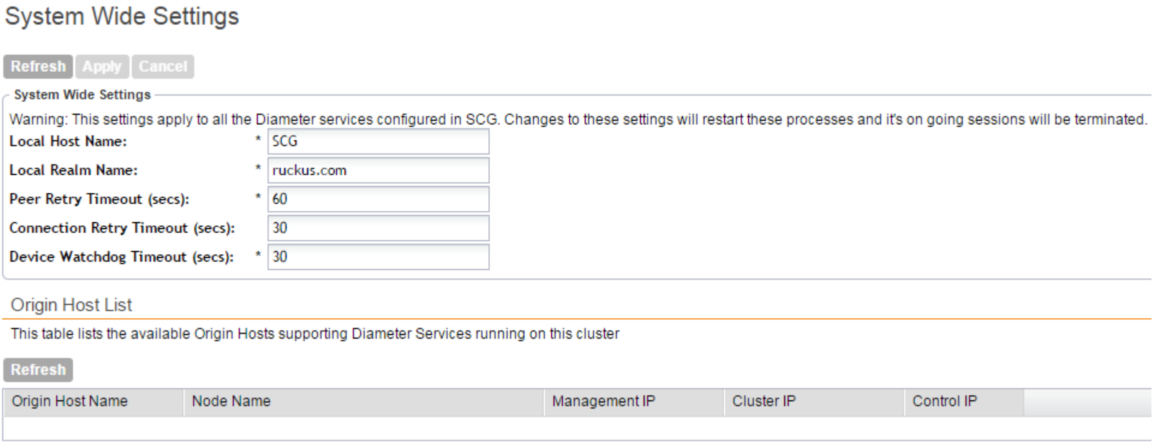
Configuring System Wide Settings

Follow these steps to configure the system wide Diameter service settings.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar, click **System Wide Settings** under *Diameter Services*.
3. In the *System Wide Settings* section, configure the following options:
   - Local Host Name
   - Local Realm Name
   - Peer Retry Timeout (in seconds)
   - Connection Retry Timeout (in seconds)
   - Device Watchdog Timeout (in seconds)
4. Click **Apply**.

You have completed configuring the system wide settings for Diameter services.

Figure 68. The System Wide Settings page



Warning: This settings apply to all the Diameter services configured in SCG. Changes to these settings will restart these processes and it's on going sessions will be terminated.

Local Host Name: * SCG

Local Realm Name: * ruckus.com

Peer Retry Timeout (secs): * 60

Connection Retry Timeout (secs): 30

Device Watchdog Timeout (secs): * 30

This table lists the available Origin Hosts supporting Diameter Services running on this cluster

Origin Host Name	Node Name	Management IP	Cluster IP	Control IP

Configuring Remote Peer Settings

Follow these steps to configure the remote peer settings for the Diameter services.

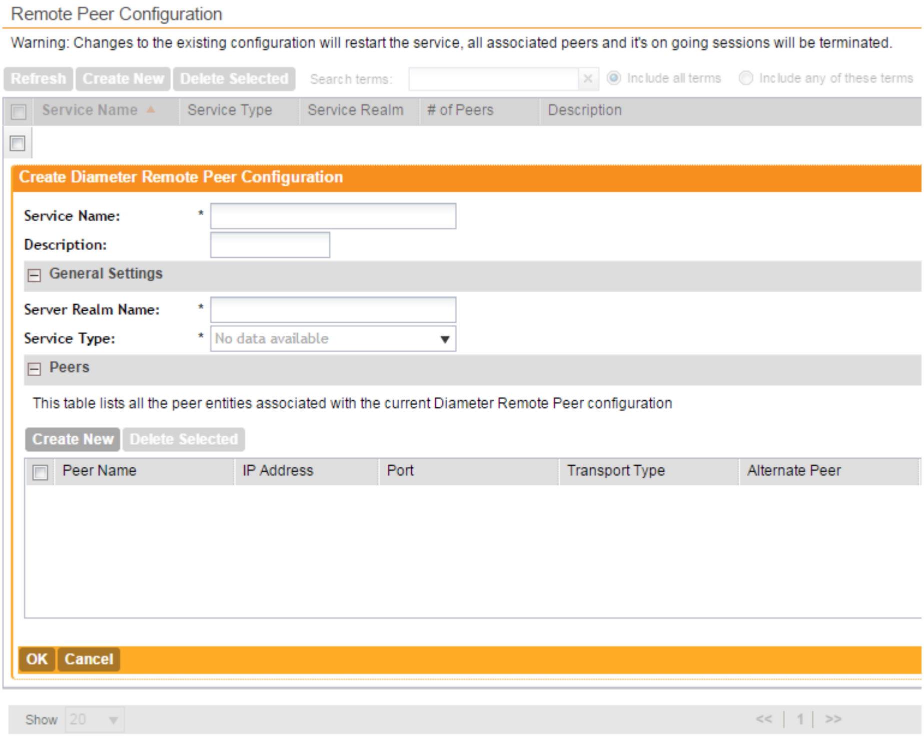
1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar, click **Remote Peer Configuration** under *Diameter Services*. The *Remote Diameter Services* page appears.
3. Click **Create New**. The *Create Remote Diameter Peer Configuration* form appears.
4. In *Service Name*, type a name for the service you are creating.
5. In *Description*, type a brief description of the service.
6. In *General Settings*, configure the following options:
   - *Server Realm Name*: Type name realm name of the server.
   - *Service Type*: Select the type of Diameter service. Options include:
     - DRA (Diameter Routing Agents)
     - OCS (Online Charging Systems)
     - PCRF (Policy and Charging Rules Functions)
     - STA

     If you select PCRF or STA, you will need to configure the *Tx Timer* (in seconds) and *Retransmit Count* settings as well.
7. In *Peers*, add a peer entity to associate with the current Diameter remote peer settings by filling out the following boxes:
   - Peer Name
   - IP Address
   - Port
   - Transport Type
   - Alternate Peer

   Click **Save** to add this peer entity to the remote peer settings. To add another peer entity, click **Create New** in the *Peers* section, and then fill out the new set of boxes that appear.
8. Click *Create New* at the bottom of the page to create the remote peer configuration.

You have completed configuring the remote peer settings for the Diameter services.

Figure 69. The Create Diameter Remote Peer Configuration form



Remote Peer Configuration

Warning: Changes to the existing configuration will restart the service, all associated peers and it's on going sessions will be terminated.

Create Diameter Remote Peer Configuration

Service Name: *

Description:

General Settings

Server Realm Name: *

Service Type: * No data available

Peers

This table lists all the peer entities associated with the current Diameter Remote Peer configuration

Configuring FTP Services

You can automatically back up statistical data, CGF server binary files, reports, and system configuration backups to an external FTP server. However, before you can do this, you must add at least one FTP server to the controller.

Follow these steps to add an FTP server to which the controller will export data automatically.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Services*, click **FTP**. The *FTP* page appears.

3 In *FTP Name*, type a name that you want to assign to the FTP server that you are adding.

4 In *FTP Host*, type the IP address of the FTP server.

5 In *Port*, type the FTP port number. The default FTP port number is 21.

6 In *User Name*, type user name of the FTP account that you want to use.

7 In *Password*, type the password that is associated with the FTP user name above.

8 In *Remote Directory*, type the path on the remote FTP server to which data will be exported from the controller. The path must start with a forward slash (/), as shown in Figure 70.

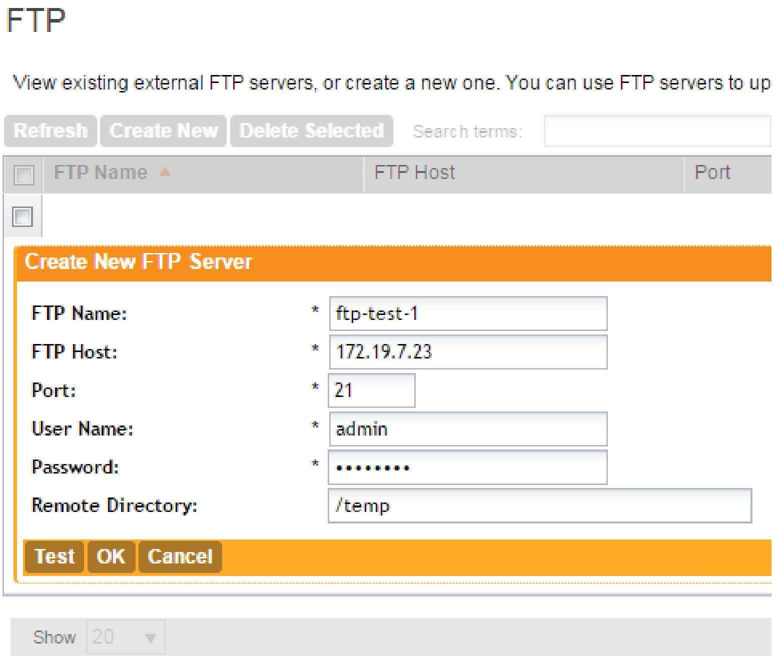
9 To verify that the FTP server settings and logon information are correct, click Test. If the server and logon settings are correct, the following message appears:

```
Test completed successfully.
```

10 Click **Create New**.

You have completed adding an FTP server to the controller. You may add additional FTP servers as required.

Figure 70. Adding an FTP server to the controller



FTP

View existing external FTP servers, or create a new one. You can use FTP servers to up

FTP Name: * ftp-test-1

FTP Host: * 172.19.7.23

Port: * 21

User Name: * admin

Password: * ••••••••

Remote Directory: /temp

Important Notes About FTP Services

Release 2.5 (and later) includes several changes to the FTP server configuration. Remember the following important notes when configuring FTP services in release 2.5 (and later).

- Duplicate FTP servers are not allowed in release 2.5 (and later). For example, you cannot add `172.19.7.23` as one FTP server and `172.19.7.23/temp` (/temp is the remote directory) as another.
- FTP servers must be added on the *Configuration* > *Services & Profiles* > *FTP* page. The FTP servers that you add on this page will appear as options on the following pages:
  - Configuration > Services & Profiles > Services > CGF services: Auto Export FTP under Binary File Options
  - System > FTP Server for Uploading Statistics
  - Reports > Export Report Results
  - System Configuration Backup and Restore: Auto Export Backup
- If, before the controller was upgraded to 2.5 (or later version), statistics upload, CGF server binary files, reports, and system configuration backup were configured to be uploaded to four *different* FTP servers, then after upgrading to 2.5 (or later version), the controller will automatically create entries for those four FTP servers on the *Configuration* > *Services & Profiles* > *FTP* page.
- If, before the controller was upgraded to 2.5, statistics upload, CGF server binary files, reports, and system configuration backup were configured to be uploaded to the *same* FTP server but using different FTP accounts, then after upgrading to 2.5 or later version, the controller will automatically create entries for those four FTP servers on the *Configuration* > *Services & Profiles* > *FTP* page.
- If, before the controller was upgraded to 2.5 (or later version), statistics upload, CGF server binary files, reports, and system configuration backup were configured to be uploaded to the *same* FTP server and using the *same* FTP account, then after upgrading to 2.5 (or later version), the controller will automatically create one FTP server entry on the *Configuration* > *Services & Profiles* > *FTP* page. If one of the previous FTP server configurations included a remote directory, the same remote directory will be applied to the new FTP server entry and all data for backup will be uploaded to this remote directory.
- In previous builds, the remote directory option was available for the CGF server binary files and reports. Statistics and system configuration backups did not have the remote directory option.

Configuring Location Services

If your organization purchased the Ruckus Wireless SmartPositioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log into the SPoT Administration Portal. The Admin Portal provides tools for configuring and managing all of your “venues” (the physical locations in which SPoT service is deployed). After a venue is successfully set up, you will need to enter the same venue information on the controller.

Adding an LBS Server

Follow these steps to add an LBS server to the controller for SPoT communication.

1 Log on to the SPoT Administration Portal.

2 On the *Venues* page, click **Config** next to the venue for which you want to configure Location services.

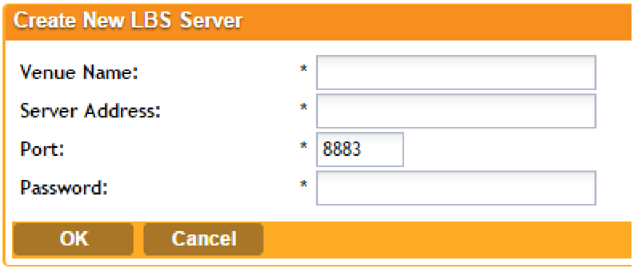
3 In *Controller Settings*, take note of the values for the following:

- Venue Name
- Server Address
- Port
- Password

4 On the controller web interface, go to *Configuration* > *Services & Profiles* > *Services* > *Location Services*.

5 Click **Create New**. The *Create New LBS Server* form appears.

Figure 71. The Create New LBS Server form



Create New LBS Server

Venue Name:	*	
Server Address:	*	
Port:	*	8883
Password:	*	

6 Enter the information you obtained in Step 3 from the SPoT Administration Portal into the four fields provided.

- Venue Name
- Server Address
- Port
- Password

7 Click **OK** to save your changes.

You have completed adding an LBS server to the controller. You can now use this LBS server along with your zone and AP group configuration (see Configuring the Controller to Use the LBS Server).

After you configure zones or AP groups to use an LBS server, you can

Configuring the Controller to Use the LBS Server

There are two ways to configure the controller to use the LBS servers you added in Adding an LBS Server. You can:

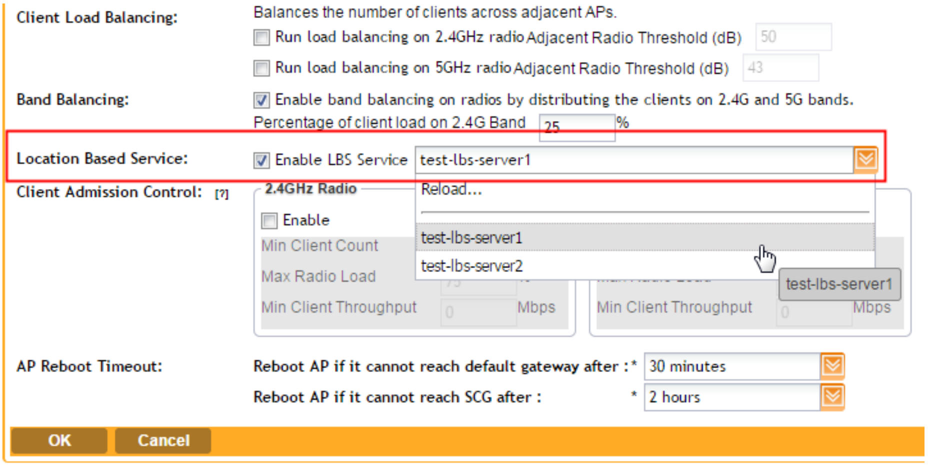
- Set an entire AP zone to use an LBS server
- Set an AP group to override the LBS settings of a zone

NOTE: For information on configuring and managing the Ruckus Wireless SmartPositioning Technology (SPoT) service, refer to the *SPoT User Guide*, which is available for download from https://support.ruckuswireless.com.

Setting an AP Zone to Use an LBS Server

When you create or edit an AP zone, you can enable the LBS service for the entire zone by selecting the **Enable LBS service** check box, and then selecting an LBS server to use.

Figure 72. Enabling and selecting an LBS in the create/edit AP zone form


Client Load Balancing: Balances the number of clients across adjacent APs.

□ Run load balancing on 2.4GHz radio Adjacent Radio Threshold (dB) 50

□ Run load balancing on 5GHz radio Adjacent Radio Threshold (dB) 43

Band Balancing: ☑ Enable band balancing on radios by distributing the clients on 2.4G and 5G bands.

Percentage of client load on 2.4G Band 25 %

Location Based Service: ☑ Enable LBS Service test-lbs-server1

Reload...

test-lbs-server1

test-lbs-server2

test-lbs-server1

Client Admission Control: [?]

2.4GHz Radio

□ Enable

Min Client Count

Max Radio Load

Min Client Throughput 0 Mbps

Min Client Throughput 0 Mbps

AP Reboot Timeout: Reboot AP if it cannot reach default gateway after :* 30 minutes

Reboot AP if it cannot reach SCG after : * 2 hours

Setting an AP Group to Override the LBS Settings of a Zone

If you want APs that belong to an AP group to use a different LBS server, you can override the LBS settings at the AP group level. Follow these steps.

1 Go to *Configuration* > *AP Zones*.

2 In the *AP Zone List*, click the zone name to which the AP group you want to configure belongs.

3 On the sidebar, click **AP Group**.

4 Click *Create New* to create a new AP group, or click the AP group name to edit it.

5 In the form that appears, scroll down to the *Advanced Options* section. Click the plus (+) sign before *Advanced Options* to display all options.

6 In *Location Based Service*, select the **Override zone config** check box.

7 Configure the LBS settings as required.

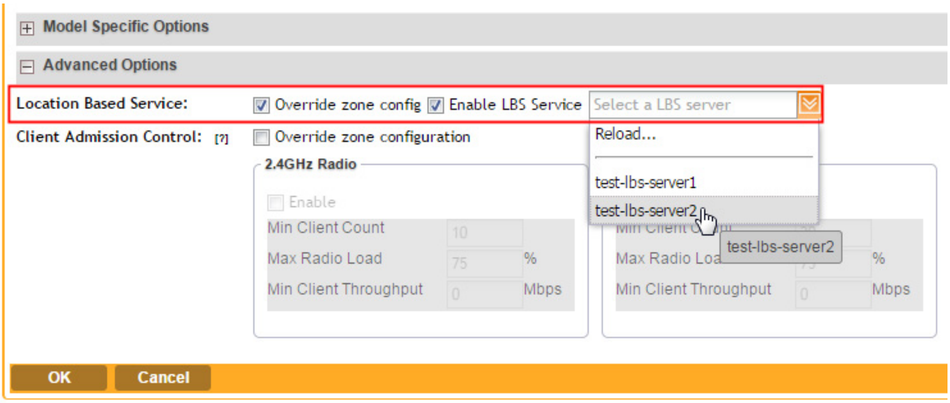
- To disable the LBS service for this AP group, clear the **Enable LBS service** check box.
- To use a different LBS server for this AP group, select the **Enable LBS service** check box, and then select the LBS server that you want to use from the drop-down list.

8 Configure the other AP group settings as required. For information on configuring AP groups, see Creating an AP Group.

9 Click **OK**.

You have completed setting an AP group to override the LBS settings of its zone.

Figure 73. Overriding the LBS settings of a zone at the AP group level



Location Based Service: ☑ Override zone config ☑ Enable LBS Service Select a LBS server

Client Admission Control: [?] □ Override zone configuration

2.4GHz Radio

□ Enable

Min Client Count 10

Max Radio Load 75 %

Min Client Throughput 0 Mbps

Configuring an SMS Server

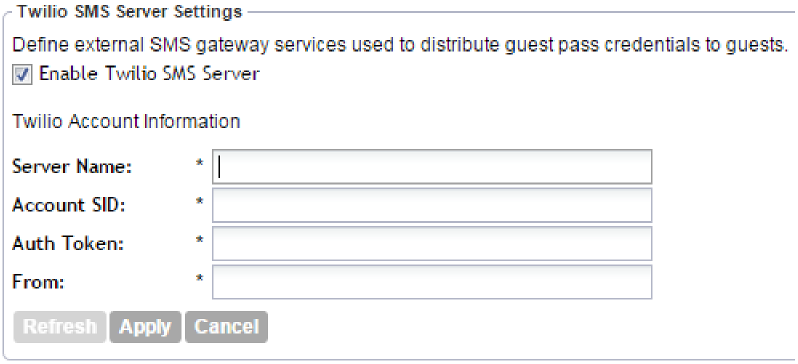
If you want to deliver guest passes to guest users via SMS, you can configure the controller use an existing Twilio account for SMS delivery. The first step is to inform the controller of your Twilio account information.

Follow these steps to configure an external SMS gateway for the controller.

1. Go to *Configuration* > *Services & Profiles* > *SMS Server.*
2. Select the **Enable Twilio SMS Server** check box.
3. Under Twilio Account Information, configure the following:
   - Server Name
   - Account SID
   - Auth TokenSCG
   - From (phone number)
4. Click **Apply.**

You have completed configuring the external SMS gateway for the controller.

Figure 74. Configuring the external SMS gateway settings



Twilio SMS Server Settings

Define external SMS gateway services used to distribute guest pass credentials to guests.

☑ Enable Twilio SMS Server

Twilio Account Information

Server Name: *	
Account SID: *	
Auth Token: *	
From: *	

Working with Profiles

This section covers:

- Working with Authentication Profiles
- Working with Accounting Profiles
- Working with Hotspot Profiles
- Working with Network Traffic Profiles
- Working with Forwarding Profiles

Working with Authentication Profiles

An authentication profile defines the authentication policy when the controller is used as a RADIUS proxy service for WLANs. RADIUS protocol is used for interfacing between access points and the controller as well as between the controller and a third party AAA server. The controller acts as RADIUS proxy for authentication and authorization and as a RADIUS client for accounting.

This section covers:

- Creating an Authentication Profile
- Viewing Authentication Profiles
- Deleting Authentication Profiles

Creating an Authentication Profile

Follow these steps to create an authentication profile.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar under *Profiles*, click **Authentication**. The *Authentication Profiles* page appears.
3. Click **Create New**. The *Create New Authentication Profile* form appears.
4. In *Name*, type a name for the authentication profile that you are adding.
5. In *Description*, type a brief description of the profile. This is an optional field.
6. To enable hosted AAA support, select the **Enable Hosted AAA Support** check box, and then configure the options under *Hosted AAA Server RADIUS Settings* and *PLMN Settings*.

   Under *Hosted AAA Server RADIUS Settings*:

- *Interim Accounting Interval (secs)*: Set the interim time interval for RADIUS clients to send accounting updates. Default is 0, which indicates that the accounting interval is disabled.
- *Sessions Timeout (secs)*: Set a time limit after which users will be disconnected and required to log on again.
- *Session Idle Timeout (secs)*: Set a value in seconds (60 to 600) after which idle clients will be disconnected.

Under *PLMN ID Settings*:

- *Mobile Country Code*: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information to the HLR.
- *Mobile Network Code*: Set the mobile network code based on the geographical location. This is required when the controller sends MAP authentication information to HLR.

7 Under *Realm Based Authentication Service*, configure the following attributes, which are required for enabling AAA support. These are also required when controller authentication works as a proxy.

- Click *No Match*, and configure the following:
  - Default Auth Service
  - Authorization Method
  - Dynamic VLAN ID
- Click *Unspecified*, and then configure the following:
  - *Default Auth Service*: If you select **NA-Request Rejected**, then the authorization method will be displayed as 'NA' but the value that will be sent is 0 (zero).
  - Authorization Method
  - Dynamic VLAN ID

8 In *Authentication Service Per Realm*, specify the authentication service for each of the realms specified in this table. If you set the authentication service for a particular realm to **NA-Request Rejected**, then the authentication request is rejected. To create a new service click, **Create New**, and then configure the following:

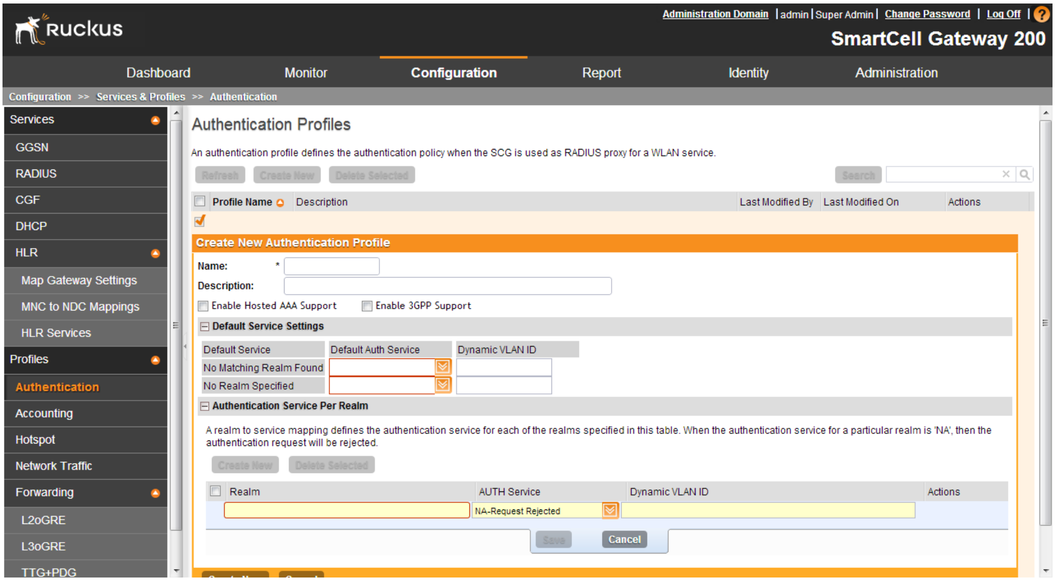
- Realm
- Auth Service
- Authorization Method

- Dynamic VLAN ID

9 Click **Create New**.

You have completed adding an authentication profile.

Figure 75. The Create New Authentication Profile form



Authentication Profiles

An authentication profile defines the authentication policy when the SCG is used as RADIUS proxy for a WLAN service.

□	Profile Name	Description	Last Modified By	Last Modified On	Actions
☑					

Create New Authentication Profile

Name: *

Description:

□ Enable Hosted AAA Support □ Enable 3GPP Support

⊟ Default Service Settings

Default Service	Default Auth Service	Dynamic VLAN ID
No Matching Realm Found		
No Realm Specified		

⊟ Authentication Service Per Realm

A realm to service mapping defines the authentication service for each of the realms specified in this table. When the authentication service for a particular realm is 'NA', then the authentication request will be rejected.

□	Realm	AUTH Service	Dynamic VLAN ID	Actions
		NA-Request Rejected		

Viewing Authentication Profiles

Follow these steps to view a list of authentication profiles that have been created on the controller.

NOTE: If you have not created an authentication profile, refer to Creating an Authentication Profile.

1 Go to *Configuration* > *Services & Profiles*.

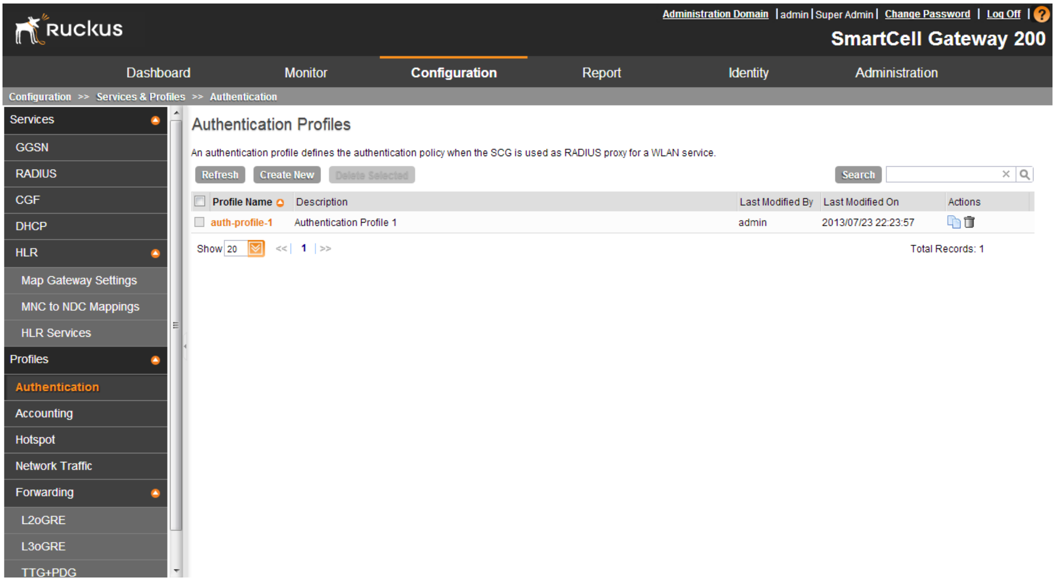
2 On the sidebar under *Profiles*, click **Authentication**. The *Authentication Profiles* page appears and displays the authentication servers that have been added to the controller. For each authentication profile, the following details are displayed:

- Profile Name
- Description
- Last Modified By
- Last Modified On

- Actions: Displays the trash bin icon, which you can click to delete the profile

You have completed viewing a list of authentication profiles.

Figure 76. The Authentication Profiles page lists the profiles that have been created on the controller



Authentication Profiles

An authentication profile defines the authentication policy when the SCG is used as RADIUS proxy for a WLAN service.

□	Profile Name	Description	Last Modified By	Last Modified On	Actions
□	auth-profile-1	Authentication Profile 1	admin	2013/07/23 22:23:57	🗑

Show 20 << | 1 | >> Total Records: 1

Deleting Authentication Profiles

Follow these steps to delete a single or multiple authentication profiles simultaneously.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Authentication**. The *Authentication Profiles* page appears and lists the profiles that have been configured on the controller.

3 Delete a single or multiple profiles.

To delete a single profile:

a From the list of existing profiles, locate the profile that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the profile. A confirmation message appears.

c Click **Yes**. The page refreshes, and the profile that you deleted disappears from the view list.

To delete multiple profiles simultaneously, follow these steps:

a From the list of existing profiles, locate the profiles that you want to delete.

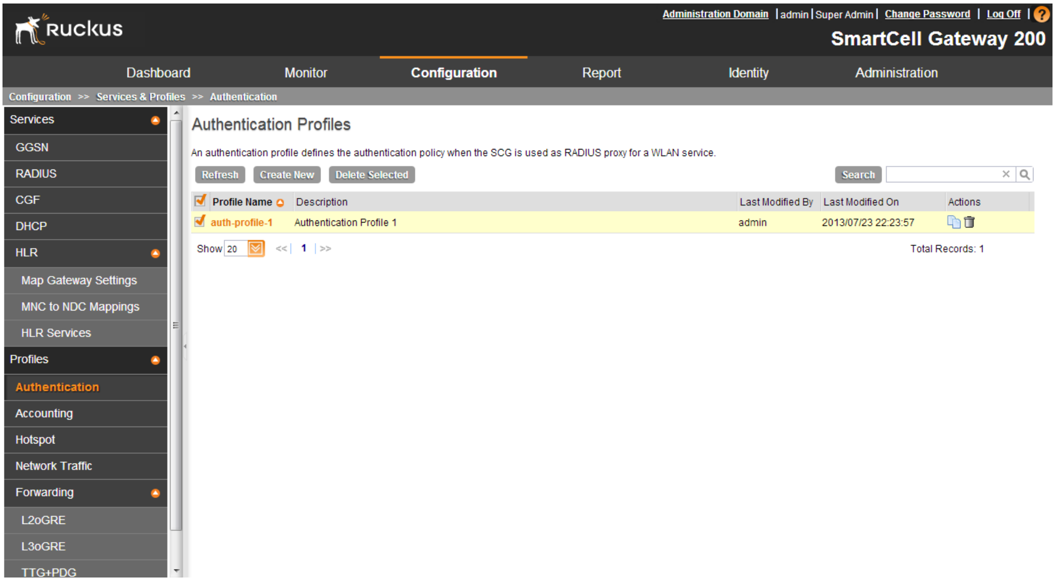
b Select the check boxes before the profiles that you want delete.

c Click **Delete Selected**. A confirmation message appears.

d Click **Yes**. The page refreshes and the profiles that you deleted disappears from the list.

You have completed deleting authentication profiles.

Figure 77. Deleting multiple profiles simultaneously



Authentication Profiles

An authentication profile defines the authentication policy when the SCG is used as RADIUS proxy for a WLAN service.

☑ Profile Name	Description	Last Modified By	Last Modified On	Actions
☑ auth-profile-1	Authentication Profile 1	admin	2013/07/23 22:23:57	

Show 20 << | 1 | >> Total Records: 1

Working with Accounting Profiles

An accounting profile defines the accounting policy when the controller is used as a RADIUS proxy for WLAN services. This section covers:

- Creating an Accounting Profile
- Viewing Accounting Profiles
- Deleting Accounting Profiles

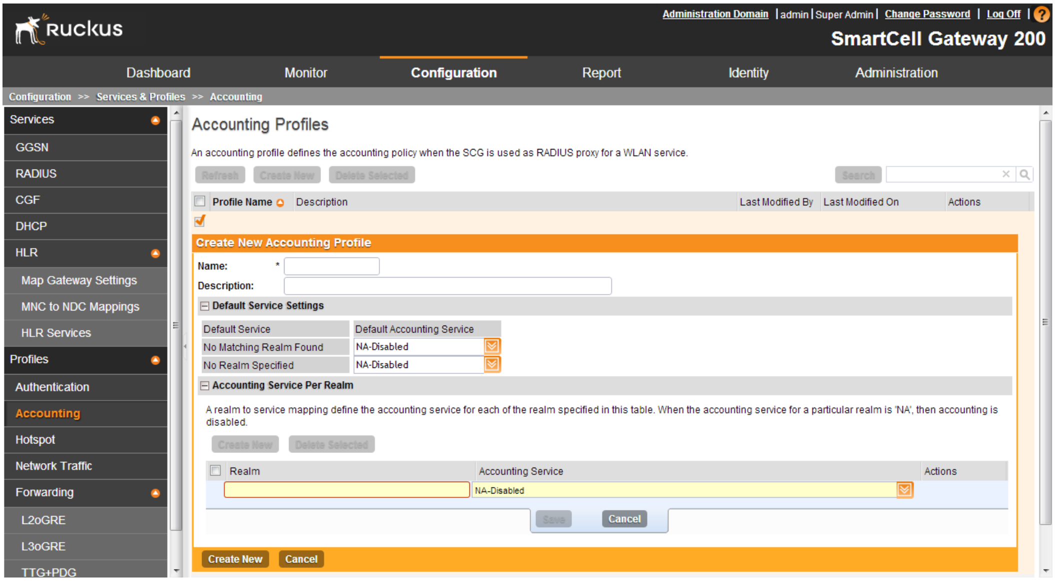
Creating an Accounting Profile

Follow these steps to create an accounting profile.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar under *Profiles*, click **Accounting**. The *Accounting Profiles* page appears
3. Click **Create New**. The *Create New Accounting Profile* form appears.
4. In *Name*, type a name for the authentication profile that you are adding.
5. In *Description*, type a brief description of the profile. This is an optional field.
6. Under *Default Service Settings*, configure the following:
   - In *No Matching Realm Found*, select a default accounting service. If you select **NA-Disabled**, then the accounting method will be displayed as 'NA' but the value that will be sent is 0 (zero).
   - In *No Realm Specified*, select a default accounting service. If you select **NA-Disabled**, then the accounting method will be displayed as 'NA' but the value that will be sent is 0 (zero).
7. In *Accounting Service Per Realm*, specify the accounting service for each of the realms specified in this table. If you set the accounting service for a particular realm to **NA-Disabled**, then the accounting request is rejected. To create a new service click, **Create New**, and then configure the following:
   - Realm
   - Accounting service
8. Click **Create New**.

You have completed adding an accounting profile.

Figure 78. The Create New Accounting Profile form



Accounting Profiles

An accounting profile defines the accounting policy when the SCG is used as RADIUS proxy for a WLAN service.

□	Profile Name	Description	Last Modified By	Last Modified On	Actions

Create New Accounting Profile

Name: *

Description:

Default Service Settings

Default Service	Default Accounting Service
No Matching Realm Found	NA-Disabled
No Realm Specified	NA-Disabled

Accounting Service Per Realm

A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

□	Realm	Accounting Service	Actions
		NA-Disabled	

Viewing Accounting Profiles

Follow these steps to view a list of accounting profiles that have been created on the controller.

NOTE: If you have not created an accounting profile, refer to Creating an Accounting Profile.

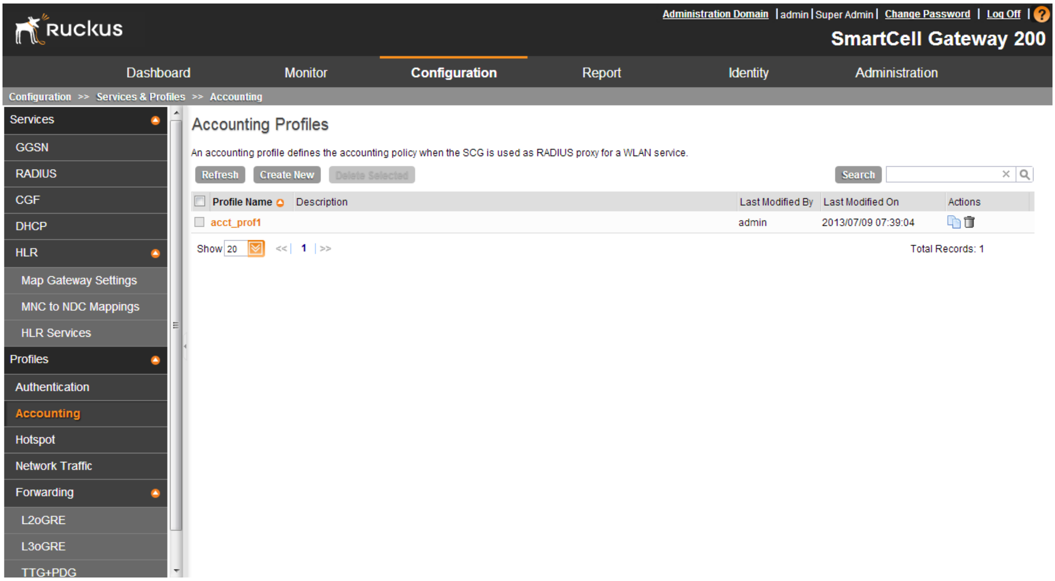
1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Accounting**. The *Accounting Profiles* page appears and displays the accounting profiles that have been added to the controller. For each accounting profile, the following details are displayed:

- Profile Name
- Description
- Last Modified By
- Last Modified On
- Actions: Displays the trash bin and clone icons. Click the trash bin icon to delete the profile. Click the clone icon to create a copy of the profile.

You have completed viewing a list of accounting profiles.

Figure 79. The Accounting Profiles page lists the profiles that have been created on the controller



Accounting Profiles

An accounting profile defines the accounting policy when the SCG is used as RADIUS proxy for a WLAN service.

□	Profile Name	Description	Last Modified By	Last Modified On	Actions
□	acct_prof1		admin	2013/07/09 07:39:04	

Deleting Accounting Profiles

Follow these steps to delete a single or multiple accounting profiles simultaneously.

1 Go to *Configuration > Services & Profiles*.

2 On the sidebar under *Profiles*, click **Accounting**. The *Accounting Profiles* page appears and lists the profiles that have been configured on the controller.

3 Delete a single or multiple profiles.

To delete a single profile:

a From the list of existing profiles, locate the profile that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the profile. A confirmation message appears.

c Click **Yes**. The page refreshes, and the profile that you deleted disappears from the view list.

To delete multiple profiles simultaneously, follow these steps:

a From the list of existing profiles, locate the profiles that you want to delete.

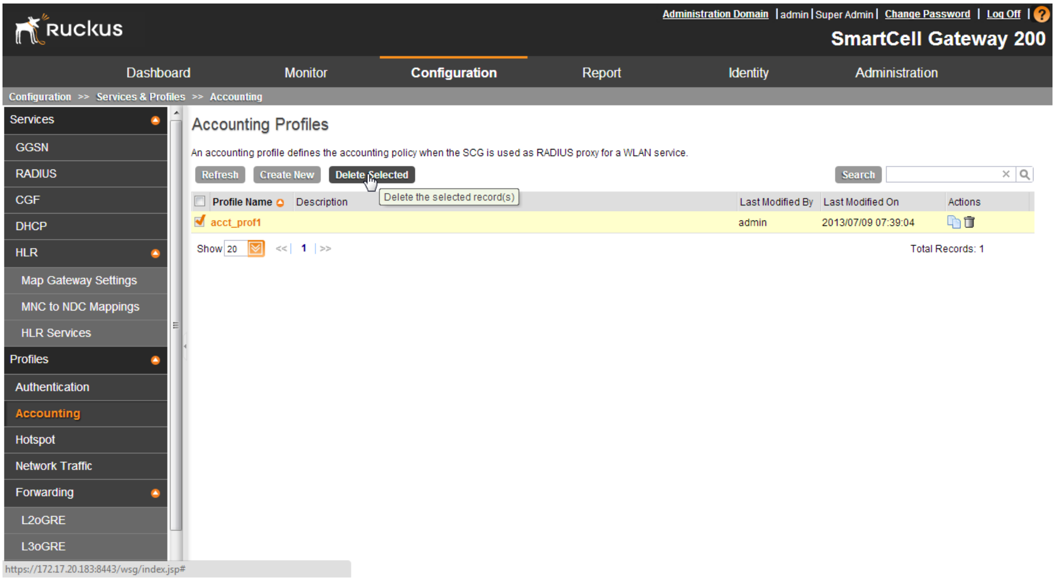
b Select the check boxes before the profiles that you want delete.

c Click **Delete Selected**. A confirmation message appears.

d Click **Yes**. The page refreshes and the profiles that you deleted disappears from the list.

You have completed deleting accounting profiles.

Figure 80. Deleting multiple profiles simultaneously



Accounting Profiles

An accounting profile defines the accounting policy when the SCG is used as RADIUS proxy for a WLAN service.

☐	Profile Name	Description	Last Modified By	Last Modified On	Actions
☑	acct_prof1		admin	2013/07/09 07:39:04	

Total Records: 1

Working with Hotspot Profiles

A hotspot profile defines the hotspot configuration that will be used for 3rd party AP zones. This section covers:

- Creating a Hotspot Profile
- Viewing Hotspot Profiles
- Deleting Hotspot Profiles

Creating a Hotspot Profile

Follow these steps to create a hotspot profile that 3rd party AP zones can use.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Hotspot**. The *Hotspot Profiles* page appears.

3 Click **Create New**. The *Create New Hotspot Profile* form appears.

4 In the *General Options* section, configure the following options:

- *Name*: Type a name for the WISPr service.
- *Description*: Type a description for the WISPr service.

5 Configure the options in the *Redirection* section.

- In *Smart Client Support*, select one of the following options:
  - **None**: Select this option to disable Smart Client support in this hotspot.
  - **Enable**: Selection this option to enable Smart Client support.
  - **Only Smart Client Allowed**: Select this option to allow only Smart Clients to connect to the hotspot. For more information, see Configuring Smart Client Support.
- In *Logon URL*, type the URL of the subscriber portal (the page where hotspot users can log on to access the hotspot portal). For more information, see Configuring the Logon URL.
- In *Start Page*, set where users will be redirected after they log in successfully:
  - **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
  - **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).

6 In the *User Session* section, configure the following options:

- *Session Timeout*: Set a time limit (in minutes) after which users will be disconnected from the hotspot portal and will be required to log on again.
- *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot portal without having to log on again.

7 In the *Location Information* section, configure the following options:

- *Location ID*: Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
  - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
  - network

  The following is an example of what the Location ID entry should look like: isocc=us,cc=1,ac=408,network=RuckusWireless

- *Location Name*: Type the name of the location of the WISPr service.

8 In *Walled Garden*, click **Create New** to add a walled garden. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account.

In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:

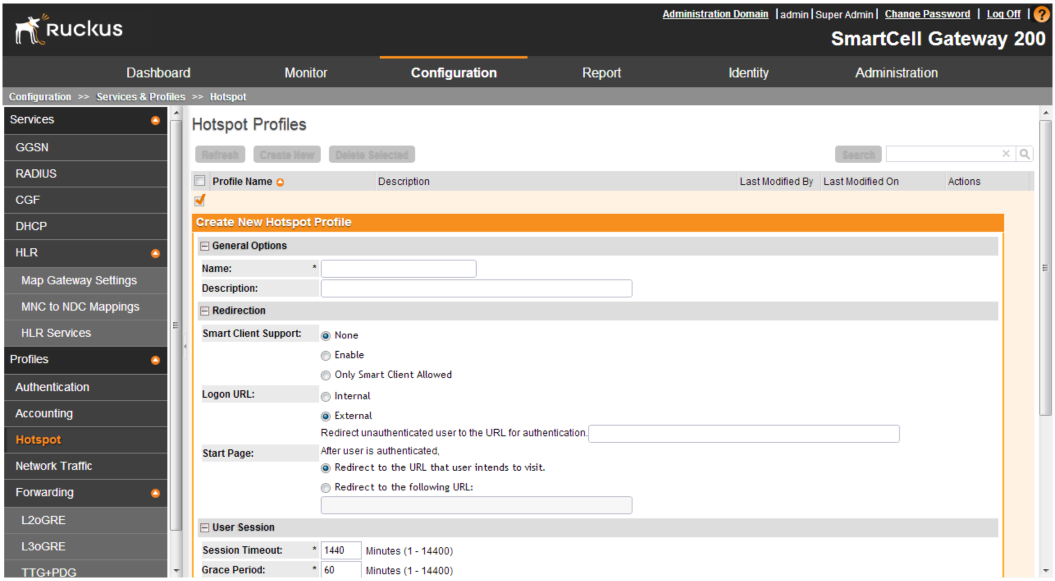
- IP address (for example, 10.11.12.13)
- IP address range (for example, 10.11.12.13-10.11.12.15)
- Classless Inter-Domain Routing or CIDR (for example, 10.11.12.100/28)
- IP address and mask (for example, 10.11.12.13 255.255.255.0)
- Exact website (for example, www.ruckuswireless.com)
- Website with special regular expression like
  - *.amazon.com
  - *.com
  - *

After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to re-authenticate when they navigate through the page.

9 Click **Create New**.

You have completed creating a hotspot profile for 3rd party AP zones.

Figure 81. The Create New Hotspot Profile form



Create New Hotspot Profile

General Options

Name: *

Description:

Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication.

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit.
○ Redirect to the following URL:

User Session

Session Timeout: * 1440 Minutes (1 - 14400)

Grace Period: * 60 Minutes (1 - 14400)

Viewing Hotspot Profiles

Follow these steps to view a list of hotspot profiles that have been created on the controller.

NOTE: If you have not created a hotspot profile, refer to Creating a Hotspot Profile.

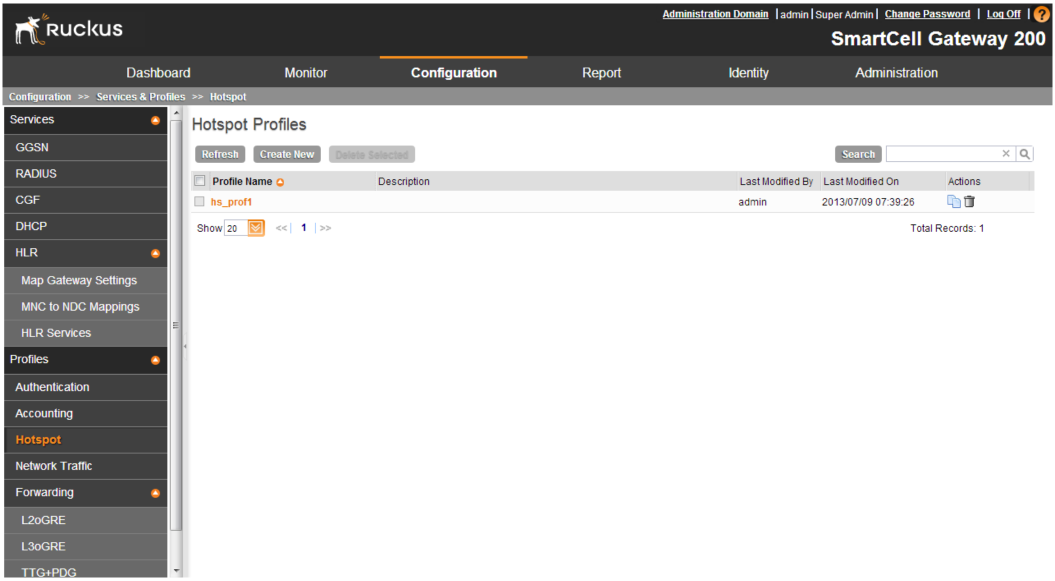
1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Hotspot**. The *Hotspot Profiles* page appears and displays the hotspot profiles that you have create. For each hotspot profile, the following details are displayed:

- Profile Name
- Description
- Last Modified By
- Last Modified On
- Actions: Displays the trash bin and clone icons. Click the trash bin icon to delete the profile. Click the clone icon to create a copy of the profile.

You have completed viewing a list of hotspot profiles.

Figure 82. The Hotspot Profiles page lists the profiles that have been created on the controller



□	Profile Name	Description	Last Modified By	Last Modified On	Actions
□	hs_prof1		admin	2013/07/09 07:39:26	

Deleting Hotspot Profiles

Follow these steps to delete a single or multiple accounting profiles simultaneously.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Hotspot**. The *Hotspot Profiles* page appears and lists the profiles that have been configured on the controller.

3 Delete a single or multiple profiles.

To delete a single profile:

a From the list of existing profiles, locate the profile that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the profile. A confirmation message appears.

c Click **Yes**. The page refreshes, and the profile that you deleted disappears from the view list.

To delete multiple profiles simultaneously, follow these steps:

a From the list of existing profiles, locate the profiles that you want to delete.

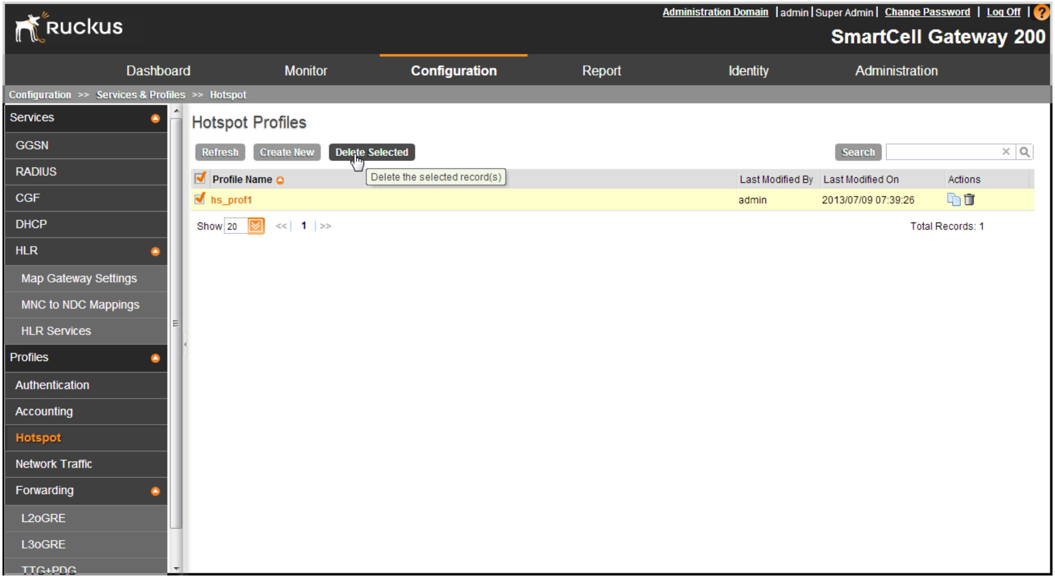
b Select the check boxes before the profiles that you want delete.

c Click **Delete Selected**. A confirmation message appears.

d Click **Yes**. The page refreshes and the profiles that you deleted disappears from the list.

You have completed deleting hotspot profiles.

Figure 83. Deleting multiple profiles simultaneously



☑ Profile Name	Last Modified By	Last Modified On	Actions
☑ hs_prof1	admin	2013/07/09 07:39:26	

Total Records: 1

Working with Network Traffic Profiles

A network traffic profile defines per AP rate limits and the access control list (ACL) rules that apply to that AP. Only super administrators have the privilege to configure network traffic profiles. MVNOs cannot view, create, edit, or delete network profiles.

Each 3rd party AP zone is required to have one network traffic profile. The controller provides a factory default network traffic profile, which is associated with a zone if an alternative is not specified while creating a new zone. The controller allows super administrators to set the default profile to a customized network traffic profile. The factory default network traffic profile is defined as no rate limits and allows all traffic.

This section covers:

- Creating a Network Traffic Profile
- Viewing Network Traffic Profiles
- Deleting Network Traffic Profiles

Creating a Network Traffic Profile

Follow these steps to create a network traffic profile.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Network Traffic**. The *Network Traffic Profiles* page appears and displays the default network traffic profile named *SCG Factory Default*.

3 Click **Create New**. The *Create New Network Traffic Profile* form appears.

4 In *Name*, type a name for the profile that you are creating.

5 In *Description*, type a brief description of the profile. This is an optional field.

6 In *Default Options*, set the *Default Traffic Handling Action* to either **Allow** or **Block**. The default setting is **Allow**.

7 In *Network Access Control List*, click **Create New** to add a network access control list, and then configure the following options:

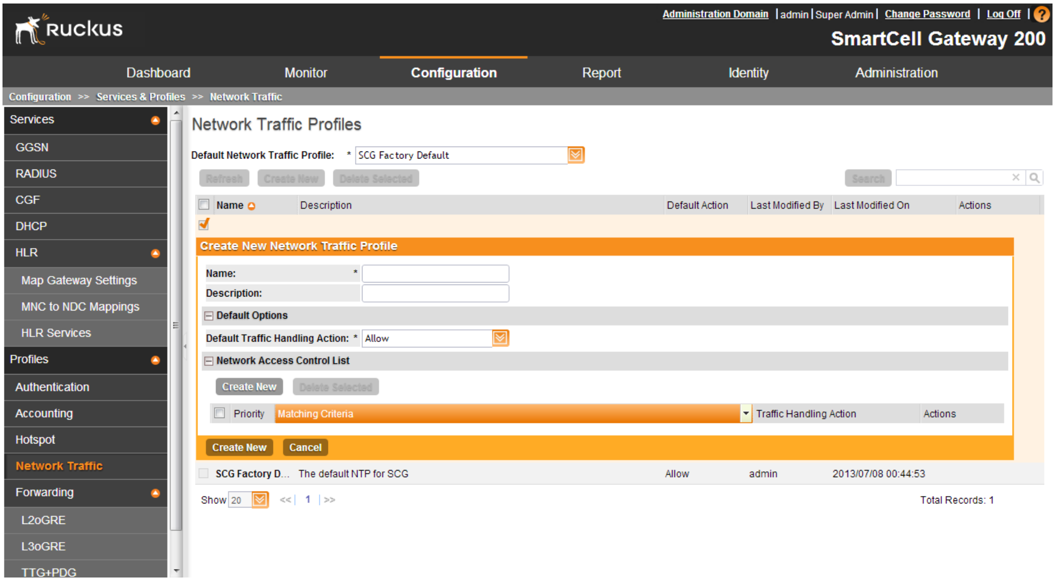
- *Source IP Range*: Type an IP address to assign to this profile, as well as a subnet mask for the IP address. This is the IP address range that will be allowed access to the network traffic profile.
- *Source Port Range*: Type a port number. To specify a range of port numbers, select the **Range** check box, and then set the starting port number and ending port number in the first and second boxes, respectively.
- *Destination IP Range*: Type the destination IP address to assign to this profile, as well as a subnet mask for the IP address. This is the IP address range that will allowed to send traffic using this network traffic profile.
- *Destination Port Range*: Type a port number. To specify a range of port numbers, select the **Range** check box, and then set the starting port number and ending port number in the first and second boxes, respectively.
- *Protocol*: Select the protocol that you want to allow or deny. If you cannot find the protocol name, type the protocol number.
- *Direction*: Select the traffic direction to which this profile will be applied. Options include **Upstream** and **Downstream** (default). This setting will limit the rate at which WLAN clients can upload or download data.

8 In *Traffic Handling Action*, set the action to apply to the traffic. Options include **Block** and **Allow**.

9 Click **Create New**.

You have completed creating a network traffic profile.

Figure 84. The Create New Network Traffic Profile form



Network Traffic Profiles

Default Network Traffic Profile: * SCG Factory Default

Create New Network Traffic Profile

Name: *

Description:

Default Options

Default Traffic Handling Action: * Allow

Network Access Control List

□	Priority	Matching Criteria	Traffic Handling Action	Actions

□	Name	Description	Default Action	Last Modified By	Last Modified On	Actions
□	SCG Factory D...	The default NTP for SCG	Allow	admin	2013/07/08 00:44:53	

Show 20 << 1 >> Total Records: 1

Viewing Network Traffic Profiles

Follow these steps to view a list of network traffic profiles that have been created on the controller.

NOTE: If you have not created a network traffic profile, refer to Creating a Network Traffic Profile.

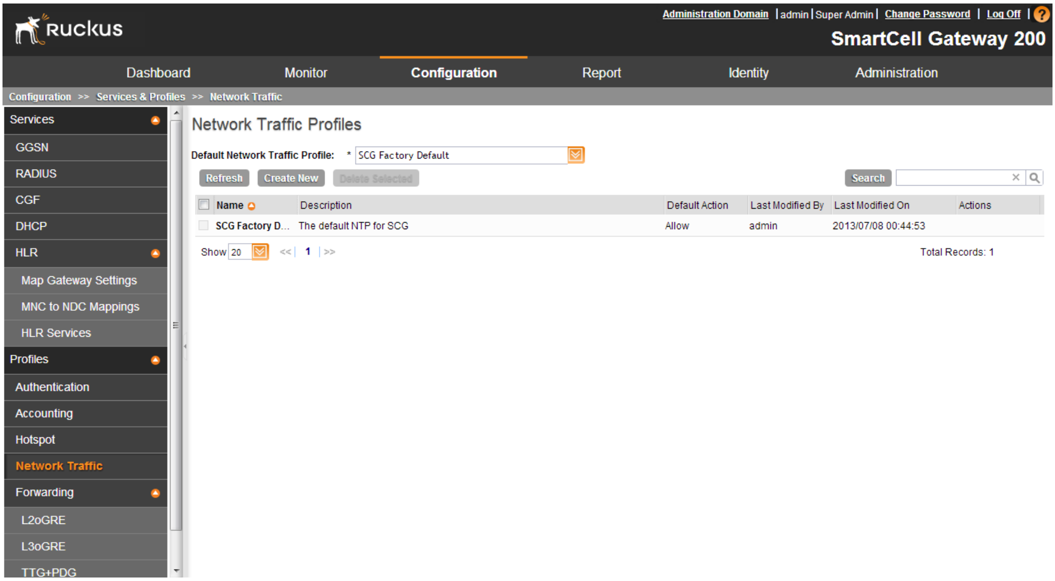
1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Network Traffic**. The *Network Traffic Profiles* page appears and displays the hotspot profiles that you have create. For each network traffic profile, the following details are displayed:

- Profile Name
- Description
- Default Action
- Last Modified By
- Last Modified On
- Actions: Displays the trash bin and clone icons. Click the trash bin icon to delete the profile. Click the clone icon to create a copy of the profile.

You have completed viewing a list of network traffic profiles.

Figure 85. The Network Traffic Profiles page lists the profiles that have been created on the controller



Network Traffic Profiles

Default Network Traffic Profile: * SCG Factory Default

□ Name	Description	Default Action	Last Modified By	Last Modified On	Actions
□ SCG Factory D...	The default NTP for SCG	Allow	admin	2013/07/08 00:44:53	

Show 20 << 1 >>
Total Records: 1

Deleting Network Traffic Profiles

Follow these steps to delete a single or multiple network traffic profiles simultaneously.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar under *Profiles*, click **Network Traffic**. The *Network Traffic Profiles* page appears and lists the profiles that have been configured on the controller.

3 Delete a single or multiple profiles.

To delete a single profile:

a From the list of existing profiles, locate the profile that you want to delete.

b Under the *Actions* column, click the icon 🗑 that is in the same row as the profile. A confirmation message appears.

c Click **Yes**. The page refreshes, and the profile that you deleted disappears from the view list.

To delete multiple profiles simultaneously, follow these steps:

a From the list of existing profiles, locate the profiles that you want to delete.

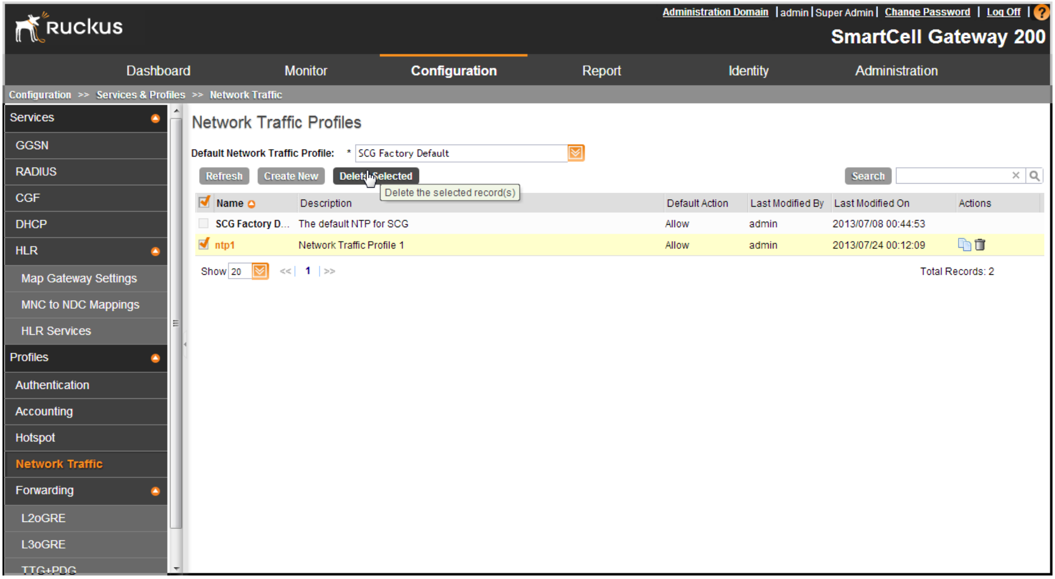
b Select the check boxes before the profiles that you want delete.

c Click **Delete Selected.** A confirmation message appears.

d Click **Yes**. The page refreshes and the profiles that you deleted disappears from the list.

You have completed deleting network traffic profiles.

Figure 86. Deleting multiple profiles simultaneously



Network Traffic Profiles

Default Network Traffic Profile: * SCG Factory Default

☑ Name	Description	Default Action	Last Modified By	Last Modified On	Actions
□ SCG Factory D...	The default NTP for SCG	Allow	admin	2013/07/08 00:44:53	
☑ ntp1	Network Traffic Profile 1	Allow	admin	2013/07/24 00:12:09	

Show 20 << 1 >> Total Records: 2

Applying a Network Traffic Profile to a 3rd Party AP Zone

NOTE: Before continuing, make sure you have already created a network traffic profile. If you have not, see Creating a Network Traffic Profile for instructions.

Follow these steps to apply a network traffic profile to a 3rd party AP zone.

1 Go to *Configuration > 3rd Party AP Zones > 3rd Party AP Zone List*.

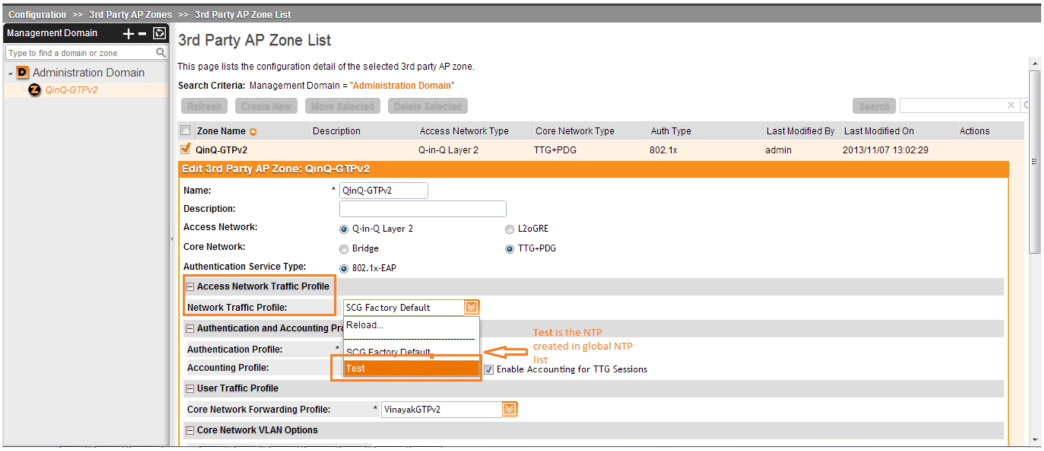
2 Under *Administration Domain*, click the 3rd party AP zone to which you want to assign a network traffic profile. The *Edit 3rd Party AP Zone: {zone-name}* form appears.

3 In *Access Network Traffic Profile*, select the network traffic profile that you want to assign to the 3rd party AP zone.

4 Click **Apply.**

You have completed applying a network traffic profile to a 3rd party AP zone.

Figure 87. In Access Network Traffic Profile, select the profile that you want to assign to the 3rd party AP zone



3rd Party AP Zone List

This page lists the configuration detail of the selected 3rd party AP zone.

Search Criteria: Management Domain = "Administration Domain"

☐	Zone Name	Description	Access Network Type	Core Network Type	Auth Type	Last Modified By	Last Modified On	Actions
☑	QinQ-GTPv2		Q-in-Q Layer 2	TTG+PDG	802.1x	admin	2013/11/07 13:02:29	

Edit 3rd Party AP Zone: QinQ-GTPv2

Name: * QinQ-GTPv2

Description:

Access Network: ● Q-in-Q Layer 2 ○ L2oGRE

Core Network: ○ Bridge ● TTG+PDG

Authentication Service Type: ● 802.1x-EAP

⊟ Access Network Traffic Profile

Network Traffic Profile: SCG Factory Default

⊟ Authentication and Accounting Pro

Authentication Profile: *

Accounting Profile: ☑ Enable Accounting for TTG Sessions

Test is the NTP created in global NTP list

⊟ User Traffic Profile

Core Network Forwarding Profile: * VinayakGTPv2

⊟ Core Network VLAN Options

Working with User Traffic Profiles

A user traffic profile defines whether the system will allow or block a particular type of traffic based on a number of attributes, including:

- Source IP address (specific IP address or IP address range)
- Source port number (specific port or port range)
- Destination IP address (specific IP address or IP address range)
- Destination port number (specific port or port range)
- Network protocol (TCP, UDP, etc.)
- Traffic direction

Creating a User Traffic Profile

Follow these steps to create a user traffic profile.

1. Go to *Configuration > Services & Profiles > Profiles > User Traffic.* The *User Traffic* page appears.
2. Click **Create New**. The *Create New User Traffic Profile* page appears.
3. In *Name*, type a name for this profile.
4. In *Description*, type a short description for this profile.

5 In *Default Access*, select whether you want the controller to allow or block users using this profile if the user traffic does not match any of the rules you defined.

6 In the *Rules* section, click **Create New**.

NOTE: By default, two default rules exist (Allow DNS and Allow DHCP) when you create a new profile. You can modify these rules or even delete them.

---

7 In *Source IP*, specify the source IP address to which this rule will apply.

- To apply this rule to an IP address range, type the network address and the subnet mask.
- To apply this rule to a single IP, clear the **Subnet** check box, and then enter the IP address.

8 In *Source Port*, specify the source port to which this rule will apply.

- To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
- To apply this rule to a single port number, clear the **Range** check box, and then enter the port number.

9 In *Destination IP*, specify the destination IP address to which this rule will apply.

- To apply this rule to an IP address range, type the network address and the subnet mask.
- To apply this rule to a single IP, clear the **Subnet** check box, and then enter the IP address.

10 In *Destination Port*, specify the source port to which this rule will apply.

- To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
- To apply this rule to a single port number, clear the Range check box, and then enter the port number.

11 In *Protocol*, select the network protocol to which this rule will apply. Supported protocols include:

- TCP
- UDP
- UDPLITE
- ICMP (ICMPv4)
- IGMP
- ESP

- AH
- SCTP

12. In *Direction*, leave as is. Only one traffic direction (upstream) is supported in this release.
13. Click **OK**.

You have completed creating a user traffic profile. The next time you a WLAN, this profile will appear as one of the options for *User Traffic Profile*.

Viewing User Traffic Profiles

Follow these steps to view a list of existing user traffic profiles.

1. Go to *Configuration > Services & Profiles > Profiles > User Traffic.* The *User Traffic Profile* page appears and displays all existing user traffic profiles and their basic settings are shown, including the:
   - User traffic profile name
   - Description
   - Default access (allow or block)
   - Actions (that you can perform)
2. To view the type of traffic that has been defined in a particular user traffic profile, click the profile name.

You have completed viewing existing user traffic profiles.

Deleting Traffic Profiles

Follow these steps to delete user traffic schedule profiles.

1. Go to *Configuration > Services & Profiles > Profiles > User Traffic.* The *User Traffic Profile* page appears.
2. Locate the profile or profiles that you want to delete.
3. Select the check boxes (first column) for the profiles that you want to delete.
4. Click **Delete Selected**.

The profiles that you selected disappear from the list. You have completed deleting user traffic profiles.

NOTE: If you are deleting a single profile, you can also click the 🗑 icon (under the *Actions* column) that is in the same row as the profile that you want to delete.

Working with Forwarding Profiles

This sections covers:

- L2oGRE Profiles
- L3oGRE Profiles
- TTG+PDG Profiles
- Mixed Mode Profiles

L2oGRE Profiles

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels. This section covers:

- Creating an L2oGRE Profile
- Viewing L2oGRE Profiles
- Deleting an L20GRE Profile

Creating an L2oGRE Profile

Follow these steps to add an L2oGRE profile.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar under *Profiles* > *Forwarding*, click **L2oGRE**. The *L2oGRE Forwarding Profiles* page appears.
3. Click **Create New**. The *Create New L2oGRE Profile* form appears.
4. In *Name*, type a name for the L2oGRE profile that you are creating.
5. In *Description*, type a brief description of the profile. This is an optional field.
6. In *Core Network Gateway Settings*, configure the following:
   - *Primary Gateway IP:* Type the IP address of the primary gateway for the L2oGRE tunnel.
   - *Secondary Gateway IP:* Type the IP address of the secondary gateway for the L2oGRE tunnel. If the primary gateway is unreachable, this gateway will be used for the L2oGRE tunnel.
   - *Gateway Path MTU*: Set it the MTU manually or use **Auto** (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.
   - *ICMP Keep-Alive Period (secs)*: Set the time in seconds between sending retry messages to the keepalive IP address. Enter an integer between 2 and 255. The default is 10 seconds.

- *ICMP Keep-Alive Retry*: Set the retry period to send messages to the keepalive IP address. The default value is 3 retries.

7 In *DHCP Relay*, configure the following options to enable the DHCP relay agent in the controller:

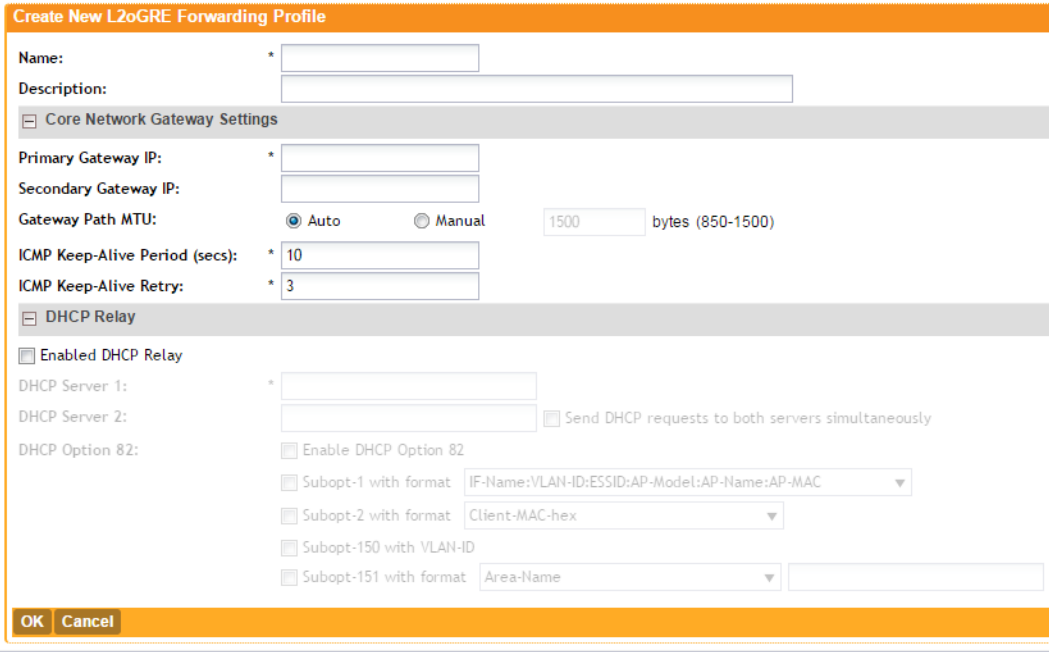
- *Enable DHCP Relay*: Select this check box to enable the DHCP relay agent in the controller.
- *DHCP Server 1*: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
- *DHCP Server 2*: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
- *DHCP Option 82*: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 suboptions by selecting the corresponding check boxes:
  - *Subopt-1 with format*: You can customize suboption 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is:

    ```
    IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC
    ```
  - Subopt 2 with format: You can customize suboption 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
  - *Subopt-150 with VLAN ID*: This suboption encapsulates the VLAN ID.
  - *Subopt-151 with format*: This suboption can encapsulate either the ESSID or a configurable Area Name.

8 Click **Create New**.

You have completed creating an L2oGRE profile.

Figure 88. The Create New L2oGRE Forwarding Profile form



Create New L2oGRE Forwarding Profile

Name: *

Description:

⊟ Core Network Gateway Settings

Primary Gateway IP: *

Secondary Gateway IP:

Gateway Path MTU: ● Auto ○ Manual 1500 bytes (850-1500)

ICMP Keep-Alive Period (secs): * 10

ICMP Keep-Alive Retry: * 3

⊟ DHCP Relay

□ Enabled DHCP Relay

DHCP Server 1: *

DHCP Server 2: □ Send DHCP requests to both servers simultaneously

DHCP Option 82: □ Enable DHCP Option 82

□ Subopt-1 with format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC ▼

□ Subopt-2 with format Client-MAC-hex ▼

□ Subopt-150 with VLAN-ID

□ Subopt-151 with format Area-Name ▼

OK Cancel

About Keep-Alive Settings

The tunnel keepalive mechanism enables, extends, and implements an interface-specific command for tunnel interfaces, and provides the ability to bring down the line protocol of a tunnel. The tunnel keepalive mechanism also addresses these additional requirements:

- The tunnel keepalive mechanism functions even if the far tunnel endpoint does not support keepalives.
- The tunnel keepalive mechanism originates keepalives.
- The tunnel keepalive mechanism processes keepalives.
- The tunnel keepalive mechanism replies to keepalive packets of the far end, even when the line protocol of the tunnel is down.

Viewing L2oGRE Profiles

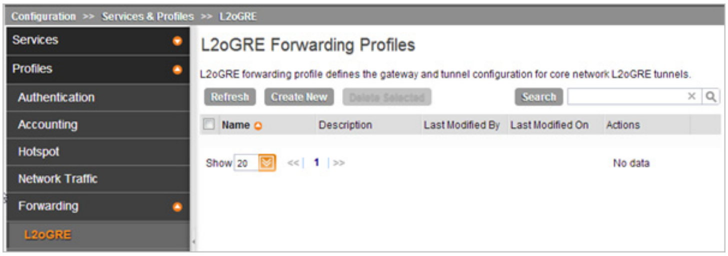
Follow these steps to view a list of L2oGRE profiles that have been created.

NOTE: If you have not created a profile, see Creating an L2oGRE Profile.

1 Go to *Configuration > Services & Profiles.*

2 On the sidebar under *Profiles > Forwarding*, click **L2oGRE**. The *L2oGRE Forwarding Profiles* page appears and displays the L2oGRE profiles that have been created.

Figure 89. List view of L2oGRE Profiles



L2oGRE Forwarding Profiles

L2oGRE forwarding profile defines the gateway and tunnel configuration for core network L2oGRE tunnels.

□	Name	Description	Last Modified By	Last Modified On	Actions

No data

Deleting an L20GRE Profile

Follow these steps to delete an L2oGRE profile.

1 On the *L2oGRE Forwarding Profiles* page, locate the L2oGRE profile that you want to delete.

2 Under the *Actions* column, click the icon 🗑 that is in the same row as the L2oGRE profile name. A confirmation message appears.

3 Click **Yes**. The page refreshes, and the L2oGRE profile that you deleted disappears from the view list.

You have completed deleting an L2oGRE profile.

L3oGRE Profiles

L3oGRE forwarding profile defines the gateway and tunnel configuration for core network of L3oGRE tunnels. This section covers:

- Viewing L3oGRE Profiles
- Adding an L3oGRE Profile
- Deleting an L20GRE Profile

Adding an L3oGRE Profile

Follow these steps to add an L3oGRE profiles.

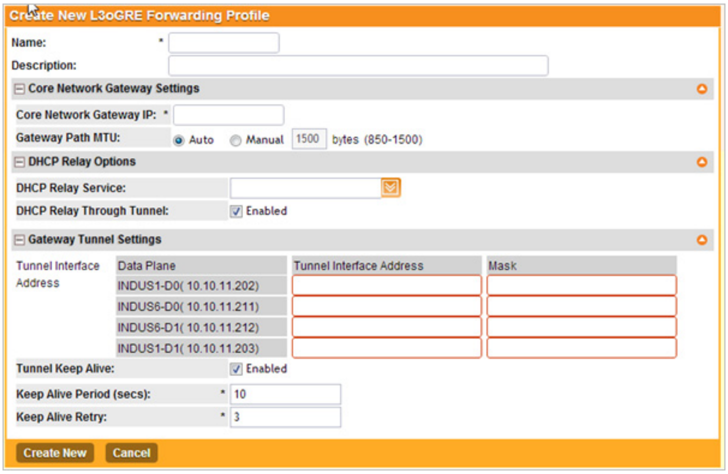
1. On the *L3oGRE Forwarding Profiles* page, click **Create New**. The *Create New* L3oGRE profiles form appears.
2. In *Name*, type a name for the L3oGRE profiles that you are adding.
3. In *Description*, give a brief description of the profile created. This is an optional field.
4. In *Core Network Gateway Settings*, configure the following:
    - *Core Network Gateway IP*
    - *Gateway Path MTU*: Set the MTU value manually or use **Auto** (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.
5. In *DHCP Relay Options*, configure the following:
    - *DHCP Relay Service*: Select the DHCP relay service that you want to use for this L3oGRE forwarding profile.
    - *DHCP Relay Through Tunnel*: Select the Enable check box to enable DHCP relay for tunneled traffic.
6. In the *Gateway Tunnel Settings* section, configure the following:
    - *Tunnel Interface Address*
    - *Tunnel Keep Alive*: Selecting the **Enable** check box enables keepalive for tunnels and allows you to configure keepalives for point-to-point GRE tunnels. The tunnel keepalive mechanism enables, extends, and implements an interface-specific command for tunnel interfaces, and delivers the ability to bring down the line protocol of a tunnel. The tunnel keepalive mechanism also addresses these additional requirements:
        - The tunnel keepalive mechanism functions even if the far tunnel endpoint does not support keepalives.

  - The tunnel keepalive mechanism originates keepalives.
  - The tunnel keepalive mechanism processes keepalives.
  - The tunnel keepalive mechanism replies to keepalive packets of the far end, even when the line protocol of the tunnel is down. You can configure keepalives with:
- *Keep Alive Period (secs)*: Specify the time in seconds between sending retry messages to the keepalive IP address. Enter an integer from 2 to 255. The default is 10.
- *Keep Alive Retry*: Specify the retry period to send messages to the keepalive IP address. The default value is 3.

7 Click **Create New** to save the new configuration details.

You have completed adding an L3oGRE profile.

Figure 90. Creating an L3oGRE Profile



Create New L3oGRE Forwarding Profile

Name: *

Description:

⊟ Core Network Gateway Settings

Core Network Gateway IP: *

Gateway Path MTU: ● Auto ○ Manual 1500 bytes (850-1500)

⊟ DHCP Relay Options

DHCP Relay Service:

DHCP Relay Through Tunnel: ☑ Enabled

⊟ Gateway Tunnel Settings

Tunnel Interface Address

Data Plane	Tunnel Interface Address	Mask
INDUS1-D0(10.10.11.202)		
INDUS6-D0(10.10.11.211)		
INDUS6-D1(10.10.11.212)		
INDUS1-D1(10.10.11.203)		

Tunnel Keep Alive: ☑ Enabled

Keep Alive Period (secs): * 10

Keep Alive Retry: * 3

Viewing L3oGRE Profiles

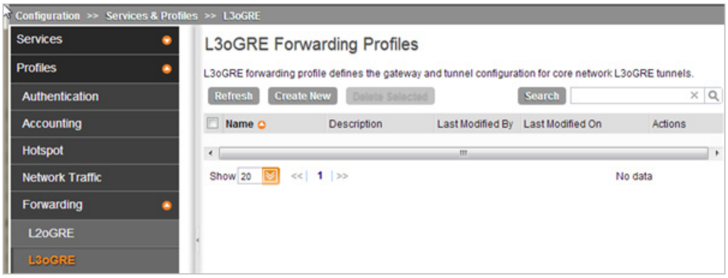
Follow these steps to view a list of L3oGRE profiles that have been created.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar, click *Forwarding* > *L3oGRE*. The *L3oGRE Forwarding Profiles* page appears, which displays the L3oGRE profiles that have been created on the controller.

If you have not created an L3oGRE profile, refer to Adding an L3oGRE Profile.

Figure 91. The L3oGRE Forwarding Profiles page lists the profiles that have been configured on the controller



L3oGRE Forwarding Profiles

L3oGRE forwarding profile defines the gateway and tunnel configuration for core network L3oGRE tunnels.

□	Name	Description	Last Modified By	Last Modified On	Actions

No data

Deleting L30GRE Profiles

Follow these steps to delete an L3oGRE profile.

1 On the *L3oGRE Forwarding Profiles* page, locate the L3oGRE profile that you want to delete.

2 Under the *Actions* column, click the icon 🗑 that is in the same row as the L3oGRE profile name. A confirmation message appears.

3 Click **Yes**. The page refreshes, and the L3oGRE profile that you deleted disappears from the view list.

You have completed deleting an L3oGRE profile.

TTG+PDG Profiles

TTG+PDG forwarding profile defines the gateway and tunnel configurations for core network GTP tunnels and LBO configurations. This section covers:

- Adding a TTG+PDG Profile
- About DHCP Relay
- Viewing TTG+PDG Profiles
- Deleting TTG+PDG Profiles

Adding a TTG+PDG Profile

Follow these steps to add a TTG+PDG profile.

1. On the *TTG+PDG Forwarding Profiles* page, click **Create New**. The *Create New TTG+PDG Forwarding Profile* form appears.
2. In *Name*, type a name for the TTG+PDG Profile that you are adding.
3. In *Description*, give a brief description of the profile created. This is an optional field.
4. In *Common Settings,* configure the following:
   - *APN Format to GSN*: Select either **DNS** or **String** from the drop-down list.
   - *APN-OI for DNS Resolution:* Specify if the APN-OI is required.
   - *# of Accounting Retry*: Specify the interval (in minutes) at which the controller will recheck the primary TTG+PDG RADIUS profile, if it is available. The default interval is 5 minutes.
   - *Accounting Retry Timeout (secs)*: Type the timeout period (in seconds) after which an expected response message is considered to have failed.
   - *PDG UE Session Idle Timeout (secs):* Type the timeout period (in seconds) after which an expected response message is considered to have failed.
5. In *DHCP Relay*, configure the following options to enable the DHCP relay agent in the controller:
   - *Enable DHCP Relay*: Select this check box to enable the DHCP relay agent in the controller.
   - *DHCP Server 1*: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
   - *DHCP Server 2*: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.

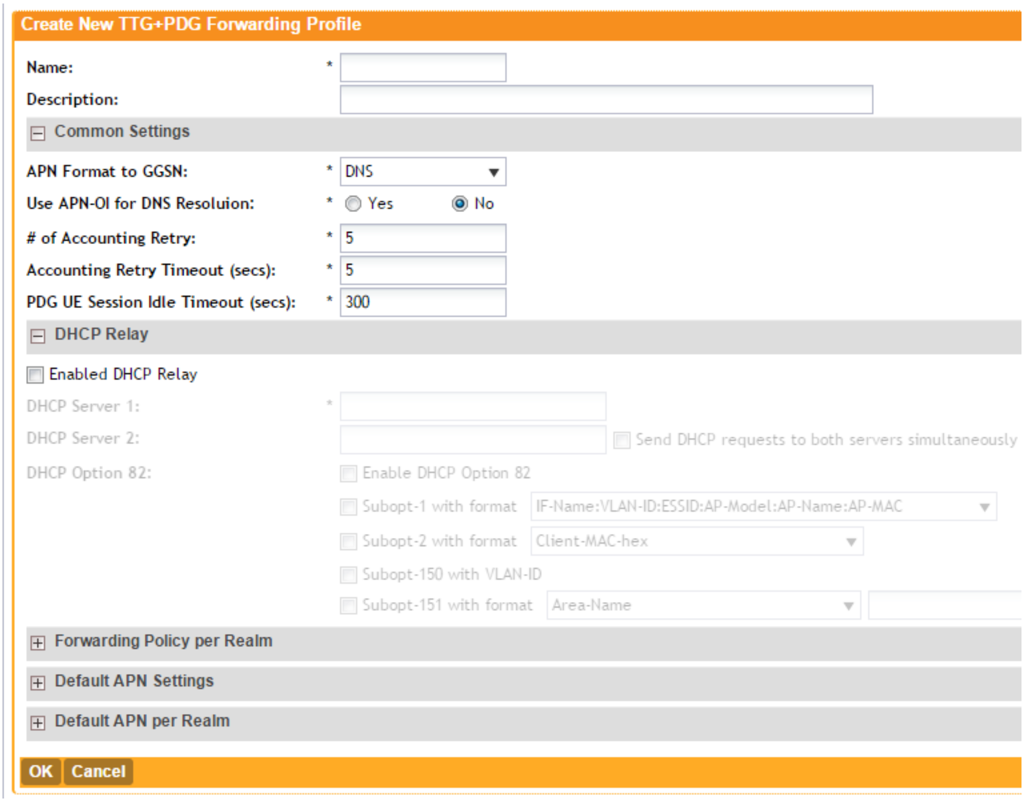
- *DHCP Option 82*: Select this check box If you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 suboptions by selecting the corresponding check boxes:
    - *Subopt-1 with format*: You can customize suboption 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is:

      ```
      IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC
      ```
    - Subopt 2 with format: You can customize suboption 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
    - *Subopt-150 with VLAN ID*: This suboption encapsulates the VLAN ID.
    - *Subopt-151 with format*: This suboption can encapsulate either the ESSID or a configurable Area Name.

6. In *Forwarding Policy Per Realm*, specify the forwarding policy for each realm in the table. Configure the following:
    - APN
    - APN Type
    - Route Type
    - Profile Name
7. In *Default APN Settings*, configure the following:
    - No Matching Realm Found
    - No Realm Specified
8. Click **Create New**.

You have completed adding a TTG+PDG profile.

Figure 92. Creating a TTG+PDG forwarding profile



Create New TTG+PDG Forwarding Profile

Name: *

Description:

⊟ Common Settings

APN Format to GGSN: * DNS

Use APN-OI for DNS Resoluion: * ○ Yes ● No

# of Accounting Retry: * 5

Accounting Retry Timeout (secs): * 5

PDG UE Session Idle Timeout (secs): * 300

⊟ DHCP Relay

□ Enabled DHCP Relay

DHCP Server 1: *

DHCP Server 2: □ Send DHCP requests to both servers simultaneously

DHCP Option 82: □ Enable DHCP Option 82

□ Subopt-1 with format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC

□ Subopt-2 with format Client-MAC-hex

□ Subopt-150 with VLAN-ID

□ Subopt-151 with format Area-Name

⊞ Forwarding Policy per Realm

⊞ Default APN Settings

⊞ Default APN per Realm

About DHCP Relay

The controller can function as a DHCP relay agent that improves network performance by converting DHCP broadcast traffic to unicast to prevent flooding the Layer 2 network (when Layer 3 Tunnel Mode is enabled, DHCP relay only applies to Tunnel Mode WLANs.)

Typically, when mobile stations acquire IP addresses through DHCP, the DHCP request and acknowledgment traffic is broadcast to all devices in the same Layer 2 environment. With Tunnel Mode WLANs, this traffic flood is wasteful in terms of bandwidth and computing power.

When DHCP Relay is enabled in a forwarding service profile, the data plane relay agent converts DHCP Discover/Request traffic to unicast UDP packets and sends them to the DHCP servers, then delivers DHCP Offer/Ack messages from the DHCP server back to the client.

The traffic flow is as follows:

1. A client sends DHCP discover broadcast.
2. The AP tunnels this DHCP discover frame to the controller.
3. The DHCP relay agent sends unicast DHCP discover packet to the DHCP server.
4. The DHCP server sends DHCP offer to the relay agent on the controller.
5. The controller sends DHCP offer back to the AP.
6. The AP sends this DHCP offer to the client.

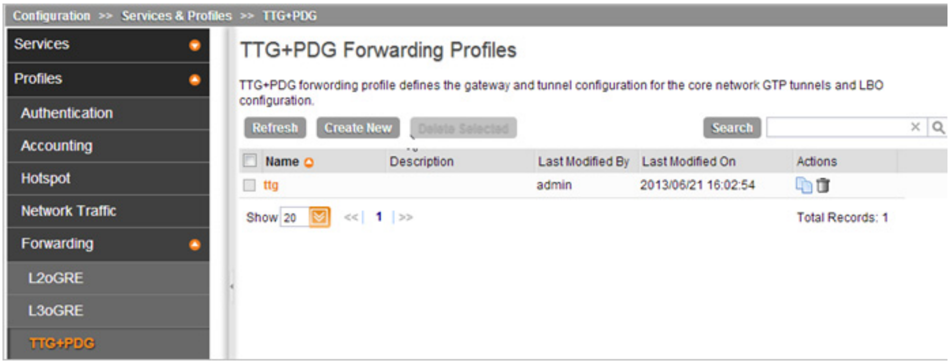
By reducing broadcast flooding, this option allows for higher client capacity in tunneled WLANs designed for VoIP phones, for example. It also allows for DHCP discovery across multiple subnets and limits DHCP broadcasts to client's AP tunnel and radio.

Viewing TTG+PDG Profiles

Follow these steps to view a list of TTG+PDG Profiles defined.

1. Go to *Configuration* > *Services & Profiles*.
2. On the sidebar, click *Forwarding* > *TTG+PDG*.
3. This section displays the TTG+PDG profile that you want to use. If you have not created a server, refer to Adding a TTG+PDG Profile.

Figure 93. List view of TTG+PDG Profiles



TTG+PDG Forwarding Profiles

TTG+PDG forwarding profile defines the gateway and tunnel configuration for the core network GTP tunnels and LBO configuration.

□	Name	Description	Last Modified By	Last Modified On	Actions
□	ttg		admin	2013/06/21 16:02:54	

Show 20 << 1 >> Total Records: 1

Deleting TTG+PDG Profiles

Follow these steps to delete a TTG+PDG Profile.

1. In the TTG+PDG Profile, locate the TTG+PDG Profile that you want to delete.
2. Under the actions column, click the icon 🗑 that is in the same row as the TTG+PDG Profile name. A confirmation message appears.
3. Click Yes.
4. The page refreshes, and the TTG+PDG Profile that you deleted disappears from the view list.

You have completed deleting a TTG+PDG profile.

PMIPv6 Profiles

A PMIPv6 forwarding profile defines the policy for handling the mobility management of a mobile node using the proxy mobile IPv6 protocol.

Configuring the Global LMA and MAG Options

Follow these steps to configure the global LMA and MAG.

1. Go to *Configuration* > *Services & Profiles*.
2. On the side menu, click *Forwarding* > *PMIPv6*. The *PMIPv6 Service Profile* page appears.
3. In the *Global LMA & MAG Options* section, configure the following sections:
   - In the *LMA Failover Options* section, configure the following:
     - **LMA keep-alive interval**: Set the number of seconds at which the mobile node will send an alive notification message to the LMA (local mobility anchor). The default is 30 seconds.
     - **LMA keep-alive retries**: Set the maximum number of attempts that the LMA will send an echo-request message to the mobile node when the mobile node is not replying. When the maximum number of retries has been reached, the LMA will declare the mobile node as unreachable. The default is five retries.
   - In the *MAG Options* section, configure the following:
     - **Binding Refresh Time**: Set the number of seconds at which the binding entries in the controller will be refreshed. The default is 300 seconds.
4. Click **Apply**.

You have completed configuring the global LMA and MAG options for the PMIPv6 service profile.

Creating a PMIPv6 Profile

Follow these steps to create a PMIPv6 profile.

1. Go to *Configuration* > *Services & Profiles*.
2. On the side menu, click *Forwarding* > *PMIPv6*. The *PMIPv6 Service Profile* page appears.
3. On the *PMIPv6 Service Profile* page, click **Create New**. The *Create PMIPv6 Profile* form appears.
4. In *Name*, type a name for the profile that you are creating.
5. In *Description*, type a short description.
6. In *Primary LMA IP*, type the IP address of the primary local mobility anchor.
7. In Secondary LMA IP, type the IP address of the secondary local mobility anchor.
8. In *MN-ID Options*, specify the identifier to use for the mobile node by selecting one of the following options:
   - *NAI from Authentication*: Select this option to use the Network Address Identifier (NAI) obtained during the authentication process.
   - *MAC48@APN*: Select this option to use the 48-bit Media Access Control (MAC) identifier.
9. Click **Create New**.

You have completed creating a PMIPv6 service profile.

Viewing PMIPv6 Profiles

Follow these steps to view the PMIPv6 profiles that have been created on the controller.

1. Go to *Configuration* > *Services & Profiles*.
2. On the side menu, click *Forwarding* > *PMIPv6*. The *PMIPv6 Service Profile* page appears.

The PMIPv6 profiles that have been created appear below the *Global LMA & MAG Options* section.

Deleting PMIPv6 Profiles

Follow these steps to delete a PMIPv6 profile.

1 Go to *Configuration* > *Services & Profiles*.

2 On the side menu, click *Forwarding* > *PMIPv6*. The *PMIPv6 Service Profile* page appears.

3 Locate the profile that you want to delete.

4 Under the *Actions* column, click the icon 🗑 that is in the same row as the mixed mode profile name. A confirmation message appears.

5 Click **Yes**. The page refreshes, and the profile that you deleted disappears from the list.

You have completed deleting a PMIPv6 profile.

Mixed Mode Profiles

A mixed mode forwarding profile defines the policy and configuration for mixed core network tunnels. This section covers:

- Adding Mixed a Mode Profile
- Viewing Mixed Mode Profiles
- Deleting Mixed Mode Profiles

Adding Mixed a Mode Profile

Follow these steps to add a mixed mode profile.

1 In *Mixed Mode Profiles*, click **Create New**. The *Create New* Mixed Mode Profiles form appears.

2 In *Name*, type a name for the mixed mode profile that you are adding.

3 In *Description*, type a brief description of the profile created. This is an optional field.

4 In *Forwarding Policy Per Realm*, specify the forwarding policy for each realm in the table. Configure the following:

   - APN
   - APN Type
   - Route Type
   - Profile Name

5 In *Default APN Settings*, configure the following:

   - No Matching Realm Found
   - No Realm Specified

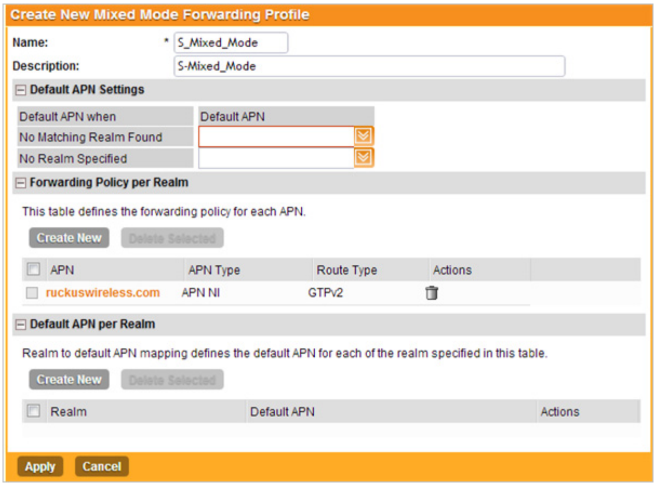
6 In *Default APN Per Realm,* configure the following:

- Realm
- Default APN

7 Click **Create New**.

You have completed adding a mixed mode profile.

Figure 94. Create a Mixed Mode Profile



Create New Mixed Mode Forwarding Profile

Name: * S_Mixed_Mode

Description: S-Mixed_Mode

⊟ Default APN Settings

Default APN when	Default APN
No Matching Realm Found	
No Realm Specified	

⊟ Forwarding Policy per Realm

This table defines the forwarding policy for each APN.

□	APN	APN Type	Route Type	Actions
□	ruckuswireless.com	APN NI	GTPv2	🗑

⊟ Default APN per Realm

Realm to default APN mapping defines the default APN for each of the realm specified in this table.

□	Realm	Default APN	Actions

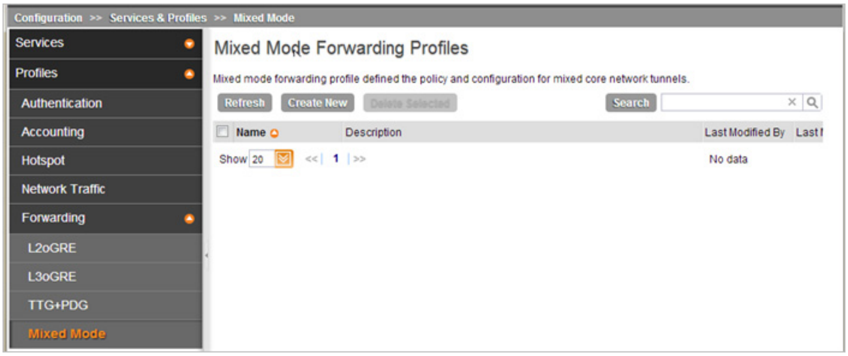
Viewing Mixed Mode Profiles

Follow these steps to view a list of mixed mode profiles that have been configured.

1 Go to *Configuration* > *Services & Profiles*. On the sidebar, click *Forwarding* > *Mixed Mode*.

2 This section displays the mixed mode profiles that you can use. If you have not created a server, refer to Adding Mixed a Mode Profile.

Figure 95. List view of Mixed Mode Profiles



Mixed Mode Forwarding Profiles

Mixed mode forwarding profile defined the policy and configuration for mixed core network tunnels.

Deleting Mixed Mode Profiles

Follow these steps to delete a mixed mode profile.

1 Go to *Configuration* > *Services & Profiles*.

2 On the sidebar, click *Forwarding* > *Mixed Mode*.

3 On the *Mixed Mode Profile* page, locate the mixed mode profile that you want to delete.

4 Under the *Actions* column, click the icon 🗑 that is in the same row as the mixed mode profile name. A confirmation message appears.

5 Click **Yes**. The page refreshes, and the mixed mode profile that you deleted disappears from the list.

You have completed deleting a mixed mode profile.

Configuring the System Settings 7

In this chapter:

- Overview of the System Settings
- Configuring General System Settings
- Configuring Cluster Planes
- Configuring Network Management
- Configuring Hosted AAA Services

Overview of the System Settings

System settings refer to general controller settings, network management settings, and plane settings.

Configuring General System Settings

To configure the general settings, go to the *Configuration* > *System* page, and then click **General System Settings** on the sidebar. Configuration tasks under general settings include:

- Setting the System Time
- Configuring the Syslog Server Settings
- Configuring the Northbound Portal Interface
- Configuring the SMTP Server Settings
- Configuring the FTP Server Settings
- Setting Critical AP Auto Tagging Rules
- Configuring Q-in-Q Ether Type
- Managing the Global User Agent Black List
- Enabling and Configuring Node Affinity
- Managing the Certificate Store
- Configuring Advanced Gateway Options

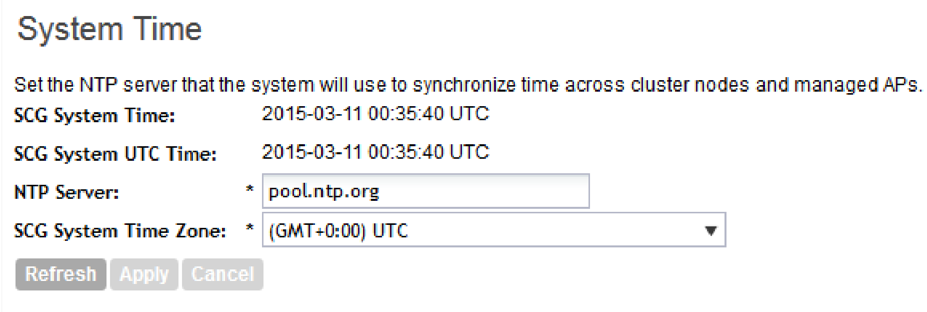
Setting the System Time

The controller uses an external network time protocol (NTP) server to synchronize the times across cluster nodes and managed access points.

Follow these steps to set the system time.

1. Go to *Configuration* > *System*.
2. Under *General System Settings*, click **System Time**.
3. In *NTP Server*, type the server address that you want to use. The default NTP server address is `pool.ntp.org`.
4. In *System Time Zone*, select the time zone that you want the controller to use. The default time zone is `(GMT +0:00) UTC`.
5. Click **Apply**.

Figure 96. System time settings



System Time

Set the NTP server that the system will use to synchronize time across cluster nodes and managed APs.

SCG System Time: 2015-03-11 00:35:40 UTC

SCG System UTC Time: 2015-03-11 00:35:40 UTC

NTP Server: * pool.ntp.org

SCG System Time Zone: * (GMT+0:00) UTC

How APs Synchronize Time with the Controller

When an AP joins the controller, it automatically synchronizes its time with the controller system time. After that, the AP automatically synchronizes its time with the controller every day.

Configuring the Syslog Server Settings

The controller maintains an internal log file of current events and this file has a fixed capacity. At a certain point, the controller will start deleting the oldest entries in log file to make room for newer entries. If you want to keep a permanent record of all events that the controller generated, you can configure the controller to send the log contents to a syslog server on the network.

Follow these steps to configure the syslog server settings.

1 Go to *Configuration* > *System*.

2 Under *General System Settings*, click **Syslog Server**. The *Syslog Server Settings* page appears.

3 Select the **Enable logging to remote syslog server** check box.

4 In *Syslog Server Host*, type the IP address of the syslog server on the network.

5 In *Syslog Server Port*, type the syslog port number on the server.

NOTE: To verify that the syslog server that you intend to use is reachable, click the **Ping Syslog Server** button.

6 In *Event Filter*, select one of the following options to specify which events will be sent to the syslog server:

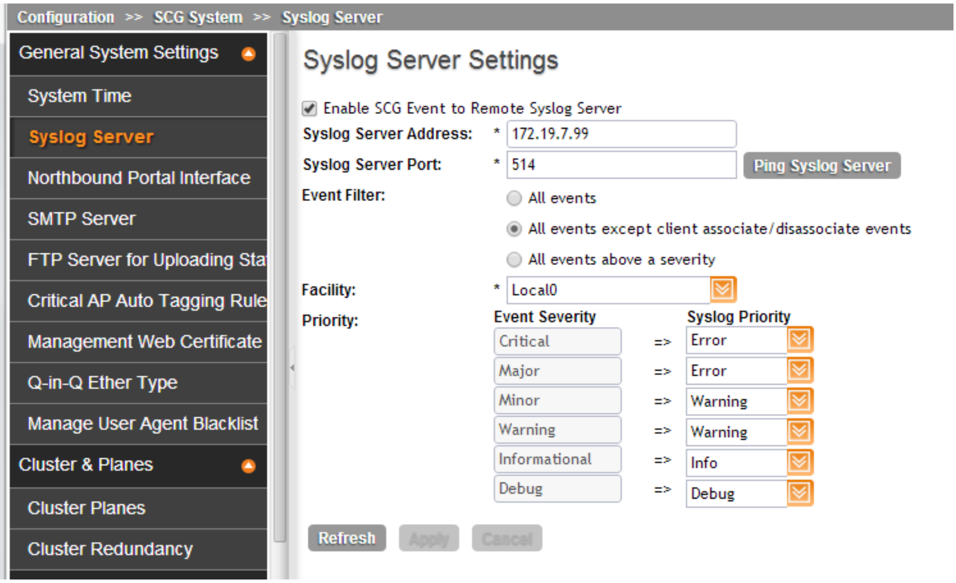
- **All events**: Click this option to send all controller events to the syslog server.
- **All events except client associate/disassociate events**: Click this option to send all controller events (except client association and disassociation events) to the syslog server.
- **All events above a severity**: Click this option to send all controller events that are above the event severity that you specify in *Event Filter Severity*.
    - *Event Filter Severity*: (This option only appears when **All events above a severity** is selected.) Select the lowest severity level for which events will be sent to the syslog server. For example, if you select **Major**, all events that are major and higher (including critical) will be sent to the syslog server. For the order of event severity that the controller follows, see Event Severity Levels.

7 In *Facility*, select the facility level that will be used by the syslog message. Options include Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7.

8 In *Priority*, accept or change the default severity to priority mapping. See Default Event Severity to Syslog Priority Mapping.

9 Click **Apply**.

Figure 97. Syslog server settings



Configuration >> SCG System >> Syslog Server
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Sta
Critical AP Auto Tagging Rule
Management Web Certificate
Q-in-Q Ether Type
Manage User Agent Blacklist
Cluster & Planes
Cluster Planes
Cluster Redundancy

Syslog Server Settings

☑ Enable SCG Event to Remote Syslog Server

Syslog Server Address: * 172.19.7.99

Syslog Server Port: * 514

Event Filter:
○ All events
● All events except client associate/disassociate events
○ All events above a severity

Facility: * Local0

Priority:

Event Severity		Syslog Priority
Critical	=>	Error
Major	=>	Error
Minor	=>	Warning
Warning	=>	Warning
Informational	=>	Info
Debug	=>	Debug

Event Severity Levels

Table 6 describes the event severity levels (1 to 6, with 1 being the most severe) that the controller follows.

Table 6. Event severity levels in the controller

Level	Message	Description
1	Critical	A critical condition that must resolved immediately
2	Major	An error condition that must be resolved
3	Minor	An error condition that must be checked to determine if it needs to be resolved
4	Warning	Warning message, not an error, but indication that an error will occur if action is not taken
5	Informational	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
6	Debug	Info useful to developers for debugging the application, not useful during operations.

Default Event Severity to Syslog Priority Mapping

Table 7 lists the default event severity to syslog priority mapping in the controller.

Table 7. Event severity to syslog priority mapping

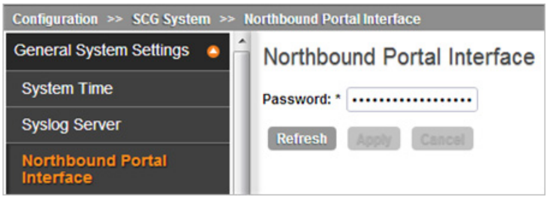
Event Severity	Syslog Priority
Critical	Error
Major	Error
Minor	Warning
Warning	Warning
Informational	Info
Debug	Debug

Configuring the Northbound Portal Interface

Follow these steps to configure the northbound portal interface.

1. Go to the *Northbound Portal Interface* section.
2. In **Password**, type the password for the northbound portal interface.
3. Click **Apply**.

Figure 98. The Northbound Portal Interface section


Configuration >> SCG System >> Northbound Portal Interface
General System Settings
System Time
Syslog Server
Northbound Portal Interface
Refresh
Apply
Cancel

Northbound Portal Interface

Password: * ••••••••••••••••••

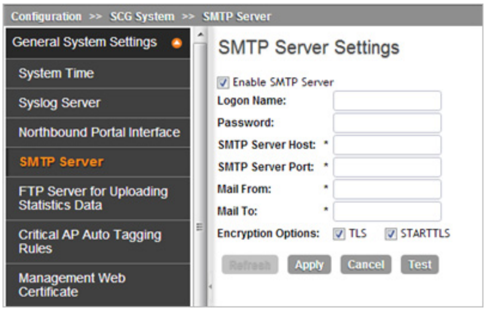
Configuring the SMTP Server Settings

If you want to receive copies of the reports that the controller generates, configure the SMTP server settings and the email address to which the controller will send the reports. Follow these steps to configure the SMTP server settings.

1. Go to the *SMTP Server Settings* section.
2. Select the **Enable SMTP Server** check box.
3. In **Logon Name**, type the logon or user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail™ or Gmail™), you typically have to type your complete email address.
4. In **Password**, type the password that is associated with the user name above.
5. In **SMTP Server Host**, type the full name of the server provided by your ISP or mail administrator. Typically, the SMTP server name is in the format smtp.company.com.

- In **SMTP Server Port**, type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is 25 or 587. The default SMTP port value is 25.
- In **Mail From**, type the email address from which the controller will send email notifications.
- In **Mail To**, type the email address to which the controller will send alarm messages. You can send alarm messages to a single email address.
- If your mail server uses encryption, select the encryption method in Encryption Options. Options include **TLS** and **STARTTLS**. Check with your ISP or mail administrator for the correct encryption settings that you need to set.
- Click **Apply**.

Figure 99. The SMTP Server Settings section



Configuration >> SCG System >> SMTP Server
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Statistics Data
Critical AP Auto Tagging Rules
Management Web Certificate
Refresh
Apply
Cancel
Test

SMTP Server Settings

☑ Enable SMTP Server
Logon Name:
Password:
SMTP Server Host: *
SMTP Server Port: *
Mail From: *
Mail To: *
Encryption Options: ☑ TLS ☑ STARTTLS

Configuring the FTP Server Settings

Follow these steps to configure the FTP server settings for uploading raw report data (in CSV format).

1 Go to the *FTP Settings for Uploading Statistics* section.

2 Select the **Enable uploading statistics data to FTP server** check box.

3 In *Statistics Data Interval*, select the time interval at which the controller uploads a copy of raw statistical data to the FTP server. Options include:

- **Hourly**: If you select this option, the controller will upload data to the FTP server every 20th minute of the hour (for example, 00:20, 01:20, 02:20 and so on).
- **Daily**: If you select this option, the controller will upload data to the FTP server at 12:35AM every day.

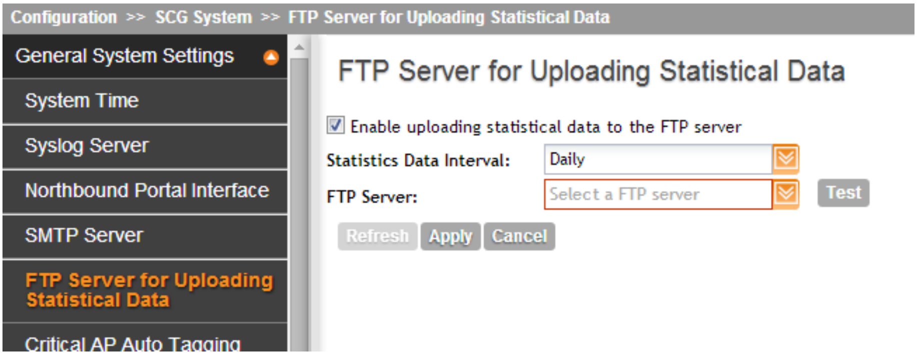
4 In *FTP Server*, select the FTP server to which you want to upload the statistics data. The FTP server options that appear here are those that you created in Configuring FTP Services.

5 To verify that the FTP server settings and logon information are correct, click **Test**. If the server and logon settings are correct, the following message appears:

```
Test completed successfully.
```

6 Click **Apply**.

Figure 100. FTP server settings



Configuration >> SCG System >> FTP Server for Uploading Statistical Data
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Statistical Data
Critical AP Auto Tagging
FTP Server for Uploading Statistical Data

☑ Enable uploading statistical data to the FTP server

Statistics Data Interval: Daily

FTP Server: Select a FTP server

Test
Refresh
Apply
Cancel

NOTE: For detailed information on the statistics files that are exported to the FTP server and their content, see Statistics Files the Controller Exports to an FTP Server.

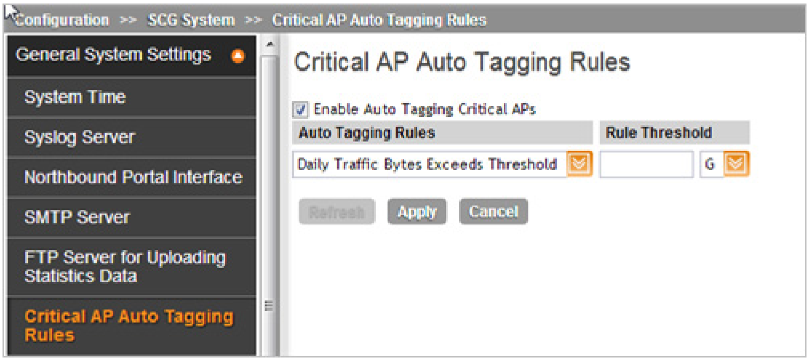
Setting Critical AP Auto Tagging Rules

A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface. Follow these steps to tag critical APs automatically.

1. Go to the *Critical AP Auto Tagging Rules* section.
2. Select the **Enable Auto Tagging Critical APs** check box.
3. Under *Auto Tagging Rules*, select **Daily Traffic Bytes Exceeds Threshold**.
4. Under *Rule Threshold*, specify the threshold:
5. In the first box, type a value that you want to set as the traffic threshold. This value will be applied in conjunction with the data unit that you will select in the second box.
6. In the second box, select the data unit for the threshold – M for megabytes or G for gigabytes.
7. Click **Apply**.

APs that exceed the daily traffic threshold that you specified will appear highlighted on the AP List page and the *Access Point* details page. Additionally, the controller will send an SNMP trap to notify that an AP has been disconnected.

Figure 101. Critical AP tagging rules


Configuration >> SCG System >> Critical AP Auto Tagging Rules
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Statistics Data
Critical AP Auto Tagging Rules
Refresh
Apply
Cancel

Critical AP Auto Tagging Rules

☑ Enable Auto Tagging Critical APs

Auto Tagging Rules	Rule Threshold
Daily Traffic Bytes Exceeds Threshold	G

Configuring Q-in-Q Ether Type

Follow these steps to configure the Q in Q Ether type.

1 Go to *Configuration* > *System*.

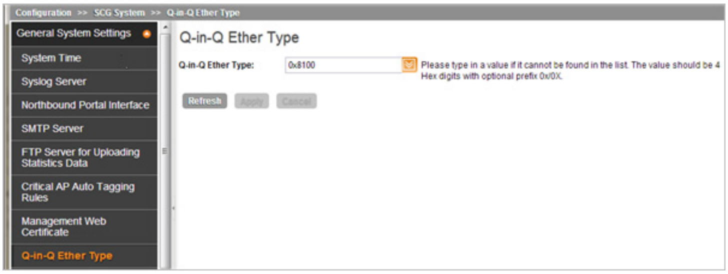
2 On the sidebar, click **Q-in-Q Ether Type**. The *Q-in-Q Ether Type* page appears.

3 From the drop-down list, select the Q-in-Q Ether Type format. Alternatively, you can type in a value if it cannot be found on the list. The value should be 4 Hex digits with optional prefix 0x/0X.

4 Click **Apply** to save the changes.

You have completed configuring the Q-in-Q Ether Type.

Figure 102. Configuring the Q-in-Q Ether Type


Configuration >> SCG System >> Q-in-Q Ether Type
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Statistics Data
Critical AP Auto Tagging Rules
Management Web Certificate
Q-in-Q Ether Type
Refresh
Apply
Cancel

Q-in-Q Ether Type

Q-in-Q Ether Type: 0x8100

Please type in a value if it cannot be found in the list. The value should be 4 Hex digits with optional prefix 0x/0X.

Managing the Global User Agent Black List

Follow these steps to configure the global user agent black list.

1 Go to *Configuration* > *System*.

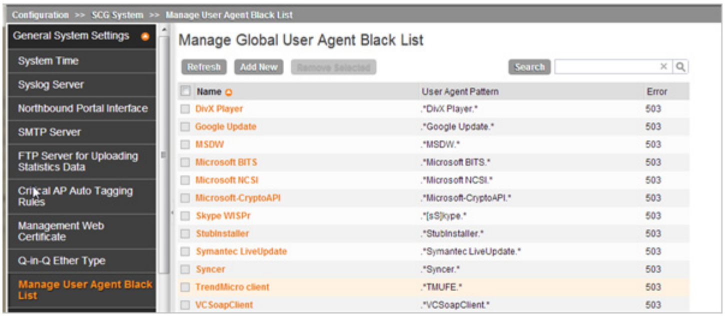
2 On the sidebar, click **Manage Global User Agent Black List** to view the page.

3 Click **Add New** to enter the name, user agent pattern, and error.

4 Click **Save**.

You have completed adding an agent to the black list.

Figure 103. Global user agent black list


Configuration >> SCG System >> Manage User Agent Black List
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Statistics Data
Critical AP Auto Tagging Rules
Management Web Certificate
Q-in-Q Ether Type
Manage User Agent Black List
Refresh
Add New
Remove Selected
Search

Manage Global User Agent Black List

Name	User Agent Pattern	Error
DivX Player	.*DivX Player.*	503
Google Update	.*Google Update.*	503
MSDW	.*MSDW.*	503
Microsoft BITS	.*Microsoft BITS.*	503
Microsoft NCSI	.*Microsoft NCSI.*	503
Microsoft-CryptoAPI	.*Microsoft-CryptoAPI.*	503
Skype WISPr	.*[sS]kype.*	503
StubInstaller	.*StubInstaller.*	503
Symantec LiveUpdate	.*Symantec LiveUpdate.*	503
Syncer	.*Syncer.*	503
TrendMicro client	.*TMUFE.*	503
VCSoapClient	.*VCSoapClient.*	503

Enabling and Configuring Node Affinity

Node affinity enables administrators to manually configure the controller nodes to which APs will connect. You do this by setting the order of preferred nodes on the Node Affinity page.

Node affinity is implemented at the AP zone level, which means that all APs that belong to a zone will have the same node affinity settings.

If you want APs that belong to the same zone to connect to the same node whenever possible, you can configure set the preferred node for a particular zone.

CAUTION! Enabling node affinity automatically disables cluster redundancy.

Follow these steps to enable and configure node affinity.

1 Go to *Configuration* > *System* > *General System Settings* > *Node Affinity*.

2 Select the **Enable Node Affinity** check box, and then click **Apply**.

3 Edit the default node affinity profile or create a new profile. An affinity profile defines the order of the nodes to which APs that belong to the same zone will connect.

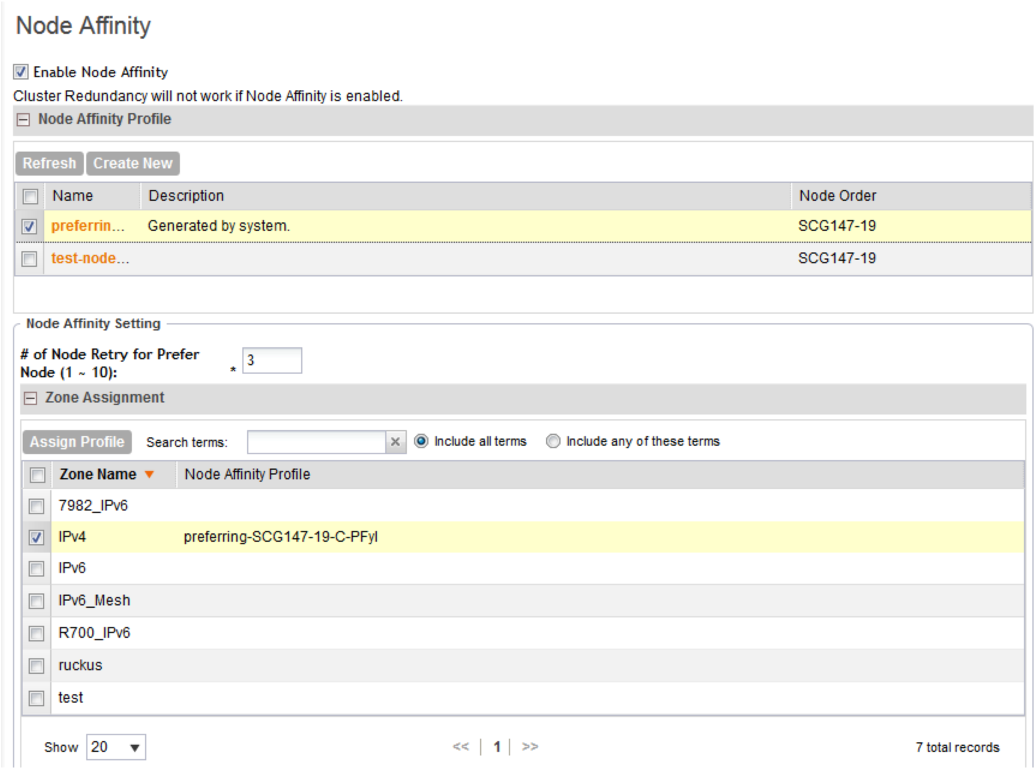
- To edit the default profile, click the profile name that appears under the *Node Affinity Profile* section. The *Edit Node Affinity Profile* form appears and displays all nodes that belong to the cluster. Click the green up and down buttons under the *Action* column to set the order of node priority. Make sure that the preferred node is at the top of the list.
- To create a new, click **Create New**. In the *Create Node Affinity Profile* form, type a name and description, and then click the green up and down buttons under the *Action* column to set the order of node priority. Make sure that the preferred node is at the top of the list. Click **OK** when done.

4. In the *Node Affinity Setting* section, set the number of times an AP will attempt to connect to the preferred node. The default value is 3 and the accepted range is 1 to 10. If the AP is unable to connect to the preferred node, it will attempt to connect to the node that is next in the order of node priority.
5. In the *Zone Assignment* section, set the node affinity profile that you want each zone to use. Do the following:

   a. Select the check box for the zone
   b. Click **Assign Profile**.
   c. In *Node Affinity Profile*, select the profile that you want to assign to the node.
   d. Click **Apply**.

   Repeat this procedure for each zone.
6. Click **Apply** at the bottom of the page to save your changes.

Figure 104. Use the Node Affinity page to set the preferred node of each zone



Node Affinity

☑ Enable Node Affinity

Cluster Redundancy will not work if Node Affinity is enabled.

⊟ Node Affinity Profile

□	Name	Description	Node Order
☑	preferrin...	Generated by system.	SCG147-19
□	test-node...		SCG147-19

Node Affinity Setting

# of Node Retry for Prefer Node (1 ~ 10): * 3

⊟ Zone Assignment

Search terms: ● Include all terms ○ Include any of these terms

□	Zone Name ▼	Node Affinity Profile
□	7982_IPv6	
☑	IPv4	preferring-SCG147-19-C-PFyl
□	IPv6	
□	IPv6_Mesh	
□	R700_IPv6	
□	ruckus	
□	test	

Show 20 ▼ << | 1 | >> 7 total records

Managing the Certificate Store

The certificate store is the central storage for all the security certificates that the controller uses for its web interface, AP portal, and hotspots.

By default, a Ruckus Wireless-signed SSL certificate (or security certificate) exists in the controller. However, because this default certificate is signed by Ruckus Wireless and is not recognized by most web browsers, a security warning appears whenever you connect to the web interface or users connect to the AP portal or a hotspot. To prevent these security warnings from appearing, you can import an SSL certificate that is issued by a recognized certificate authority.

This section describes the steps you need to perform to import and apply an SSL certificate to the web interface, AP portal, or hotspots. Topics include:

- Generating a Certificate Signing Request
- Importing an SSL Certificate
- Assigning Certificates to Services

CAUTION! The certificate that you will use for Hotspot 2.0 OSEN must be issued by a certificate authority (CA) authorized by the Wi-Fi Alliance (WFA). Otherwise, it will not appear on the list of certificates that you can use for Hotspot 2.0 OSEN.

NOTE: If you are implementing Hotspot 2.0 on the network and you want to support anonymous authentication using OSU Server-Only Authenticated L2 Encryption Network (OSEN), you will need to import a trust root certificate, server or intermediate certificate and private key.

Generating a Certificate Signing Request

This section describes how to generate a certificate signing request (which you need to obtain a signed certificate) and how to import a signed certificate into the controller.

NOTE: If you already have an SSL certificate that you want to import into the controller, go to Importing an SSL Certificate.

If you do not have an SSL certificate, you will need to create a certificate signing request (CSR) file and send it to an SSL certificate provider to purchase an SSL certificate. The controller web interface provides a form that you can use to create the CSR file. Follow these steps to generate a certificate request.

1. Go to *Configuration* > *System*.
2. On the sidebar, click **Certificate Store**. The *Certificate Store* page appears.
3. In the *Certificate Signing Request (CSR)* section, click **Generate**. The *Generate New Certificate Signing Request (CSR)* form appears.
4. In *Name*, type a name for this CSR.
5. In *Description*, type a description for this CSR.
6. In the *Certificates Signing Request (CSR)* section, fill out the following boxes:
   - *Common Name*: Type the fully qualified domain name of your Web server. This must be an exact match (for example, `www.ruckuswireless.com`).
   - *Email*: Type your email address (for example, `joe@ruckuswireless.com`).
   - *Organization*: Type the complete legal name of your organization (for example, `Ruckus Wireless, Inc.`). Do not abbreviate your organization name.
   - *Organization Unit*: Type the name of the division, department, or section in your organization that manages network security (for example, `Network Management`).
   - *Locality/City*: Type the city where your organization is legally located (for example, `Sunnyvale`).
   - *State/Province*: Type the state or province where your organization is legally located (for example, `California`) Do not abbreviate the state or province name.
   - *Country*: Select the country where your organization is location from the drop-down list.

7 Click **OK**. The controller generates the certificate request. When the certificate request file is ready, your web browser automatically downloads it.

8 Go to the default download folder of your Web browser and locate the certificate request file. The file name is `myreq.zip`.

9 Use a text editor (for example, Notepad) to open the certificate request file.

10 Go to the website of your preferred SSL certificate provider, and then follow the instructions for purchasing an SSL certificate.

11 When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr, and then complete the purchase.

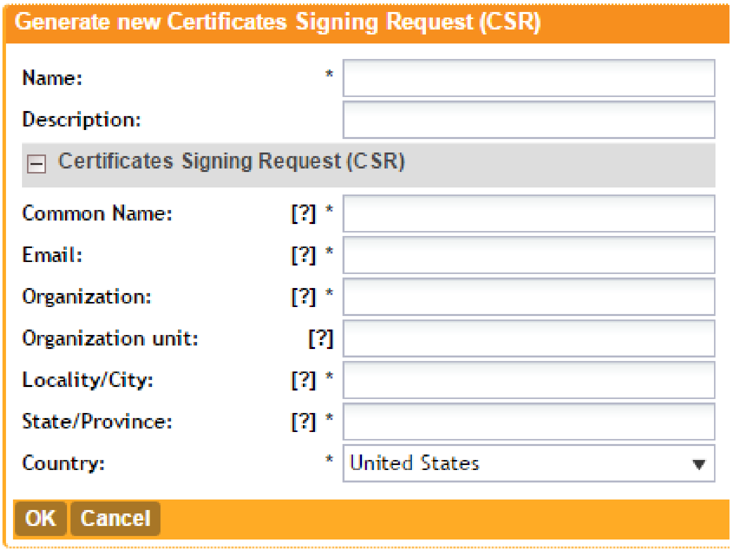
After the SSL certificate provider approves your CSR, you will receive the signed certificate via email. The following is an example of a signed certificate that you will receive from your SSL certificate provider:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBƒnsDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLC
BJbmMuMR8wHQYDVQQLƒnBgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLnZlcmlzaWduLmNvƒnbTBDBggrBgEFBQcwAoY3aHR0cD
ovL1NWUlNlY3VyZS1haWEudmVyaXNpZ24uY29tƒnL1NWUlNlY3VyZTIw
MDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWƒnFglpbW
FnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGD
AmƒnFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYw
DQYJKoZIhvcNƒnAQEFBQADggEBAI/S2dmm/kgPeVAlsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMƒnnoc3DMyDjx0SrI9lkPsn223
CV3UVBZo385g1T4iKwXgcQ7/WF6QcUYOE6HK+4ZGcƒnHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
ƒn0pykSldW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwH3BuB9wqpRjUahTiƒnK1V1-
ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGn
wSxAƒnYtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=ƒn
-----END CERTIFICATE-----
```

12 Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You may now import the signed certificate into the controller. Refer to Importing an SSL Certificate for more information.

Figure 105. Generating a certificate signing request



Generate new Certificates Signing Request (CSR)

Name: *

Description:

⊟ Certificates Signing Request (CSR)

Common Name: [?] *

Email: [?] *

Organization: [?] *

Organization unit: [?]

Locality/City: [?] *

State/Province: [?] *

Country: * United States ▼

Importing an SSL Certificate

When you have an SSL certificate issued by an SSL certificate provider, you can import it into the controller and use it for HTTPS communication. To complete this procedure, you will need the following items:

- The signed server certificate
- The intermediate CA certificate (at least one)
- The private key file

NOTE: The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

Follow these steps to import a signed server certificate.

1 Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.

2 Go to *Configuration* > *System*.

3 On the sidebar, click **Certificate Store**. The *Certificate Store* page appears.

4 In the *Installed Certificates* section, click **Import**. The *Import New Certificate* form appears.

5 Import the server certificate by completing the following steps:

   a In *Server Certificate*, click **Browse**. The *Open* dialog box appears.

   b Locate and select the certificate file, and then click **Open**.

6 Import the intermediate CA certificate by completing the following steps:

   a In *Intermediate CA certificate*, click **Browse**. The *Open* dialog box appears.

   b Locate and select the intermediate CA certificate file, and then click **Open**.

7 If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, repeat the above step.

NOTE: If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate. See the *Hotspot 2.0 Portal Integration Reference Guide* for this release.

8 When you finish uploading all the required intermediate certificates, import the private key file either by uploading file itself or selecting the CSR you generated earlier.

   - To upload the private key file, click **Upload**, then click **Browse**, then locate and select the private key file, and then click **Open**.

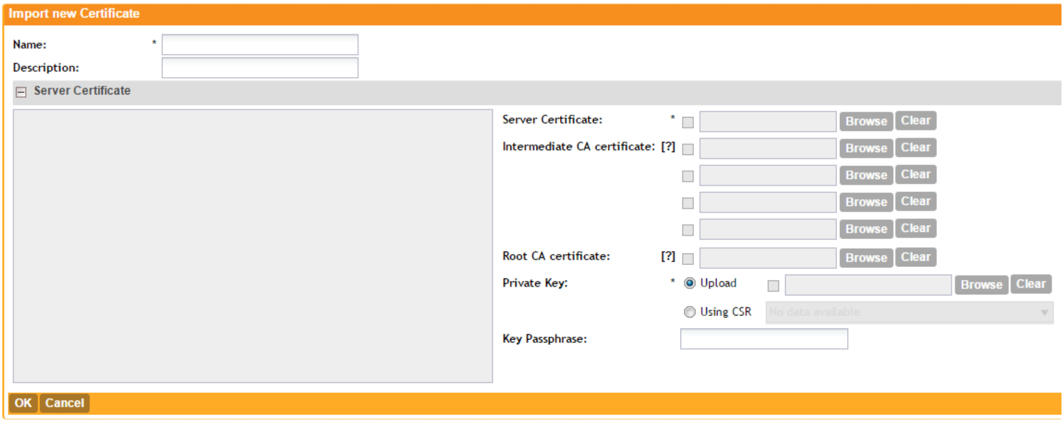
   a To select the CSR, click **Using CSR**, then select the CSR that you generated earlier.

9 In *Key Passphrase*, enter the passphrase that has been assigned to private key file.

10 Click **OK**. The page refreshes and the certificate you imported appears in the Installed Certificate section.

You have completed importing a signed SSL certificate to the controller.

Figure 106. The Import New Certificate form



Import new Certificate

Name: *

Description:

Server Certificate

Server Certificate: * □

Intermediate CA certificate: [?] □ □ □ □ □

Root CA certificate: [?] □

Private Key: * ● Upload □ ○ Using CSR No data available

Key Passphrase:

Assigning Certificates to Services

Follow these steps to specify the certificate that each secure service will use.

1 Go to *Configuration* > *System*.

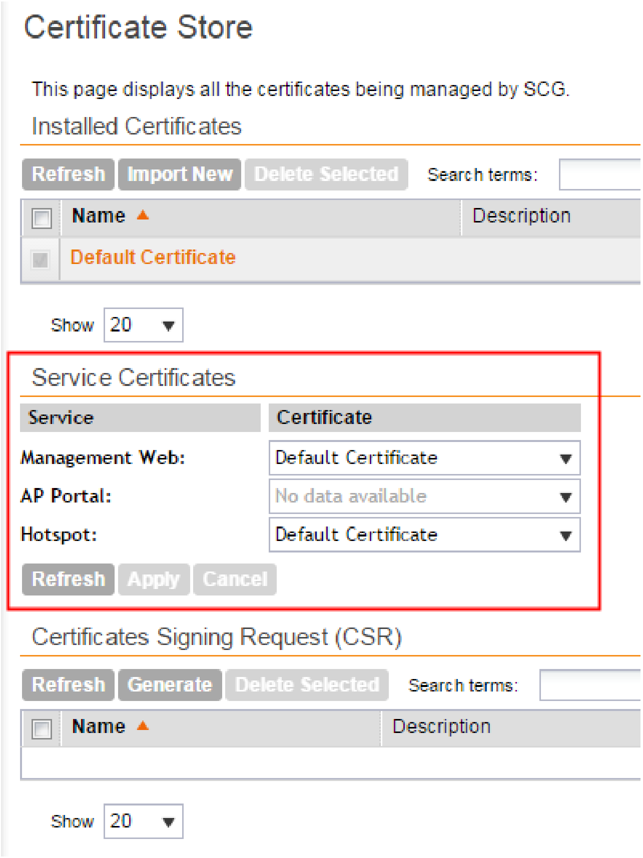
2 On the sidebar, click **Certificate Store**. The *Certificate Store* page appears.

3 In the *Service Certificates* section, select the certificate that you want to use for each service.

4 Click **Apply**.

You have completed assigning certificates to services.

Figure 107. The Service Certificates section



Certificate Store

This page displays all the certificates being managed by SCG.

Installed Certificates

□	Name ▲	Description
☑	Default Certificate	

Show: 20

Service Certificates

Service	Certificate
Management Web:	Default Certificate
AP Portal:	No data available
Hotspot:	Default Certificate

Certificates Signing Request (CSR)

□	Name ▲	Description

Show: 20

Configuring Advanced Gateway Options

As part of the TTG enhancements in this release, a number of features (collectively known as advanced gateway options) are now configurable from the web interface – these features no longer depend on flat file changes.

Follow these steps to configure advanced gateway options.

1 Go to the *Configuration* > *General System Settings* > *Gateway Advanced Options* page.

2 Configure the following options:

- *Allow Session on Accounting Fail*: This setting allows the controller TTG to terminate calls if accounting response fails. The default setting is **No**.

- *GTP Network Service Access Point Identifier [NSAPI]*: This setting is used to select NSAPI for GTP message. The default setting is 1.
- *Include IMEI IE in GTP Messages*: This setting is used to enable or disable IMEI IE in GTP messages. The default setting is **No**.

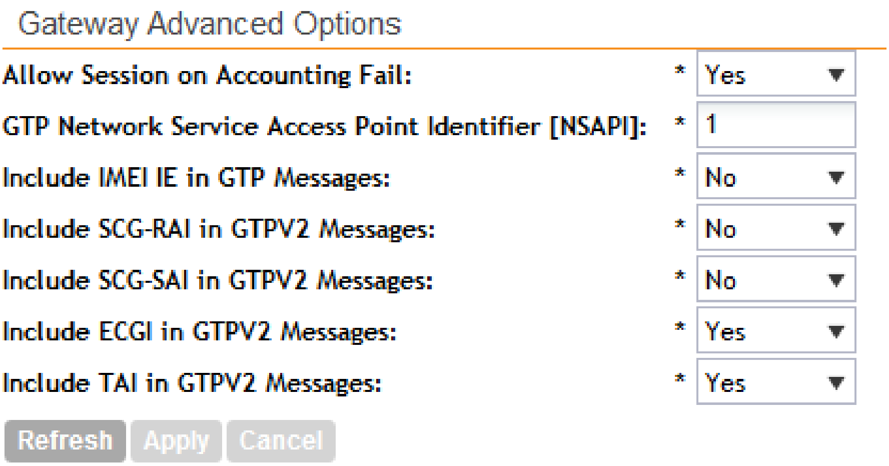
NOTE: In IMEI IE, the controller will send the MAC address of the UE appended with FFFE.

- *Include SCG-RAI in GTPV2*: This setting will only be used when the S5/S8 interface is used for GTPv2.
- *Include SCG-SAI in GTPV2*: This setting will only be used when the S5/S8 interface is used for GTPv2
- *Include ECGI in GTPV2*: This setting will only be used when the S5/S8 interface is used for GTPv2:
- *Include TAI in GTPV2*: This setting will only be used when the S5/S8 interface is used for GTPv2.

NOTE: The default GTPv2 interface for the controller is S2a.

3 Click **Apply**.

Figure 108. Configure the gateway advanced options as needed



Gateway Advanced Options

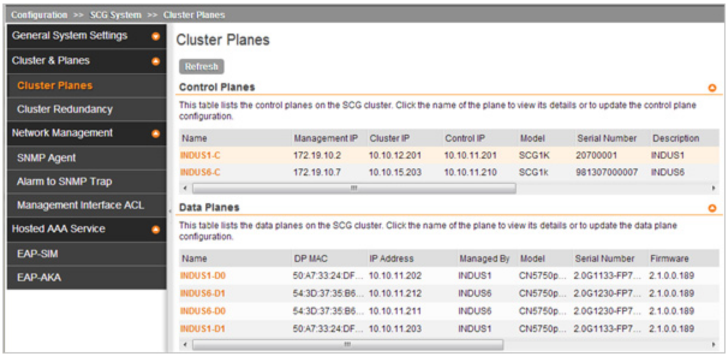
Allow Session on Accounting Fail:	*	Yes
GTP Network Service Access Point Identifier [NSAPI]:	*	1
Include IMEI IE in GTP Messages:	*	No
Include SCG-RAI in GTPV2 Messages:	*	No
Include SCG-SAI in GTPV2 Messages:	*	No
Include ECGI in GTPV2 Messages:	*	Yes
Include TAI in GTPV2 Messages:	*	Yes

Configuring Cluster Planes

To view the cluster planes that exist in the cluster, go to *Configuration* > *System* > *Cluster Planes*. The *Cluster Planes* page appears and displays a summary of the data planes and control planes that belong to the cluster. This section covers:

- Configuring Control Planes
- Configuring Cluster Redundancy

Figure 109. Cluster Plane view



Control Planes

This table lists the control planes on the SCG cluster. Click the name of the plane to view its details or to update the control plane configuration.

Name	Management IP	Cluster IP	Control IP	Model	Serial Number	Description
INDUS1-C	172.19.10.2	10.10.12.201	10.10.11.201	SCG1K	20700001	INDUS1
INDUS6-C	172.19.10.7	10.10.15.203	10.10.11.210	SCG1k	981307000007	INDUS6

Data Planes

This table lists the data planes on the SCG cluster. Click the name of the plane to view its details or to update the data plane configuration.

Name	DP MAC	IP Address	Managed By	Model	Serial Number	Firmware
INDUS1-D0	50:A7:33:24:DF...	10.10.11.202	INDUS1	CN5750p...	2.0G1133-FP7...	2.1.0.0.189
INDUS6-D1	54:3D:37:35:B6...	10.10.11.212	INDUS6	CN5750p...	2.0G1230-FP7...	2.1.0.0.189
INDUS6-D0	54:3D:37:35:B6...	10.10.11.211	INDUS6	CN5750p...	2.0G1230-FP7...	2.1.0.0.189
INDUS1-D1	50:A7:33:24:DF...	10.10.11.203	INDUS1	CN5750p...	2.0G1133-FP7...	2.1.0.0.189

Setting the System IP Mode

The controller supports IPv4 only and IPv4 and IPv6 addressing modes. The system IP mode controls the format of the IP address that you need to enter in a number of IP address-related settings (for example, cluster plane addresses, static routes, management ACLs, etc.)

Follow these steps to change the controller's system IP mode.

1 Go to *Configuration* > *System*.

2 On the sidebar, click **Cluster Planes**.

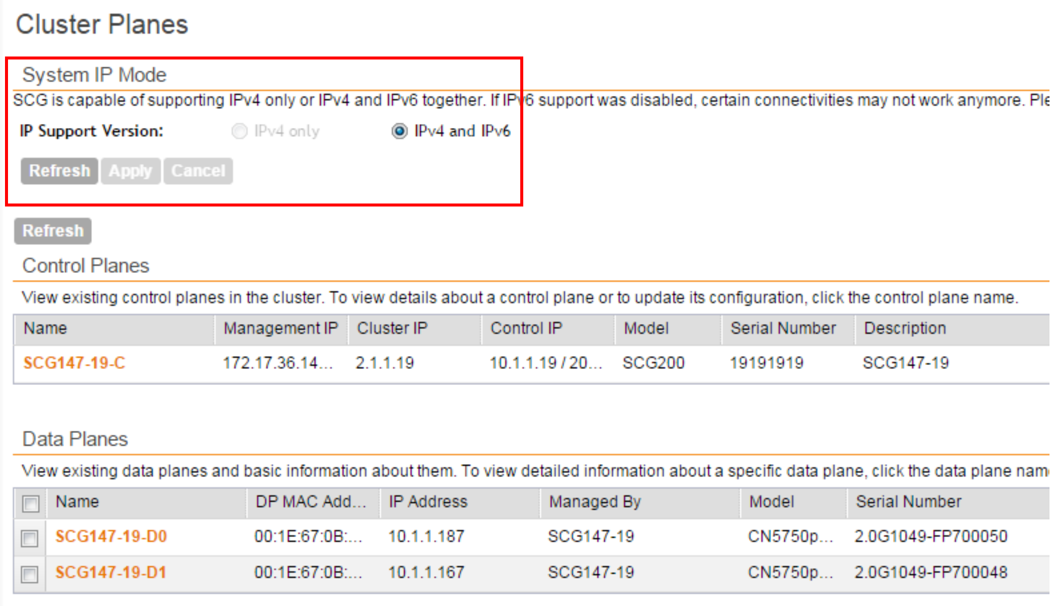
3 In the *System IP Mode* section, select the system IP mode that you want to controller to use. Options include:

- **IPv4 Only**
- **IPv4 and IPv6**

4 Click **Apply**.

You have completed setting the system IP mode.

Figure 110. The System IP Mode section



Cluster Planes

System IP Mode

SCG is capable of supporting IPv4 only or IPv4 and IPv6 together. If IPv6 support was disabled, certain connectivities may not work anymore. Ple

IP Support Version: ○ IPv4 only ● IPv4 and IPv6

Control Planes

View existing control planes in the cluster. To view details about a control plane or to update its configuration, click the control plane name.

Name	Management IP	Cluster IP	Control IP	Model	Serial Number	Description
SCG147-19-C	172.17.36.14...	2.1.1.19	10.1.1.19 / 20...	SCG200	19191919	SCG147-19

Data Planes

View existing data planes and basic information about them. To view detailed information about a specific data plane, click the data plane nam

□	Name	DP MAC Add...	IP Address	Managed By	Model	Serial Number
□	SCG147-19-D0	00:1E:67:0B:...	10.1.1.187	SCG147-19	CN5750p...	2.0G1049-FP700050
□	SCG147-19-D1	00:1E:67:0B:...	10.1.1.167	SCG147-19	CN5750p...	2.0G1049-FP700048

Configuring Control Planes

Three tabs exist in the control plane:

- Physical Interface Tab
- User Defined Interface Tab
- Static Routes Tab

Refer to the following sections on how to configure the settings on these three tabs.

CAUTION! If you disable the control plane interface, you will no longer be able to access the controller web interface to perform any management or administrative tasks.

Physical Interface Tab

Follow these steps to configure the physical interface settings of a control plane.

WARNING! You must configure the control, cluster, and management interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

---

1 Locate the interface settings that you want to update. You can update any of the following interfaces:

  a Control interface

  b Cluster interface

  c Management interface

CAUTION! Although it is possible to use DHCP to assign IP address settings to the management interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

---

2 Configure the following settings for the IPv4 interfaces that you want to update.

  a *IP Mode*: Configure the IP address mode by clicking one of the following options:

  - **Static**: Click this if you want to assign an IP address to this interface manually.
  - **DHCP**: Click this if you want this interface to obtain an IP address automatically from a DHCP server on the network. After you click this option, most of the options below it will be grayed out. Continue to Step 3.

  b *IP Address*: Enter the IP address that you want to the assign to this interface.

  c *Subnet Mask*: Enter the subnet mask for the IP address above.

  d *Gateway*: Enter the IP address of the gateway router.

  e *Primary DNS*: Enter the IP address of the primary DNS server.

  f *Secondary DNS*: Enter the IP address of the secondary DNS server.

3 If the system IP mode is set to **IPv4 and IPv6**, you will also need to configure the IPv6 interfaces. Configure the following settings:

  a *IP Mode*: Configure the IPv6 address mode by clicking one of the following options:

  - **Static**: Click this if you want to assign an IPv6 address to this interface manually, and then configure the following:

  - *IP Address*: Enter an IPv6 address (global only) with a prefix length (for example, `1234::5678:0:C12/123`) is required. Link-local addresses are unsupported.
  - Gateway: Enter an IPv6 address (global or link-local) without a prefix length. For example, `1234::5678:0:C12` (global address without a prefix length) and `fe80::5678:0:C12` (link-local address without a prefix length).
- **Auto**: Click this if you want the interface to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.

4 In *Access & Core Separation*, select the **Enable** check box if you want the management interface (core side) to be the system default gateway. The control interface (access side) will be used for access traffic only.

5 In *Default Gateway*, select the gateway that you want to use the IPv4 and IPv6 interfaces (if enabled). The options that appear here are the gateways that you have defined for control, cluster, and management interfaces.

NOTE: When *Access & Core Separation* is enabled, the **Default Gateway** field is hidden.

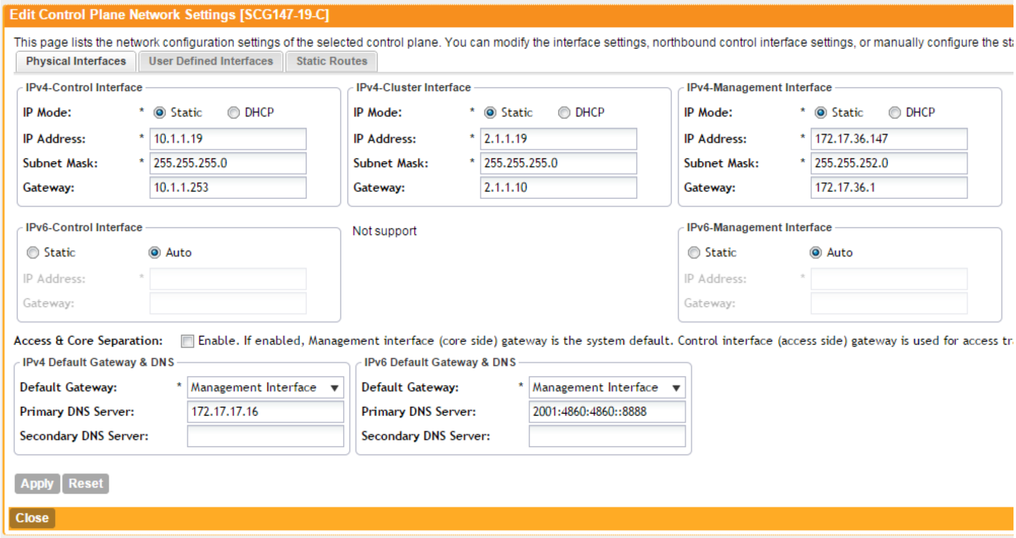
6 (Optional) In *Primary DNS Server* and *Secondary DNS Server*, configure the DNS servers that you want the controller to use.

7 Click **Apply** to save your changes.

The controller restarts and applies the updated network interface settings. You have completed updating the physical interface settings.

NOTE: For information on how to configure the management IP address from the command line interface, refer to Changing the Management IP Address from the CLI.

Figure 111. The Physical Interface tab



Edit Control Plane Network Settings [SCG147-19-C]

This page lists the network configuration settings of the selected control plane. You can modify the interface settings, northbound control interface settings, or manually configure the st

Physical Interfaces | User Defined Interfaces | Static Routes

IPv4-Control Interface

- IP Mode: * ● Static ○ DHCP
- IP Address: * 10.1.1.19
- Subnet Mask: * 255.255.255.0
- Gateway: 10.1.1.253

IPv4-Cluster Interface

- IP Mode: * ● Static ○ DHCP
- IP Address: * 2.1.1.19
- Subnet Mask: * 255.255.255.0
- Gateway: 2.1.1.10

IPv4-Management Interface

- IP Mode: * ● Static ○ DHCP
- IP Address: * 172.17.36.147
- Subnet Mask: * 255.255.252.0
- Gateway: 172.17.36.1

IPv6-Control Interface

- ○ Static ● Auto
- IP Address: *
- Gateway:

Not support

IPv6-Management Interface

- ○ Static ● Auto
- IP Address: *
- Gateway:

Access & Core Separation: □ Enable. If enabled, Management interface (core side) gateway is the system default. Control interface (access side) gateway is used for access tr

IPv4 Default Gateway & DNS

- Default Gateway: * Management Interface
- Primary DNS Server: 172.17.17.16
- Secondary DNS Server:

IPv6 Default Gateway & DNS

- Default Gateway: * Management Interface
- Primary DNS Server: 2001:4860:4860::8888
- Secondary DNS Server:

Apply | Reset

Close

User Defined Interface Tab

NOTE: The user defined interface (UDI) is unavailable in Virtual SmartZone (High-Scale and Essentials).

Use the User Defined Interface tab to configure the service settings (captive portal, subscriber portal, and Web proxy). Note that you can only create one user defined interface, and it must be for a service and must use the control interface as its physical interface.

NOTE: The control plane and the user-defined interface (UDI) must be on different subnets. If the control plane and UDI are on the same subnet and assigned the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.

Follow these steps to configure the settings on the User Defined Interface tab.

1 Click the **User Defined Interfaces** tab.

2 Click the **Create New** button.

3 Configure the following interface settings:

   a *Name*: Enter a name for this interface.

b *IP Address*: Enter an IP address to assign to this interface.

c *Subnet Mask*: Enter a subnet mask for the IP address above.

d *Gateway*: Enter the IP address of the gateway router.

e *VLAN*: Enter the VLAN ID that you want to assign to this interface.

f *Physical Interface*: Select either **Control Interface** or **Management Interface**.

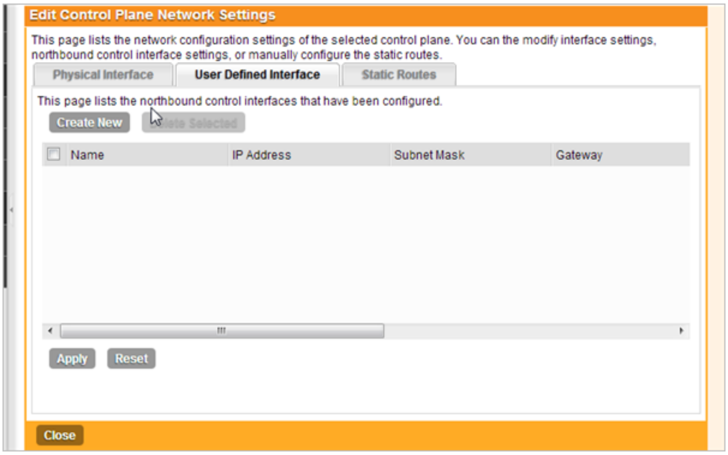
g *Service*: Select **Hotspot** or **Not Specified**.

4 Click **Save**.

5 Click **Apply**.

You have completed configuring the northbound portal interface settings.

Figure 112. The User Defined Interface tab



Edit Control Plane Network Settings

This page lists the network configuration settings of the selected control plane. You can the modify interface settings, northbound control interface settings, or manually configure the static routes.

This page lists the northbound control interfaces that have been configured.

□	Name	IP Address	Subnet Mask	Gateway

Static Routes Tab

To configure a static route, enter the destination IP address and related information for the destination. You can also assign a metric (or priority) to help the controller determines the route to choose when there are multiple routes to the same destination.

Follow these steps to configure a static route.

1 Click the **Static Routes** tab.

2 Click the **Create New** button.

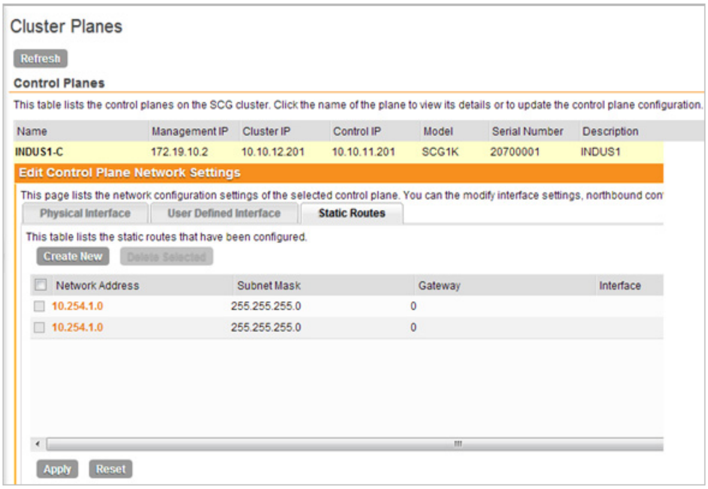
3 Configure the following interface settings:

   a. *Network Address*: Enter the destination IP address of this route.
   b. *Subnet Mask*: Enter a subnet mask for the IP address above.
   c. *Gateway*: Enter the IP address of the gateway router.
   d. *Interface*: Select the physical interface to use for this route.
   e. *Metric*: This represents the number of routers between the network and the destination.

4. Click **Save**.
5. Click **Apply** to save your changes.

You have completed configuring a static route.

Figure 113. The Static Route tab



Cluster Planes

Control Planes

This table lists the control planes on the SCG cluster. Click the name of the plane to view its details or to update the control plane configuration.

Name	Management IP	Cluster IP	Control IP	Model	Serial Number	Description
INDUS1-C	172.19.10.2	10.10.12.201	10.10.11.201	SCG1K	20700001	INDUS1

Edit Control Plane Network Settings

This page lists the network configuration settings of the selected control plane. You can the modify interface settings, northbound con

This table lists the static routes that have been configured.

□ Network Address	Subnet Mask	Gateway	Interface
□ 10.254.1.0	255.255.255.0	0	
□ 10.254.1.0	255.255.255.0	0	

Configuring a Data Plane

By default, the controller sends traffic from its data plane from a single interface. If your organization's network requires separation of the access and core traffic, configure access and core separation on the controller.

Follow these steps to configure the interface settings of a data plane.

1. Go to **Configuration** > **System**.
2. On the side menu, click **Cluster Planes**. The *Cluster Planes* page appears.
3. Scroll down to the *Data Planes* section, and then click the name of the data plane that you want to configure. The Edit Data Plane Network Settings [{node name}] form appears.

4 In *Interface Mode*, select one of the following options:

- Single Interface (default): Select this option if you want the controller to send traffic from its data plane from a single interface.
- Access and Core Interfaces: Select this option if you want the controller to send traffic to the access and core networks separately.

If you choose to separate the access and core networks, take note of the following:

- If the data plane is required to connect to IP addresses in the core network (for example, for DHCP relay or L2oGRE termination) and the destination IP addresses are not part of the core subnet, you must use static routes.
- There are no predefined access and core interfaces on the SCG-200. You can use either ports on the rear panel of the controller to connect to the access network and core network.

5 In the *Primary (Access) Interface* section, configure the primary interface settings:

a IP Mode: Click one of the following options:

- Static: Click this if you want to assign an IP address to this interface manually.
- DHCP: Click this if you want this interface to obtain an IP address automatically from a DHCP server on the network. After you click this option, most of the options below it will be grayed out. Continue to Step 3.

b IP Address: Enter the IP address that you want to the assign to this interface.

c Subnet Mask: Enter the subnet mask for the IP address above.

d Gateway: Enter the IP address of the gateway router.

e Primary DNS: Enter the IP address of the primary DNS server.

f Secondary DNS: Enter the IP address of the secondary DNS server.

6 In the *Secondary (Core) Interface* section, configure the secondary interface settings:

a IP Address: Enter the IP address of the core network interface. The secondary/core interface IP address is must be configured manually; DHCP is unsupported.

b Subnet Mask: Enter the subnet mask for the IP address above.

c VLAN: If you need to tag traffic with a VLAN ID, enter the VLAN ID number.

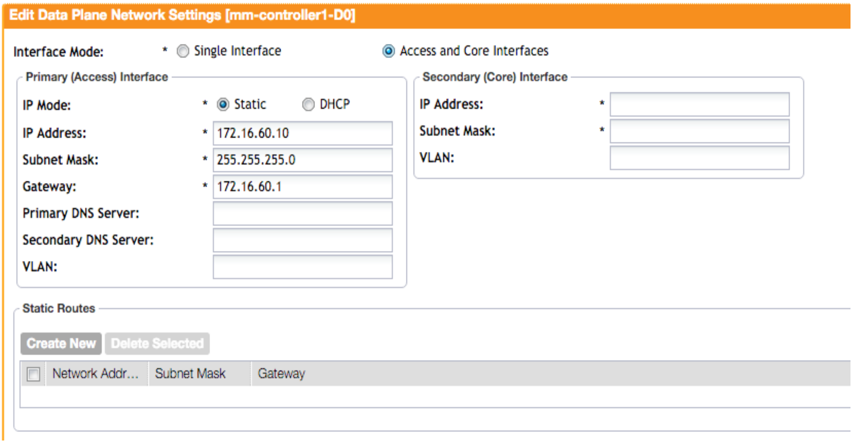
If VLANS are configured on both the access and core networks, the VLAN ID that you enter here must be different from the VLAN ID that you entered for the primary/ access interface.

d NAT IP: Enter the IP address of the network address translation (NAT) server on the network.

7 Click Apply to save your changes.

You have completed configuring the interface settings of a data plane.

Figure 114. Configuring data planes



Edit Data Plane Network Settings [mm-controller1-D0]

Interface Mode: * ○ Single Interface ● Access and Core Interfaces

Primary (Access) Interface

IP Mode: *	● Static ○ DHCP
IP Address: *	172.16.60.10
Subnet Mask: *	255.255.255.0
Gateway: *	172.16.60.1
Primary DNS Server:	
Secondary DNS Server:	
VLAN:	

Secondary (Core) Interface

IP Address: *	
Subnet Mask: *	
VLAN:	

Static Routes

□	Network Addr...	Subnet Mask	Gateway

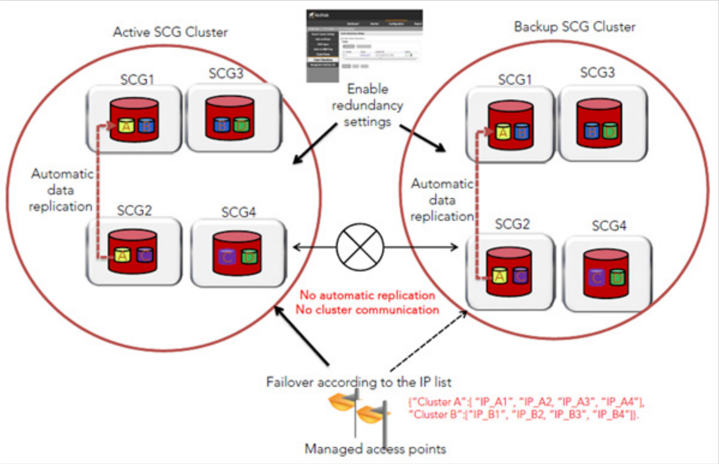
Configuring Cluster Redundancy

If you have multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to fail over automatically to another cluster if their parent cluster goes out of service or becomes unavailable.

Before you configure cluster redundancy, take note of the following:

- Cluster redundancy is disabled by default.
- Only super administrators have the capability to configure the cluster redundancy settings.
- To configure cluster redundancy, you will need to retrieve the IP addresses assigned to the control interfaces of all nodes on clusters that you want to configure.

Figure 115. Cluster redundancy


Active SCG Cluster
Backup SCG Cluster
SCG1
SCG3
SCG2
SCG4
Enable redundancy settings
Automatic data replication
No automatic replication
No cluster communication
Failover according to the IP list
{"Cluster A":["IP_A1", "IP_A2, "IP_A3", "IP_A4"],
"Cluster B":["IP_B1", "IP_B2, "IP_B3", "IP_B4"]}.
Managed access points

Follow these steps to configure redundancy for a cluster on the network.

1 Go to Configuration > Cluster Planes.

2 Select the Enable Cluster Redundancy check box.

3 Click the Create New button to create a record for a failover cluster. The Cluster form appears.

4 Configure the settings in the Cluster form.

   a In Name, type a name for the cluster (for example, type Cluster B).

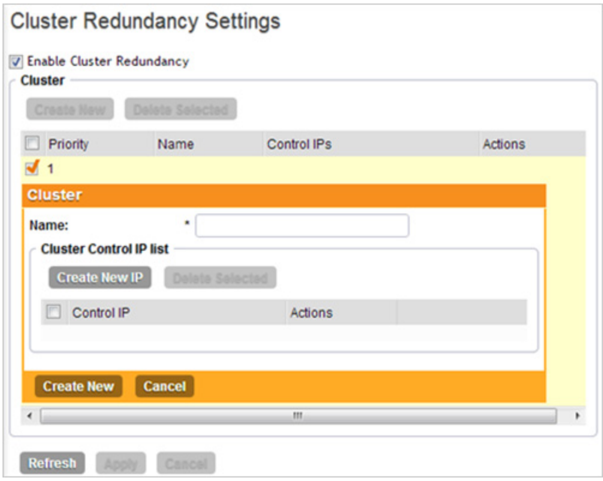
   b Under Cluster Control IP List, click the Create New IP button.

   c In the text box that appears, type the control interface IP address of a node in this cluster.

   d Click Save.

   e Repeat steps b to d for every node in the cluster. If this cluster has two nodes, for example, this cluster control IP list must have two IP addresses. You can add up to four control IP addresses to the list.

Figure 116. Use the Cluster form to set the cluster control IP addresses



Cluster Redundancy Settings

☑ Enable Cluster Redundancy

□	Priority	Name	Control IPs	Actions
☑	1			

Cluster

Name: *

5 Click Apply in the Cluster form to save the cluster control IP list.

6 To add another cluster control IP list (for example, for Cluster C), click Create New. You can add up to four cluster control IP lists.

7 Click Apply on the Cluster Redundancy Settings page.

You have completed configuring cluster redundancy.

NOTE: After configuring redundancy for a cluster, Ruckus Wireless strongly recommends backing up the controller configuration.

How Cluster Redundancy Works

The following simplified scenario describes how cluster redundancy works and how managed APs fail over from one controller cluster to another.

1 After you enable and configure cluster redundancy on the controller, managed APs obtain the updated configuration (which now includes the failover settings) from the controller. If you have two clusters, for example, managed APs will obtain a failover list similar to the following:

{“Cluster A”:[“IP_A1”, “IP_A2, “IP_A3”, “IP_A4”], “Cluster B”:[“IP_B1”, “IP_B2, “IP_B3”, “IP_B4”]}.

2 If Cluster A goes out of service or becomes unavailable, APs managed by Cluster A will attempt to connect to the IP addresses (one node at a time) specified for Cluster A.

3 If managed APs are unable to connect to the IP addresses specified for Cluster A, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster B.

4 If managed APs are able to connect to one of the IP address specified for Cluster B, they fail over to Cluster B. Then, they apply the registration rules that have been configured for Cluster B and renew their certificates.

NOTE: The second cluster to which APs fail over must have sufficient license seats to accommodate the new APs that it will be managing. If the second cluster has insufficient license seats, the failover will be unsuccessful.

After the APs apply the registration rules and renew their certificates, the failover process is complete. These APs will continue to be managed by the failover cluster until you restore them to the original cluster (rehome) manually.

Rehoming Managed APs

Rehoming is the process of returning the APs that have failed over to the second cluster back to their original cluster (once it becomes available). Rehoming must be done manually. APs that have failed over will continue to be managed by the failover cluster until you rehome them.

Rehoming APs must be done on a per-zone basis. Follow these steps to rehome managed APs to the original cluster.

1 Go to Configuration > AP Zones.

2 From the AP Zone List, click the AP zone name that you want to rehome. The AP Zone Configuration Details page appears.

3 Click the Switchover Cluster button. The Switchover Cluster dialog box appears.

4 From the drop-down menu, select the cluster to which you want the AP zone to switch over (for example, the original cluster to which APs in this zone belonged).

5 Click Apply.

You have completed rehoming the APs in the zone.

Configuring Network Management

This section covers:

- Configuring the SNMPv2 and SNMPv3 Agents
- Sending SNMP Traps and Email Notifications for Events
- Controlling Access to the Management Interfaces

Configuring the SNMPv2 and SNMPv3 Agents

The controller supports the Simple Network Management Protocol (SNMP v2 and v3), which allows you to query controller information, such as system status, AP list, AP zones, etc., and to set a number of system settings using a Network Management System (NMS) or SNMP MIB browser. You can also enable SNMP traps to receive immediate notifications for possible AP and system issues.

The procedure for enabling the internal SNMP agents depends on whether your network is using SNMPv2 or SNMPv3. SNMPv3 mainly provides security enhancements over the earlier version, and therefore requires you to enter authorization passwords and encryption settings, instead of simple clear text community strings.

Both SNMPv2 and SNMPv3 can be enabled at the same time. The SNMPv3 framework provides backward compatibility for SNMPv1 and SNMPv2c management applications so that existing management applications can still be used to manage the controller with SNMPv3 enabled.

This section covers the following topics:

- Enabling Global SNMP Traps
- Configuring the SNMPv2 Agent
- Configuring the SNMPv3 Agent

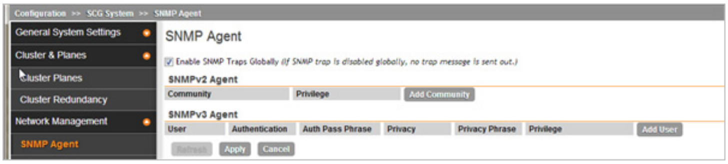
Enabling Global SNMP Traps

By default, the global SNMP trap setting is disabled, which means that the controller will be unable to send out trap notifications, even if you enabled the SNMPv2 and SNMPv3 agents to send out traps.

Follow these steps to enable global SNMP traps.

1. Go to the SNMP Agent section.
2. Select the Enable SNMP Traps Globally check box.
3. Click Apply. A message appears, confirming that you have updated the global trap settings.

Figure 117. The SNMP Agent section



☑ Enable SNMP Traps Globally *(If SNMP trap is disabled globally, no trap message is sent out.)*

Configuring the SNMPv2 Agent

Follow these steps to configure the SNMPv2 agent.

1. In the SNMPv2 Agent section, click Add Community. Options for adding a community appear.
2. Configure the read-only community settings by following these steps:
   a. In the text box under Community, type the read-only community string (for example, public). Applications that send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.
   b. Under Privilege, select the check boxes for the privileges that you want to grant to this community. A read-only community is typically granted the Read privilege. Available privileges include:
      - Read
      - Write
      - Trap: Select this privilege if you want to send SNMP trap notifications for this community. To add a trap target, click Add Trap Target, and then configure the following options (required) that appear below:
      - Target IP Address: Type the IP address of the SNMP trap server on the network.
      - Target Port: Type the SNMP trap server port.
3. Click Add Community again. A second set of configuration options for adding a community appears.
4. Configure the read-write community settings by following these steps:
   a. In the text box under Community, type the read-write community string (for example, private). Applications that send SNMP Set-Requests to the controller (to set certain SNMP MIB variables) will need to send this string along with the request before they will be allowed access. The default value is private.

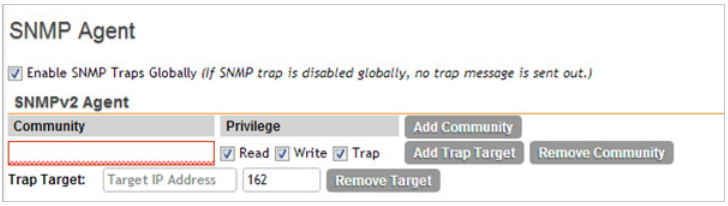
b Under Privilege, select the check boxes for the privileges that you want to grant to this community. A read-write community is typically granted the Read and Write privileges. Available privileges include:

- Read
- Write
- Trap: Select this privilege if you want to send SNMP trap notifications for this community. When this check box is selected, the Add Trap Target button becomes active. Click Add Trap Target, and then configure the following settings (required):
  - Target IP Address: Type the IP address of the SNMP trap server on the network.
  - Target Port: Type the SNMP trap server port.

5 Click Apply.

You have completed configuring the read-only and read-write communities for the SNMPv2 agent. To add another community, click Add Community again, and then repeat the procedure above.

Figure 118. The SNMPv2 Agent section



SNMP Agent

☑ Enable SNMP Traps Globally *(If SNMP trap is disabled globally, no trap message is sent out.)*

SNMPv2 Agent

Community	Privilege
	☑ Read ☑ Write ☑ Trap

Trap Target: Target IP Address 162

Configuring the SNMPv3 Agent

Follow these steps to configure the SNMPv3 agent.

1 In the SNMPv3 Agent section, click Add User. Options for adding a user appear.

2 Under User, type a user name between 1 and 31 characters.

3 Under Authentication, select one of the following authentication methods:

- None: Use no authentication.
- MD5: Message-Digest algorithm 5, message hash function with 128-bit output.
- SHA: Secure Hash Algorithm, message hash function with 160-bit output.

4 Under Auth Pass Phrase, type a pass phrase between 8 and 32 characters in length.

5 Under Privacy, select one of the following privacy methods:

- None: Use no privacy method.
- DES: Data Encryption Standard, data block cipher.
- AES: Advanced Encryption Standard, data block cipher.

6 Under Privacy Phrase (active only if you selected either DES or AES above), enter a privacy phrase between 8 and 32 characters in length.

7 Under Privilege, select the check boxes for the privileges that you want to grant to this community. A read-only community is typically granted the Read privilege, whereas a read-write community is granted the Read and Write privileges. Available privileges include:

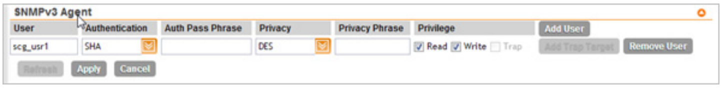
- Read
- Write
- Trap: Select this privilege if you want to send SNMP trap notifications for this community. When this check box is selected, the Add Trap Target button becomes active. Click Add Trap Target, and then configure the following settings (required):
  - Target IP Address: Type the IP address of the SNMP trap server on the network.
  - Target Port: Type the SNMP trap server port.

8 Repeat the steps above to create as many SNMPv3 agent users are you require.

9 Click Apply.

You have completed configuring the SNMPv3 agent settings.

Figure 119. SNMPv3 Agent section



SNMPv3 Agent

User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase	Privilege
scg_usr1	SHA		DES		☑ Read ☑ Write □ Trap

Sending SNMP Traps and Email Notifications for Events

NOTE: Verify that global SNMP traps are enabled to ensure that the controller can send SNMP traps for alarms. For information on how to enable global SNMP traps, refer to Enabling Global SNMP Traps.

By default, the controller saves a record of all events that occur to its database. You can configure the controller to also send SNMP traps and email notifications for specific events whenever they occur.

Follow these steps to configure the controller to send traps and email notifications for events.

1. Go to *Configuration* > *System*.
2. On the sidebar, click **Event Management**. If **Event Management** is not visible on the sidebar, click **Network Management** to expand its submenu, which contains the **Event Management** link. The *Event Management* page appears.
3. In the *Email Notification* section, select the **Enable** check box, and then type an email address or email addresses in the *Mail To* box. If you want to send notifications to multiple recipients, use a comma to separate the email addresses.
4. In the *Events* section, go over the table and select the events for which you want to send traps or email notifications (or both).
   - If you know the event code, event type, or description, type the full or partial text into the search box in the upper-right hand corner of the table, and then click the magnifying glass (search) icon.
   - If you want to select all events, click the check box before the *Code* table heading.

NOTE: By default, the *Events* table displays up to 20 events per page. If you are enabling SNMP traps and email notifications for 10 or more events, Ruckus Wireless recommends changing the number of events shown per page. To do this, scroll down to the bottom of the page, and then change the value for **Show** to `250` (maximum).

5. After you have selected all of the events for which you want to send traps or email notifications, scroll up to the beginning of the *Events* table, and then click **Enable**. A submenu appears and displays the following links:
   - **Enable SNMP Trap**: Click this link to enable SNMP trap notifications for all selected events.

- **Enable Email**: Click this link to enable email notifications for all selected events.
- **Enable DB Persistence**: Click this link to enable saving of all selected events to the controller database. If an event is already currently enabled, it will stay enabled after you click this link.

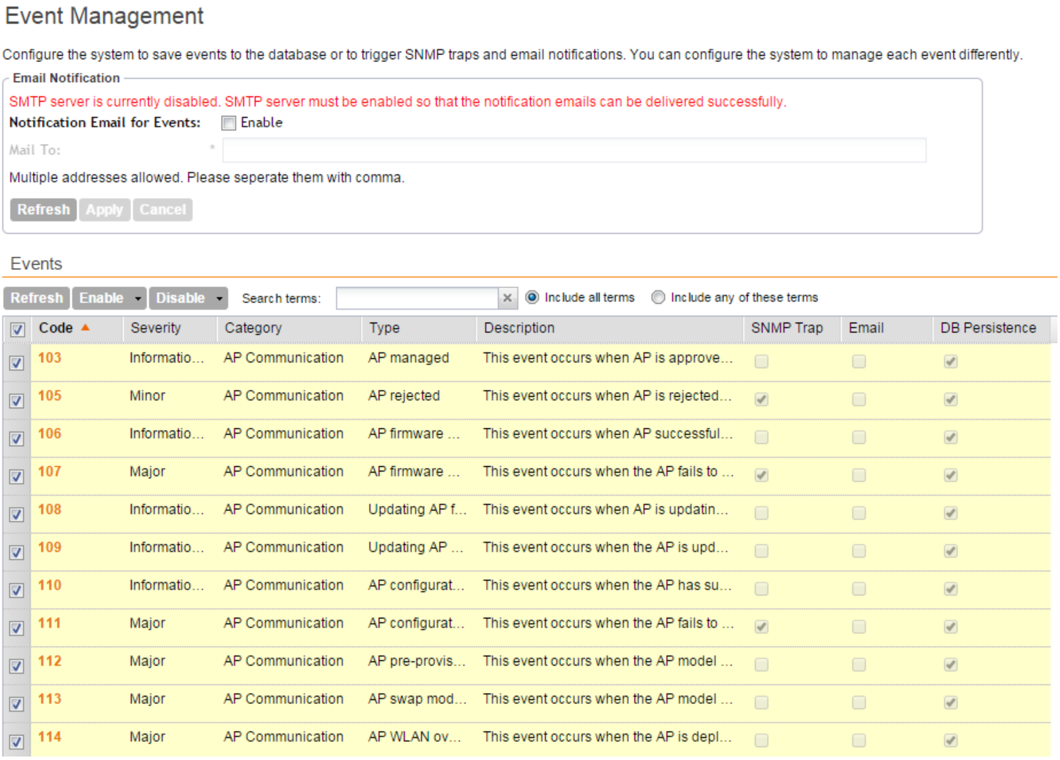
A confirmation message appears.

6 Click **Yes**.

NOTE: You can only enable one of these three notification options at a time (for example, SNMP trap notifications only). If you want to enable another option, repeat steps 5 and 6.

You have completed enabling a notification option for the selected events.

Figure 120. Selecting all events on the Event Management page



Event Management

Configure the system to save events to the database or to trigger SNMP traps and email notifications. You can configure the system to manage each event differently.

Email Notification

SMTP server is currently disabled. SMTP server must be enabled so that the notification emails can be delivered successfully.

Notification Email for Events: □ Enable

Mail To: *

Multiple addresses allowed. Please seperate them with comma.

Events

Search terms: ● Include all terms ○ Include any of these terms

☑	Code	Severity	Category	Type	Description	SNMP Trap	Email	DB Persistence
☑	103	Informatio...	AP Communication	AP managed	This event occurs when AP is approve...	□	□	☑
☑	105	Minor	AP Communication	AP rejected	This event occurs when AP is rejected...	☑	□	☑
☑	106	Informatio...	AP Communication	AP firmware ...	This event occurs when AP successful...	□	□	☑
☑	107	Major	AP Communication	AP firmware ...	This event occurs when the AP fails to ...	☑	□	☑
☑	108	Informatio...	AP Communication	Updating AP f...	This event occurs when AP is updatin...	□	□	☑
☑	109	Informatio...	AP Communication	Updating AP ...	This event occurs when the AP is upd...	□	□	☑
☑	110	Informatio...	AP Communication	AP configurat...	This event occurs when the AP has su...	□	□	☑
☑	111	Major	AP Communication	AP configurat...	This event occurs when the AP fails to ...	☑	□	☑
☑	112	Major	AP Communication	AP pre-provis...	This event occurs when the AP model ...	□	□	☑
☑	113	Major	AP Communication	AP swap mod...	This event occurs when the AP model ...	□	□	☑
☑	114	Major	AP Communication	AP WLAN ov...	This event occurs when the AP is depl...	□	□	☑

Enabling or Disabling Notifications for a Single Event

Follow these steps to enable or disable notifications for a single event.

1 Go to *Configuration* > *System*.

2 On the sidebar, click **Event Management**.

3 Under *Events*, locate the event for which you want to enable or disable notifications.

4 Click the event code. The *Edit Event [Event Code]* form appears.

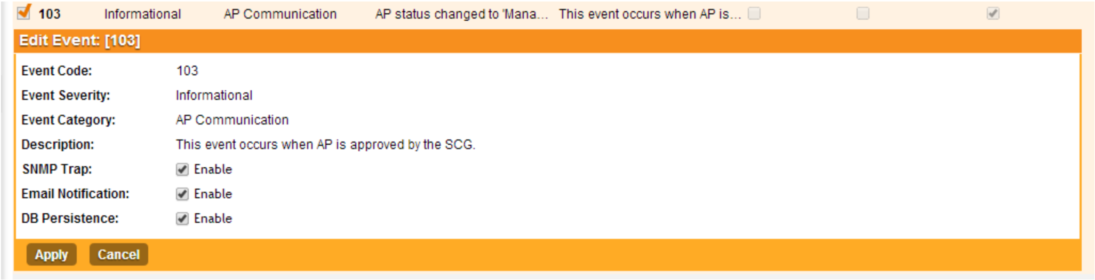
5 Select the check box for a notification type to enable it, or clear the check box to disable it. Options include:

- SNMP Trap
- Email Notification
- DB Persistence

6 Click **Apply**.

You have completed enable or disabling notifications for a single event.

Figure 121. Select or clear check boxes to enable or disable notifications



☑ 103 Informational AP Communication AP status changed to 'Mana... This event occurs when AP is... □ □ ☑

Edit Event: [103]

Event Code: 103
Event Severity: Informational
Event Category: AP Communication
Description: This event occurs when AP is approved by the SCG.
SNMP Trap: ☑ Enable
Email Notification: ☑ Enable
DB Persistence: ☑ Enable

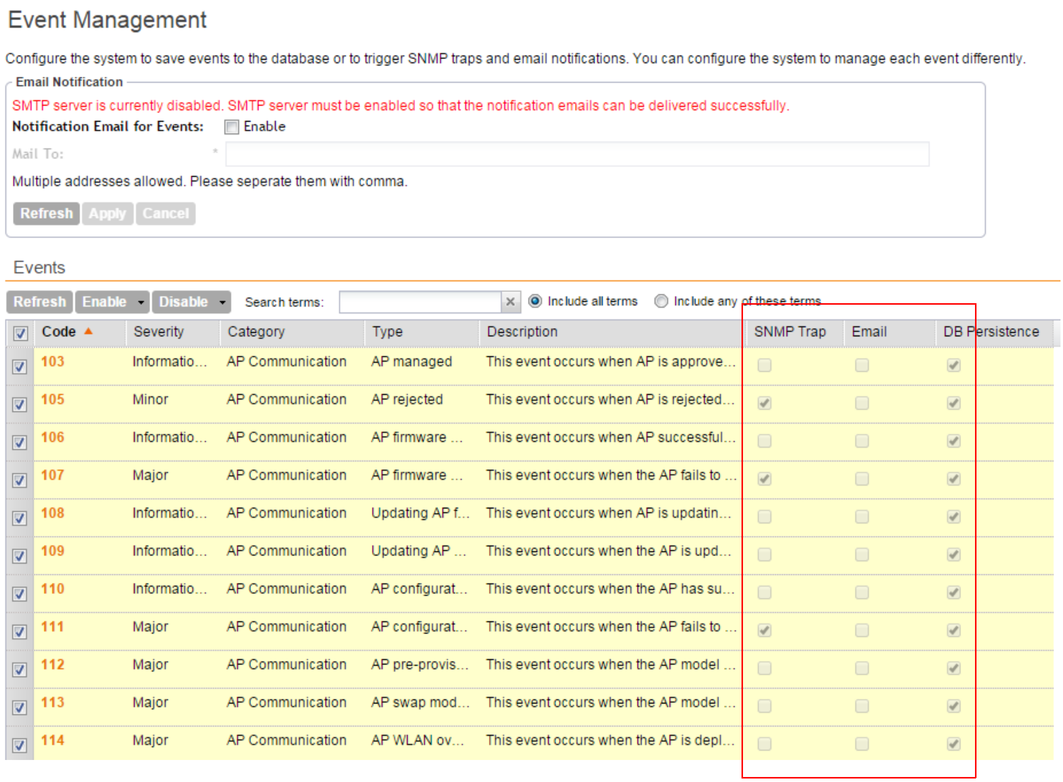
Viewing Enabled Notifications for Events

Follow these steps to view the notification types that are enabled for events.

1. Go to *Configuration* > *System*.
2. On the sidebar, click **Event Management**.
3. Scroll down to the bottom of the page, and then select **250** in *Show*. The page refreshes, and then displays up to 250 events.
4. Check the *SNMP Trap*, *Email*, and *DB Persistence* columns on the right side of the table. A check mark under each column indicates that the notification option is enabled for the event.

To view the notification options that are enabled for the events on the next page, click **>>** at the bottom of the table. The page refreshes, and then displays the remaining events.

Figure 122. A check mark under a column indicates the notification is enabled for the event



Event Management

Configure the system to save events to the database or to trigger SNMP traps and email notifications. You can configure the system to manage each event differently.

Email Notification

SMTP server is currently disabled. SMTP server must be enabled so that the notification emails can be delivered successfully.

Notification Email for Events: □ Enable

Mail To: *

Multiple addresses allowed. Please seperate them with comma.

Events

Search terms: ● Include all terms ○ Include any of these terms

☑	Code ▲	Severity	Category	Type	Description	SNMP Trap	Email	DB Persistence
☑	103	Informatio...	AP Communication	AP managed	This event occurs when AP is approve...	□	□	☑
☑	105	Minor	AP Communication	AP rejected	This event occurs when AP is rejected...	☑	□	☑
☑	106	Informatio...	AP Communication	AP firmware ...	This event occurs when AP successful...	□	□	☑
☑	107	Major	AP Communication	AP firmware ...	This event occurs when the AP fails to ...	☑	□	☑
☑	108	Informatio...	AP Communication	Updating AP f...	This event occurs when AP is updatin...	□	□	☑
☑	109	Informatio...	AP Communication	Updating AP ...	This event occurs when the AP is upd...	□	□	☑
☑	110	Informatio...	AP Communication	AP configurat...	This event occurs when the AP has su...	□	□	☑
☑	111	Major	AP Communication	AP configurat...	This event occurs when the AP fails to ...	☑	□	☑
☑	112	Major	AP Communication	AP pre-provis...	This event occurs when the AP model ...	□	□	☑
☑	113	Major	AP Communication	AP swap mod...	This event occurs when the AP model ...	□	□	☑
☑	114	Major	AP Communication	AP WLAN ov...	This event occurs when the AP is depl...	□	□	☑

Configuring Event Thresholds

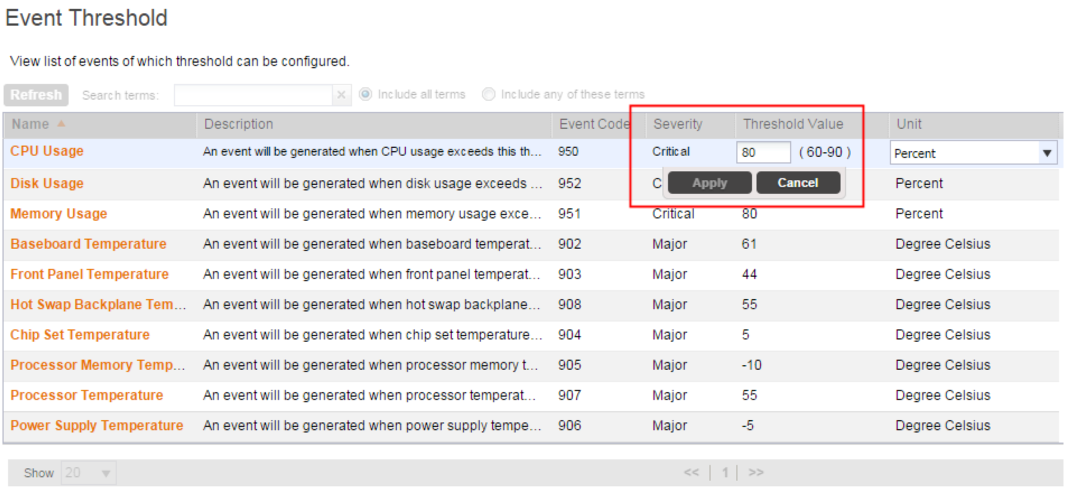
An event threshold defines a set of conditions related to the controller hardware that need to be met before the controller triggers an event. You can accept the default threshold values or you can update the threshold values to make them more suitable to your deployment or controller environment.

Follow these steps to configure the threshold for an event.

1. Go to *Configuration* > *System*.
2. On the sidebar, click *Network Management* > *Event Threshold*. The Event Threshold page appears and displays the list of events with configurable thresholds (see Table 8), including the event code, severity level, default value and accepted range, and unit of measurement for each event.
3. Locate the event threshold that you want to configure.
4. Click the event name under the *Name* column. The threshold value for the event become edits. Next to the threshold value, the acceptable range is shown.
5. Edit the threshold value.
6. Click **Apply.**

Repeat the same procedure to edit the threshold of another event.

Figure 123. Configuring the CPU Usage event threshold



Event Threshold

View list of events of which threshold can be configured.

Name	Description	Event Code	Severity	Threshold Value	Unit
CPU Usage	An event will be generated when CPU usage exceeds this th...	950	Critical	80 (60-90)	Percent
Disk Usage	An event will be generated when disk usage exceeds ...	952	C	Apply Cancel	Percent
Memory Usage	An event will be generated when memory usage exce...	951	Critical	80	Percent
Baseboard Temperature	An event will be generated when baseboard temperat...	902	Major	61	Degree Celsius
Front Panel Temperature	An event will be generated when front panel temperat...	903	Major	44	Degree Celsius
Hot Swap Backplane Tem...	An event will be generated when hot swap backplane...	908	Major	55	Degree Celsius
Chip Set Temperature	An event will be generated when chip set temperature...	904	Major	5	Degree Celsius
Processor Memory Temp...	An event will be generated when processor memory t...	905	Major	-10	Degree Celsius
Processor Temperature	An event will be generated when processor temperat...	907	Major	55	Degree Celsius
Power Supply Temperature	An event will be generated when power supply tempe...	906	Major	-5	Degree Celsius

Events with Configurable Thresholds

Table 8 lists controller hardware events for which you can configure the event thresholds, including their default values and acceptable ranges.

Table 8. List of hardware events with configurable thresholds

Event	Event Code	Severity	Threshold Value	Unit
CPU Usage	950	Critical	Default: 80 Range: 60 to 90	Percent
Disk Usage	952	Critical	Default: 80 Range: 60 to 90	Percent
Memory Usage	951	Critical	Default: 80 Range: 60 to 90	Percent
Baseboard Temperature	902	Major	Default: 61 Range: 10 to 61	Degree Celsius
Chip Set Temperature	904	Major	Default: 5 Range: -20 to 5	Degree Celsius
Front Panel Temperature	903	Major	Default: 44 Range: 5 to 44	Degree Celsius
Hot Swap Backplane Temperature	907	Major	Default:55 Range: 9 to 55	Degree Celsius
Power Supply Temperature	906	Major	Default: -5 Range:	Degree Celsius
Processor Memory Temperature	905	Major	Default: -10 Range: -20 to 5	Degree Celsius
Processor Temperature	907	Major	Default: 55 Default: 9 to 55	Degree Celsius

Controlling Access to the Management Interfaces

Management interfaces, which include the web interface and the command line interface, are the primary methods through which you configure the controller and its managed devices. Access to these interfaces is password-protected.

To prevent unauthorized devices from accessing these management interfaces, you can create ACLs. Management interface ACLs in the controller are whitelist (as opposed to blacklists), which are lists that contain only the IP addresses or IP address range that are allowed access to the management interfaces.

Follow these steps to configure the management interface ACL.

1. Go to *Configuration* > *System*.
2. On the sidebar, click **Management Interface ACL**.
3. In *Access Control of Management Interface*, click the **Enable** option.
4. In *Name*, type a name for this ACL.
5. In *Description*, type a brief description for this ACL.
6. In *Type*, select one of the following options, and then provide the required information:

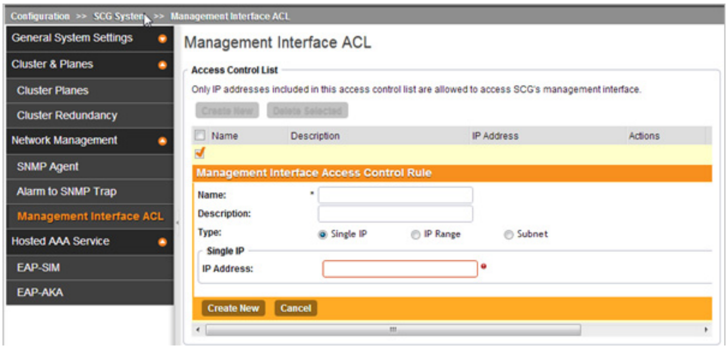
NOTE: Depending on the system IP mode that you selected, you can enter either IPv4 or IPv6 addresses (or both).

- *Single IP*: Type the IP address that you want to allow access to the management interfaces. For example, you can type `192.168.1.1` (IPv4) or `::123` (IPv6).
- *IP Range*: Type the IP address range that you want to allow access to the management interfaces by filling out the Start IP Address and the End IP Address boxes. For example, you can type `192.168.1.2 - 192.168.1.20` (IPv4) or `::123 - ::456` (IPv6).
- *Subnet*: Fill out the Network Address and Subnet Mask boxes. For example, you can type 192.168.1.1/255.255.255.0 or 192.168.1.1/24.

7. Click **Create New**. The page refreshes, and then the ACL that you created appears in the ACL list.
8. Create additional ACLs as needed.
9. Click **Apply**.

You have completed creating ACLs to control access to the management interfaces.

Figure 124. The Management Interface ACL page



Management Interface ACL

Access Control List

Only IP addresses included in this access control list are allowed to access SCG's management interface.

□	Name	Description	IP Address	Actions
☑				

Management Interface Access Control Rule

Name: *

Description:

Type: ● Single IP ○ IP Range ○ Subnet

Single IP

IP Address: *

Configuring Hosted AAA Services

SIM Authentication module enables you to provide IP-based services such as public WLAN access, and Unlicensed Mobile Alliance (UMA) and Femtocell access to subscribers, which is appropriate for GSM (Global System for Mobile Communications) infrastructure.

SIM authentication provides AAA services for EAP 802.1X and non-802.1X hotspots and Unlicensed Mobile Access (UMA) networks. Along with this, a user can be offered secure hotspot access via EAP 802.1X and Extensible Authentication Protocol - Subscriber Identity Module (EAP-SIM) or Extensible Authentication Protocol -Authentication and Key Agreement (EAP-AKA) user authentication.

SIM authentication module extends mobile services over IP access networks for UMA environments, providing the same mobile identity on unlicensed wireless networks as on mobile networks, and enables roaming and handover between networks.

This section covers:

- EAP-SIM Configuration
- EAP-AKA Configuration

EAP-SIM Configuration

The SIM authentication module handles EAP-SIM authentication for clients using SIM cards. Follow these steps to configure the EAP-SIM module.

1. In *EAP-SIM Configuration*, verify that the **Enable** option is selected (default). This will enable clients using GSM SIM cards to authenticate with AAA services.
2. In the *EAP-SIM Configuration* section, configure the following settings for EAP-SIM access:
   - **User ID Privacy Support**: Click this option to add an *Active Secret Key*.
   - **Fast Reauthentication Support**: Click this option to enable fast reauthentication, which is useful when SIM authentication happens frequently.
   - **Reauthentication Realm**: Type the reauthentication realm. The default realm is the realm from the permanent identity of the client.
   - **Max Successive Reauthentication**: Set the number of allowed reauthentication attempts before requesting fresh triplets and performing a complete authentication. The default is 256. If you enter 0, reauthentication identities will not generated.

3 In the *EAP-SIM Secret Key Configuration* section, configure the secret keys, which are used to encrypt the permanent identity to generate pseudonym and reauthentication identity.

   a Click the **Create New** option to add a key.

   b In *Key*, type any text string up to 32 characters. If you do not specify a secret, pseudonyms will not be generated. If you change this value, all pseudonyms assigned to currently authenticated clients will be invalidated and they will require reauthentication.

   c Click **Save**.

4 In the *EAP-SIM Cache Cleanup Configuration* section, configure the cleanup time for the cache to be cleaned. At cleanup time, all the cache entries (except the ones which were used during the last history length) will be deleted.

   a In *Cache*, click the **Enable** option to enable cache cleanup. This option is disabled by default.

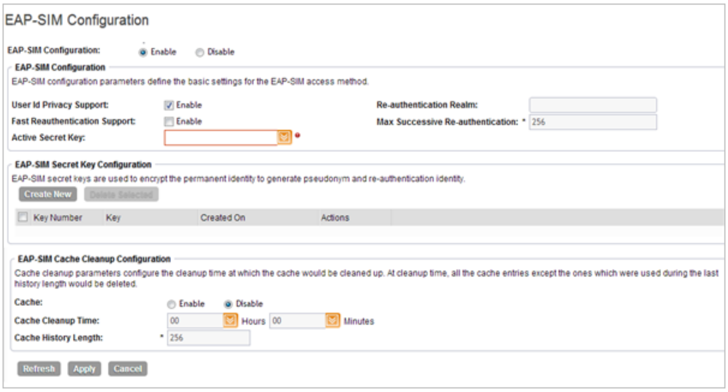
   b In *Cache Cleanup Time*, set the time (hour and minute) when cache cleanup will be triggered.

   c In *Cache History Length,* set the maximum size of cache entries. The default it 256.

5 Click **Apply.**

You have completed configuring EAP-SIM based authentication using AAA server.

Figure 125. Configuring EAP-SIM authentication



EAP-SIM Configuration

EAP-SIM Configuration: ● Enable ○ Disable

EAP-SIM Configuration

EAP-SIM configuration parameters define the basic settings for the EAP-SIM access method.

User Id Privacy Support: ☑ Enable
Fast Reauthentication Support: □ Enable
Active Secret Key: *
Re-authentication Realm:
Max Successive Re-authentication: * 256

EAP-SIM Secret Key Configuration

EAP-SIM secret keys are used to encrypt the permanent identity to generate pseudonym and re-authentication identity.

□ Key Number	Key	Created On	Actions

EAP-SIM Cache Cleanup Configuration

Cache cleanup parameters configure the cleanup time at which the cache would be cleaned up. At cleanup time, all the cache entries except the ones which were used during the last history length would be deleted.

Cache: ○ Enable ● Disable
Cache Cleanup Time: 00 Hours 00 Minutes
Cache History Length: * 256

EAP-AKA Configuration

The AKA authentication module handles EAP-AKA authentication for clients using USIM cards. Follow these steps to the EAP-AKA module.

1 In *EAP-AKA Configuration*, verify that the **Enable** option is selected (default). This will enable clients using 3G USIM cards to authenticate with AAA services.

- In EAP-AKA Configuration section, configure the following settings for EAP-AKA access:
  - **User ID Privacy Support**: Click this option to add an Active Secret Key.
  - **Fast Reauthentication Support**: Click this option to enable fast reauthentication, which is useful when AKA authentication happens frequently.
  - **Reauthentication Realm**: Type the reauthentication realm. The default realm is the realm from the permanent identity of the client.
  - **Max Successive Reauthentication**: Set the number of allowed reauthentication attempts before requesting fresh triplets and performing a complete authentication. The default is 256. If you enter 0, reauthentication identities will not generated.

2 In the *EAP-AKA Secret Key Configuration* section, configure the secret keys, which are used to encrypt the permanent identity to generate pseudonym and reauthentication identity.

a Click the **Create New** option to add a key.

b In *Key*, type any text string up to 32 characters. If you do not specify a secret, pseudonyms will not be generated. If you change this value, all pseudonyms assigned to currently authenticated clients will be invalidated and they will require reauthentication.

c Click **Save**.

3 In the *EAP-AKA Cache Cleanup Configuration* section, configure the cleanup time for the cache to be cleaned. At cleanup time, all the cache entries (except the ones which were used during the last history length) will be deleted.

a In *Cache*, click the **Enable** option to enable cache cleanup. This option is disabled by default.

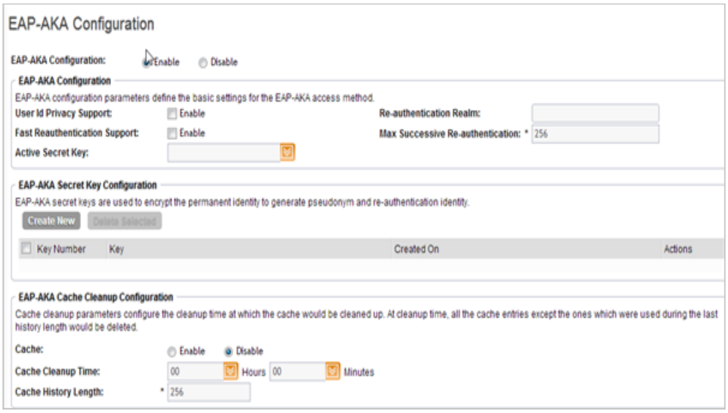
b In *Cache Cleanup Time*, set the time (hour and minute) when cache cleanup will be triggered.

c In *Cache History Length,* set the maximum size of cache entries. The default it 256.

4 Click **Apply**.

You have completed configuring EAP-AKA based authentication using AAA server.

Figure 126. Configuring EAP-AKA authentication



EAP-AKA Configuration

EAP-AKA Configuration: ● Enable ○ Disable

EAP-AKA Configuration

EAP-AKA configuration parameters define the basic settings for the EAP-AKA access method.

User Id Privacy Support: □ Enable

Fast Reauthentication Support: □ Enable

Active Secret Key:

Re-authentication Realm:

Max Successive Re-authentication: * 256

EAP-AKA Secret Key Configuration

EAP-AKA secret keys are used to encrypt the permanent identity to generate pseudonym and re-authentication identity.

□ Key Number	Key	Created On	Actions

EAP-AKA Cache Cleanup Configuration

Cache cleanup parameters configure the cleanup time at which the cache would be cleaned up. At cleanup time, all the cache entries except the ones which were used during the last history length would be deleted.

Cache: ○ Enable ● Disable

Cache Cleanup Time: 00 Hours 00 Minutes

Cache History Length: * 256

Working with Management Domains

8

In this chapter:

- Overview of Management Domains
- Viewing a List of Management Domains
- Creating a New Management Domain
- Deleting a Management Domain

Overview of Management Domains

Management domains allow you to segment managed access points into different groups and assign them to different AP zones and administrators. By default, a primary management domain named Administration Domain exists. You can create additional subdomains under the Administration Domain and assign access points to these subdomains.

Viewing a List of Management Domains

Follow these steps to view a list of existing management domains.

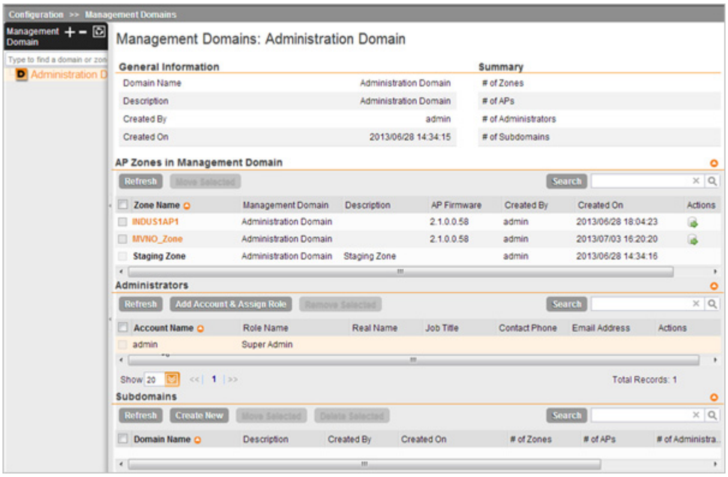
1. Go to **Configuration** > **Management Domains**. The *Management Domain: Administration Domain* page appears.
2. To view a summary of the administration domain, check the *Summary* section at the top of the page. This section displays the following information about the administration domain:
   - Domain Name
   - Description
   - Created By
   - Created On
   - # of Zones (more details in the AP Zones in Management Domain section)
   - # of APs
   - # of Administrators (more details in the Administrators section)

- # of Subdomains

3 To view a list of subdomains that have been created, scroll down to the Subdomains section. The table in this section shows a list of existing subdomains, as well as the following information for each subdomain:

- Domain Name
- Description
- Created By
- Created On
- # of Zones
- # of APs
- # of Administrators
- # of Subdomains
- Actions that you can perform

Figure 127. View list of domains



Management Domains: Administration Domain

General Information

Domain Name	Administration Domain
Description	Administration Domain
Created By	admin
Created On	2013/06/28 14:34:15

Summary

of Zones
of APs
of Administrators
of Subdomains

AP Zones in Management Domain

□	Zone Name	Management Domain	Description	AP Firmware	Created By	Created On	Actions
□	INDUS1AP1	Administration Domain		2.1.0.0.58	admin	2013/06/28 18:04:23	
□	MVNO_Zone	Administration Domain		2.1.0.0.58	admin	2013/07/03 16:20:20	
□	Staging Zone	Administration Domain	Staging Zone		admin	2013/06/28 14:34:16	

Administrators

□	Account Name	Role Name	Real Name	Job Title	Contact Phone	Email Address	Actions
□	admin	Super Admin					

Subdomains

□	Domain Name	Description	Created By	Created On	# of Zones	# of APs	# of Administra...

Creating a New Management Domain

Follow these steps to create a new management domain.

1 In the Subdomains section, click Create New. The Create New Management Domain form appears.

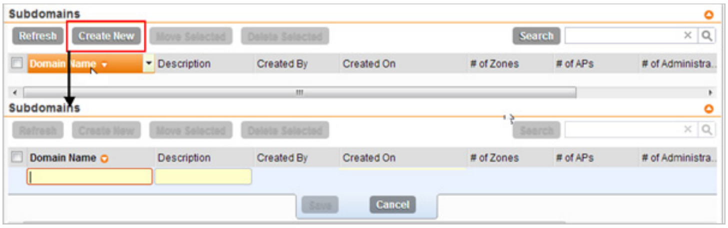
2 In Domain Name, type a name for the management domain that you are creating.

3 In Description, type a short description for the management domain.

4 Click OK.

5 The page refreshes, and then the management domain that you created appears under the Subdomains table.

Figure 128. The Create New Management Domain form



Deleting a Management Domain

Before you can delete a management domain, you must move all AP zones that belong to it to another management domain.

Follow these steps to delete an existing management domain.

- In the Subdomains section, locate the management domain that you want to delete.
- Under the Actions column, click the 🗑 icon that is in the same row as the management domain name. A confirmation message appears.
- Click Yes.

You have completed deleting a management domain.

To delete multiple management domains simultaneously, select the check boxes for the management domains, and then click the Delete Selected button. When the confirmation message appears, click Yes.

Managing Administrator Accounts 9

In this chapter:

- Overview of Administrator Accounts and Roles
- Viewing a List of Administrator Accounts, Roles, and RADIUS Servers
- Creating an Administrator Account
- Creating a New Administrator Role
- Editing an Administrator Role
- Cloning an Existing Administrator Role
- Adding a RADIUS Server for Administrators
- Using a Backup RADIUS Server
- Deleting an Administrator Account, Role, or RADIUS Server

Overview of Administrator Accounts and Roles

The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization.

In addition to creating administrator accounts, you can also create administrator roles, which define the tasks that each administrator can perform. You can also add RADIUS servers that you want to use for authorizing and authenticating administrators.

Viewing a List of Administrator Accounts, Roles, and RADIUS Servers

Follow these steps to view a list of existing administrator accounts, roles and RADIUS servers as seen in Figure 129.

1 Go to **Configuration** > **Administrators**. The Administrator Accounts lists a table of existing administrator accounts along with their basic details as mentioned below.

2 Click the account name to view the account details or to edit the account.

- Account Name
- Real Name
- # of Assigned Domains: The number of domains that this administrator account manages.
- Job Title
- Contact Phone
- Email Address
- Created By
- Created On
- Actions that you can perform

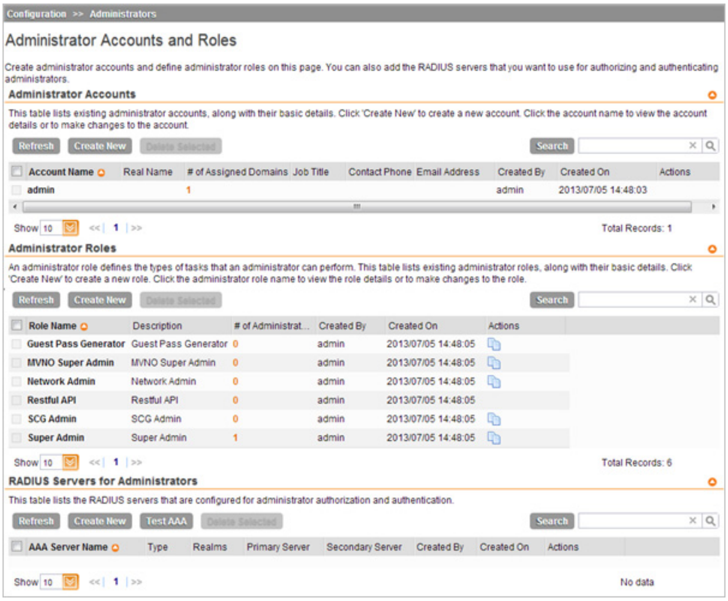
3 Click the role name to view the role details or to edit the role. The Administrator Role defines the tasks assigned to an administrator. The table lists the existing administrator roles with their basic details as mentioned below.

- Role Name
- Description
- # of Administrators: The number of administrators assigned to a role
- Created By
- Created On
- Actions that you can perform

4 The RADIUS Servers for Administrators Role lists the RADIUS servers assigned to an administrator for authorization and authentication.

- AAA Server Name
- Type
- Realms
- Primary Server
- Secondary Server
- Created By
- Created On
- Actions that you can perform

Figure 129. Administrator View of Accounts, Roles and RADIUS Servers



Administrator Accounts and Roles

Create administrator accounts and define administrator roles on this page. You can also add the RADIUS servers that you want to use for authorizing and authenticating administrators.

Administrator Accounts

This table lists existing administrator accounts, along with their basic details. Click 'Create New' to create a new account. Click the account name to view the account details or to make changes to the account.

☐	Account Name	Real Name	# of Assigned Domains	Job Title	Contact Phone	Email Address	Created By	Created On	Actions
☐	admin		1				admin	2013/07/05 14:48:03	

Total Records: 1

Administrator Roles

An administrator role defines the types of tasks that an administrator can perform. This table lists existing administrator roles, along with their basic details. Click 'Create New' to create a new role. Click the administrator role name to view the role details or to make changes to the role.

☐	Role Name	Description	# of Administrat...	Created By	Created On	Actions
☐	Guest Pass Generator	Guest Pass Generator	0	admin	2013/07/05 14:48:05	⧉
☐	MVNO Super Admin	MVNO Super Admin	0	admin	2013/07/05 14:48:05	⧉
☐	Network Admin	Network Admin	0	admin	2013/07/05 14:48:05	⧉
☐	Restful API	Restful API	0	admin	2013/07/05 14:48:05	
☐	SCG Admin	SCG Admin	0	admin	2013/07/05 14:48:05	⧉
☐	Super Admin	Super Admin	1	admin	2013/07/05 14:48:05	⧉

Total Records: 6

RADIUS Servers for Administrators

This table lists the RADIUS servers that are configured for administrator authorization and authentication.

☐	AAA Server Name	Type	Realms	Primary Server	Secondary Server	Created By	Created On	Actions

No data

Creating an Administrator Account

Follow these steps to create an administrator account.

1 In the Administrator Accounts section, click Create New. The Create New Administrator Account form appears.

2 In Account Name, type the name that this administrator will use to log on to the controller.

3 In Real Name, type the actual name (for example, John Smith) of the administrator.

4 In Password, type the password that this administrator will use (in conjunction with the Account Name) to log on to the controller.

5 In Confirm Password, type the same password as above.

6 In Phone, type the phone number of this administrator.

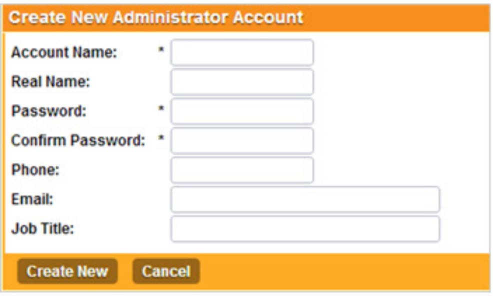
7 In Email, type the email address of this administrator.

8 In Job Title, type the job title or position of this administrator in your organization.

9 Click Create New.

The page refreshes, and then the administrator account that you created appears in the Administrator Accounts section.

Figure 130. The Create New Administrator Account form



Create New Administrator Account

Account Name: *

Real Name:

Password: *

Confirm Password: *

Phone:

Email:

Job Title:

Creating a New Administrator Role

An administrator role defines the tasks that an administrator can perform. Follow these steps to create a new administrator role.

1 In the Administrator Roles section, click Create New. The Create New Administrator Role form appears.

2 In Role Name, type a name for the administrator role that you are creating.

3 In Description, type a short description for the administrator role.

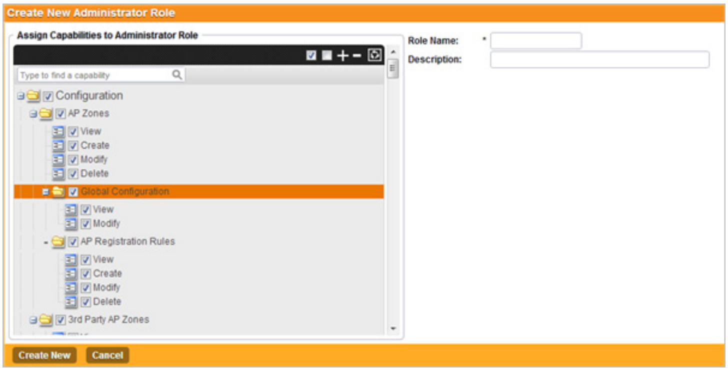
4 In the Assign Capabilities to Administrator Role tree (located on the left side of the form), select the administrator capabilities that you want to assign to this role. If you plan to grant this administrator role most of the capabilities that are available, click Select All, and then clear the check boxes for the capabilities that you do not want this role to have.

5 Remember to click the ⊞ icon next to each folder to view all capabilities that are included.

6 Click Create New.

You have completed creating an administrator role.

Figure 131. The Create New Administrator Role form



Create New Administrator Role

Assign Capabilities to Administrator Role

Type to find a capability

- ☑ Configuration
  - ☑ AP Zones
    - ☑ View
    - ☑ Create
    - ☑ Modify
    - ☑ Delete
  - ☑ Global Configuration
    - ☑ View
    - ☑ Modify
  - ☑ AP Registration Rules
    - ☑ View
    - ☑ Create
    - ☑ Modify
    - ☑ Delete
  - ☑ 3rd Party AP Zones

Role Name: *

Description:

Editing an Administrator Role

Follow these steps to edit an existing administrator role.

1. In the Administrator Roles section, locate the role that you want to edit.
2. Click the name of the administrator role that you want to edit. The Edit Administrator Role form appears.
3. In the Assign Capabilities to Administrator Role tree (located on the left side of the form), add or remove capabilities from the role. Remember to click the icon next to each folder to view all capabilities that are included.
4. To add a capability, select the check box next to it.
5. To remove a capability, clear the check box next to it.
6. Click Apply. A message appears, confirming that the role has been updated.
7. Click Yes to close the message.

You have completed editing an administrator role.

NOTE The system-created administrator account and role, which is present by default on the controller, cannot be edited.

Cloning an Existing Administrator Role

If you want to create a new administrator role with capabilities that are similar to an existing role, cloning the existing administrator role may be the faster way to create that new role.

1. Follow these steps to clone an existing administrator role.
2. In the Administrator Roles section, locate the role that you want to clone.
3. Under the Actions column, click the ⧉ icon that is in the same row as the role that you want to clone. A dialog appears and prompts you for the name that you want to assign to the clone role. The default name is Clone of [Original Role Name].
4. Type a new name or leave the name as is.
5. Click Apply. The page refreshes, and then the role that you created appears under the Administrator Roles section.

You have completed cloning an existing administrator role. Unless you want the new role to have exactly the same capabilities as the original role, you may want to edit it. For the steps on editing the role, refer to Editing an Administrator Role.

Adding a RADIUS Server for Administrators

Follow these steps to add a RADIUS server for authenticating administrators.

NOTE: If you want to use a primary and secondary RADIUS servers for authenticating administrator, follow the steps in Using a Backup RADIUS Server for Authenticating Administrators.

1. Go to **Configuration** > **Administrators**.
2. In the *RADIUS Servers for Administrators* section, click **Create New**. The *Create New Administrator RADIUS Server* form appears.
3. In *Name*, type a name for the RADIUS server.
4. In *Type*, select the type of RADIUS server that you are using. Options include:
   - **RADIUS**: Click this option to use a Remote Authentication Dial-In User Service (RADIUS) server on the network for authenticating controller administrators.
   - **TACACS+**: Click this option to use a Terminal Access Controller Access-Control System Plus (TACACS+) server on the network for authentication controller administrators. See About TACACS+ Support for more information.

5 In *Realm*, type the realm (or realms) to which the RADIUS server belongs. If the RADIUS server belongs to multiple realms, use a comma (,) to separate the realm names.

6 Make sure that the **Enable backup RADIUS support** check box is not selected. If you want to use a backup RADIUS server, follow the steps in Using a Backup RADIUS Server instead.

7 In *IP Address*, type the IP address of the RADIUS server.

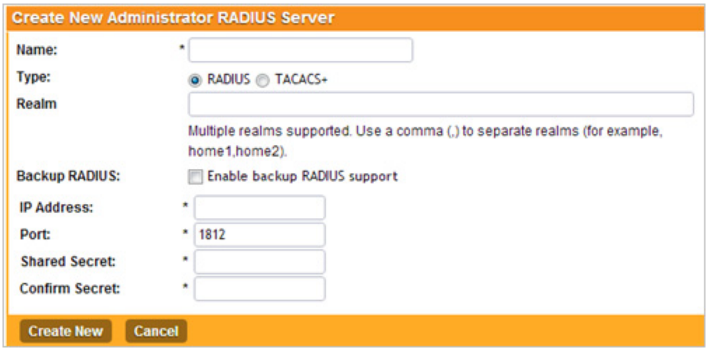
8 In *Port*, type the UDP port that the RADIUS server is using. The default port is 1812.

9 In *Shared Secret*, type the shared secret. Retype the same secret in *Confirm Secret*.

10 Click **Create New**.

You have completed adding a RADIUS server for authenticating administrators.

Figure 132. The Create New Administrator RADIUS Server form



Create New Administrator RADIUS Server

Name:	*
Type:	● RADIUS ○ TACACS+
Realm	Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2).
Backup RADIUS:	□ Enable backup RADIUS support
IP Address:	*
Port:	* 1812
Shared Secret:	*
Confirm Secret:	*

About TACACS+ Support

Terminal Access Controller Access-Control System Plus (TACACS+) is one of the Authentication, Authorization and Accounting protocols that can be used to authenticate controller administrators.TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery.

In addition to selecting TACACS+ as the RADIUS type in Adding a RADIUS Server for Administrators, you must also complete the following steps for TACACS+ based authentication to work.

1. Edit the TACACS+ configuration file (`tac.cfg`) on the TACACS+ server to include the service user name. See the example below.

   ```
   key = test@1234
   accounting file = /var/log/tac_acct.log
   user = username {
           member = show
           login = cleartext "password1234!"
           }
   group = show {
           service = super-login {
                 user-name = super <<==mapped to the user account
   in the controller
                   }
   ```

2. On the controller web interface, go to the *Configuration* > *Administrators* page, and then create an administrator account with “super” as the user name.
3. Go to the *Configuration* > *Management Domains* page, and then assign the “super” administrator account an administrator role.
4. When you add a RADIUS server for administrators (see Adding a RADIUS Server for Administrators), select TACACS+ as the authentication type.
5. After you add the RADIUS server for administrators, test it using the account “username@super-login”.

You have completed the configuration steps required to ensure that TACACS+ authentication for administrators work on the controller.

Using a Backup RADIUS Server

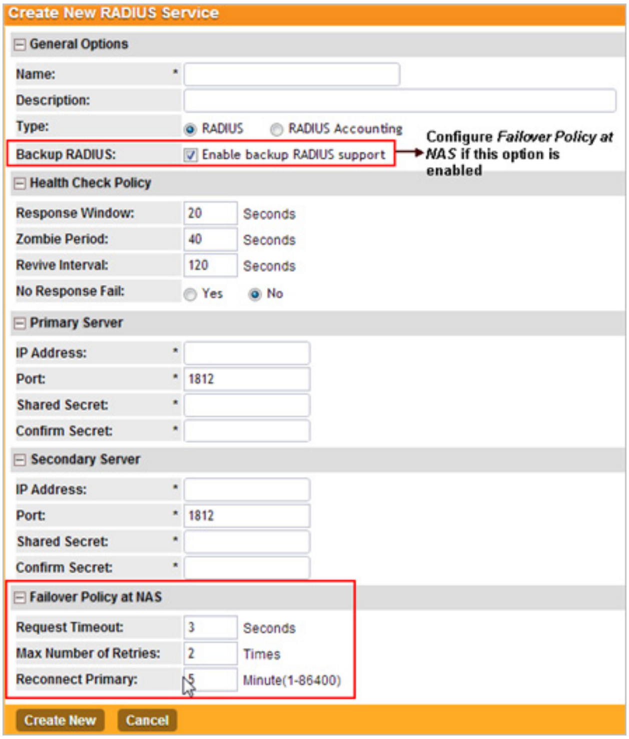
If a backup RADIUS server is available on the network, you can select the **Enable backup RADIUS server support** check box to use the backup server when the primary server is unavailable. When you select the check box, additional fields appear that you need to fill in.

Follow these steps to enable support for a backup RADIUS server for authenticating administrators.

1. Select the check box next to Enable backup RADIUS support.
2. In the Primary Server section, fill out the IP address, port number, and shared secret as you did in the previous section.
3. In the Secondary Server section, fill out the IP Address, port number and shared secret for the backup server (these fields can neither be left empty nor be the same values as those of the primary server).
4. In the Failover Policy section, configure the following settings:
   - Request Timeout: Type the timeout period (in seconds) after which an expected RADIUS response message is considered to have failed.
   - Max Number of Retries: Type the number of failed connection attempts after which the controller will fail over to the backup RADIUS server.
   - Reconnect Primary: Type the number of minutes after which the controller will attempt to reconnect to the primary RADIUS server after failover to the backup server.
5. Click Apply.

You have completed adding primary and secondary RADIUS servers for authenticating administrators.

Figure 133. Enabling the backup RADIUS server



Create New RADIUS Service

⊟ **General Options**

Name: *		
Description:		
Type:	● RADIUS ○ RADIUS Accounting	
Backup RADIUS:	☑ Enable backup RADIUS support	

Configure *Failover Policy at NAS* if this option is enabled

⊟ **Health Check Policy**

Response Window:	20	Seconds
Zombie Period:	40	Seconds
Revive Interval:	120	Seconds
No Response Fail:	○ Yes ● No	

⊟ **Primary Server**

IP Address: *	
Port: *	1812
Shared Secret: *	
Confirm Secret: *	

⊟ **Secondary Server**

IP Address: *	
Port: *	1812
Shared Secret: *	
Confirm Secret: *	

⊟ **Failover Policy at NAS**

Request Timeout:	3	Seconds
Max Number of Retries:	2	Times
Reconnect Primary:	5	Minute(1-86400)

Testing an AAA Server

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus Wireless strongly recommends testing the AAA server after you set it up. The test queries the RADIUS server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

Follow these steps to test an AAA server.

1 Go to **Configuration** > **Administrators**.

2 Scroll down to the *RADIUS Servers for Administrators* section.

3 Click **Test AAA**. The Test AAA Servers for appears.

4 In *Name*, select one of the AAA servers that you previous created.

5 In *User Name*, type an existing user name on the AAA server that you selected.

6 In *Password*, type the password for the user name you specified.

7 Click **Test**.

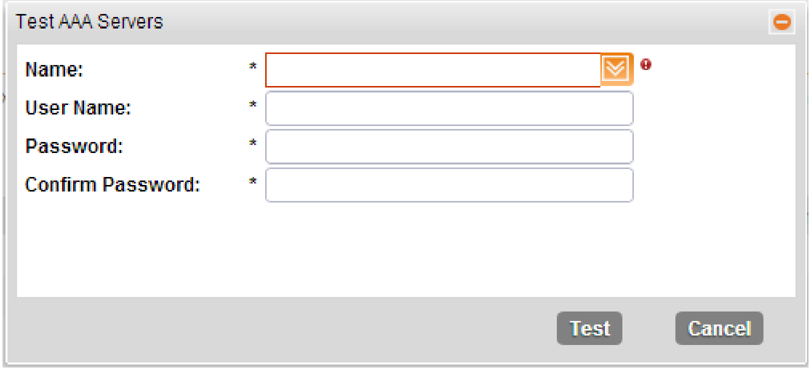
If the controller was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page.

If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly:

- Admin invalid
- User name or password invalid

These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

Figure 134. The Test AAA Servers form



Deleting an Administrator Account, Role, or RADIUS Server

Follow these steps to delete an administrator account, role, or RADIUS server that is used for authenticating administrators.

1 Go to **Configuration** > **Administrators**.

2 Locate the administrator account, role, or the RADIUS server that you want to delete.

3 Under the *Actions* column, click the 🗑 icon that is in the same row as the account, role, or RADIUS server name. A confirmation message appears.

4 Click **Yes**. The page refreshes, and then the administrator account, role, or RADIUS server that you deleted disappears from the *Administrators* page.

You have completed deleting an administrator account, role, or RADIUS server used for authenticating administrators.

NOTE The default administrator account and role, which exist on the controller by default, cannot be deleted.

Managing Mobile Virtual Network Operator Accounts 10

In this chapter:

- Overview of Mobile Virtual Network Operator Accounts
- Viewing a List of MVNOs
- Creating a New MVNO Account
- Using a Backup RADIUS Server for Authorizing and Authenticating MVNOs
- Editing an MVNO Account
- Deleting an MVNO Account

Overview of Mobile Virtual Network Operator Accounts

This section describes how to create, edit, and delete mobile virtual network operator accounts.

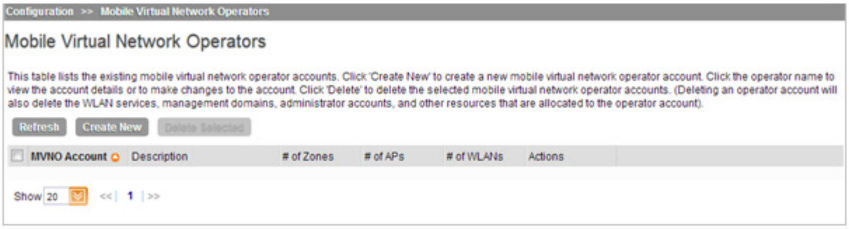
Viewing a List of MVNOs

Follow these steps to view a list of mobile virtual network operator (MVNO) accounts.

1 Go to **Configuration** > **Mobile Virtual Network Operators**.

2 The MVNO table appears and displays a summary of mobile virtual network operator accounts that have been created.

Figure 135. The Mobile Virtual Network Operators page



Configuration >> Mobile Virtual Network Operators

Mobile Virtual Network Operators

This table lists the existing mobile virtual network operator accounts. Click 'Create New' to create a new mobile virtual network operator account. Click the operator name to view the account details or to make changes to the account. Click 'Delete' to delete the selected mobile virtual network operator accounts. (Deleting an operator account will also delete the WLAN services, management domains, administrator accounts, and other resources that are allocated to the operator account).

□	MVNO Account	Description	# of Zones	# of APs	# of WLANs	Actions

Creating a New MVNO Account

Follow these steps to create a new virtual network operator account.

1 On the MVNO page, click **Create New**. The *Mobile Virtual Network Operator* form appears.

2 In *Mobile Virtual Network Operator Summary* section:

- Type a domain name to which this account will be assigned in the Domain Name box.
- In Description, type a brief description about this domain name.

3 In Configure the AP zones to which the MVNO account that you are creating will have management privileges. Click *Add AP Zone* to create an AP Zone(s)

- In AP Zone, select the AP zone to which the MVNO account will have management privileges.

NOTE: You can only select a single AP zone at a time. If you want to grant the MVNO account management privileges to multiple AP zones, select them one at time.

- Click **Apply**. The AP Zones of Mobile Virtual Network Operator section refreshes. The AP zone or zones that you selected appears in the section.

4 In Configure the WLAN services, follow these steps to configure the WLAN services to which the MVNO account that you are creating will have management privileges.

- In the WLAN services section, click Add WLAN(s).
- In SSID, select the WLAN to which the MVNO account will have management privileges.

NOTE: You can only select one WLAN service at a time. If you want to grant the MVNO account management privileges to multiple WLAN service zones, select them one at time.

- Click Apply. The WLAN services section refreshes. The WLAN service or services that you selected appears in the section.

5 In Create the Super Administrator Account, follow these steps to create the MVNO account and define the logon details and management capabilities that will be assigned to the account.

- Scroll down to the Super Administrator section.

- In Account Name, type the name that this MVNO will use to log on to the controller.
- In Real Name, type the actual name (for example, John Smith) of the MVNO.
- In Password, type the password that this MVNO will use (in conjunction with the Account Name) to log on to the controller.
- In Confirm Password, type the same password as above.
- In Phone, type the phone number of this MVNO.
- In Email, type the email address of this MVNO.
- In Job Title, type the job title or position of this MVNO in his organization.
- In the Assign Capabilities to Administrator Role tree (located on the right side of the form), select the administrator capabilities that you want to assign to this MVNO. If you plan to grant this MVNO most of the capabilities that are available, click Select All, and then clear the check boxes for the capabilities that you do not want this MVNO to have.
- Remember to click the ⊞ icon next to each folder to view all capabilities that are included.

6. In RADIUS Server for Administrator Authorization and Authentication, follow these steps to add a RADIUS server for authenticating this MVNO.

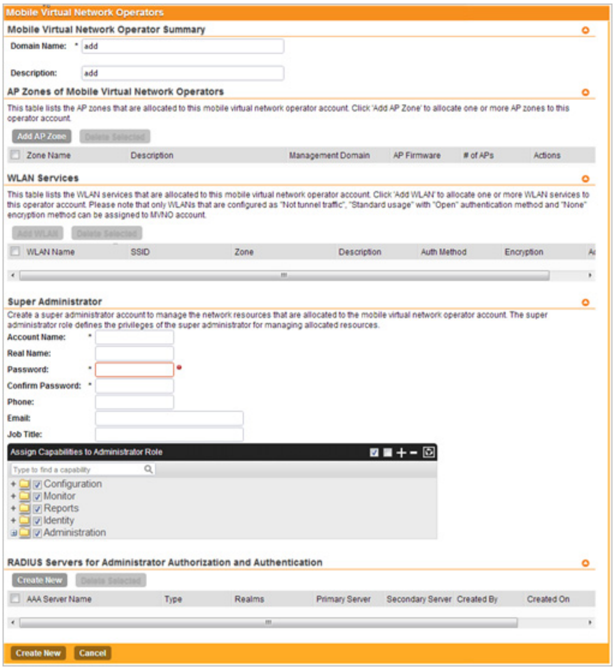
NOTE: If you want to use a primary and secondary RADIUS servers for authenticating administrator, follow the steps in Using a Backup RADIUS Server for Authorizing and Authenticating MVNOs.

- In the RADIUS Servers for Administrator Authorization and Authentication section, click *Create New*. The RADIUS Servers for Administrator Authorization and Authentication form appears.
- In Name, type a name for the RADIUS service.
- In Realm, type the realm or realms to which the RADIUS server belongs. If the RADIUS server belongs to multiple realms, use a comma (,) to separate the realm names.
- Make sure that the Enable backup RADIUS support check box is not selected.
- If you want to use a backup RADIUS server, follow the steps in Using a Backup RADIUS Server for Authenticating Administrators instead.
- In IP Address, type the IP address of the RADIUS server.
- In Port, type the UDP port that the server is using. The default port is 1812.

- In Shared Secret, type the shared secret. Retype the same secret in Confirm Secret.
- Click Apply.

After you complete steps 1 through 6, click *Create New* to save the MVNO account. The page refreshes, and the MVNO account that you created appears on the list of existing MVNO accounts.

Figure 136. The Create New Virtual Network Operator form



Mobile Virtual Network Operators

Mobile Virtual Network Operator Summary

Domain Name: *	add
Description:	add

AP Zones of Mobile Virtual Network Operators

This table lists the AP zones that are allocated to this mobile virtual network operator account. Click 'Add AP Zone' to allocate one or more AP zones to this operator account.

□	Zone Name	Description	Management Domain	AP Firmware	# of APs	Actions

WLAN Services

This table lists the WLAN services that are allocated to this mobile virtual network operator account. Click 'Add WLAN' to allocate one or more WLAN services to this operator account. Please note that only WLANs that are configured as "Not tunnel traffic", "Standard usage" with "Open" authentication method and "None" encryption method can be assigned to MVNO account.

□	WLAN Name	SSID	Zone	Description	Auth Method	Encryption	A

Super Administrator

Create a super administrator account to manage the network resources that are allocated to the mobile virtual network operator account. The super administrator role defines the privileges of the super administrator for managing allocated resources.

Account Name: *	
Real Name:	
Password: *	
Confirm Password: *	
Phone:	
Email:	
Job Title:	

Assign Capabilities to Administrator Role

- ☑ Configuration
- ☑ Monitor
- ☑ Reports
- ☑ Identity
- ☑ Administration

RADIUS Servers for Administrator Authorization and Authentication

□	AAA Server Name	Type	Realms	Primary Server	Secondary Server	Created By	Created On

Using a Backup RADIUS Server for Authorizing and Authenticating MVNOs

If a backup RADIUS server is available on the network, you can select the Enable backup RADIUS server support check box to use the backup server when the primary server is unavailable. When you select the check box, additional fields appear that you need to fill in.

Follow these steps to enable support for a backup RADIUS server for authorizing and authenticating MVNOs.

1. Select the check box next to **Enable backup RADIUS support**.
2. In the *Primary Server* section, fill out the IP address, port number, and shared secret as you did in the previous section.
3. In the *Secondary Server* section, fill out the IP Address, port number and shared secret for the backup server (these fields can neither be left empty nor be the same values as those of the primary server).
4. Click **Apply**.

You have completed adding primary and secondary RADIUS servers for authorizing and authenticating MVNOs.

Editing an MVNO Account

Follow these steps to edit an existing virtual network operator account.

1. Go to *Configuration > Mobile Virtual Network Operators*. The *Mobile Virtual Network Operator* page appears, displaying all MVNO accounts that have been created.
2. Click the domain name of the MVNO account that you want to edit.
3. Edit or update the account details in the following sections as required:
   - Mobile Virtual Network Operator Summary
   - AP Zones of Mobile Virtual Network Operator
   - WLAN services
   - Super Administrator (and Assign Capabilities to Administrator Role)
   - RADIUS Servers for Administrator Authorization and Authentication
4. Click **Apply**.

You have completed editing the MVNO account.

Deleting an MVNO Account

Follow these steps to delete an existing virtual network operator account.

1. Go to Configuration > Mobile Virtual Network Operators. The Mobile Virtual Network Operator page appears, displaying all MVNO accounts that have been created.
2. Locate the domain name of the MVNO account that you want to delete.
3. Once you locate the MVNO account, click the 🗑 icon that is under the Actions column. A confirmation message appears.
4. Click Yes. The list of MVNO accounts refreshes, and then the MVNO account that you deleted disappears from the list.

You have completed deleting an MVNO account.

Creating and Managing Hotspots 11

In this chapter:

- Overview of Hotspot Management
- Hotspot Terminologies
- How Hotspot Authentication Works
- Call Flow for Devices That Use a Web Proxy
- User Agent Blacklist
- Notes on Using iOS Devices to Access the Hotspot
- What You Will Need
- Hotspot Configuration Options
- Downloading Captive Portal and Subscriber Portal Logs

Overview of Hotspot Management

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability, such as notebooks and smart phones. Hotspots are commonly available in public venues such as hotels, airports, coffee shops, and shopping malls.

All Ruckus Wireless access points have a built-in hotspot module that can be enabled and deployed on available WLANs. In addition to the hotspot capability of Ruckus Wireless access points, the controller provides the Captive Portal and Subscriber Portal modules, which are required by a hotspot infrastructure.

This chapter provides information on how to enable and configure the hotspot portal that the controller-managed access points provide.

NOTE: Ruckus Wireless hotspot portals are based on the Wireless Internet Service Provider roaming (WISPr) standards.

Hotspot Terminologies

Table 9 lists the hotspot terms that are used in this guide. Before continuing, Ruckus Wireless recommends that you become familiar with these terms.

Table 9. Hotspot terms

Term	Definition
Hotspot client	A wireless client or device that is associating with a hotspot portal
Hotspot user	A human user using the hotspot portal on the hotspot client
Captive Portal	A controller module that intercepts a hotspot user’s initial connection attempt to the Internet and redirects the connection to the Subscriber Portal (either internal or external). The Captive Portal and the Subscriber Portal make up the hotspot module of the controller.
Subscriber Portal	A controller module that allows a hotspot user to enter his or her hotspot user name and password to gain access to the hotspot portal (either through browser-based logon or Smart Client logon).
Authenticated user	A user who has passed the authentication process
Unauthenticated user	A user who has not passed the authentication process or has failed authentication
Walled garden	The purpose of the walled garden is to let unauthenticated users access online registration, payment services, or other websites (such as a hotel reservation page) without needing to log on first. All other sites are off-limits.

How Hotspot Authentication Works

This section describes the steps that a hotspot user performs to gain access to the hotspot portal and how the controller handles the hotspot access request.

NOTE: Ruckus Wireless hotspot portals are based on the Wireless Internet Service Provider roaming (WISPr) standards.

---

1 A hotspot client associates with the hotspot WLAN service (which is typically unencrypted) that is provided by a Ruckus Wireless AP.

NOTE: The hotspot modules – Captive Portal and Subscriber Portal – communicate with the AP through the user defined interface (if configured) or the control Interface. For information on creating a user defined interface, refer to Creating a User Defined Interface.

---

2 The hotspot user attempts to browse the Web (for example, www.ruckuswireless.com) on the hotspot client.

3 The AP detects the user state (which, in this case, is unauthenticated) and performs network address translation (NAT) to the related port on the Captive Portal. The AP also adds information to the HTTP header, including the AP SSID and device MAC address and IP address.

4 The Captive Portal module first applies the blacklist user-agent (see User Agent Blacklist), and then the walled garden list to the request (URL whitelist, only for UEs configured with web proxy. The AP handles the walled garden for non-web proxy UEs). If the request passes these two filters, the Captive Portal redirects the hotspot user to the configured portal URL. In case it was configured as an internal portal, the Subscriber Portal module handles the request and displays the hotspot logon page.

NOTE: The controller provides a built-in Subscriber Portal module that you can use immediately.

---

5 The hotspot user enters the user name and password provided by the hotspot operator on the logon page that is presented by the Subscriber Portal.

6 The portal sends a JSON HTTP request to the controller’s northbound interface, which identifies (based on some parameters) the configured AAA server for this request. It then sends the authentication request to the AAA server.

7 The AAA server responds with an Access Accept or Access Reject message.

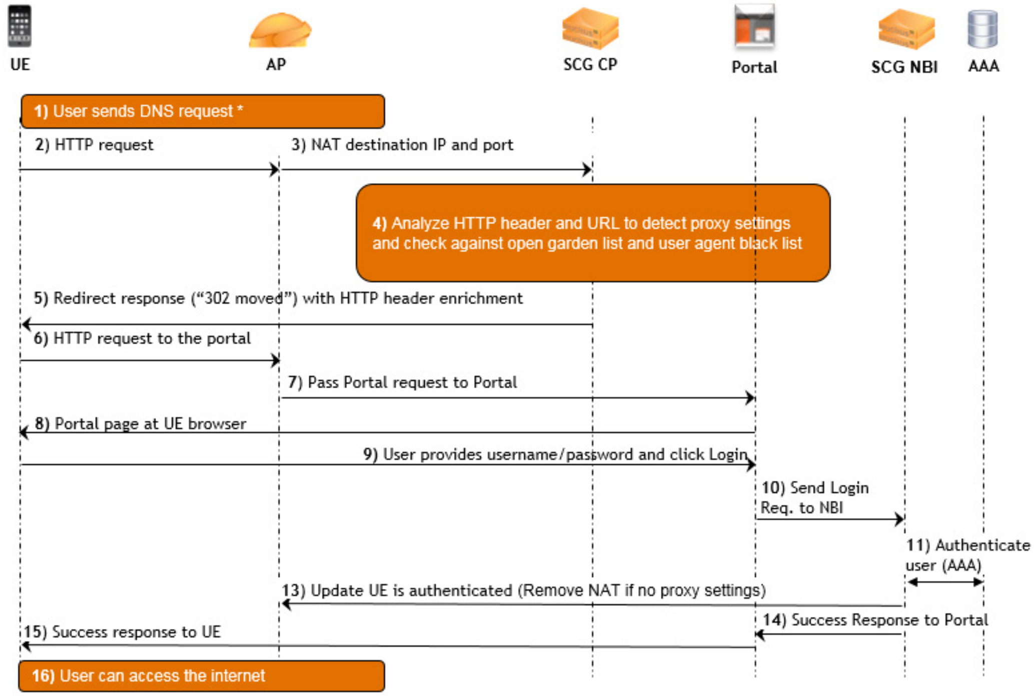
8 If the user was authenticated successfully, the controller's northbound interface sends a command to the AP to change its state to "Authorized," so any further traffic from this UE will be permitted. The northbound interface also sends a "successful" response to the portal.

If the portal is an internal portal, a "successful" message appears to the user and the user must click the **Continue** button on the browser page to go to the original URL that he or she intended to visit. Once logged on to the hotspot, all traffic from the UE is routed directly through the AP to the Internet, unless tunnel mode is enabled on the WLAN or the user is using a web proxy.

Alternatively, instead of redirecting the UE after a successful authentication to the original URL that he or she intended to visit, the portal can be configured to redirect the user to a different page (for example, if the hotspot is in a shopping mall, the user can be redirected to the shopping mall home page after he or she clicks the **Continue** button).

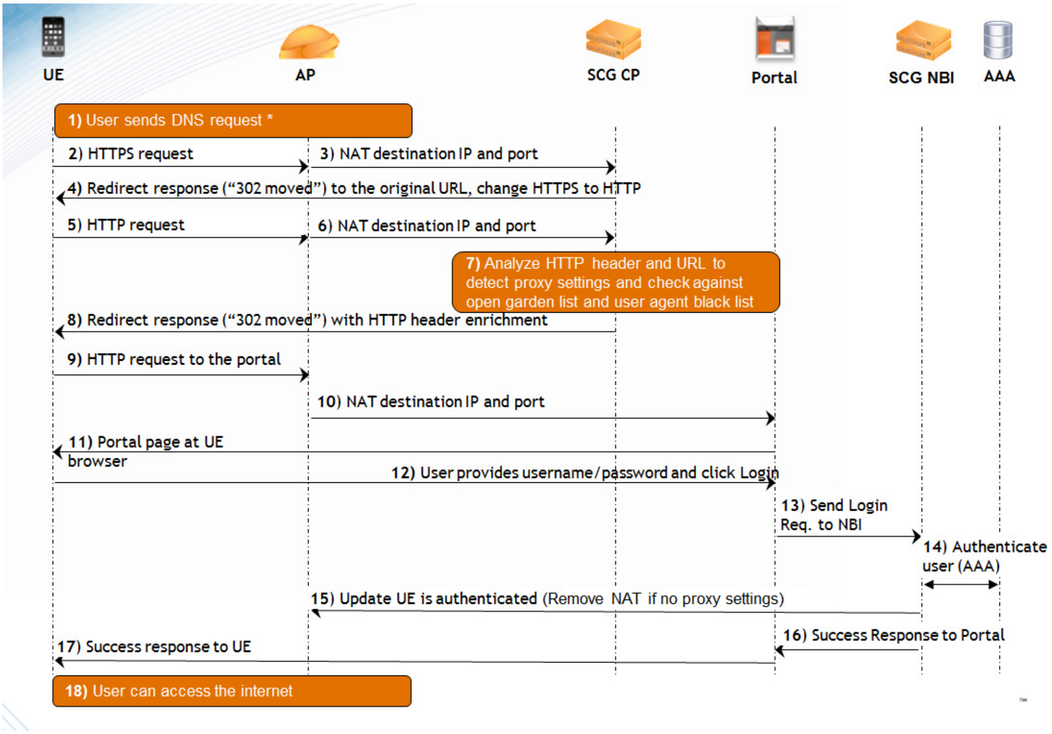
The user has completed the hotspot authentication process and is now able to connect to the Internet.

Figure 137. Basic flow of the hotspot authentication process for an HTTP-based request


UE
AP
SCG CP
Portal
SCG NBI
AAA
1) User sends DNS request *
2) HTTP request
3) NAT destination IP and port
4) Analyze HTTP header and URL to detect proxy settings and check against open garden list and user agent black list
5) Redirect response ("302 moved") with HTTP header enrichment
6) HTTP request to the portal
7) Pass Portal request to Portal
8) Portal page at UE browser
9) User provides username/password and click Login
10) Send Login Req. to NBI
11) Authenticate user (AAA)
13) Update UE is authenticated (Remove NAT if no proxy settings)
14) Success Response to Portal
15) Success response to UE
16) User can access the internet

CAUTION! For users to be able to access the subscriber portal, it must be resolved to the UEs directly as well as to the controller itself. This is because UEs that use proxy settings are unable to resolve the subscriber-portal URL directly (but are able to resolve the captive portal). One of the following alternatives needs to be performed: (1) The DNS server with which users are associated must resolve the subscriber portal URL. Likewise, the DNS server with which the controller is associated must resolve the subscriber portal URL. (2) The UEs and the controller must be associated with the same DNS server and the DNS server must resolve the subscriber portal URL.

Figure 138. Basic flow of the hotspot authentication process for an HTTPS-based request (double-redirect approach)


UE
AP
SCG CP
Portal
SCG NBI
AAA
1) User sends DNS request *
2) HTTPS request
3) NAT destination IP and port
4) Redirect response ("302 moved") to the original URL, change HTTPS to HTTP
5) HTTP request
6) NAT destination IP and port
7) Analyze HTTP header and URL to detect proxy settings and check against open garden list and user agent black list
8) Redirect response ("302 moved") with HTTP header enrichment
9) HTTP request to the portal
10) NAT destination IP and port
11) Portal page at UE browser
12) User provides username/password and click Login
13) Send Login Req. to NBI
14) Authenticate user (AAA)
15) Update UE is authenticated (Remove NAT if no proxy settings)
16) Success Response to Portal
17) Success response to UE
18) User can access the internet

Call Flow for Devices That Use a Web Proxy

If a user device is configured to use a Web proxy server to gain access to the Internet, the call flow for the hotspot authentication process is different. This is because the AP needs to perform network address translation (NAT) on the HTTP or HTTPS request from the user device and the Captive Portal functions as a proxy between the user device and Web server on which the requested URL is hosted.

Figure 139 illustrates that call flow for the hotspot authentication process if the user device is using a Web proxy server to connect to the Internet.

NOTE: Every request from the user device goes through the Captive Portal, even after the user device is authenticated.

Figure 139. Basic flow of the hotspot authentication process for an HTTP proxy-based request

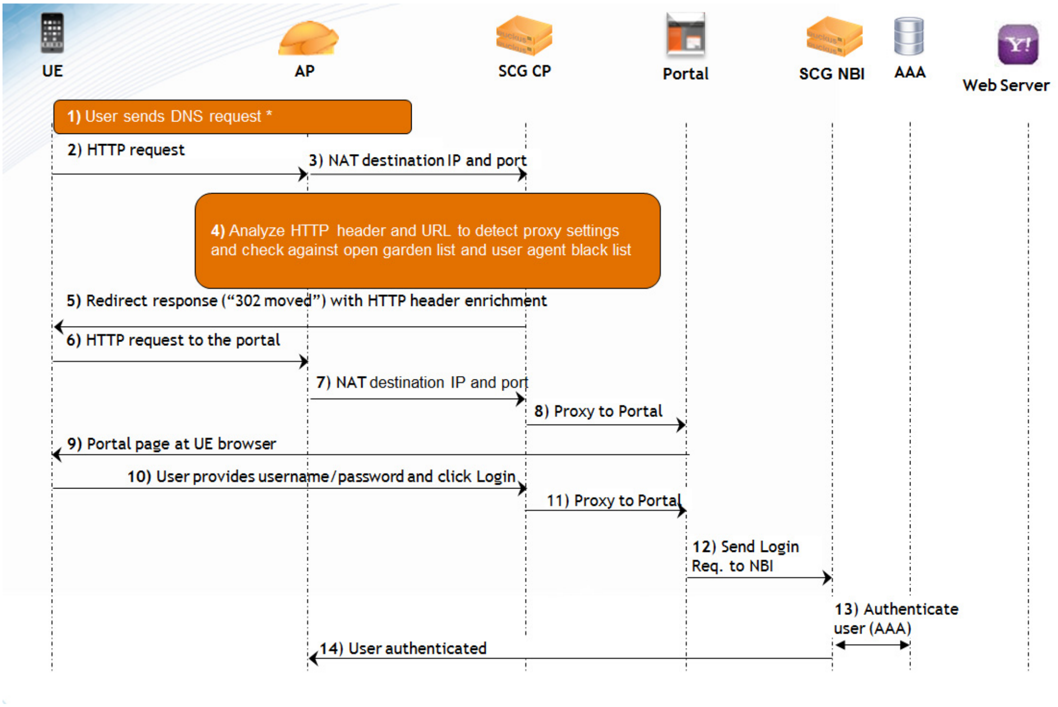
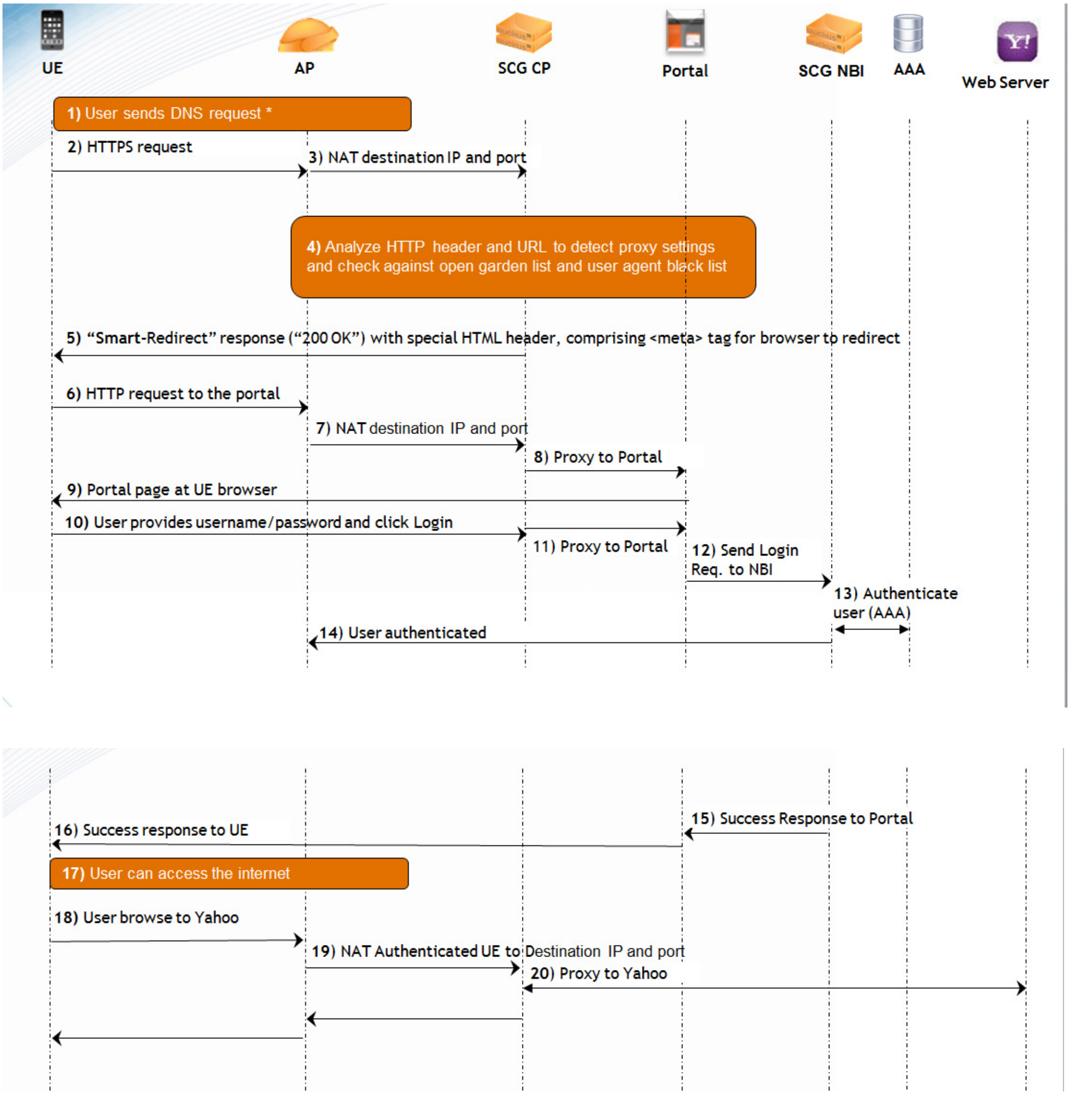

UE
AP
SCG CP
Portal
SCG NBI
AAA
Web Server
1) User sends DNS request *
2) HTTP request
3) NAT destination IP and port
4) Analyze HTTP header and URL to detect proxy settings and check against open garden list and user agent black list
5) Redirect response ("302 moved") with HTTP header enrichment
6) HTTP request to the portal
7) NAT destination IP and port
8) Proxy to Portal
9) Portal page at UE browser
10) User provides username/password and click Login
11) Proxy to Portal
12) Send Login Req. to NBI
13) Authenticate user (AAA)
14) User authenticated

Figure 140. Basic flow of the hotspot authentication process for an HTTPS proxy-based request


UE
AP
SCG CP
Portal
SCG NBI
AAA
Web Server
1) User sends DNS request *
2) HTTPS request
3) NAT destination IP and port
4) Analyze HTTP header and URL to detect proxy settings and check against open garden list and user agent black list
5) "Smart-Redirect" response ("200 OK") with special HTML header, comprising <meta> tag for browser to redirect
6) HTTP request to the portal
7) NAT destination IP and port
8) Proxy to Portal
9) Portal page at UE browser
10) User provides username/password and click Login
11) Proxy to Portal
12) Send Login Req. to NBI
13) Authenticate user (AAA)
14) User authenticated
15) Success Response to Portal
16) Success response to UE
17) User can access the internet
18) User browse to Yahoo
19) NAT Authenticated UE to Destination IP and port
20) Proxy to Yahoo

Devices Using a Static Web Proxy

If a client device is configured to use a static Web proxy, the client Web browser will use predefined proxy settings, which will prevent it from being redirected to the Captive Portal successfully. The controller's built-in Web proxy application can establish a connection with the browser, assume the role of a proxy, and then redirect the user to the logon page for authentication and, after a successful authentication, to the requested page.

Devices Using a Dynamic Web Proxy

If a client device is configured to use a dynamic Web proxy, it typically receives its proxy settings in a proxy auto-config (PAC) file from a server on the local network. If you have such client devices on the network, you can use the Captive Portal to respond to the request for a PAC file from these devices with a preconfigured PAC file. This preconfigured PAC file disables the proxy settings on client devices and enables them to connect to the network without going through a proxy server. The preconfigured PAC file is located in the configuration directory of the Captive Portal.

The controller supports both proxy auto-config (PAC) and Web Proxy Autodiscovery Protocol (WPAD). Currently, the controller uses a PAC file that supports requests for both PAC and WPAD proxy configuration files.

User Agent Blacklist

By default, the controller automatically blocks certain user agents (or software used by a user) from accessing the hotspot. These blocked user agents include:

- ZoneAlarm
- VCSoapClient
- XTier NetIdentity
- DivX Player
- Symantec LiveUpdate
- Windows Live Messenger
- StubInstaller
- windows-update-agent
- Windows Live Essentials
- Microsoft Dr. Watson for Windows (MSDW)
- Avast Antivirus Syncer

- Microsoft Background Intelligent Transfer Service (BITS)
- Google Update
- TrendMicro client
- Skype WISPr

When the controller blocks any of these user agents, an error message appears on the user device.

You can add or remove user agents to this blacklist. For more information, see Managing the Global User Agent Black List.

NOTE: In release 3.0, Microsoft NCSI was included in the user agent blacklist. This prevented Windows Network Awareness, a feature that allows Windows services and applications to automatically select the network connection best suited to their tasks, from working properly. Microsoft NCSI has been removed from the user agent blacklist in release 3.1 and later.

Notes on Using iOS Devices to Access the Hotspot

When an iOS device (for example, Apple iPhone or iPad) associates with a hotspot, it probes for an Internet connection by sending an HTTP request to the following Web page:

```
http://www.apple.com/library/test/success.html
```

NOTE: Devices running on newer iOS versions issue a request with a special User-Agent, which contains the "CaptiveNetworkSupport" string in the User-Agent header.

If the iOS device does not receive an appropriate response from www.apple.com, the hotspot logon page does not appear on the device. If the iOS device user closes or skips the hotspot logon page, the device is disconnected from the network and is unable to browse even the network destinations (IP addresses or Web addresses) defined in the walled garden.

Since the walled garden is not URI-capable and adding www.apple.com to the walled garden can cause significant data consumption on the controller server, Ruckus Wireless has designed the Captive Portal to respond to the HTTP request sent by the iOS device with the following page:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD>
         <TITLE>Success</TITLE>
</HEAD>
<BODY>
Success
</BODY>
</HTML>
```

Notes on Using Amazon Kindle Fire to Access the Hotspot

The behavior of Amazon Kindle Fire devices is similar to the behavior of devices running older iOS versions, except HTTP requests from Kindle devices use a different URL:

```
 http://spectrum.s3.amazonaws.com/kindle-wifi/
wifistub.html
```

Ruckus Wireless has designed the Captive Portal to respond to the HTTP request sent by the Kindle Fire device with the following page:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://
www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>Kindle Reachability Probe Page</title>
<META http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
<!--81ce4465-7167-4dcb-835b-dcc9e44c112a created with
python 2.5 uuid.uuid4()-->
</head>
<body bgcolor="#ffffff" text="#000000">
81ce4465-7167-4dcb-835b-dcc9e44c112a
</body>
</html>
```

What You Will Need

To enable controller-managed access points to provide hotspot portals, you will need the following:

1 RADIUS server for authenticating hotspot users

2 RADIUS accounting server (optional) for monitoring usage of hotspot users.

Hotspot Configuration Options

You can create a hotspot portal when you configure one of the following:

- A WLAN service of an AP zone
- A zone template
- A WLAN template

The steps described in this section must be completed when you configure a WLAN service of an AP zone or when you create a zone template or WLAN template.

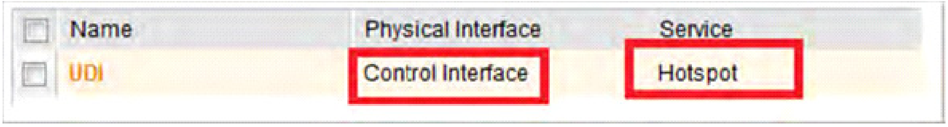
This section provides additional information on the hotspot configuration options that are available from within the forms for creating a zone template or WLAN template.

Why Create a User Defined Interface

APs use the control interface to communicate receive configuration updates from the controller. If you want to have a logical separation of the UE traffic and the AP control traffic, you can create a user defined interface (UDI).

If a UDI is configured (using the control interface as its physical interface and providing a hotspot portal as shown below), APs use it to perform Destination Network Address Translation (DNAT) of requests from unauthorized UEs to the controller's captive portal (otherwise, APs use the control interface)

Figure 141. A UDI configured to use the control interface as its physical interface and to provide a hotspot portal



□	Name	Physical Interface	Service
□	UDI	Control Interface	Hotspot

The controller's captive portal redirects the UE to the configured portal logon page URL. When the UE triggers this portal URL request, the AP lets the request through (without performing DNAT to the controller's captive portal), as it is configured as an ACL on AP, directly to the external portal server.

Creating a User Defined Interface

The hotspot modules – Captive Portal and Subscriber Portal – require a user defined interface to communicate with the hotspot AP. The controller uses this user defined interface (which you will need to create) to receive hotspot logon data from hotspot users.

This section describes how to create a user defined interface that you can use for the hotspot portal and how to enable the northbound portal interface.

Follow these steps to create a user defined interface.

1. Go to *Configuration* > *System* > *Cluster Planes*.
2. In the *Control Plane* section, click the control plane on which you want to create the user defined interface for the hotspot portal. The *Edit Control Plane Network Settings* form appears.
3. Click the *User Defined Interface* tab.
4. Click **Create New**. Empty boxes on the *User Defined Interface* tab appear.
5. Configure the following interface settings:
   - *Name*: Assign a name to this user defined interface.
   - IP Address
   - Subnet Mask
   - Gateway
   - *VLAN*: Assign a VLAN ID to the user defined interface.
   - *Physical Interface*: Select **Control Interface**.
   - *Service*: Select **Hotspot**.
6. Click **Apply**. A confirmation message appears.
7. Click **Yes**. The controller restarts automatically and applies the changes you made to the user defined interface. When the controller completes applying the changes, the following message appears:

   ```
   Control plane configuration updated successfully.
   ```
8. Click **Close** at the bottom of the form to close it.
9. Go to *Configuration* > *System* > *General System Settings*.

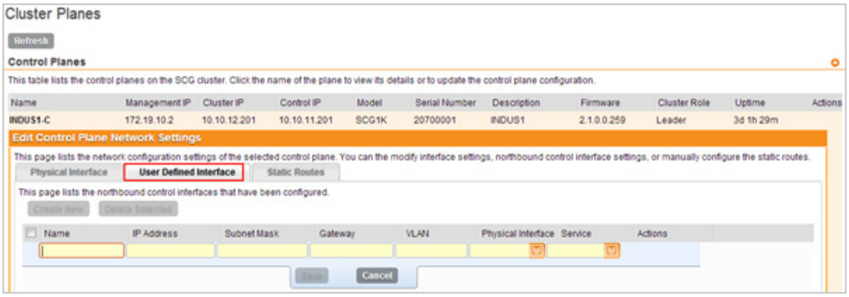
NOTE: If you are using the internal Subscriber Portal, skip Step 10 and Step 11. The controller automatically generates a 32-character random password for the northbound portal interface. If you are using an external Subscriber Portal, set the northbound portal interface password on the General System Settings page, and then enter the password in Step 10.

10 In the *Northbound Portal Interface* section, type the password for the northbound interface in the box provided.

11 Click **Apply**.

You have completed creating a user defined interface for the hotspot.

Figure 142. Creating a user defined interface



Cluster Planes

Control Planes

This table lists the control planes on the SCG cluster. Click the name of the plane to view its details or to update the control plane configuration.

Name	Management IP	Cluster IP	Control IP	Model	Serial Number	Description	Firmware	Cluster Role	Uptime	Actions
INDUS1-C	172.19.10.2	10.10.12.201	10.10.11.201	SCG1K	20700001	INDUS1	2.1.0.0.259	Leader	3d 1h 29m	

Edit Control Plane Network Settings

This page lists the network configuration settings of the selected control plane. You can the modify interface settings, northbound control interface settings, or manually configure the static routes.

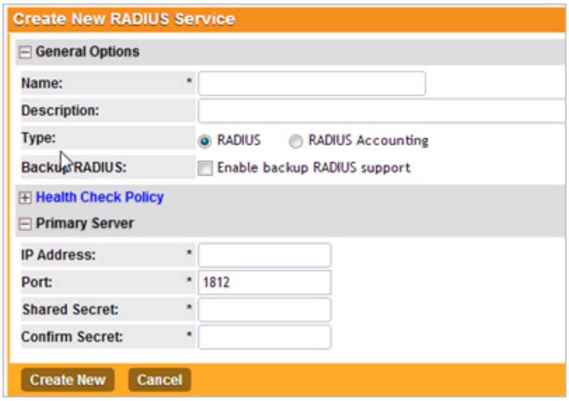
This page lists the northbound control interfaces that have been configured.

□	Name	IP Address	Subnet Mask	Gateway	VLAN	Physical Interface	Service	Actions

Adding a RADIUS Server to the Controller

A hotspot requires a RADIUS server to authenticate users that are attempting to access the hotspot portal. Use the form shown below to add a RADIUS server.

Figure 143. The Create New RADIUS Service form



Create New RADIUS Service

⊟ General Options

Name:	*	
Description:		
Type:		● RADIUS ○ RADIUS Accounting
Backup RADIUS:		□ Enable backup RADIUS support

⊞ Health Check Policy

⊟ Primary Server

IP Address:	*	
Port:	*	1812
Shared Secret:	*	
Confirm Secret:	*	

Adding a RADIUS Accounting Server

If you want to monitor the usage of hotspot users (for example, for billing purposes), you can also add a RADIUS accounting to the controller. The form for adding a RADIUS accounting server is the same as for adding a RADIUS server – you only need to click RADIUS Accounting instead of RADIUS.

Creating a Hotspot WLAN

You can create a hotspot portal when you configure a WLAN service of an AP zone (see Creating a WLAN). When you reach the *WLAN Usage Type* section, click **Hotspot (WISPr)**.

Configuring Smart Client Support

Ruckus Wireless hotspots support the WISPr Smart Client feature, which allows client devices to log on to a hotspot seamlessly without requiring the user to go through the logon page. The controller provides the following options for supporting Smart Clients:

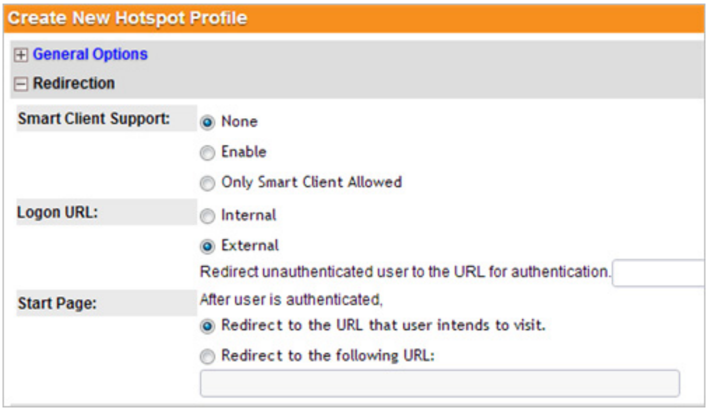
- *None*: Click this option to prevent Smart Client applications from logging on to WLANs that include this hotspot configuration.

- *Enable*: Click this option to allow Smart Client applications to log on to WLANs that include this hotspot configuration.
- *Only Smart Client Allowed*: Click this option to allow only Smart Client applications to log on to WLANs that include this hotspot configuration. All other applications or browsers that attempt to access the hotspot will be shown a custom message, which you can enter in the box provided.

CAUTION! Clicking **Only Smart Client Allowed** requires the use of the internal Subscriber Portal. The Logon URL and Start Page options are unavailable when the **Only Smart Client Allowed** option is selected

---

Figure 144. Smart Client support options



Create New Hotspot Profile

⊞ General Options

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication.

Start Page: After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL:

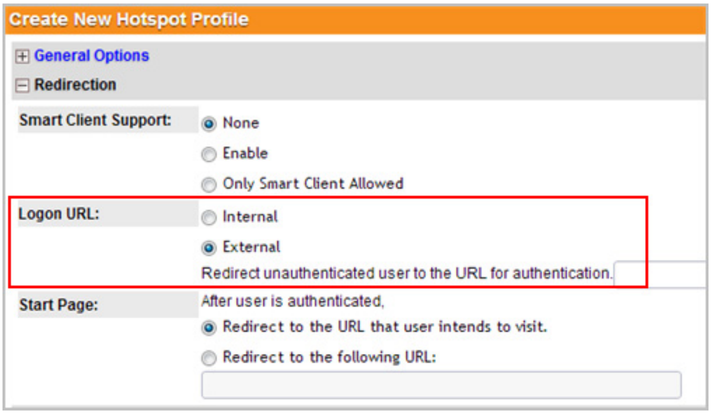
Configuring the Logon URL

Logon URL refers to the location of the Subscriber Portal module that serves the logon form for authenticating hotspot users. There are two options available for the logon URL: Internal and External.

- **Internal**: Click this option if you want to use the Subscriber Portal module that is built into the controller.
- **External**: Click this option if you want to use the Subscriber Portal module that is installed on an external server. In the text box below, type the URL to the Subscriber Portal on the external server. In the example below, the Subscriber Portal module is installed on a server with the IP address 172.21.11.248, hence the logon URL is:

```
http://172.21.11.248:9997/SubscriberPortal/login
```

Figure 145. In Logon URL, click either Internal or External



Create New Hotspot Profile

⊞ General Options

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication.

Start Page: After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL:

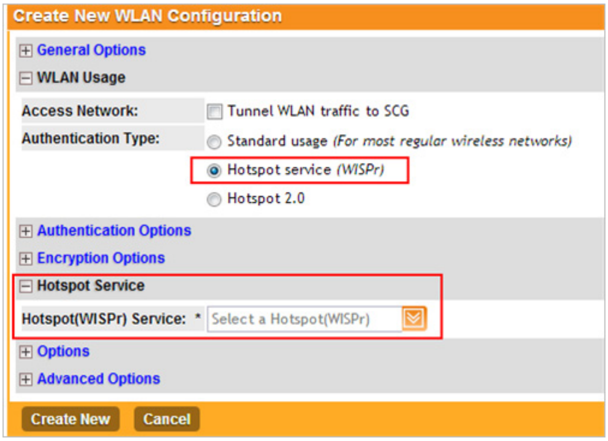
Creating a WLAN

Now that you have created a hotspot portal, you are ready to create a hotspot WLAN.

1. In the *WLAN Usage* section, click **Hotspot (WISPr)**.
2. In *Hotspot Portal*, select the hotspot portal that you created in Creating a Hotspot WLAN.
3. Configure other settings are described in Working with WLANs and WLAN Groups.
4. Save the template.

NOTE: Hotspot creation requires that you select a hotspot portal to use. Make sure that you already created a hotspot portal before you create a hotspot WLAN.

Figure 146. Select the hotspot portal that you created earlier



Create New WLAN Configuration

⊞ General Options

⊟ WLAN Usage

Access Network: □ Tunnel WLAN traffic to SCG

Authentication Type: ○ Standard usage *(For most regular wireless networks)*
● Hotspot service *(WISPr)*
○ Hotspot 2.0

⊞ Authentication Options

⊞ Encryption Options

⊟ Hotspot Service

Hotspot(WISPr) Service: * Select a Hotspot(WISPr)

⊞ Options

⊞ Advanced Options

Create New | Cancel

You have completed configuring the hotspot settings in the zone template or WLAN template.

Downloading Captive Portal and Subscriber Portal Logs

Follow these steps to download the Captive Portal and Subscriber Portal logs from the controller.

1 Go to *Administration* > *Diagnostics*. The *Diagnostics* page appears.

2 On the sidebar, click **Application Logs & Status**. The *Application Logs & Status* page appears.

3 In *Select Control Plane*, select the control plane to which the Captive Portal module is connected.

4 In the table below, locate the application named *CaptivePortal*. You can view the following information about CaptivePortal, as well as the other applications in the controller:

- Health Status
- Log Level
- # of Logs

5 Under the *Actions* column, click the 💾 icon that is in the same row as *CaptivePortal*. Your web browser downloads the logs in GZIP Compressed Tar Archive (with .TGZ extension) to its default download location.

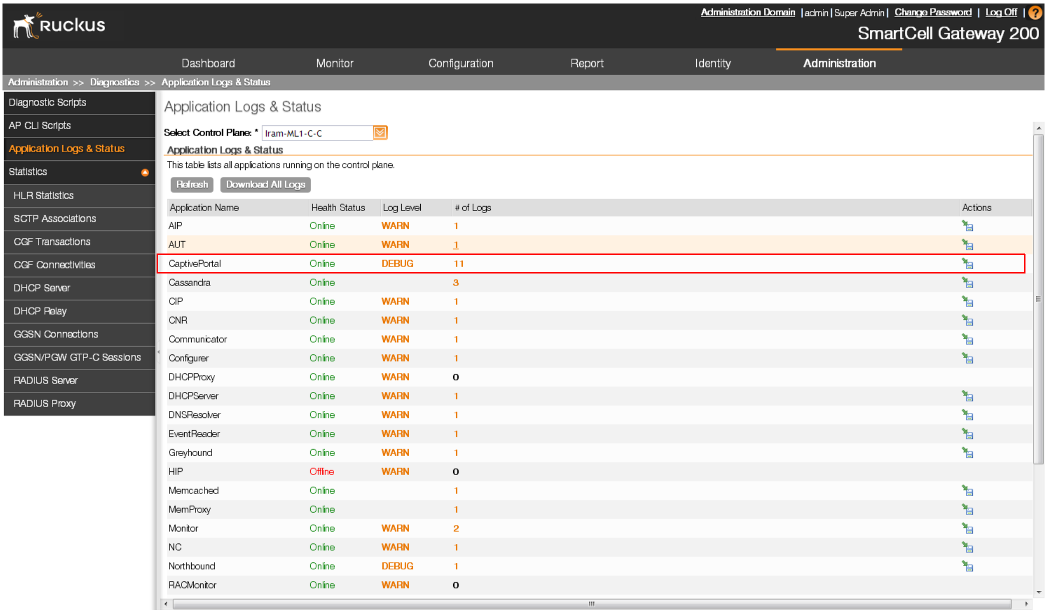
6 Go to your web browser's default download location and verify that the TGZ file was downloaded successfully.

7 Use your preferred compression/decompression program to extract the log files from the TGZ file.

You have completed downloading the Captive Portal logs from the controller.

If you are using the built-in Subscriber Portal, scroll down the table to locate the *SubscriberPortal* application, and then click the 💾 icon that is in the same row as *SubscriberPortal* to download its logs.

Figure 147. Click the save to disk icon to download the Captive Portal logs



Application Logs & Status

Select Control Plane: * Iram-ML1-C-C

Application Logs & Status

This table lists all applications running on the control plane.

Application Name	Health Status	Log Level	# of Logs	Actions
AIP	Online	WARN	1	💾
AUT	Online	WARN	1	💾
CaptivePortal	Online	DEBUG	11	💾
Cassandra	Online		3	💾
CIP	Online	WARN	1	💾
CNR	Online	WARN	1	💾
Communicator	Online	WARN	1	💾
Configurer	Online	WARN	1	💾
DHCPProxy	Online	WARN	0	
DHCPServer	Online	WARN	1	💾
DNSResolver	Online	WARN	1	💾
EventReader	Online	WARN	1	💾
Greyhound	Online	WARN	1	💾
HIP	Offline	WARN	0	
Memcached	Online		1	💾
MemProxy	Online		1	💾
Monitor	Online	WARN	2	💾
NC	Online	WARN	1	💾
Northbound	Online	DEBUG	1	💾
RACMonitor	Online	WARN	0	

Monitoring AP Zones, Access Points, and Wireless Clients

12

In this chapter:

- Monitoring AP Zones
- Monitoring Managed Access Points
- Monitoring Wireless Clients

Monitoring AP Zones

This section provides information on how to monitor and view information about AP zones. Topics covered include:

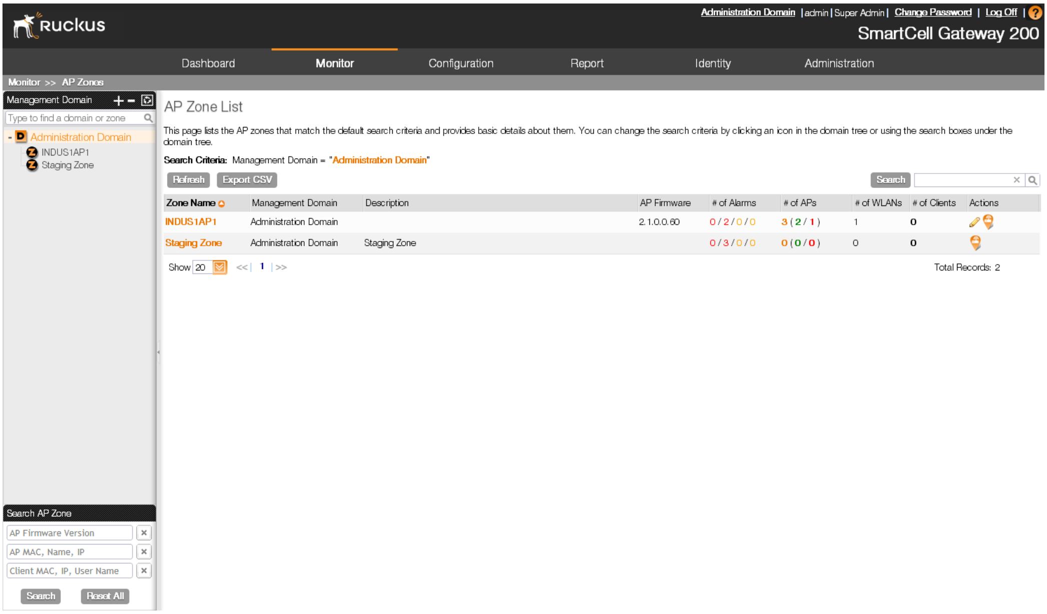
- Viewing a Summary of AP Zones
- Exporting the AP Zone List to CSV
- Viewing the Configuration of an AP Zone
- Viewing All APs That Belong to an AP Zone on Google Maps

Viewing a Summary of AP Zones

Follow these steps to view a summary of existing AP zones.

Go to *Monitor* > *AP Zones*. The *AP Zones in Management Domain* page appears and displays a table of all existing AP zones.

Figure 148. Select Administration Domain in the domain tree to view all existing AP zones



AP Zone List

This page lists the AP zones that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Management Domain = "Administration Domain"

Zone Name	Management Domain	Description	AP Firmware	# of Alarms	# of APs	# of WLANs	# of Clients	Actions
INDUS1AP1	Administration Domain		2.1.0.0.60	0 / 2 / 0 / 0	3 (2 / 1)	1	0	
Staging Zone	Administration Domain	Staging Zone		0 / 3 / 0 / 0	0 (0 / 0)	0	0	

Show 20 << 1 >> Total Records: 2

When you go to the *Monitor > AP Zones* page, the *Administrator Domain* is selected by default in the domain tree, which results in all existing AP zones being displayed in the table.

If you want to view only AP zones that belong to a particular subdomain (denoted by the D icon in the domain tree), click the subdomain icon. The table refreshes and displays only AP Zones that belong to that subdomain.

Table 10 lists the AP zone details that are shown in the table.

Table 10. AP zone details

Column Name	Description
Zone Name	Name of the AP zone. Clicking the AP zone name (link) loads a page that displays detailed information about the zone. See Viewing the Configuration of an AP Zone.
Management Domain	Administration Domain or subdomain name to which the AP zone belongs. Clicking this link displays detailed information about the Administration domain or subdomain.
Description	Brief description of the AP zone

Table 10. AP zone details

Column Name	Description
AP Firmware	Ruckus Wireless firmware version that is installed on the APs that belong to the zone
# of Alarms	Number of alarms that have occurred in the AP zone. The numbers that are separated by a forward slash indicate the number of alarms per alarm type (from left to right order): • Critical alarms (red) • Major alarms (red) • Minor alarms (orange) • Warnings (orange)
# of APs	Number of APs that belong to this zone. The numbers that are separated by a forward slash indicate the total number of APs in the zone (orange), the number of APs that are currently online (green), and the number of APs that are currently offline (red). Clicking the number of APs (link, except when zero) loads a page that displays detailed information about the APs. See Viewing a Summary of Access Points.
# of WLANs	Number of WLAN services that exist in this zone
# of Clients	Number of wireless clients that are currently associated with APs in this zone. Clicking the number of clients (link, except when zero) loads a page that displays detailed information about the wireless clients. See Viewing a Summary of Wireless Clients.
Actions	Icons for actions that you can perform, including: • ✏ – Click to view detailed configuration of this AP zone. • 📍 – Click to view all access points that belong to this AP zone on Google Maps. See Viewing All APs That Belong to an AP Zone on Google Maps. • 📡 – Click to view the mesh topology of this AP zone.

Exporting the AP Zone List to CSV

Follow these steps to export the AP zone list to a CSV file.

1 Go to *Monitor* > *AP Zones*. The AP Zone List page appears.

2 Click the **Export CSV** button in the content area. The following message appears:

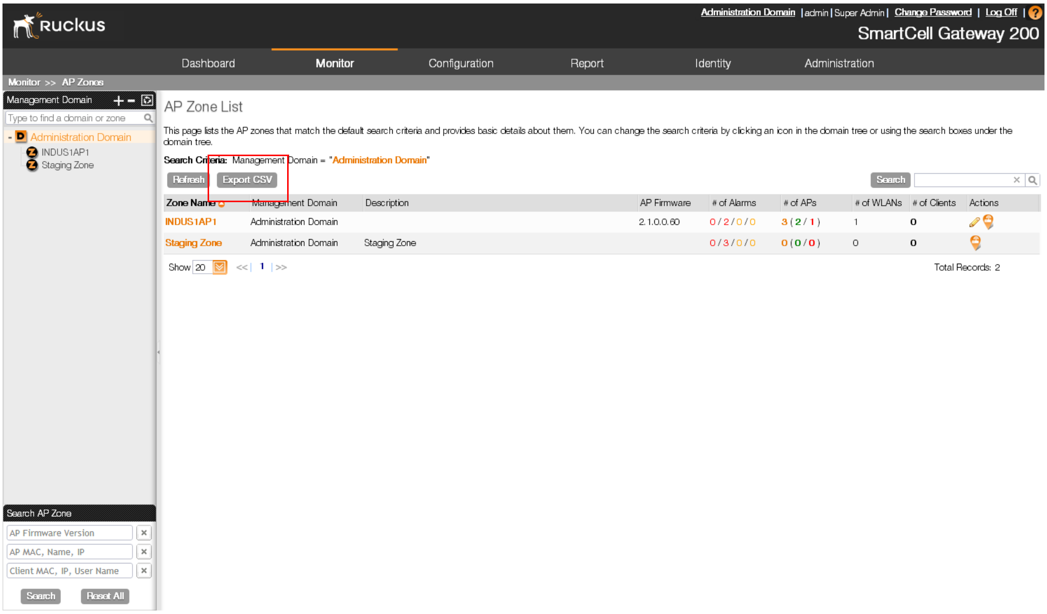
```
Downloading AP Zone Data. Please wait...
```

3 When the message disappears, check the default download folder for your web browser and look for a file named `zone.csv`.

4 Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the AP zone list to CSV.

Figure 149. Click the Export CSV button



AP Zone List

This page lists the AP zones that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Management Domain = "Administration Domain"

Zone Name	Management Domain	Description	AP Firmware	# of Alarms	# of APs	# of WLANs	# of Clients	Actions
INDUS1AP1	Administration Domain		2.1.0.0.60	0 / 2 / 0 / 0	3 (2 / 1)	1	0	
Staging Zone	Administration Domain	Staging Zone		0 / 3 / 0 / 0	0 (0 / 0)	0	0	

Total Records: 2

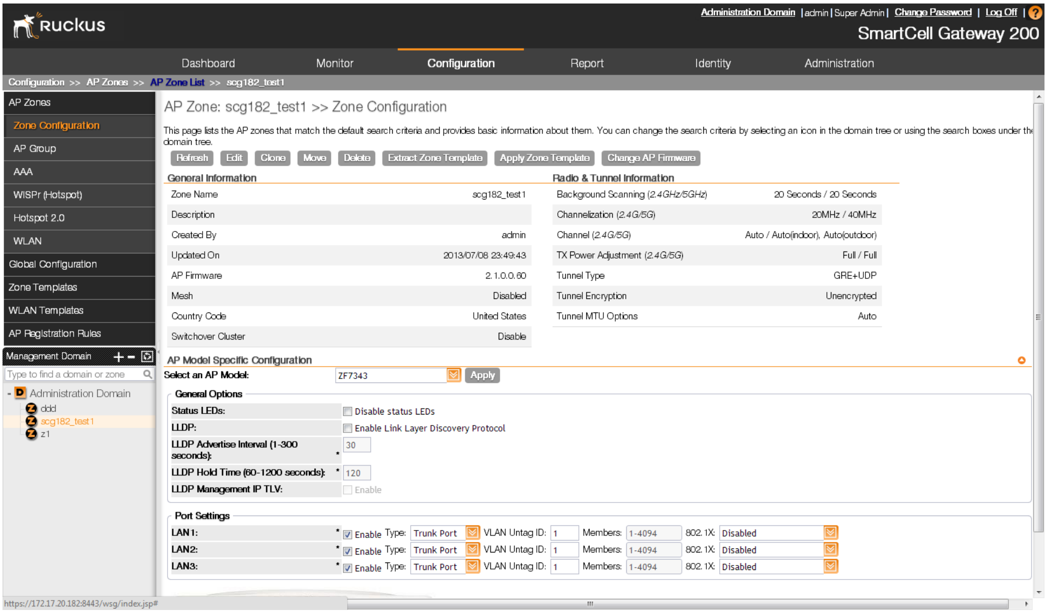
Viewing the Configuration of an AP Zone

Follow these steps to view the configuration of an AP zone.

1. On the *AP Zone List* page, locate the AP zone whose details you want to view.
2. Under the *Actions* column, click the ✎ icon that is in the same row as the AP zone name.

The page refreshes and displays the AP zone configuration details (shown in Figure 150).

Figure 150. Page showing the AP zone configuration details



AP Zone: scg182_test1 >> Zone Configuration

This page lists the AP zones that match the default search criteria and provides basic information about them. You can change the search criteria by selecting an icon in the domain tree or using the search boxes under the domain tree.

General Information

Zone Name	scg182_test1
Description	
Created By	admin
Updated On	2013/07/08 23:49:43
AP Firmware	2.1.0.0.60
Mesh	Disabled
Country Code	United States
Switchover Cluster	Disable

Radio & Tunnel Information

Background Scanning (2.4GHz/5GHz)	20 Seconds / 20 Seconds
Channelization (2.4G/5G)	20MHz / 40MHz
Channel (2.4G/5G)	Auto / Auto(indoor), Auto(outdoor)
TX Power Adjustment (2.4G/5G)	Full / Full
Tunnel Type	GRE+UDP
Tunnel Encryption	Unencrypted
Tunnel MTU Options	Auto

AP Model Specific Configuration

Select an AP Model: ZF7343

General Options

Status LEDs: □ Disable status LEDs

LLDP: □ Enable Link Layer Discovery Protocol

LLDP Advertise Interval (1-300 seconds): * 30

LLDP Hold Time (60-1200 seconds): * 120

LLDP Management IP TLV: □ Enable

Port Settings

LAN1: * ☑ Enable Type: Trunk Port VLAN Untag ID: 1 Members: 1-4094 802.1X: Disabled

LAN2: * ☑ Enable Type: Trunk Port VLAN Untag ID: 1 Members: 1-4094 802.1X: Disabled

LAN3: * ☑ Enable Type: Trunk Port VLAN Untag ID: 1 Members: 1-4094 802.1X: Disabled

Viewing All APs That Belong to an AP Zone on Google Maps

Follow these steps to view all APs that belong to a particular AP zone on Google Maps.

1 On the *AP Zone List* page, locate the AP zone that you want to view.

2 Under the *Actions* column, click the 📍 icon that is in the same row as the AP zone name. The page refreshes and displays the locations of all APs that belong to the zone on Google Maps.

3 To view a summary of details about an AP on the map, click the icon for the AP. A text bubble appears and displays the AP details.

The AP icons are color-coded green, or yellow, or red on Google Maps according to their status. The color codes are explained in Table 11.

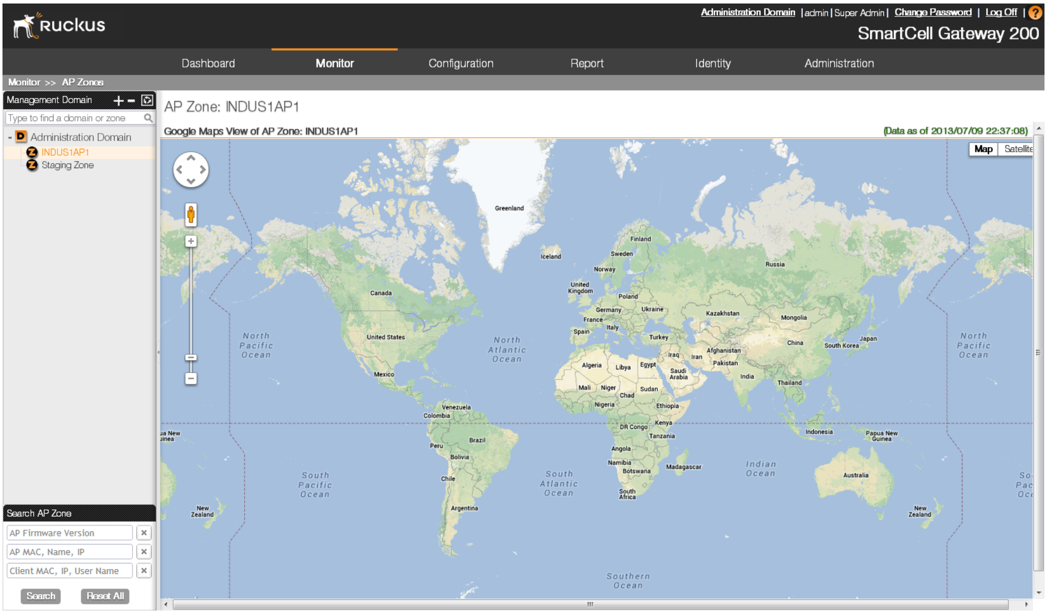
Table 11. Color codes of APs on Google Maps

Icon	Description
🟩	The AP is connected and at least one client is associated with it.
🟨	The AP is connected but it is idle or no client has connected to it.
🟥	The AP is disconnected.
🟩	The eMesh AP is connected and at least one client is associated with it.
🟨	The eMesh AP is connected but it is idle or no client has connected to it.
🟥	The eMesh AP is disconnected.
🟩	The mesh AP is connected and at least one client is associated with it.

Table 11. Color codes of APs on Google Maps

Icon	Description
🟨	The mesh AP is connected but it is idle or no client has connected to it.
🟥	The mesh AP is disconnected.
🟩	The root AP is connected and at least one client is associated with it.
🟨	The root AP is connected but it is idle or no client has connected to it.
🟥	The root AP is disconnected.

Figure 151. Page showing APs that belong to the AP zone on Google Maps



Administration Domain | admin | Super Admin | Change Password | Log Off |
SmartCell Gateway 200

Monitor >> AP Zones

Management Domain
Type to find a domain or zone
- Administration Domain
INDUS1AP1
Staging Zone

AP Zone: INDUS1AP1

Google Maps View of AP Zone: INDUS1AP1

(Data as of 2013/07/09 22:37:08)

Search AP Zone
AP Firmware Version
AP MAC, Name, IP
Client MAC, IP, User Name

Monitoring Managed Access Points

This section provides information on how to monitor and view information about the access points (both Ruckus Wireless access points and 3rd party access points) that you are managing using the controller.

Topics covered include:

- Viewing a Summary of Access Points
- Exporting the Access Point List to CSV
- Viewing the Configuration of an Access Point
- Downloading the Support Log from an Access Point

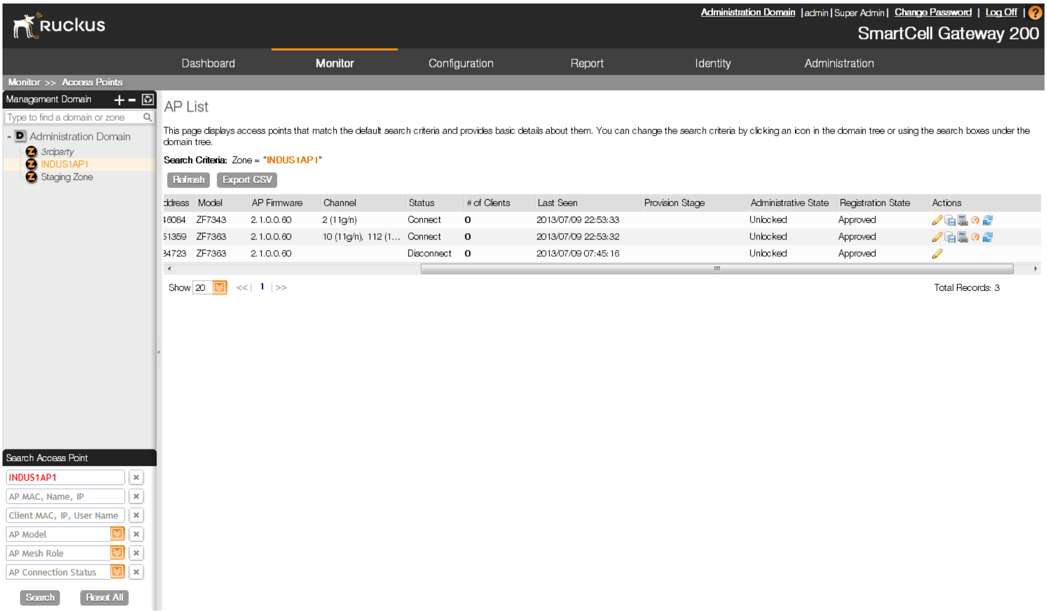
Viewing a Summary of Access Points

Follow these steps to view a summary of existing access points.

Go to *Monitor* > *Access Points*. The *AP List* page appears and displays a table that lists all existing access points in the selected AP zone.

If you are using the controller to manage 3rd party access points, the 3rd party AP zones that you created to managed those access points will also appear in the domain tree. Click the 3rd party AP zone name to view all 3rd party access points that belong to that zone.

Figure 152. Click an AP zone in the tree to view all access points that belong to it



INDUS1AP1

AP List

This page displays access points that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "INDUS1AP1"

ddress	Model	AP Firmware	Channel	Status	# of Clients	Last Seen	Provision Stage	Administrative State	Registration State	Actions
46084	ZF7343	2.1.0.0.60	2 (11g/n)	Connect	0	2013/07/09 22:53:33		Unlocked	Approved	
51359	ZF7363	2.1.0.0.60	10 (11g/n), 112 (1...	Connect	0	2013/07/09 22:53:32		Unlocked	Approved	
34723	ZF7363	2.1.0.0.60		Disconnect	0	2013/07/09 07:45:16		Unlocked	Approved	

Total Records: 3

Table 12 lists the access point details are shown in the table on the *AP List* page. If the selected zone is a 3rd party AP zone, only the following columns are available.

- AP MAC Address
- Zone
- IP Address
- # of Clients

- Last Seen

Table 12. Access point details

Column Name	Description
AP MAC Address	MAC address of the access point. Clicking this link loads a page that displays detailed information about the access point. See Viewing the Configuration of an Access Point.
AP Name	Name assigned to the access point
Zone	Name of the AP zone to which the access point belongs. Clicking the AP zone name (link) loads a page that displays detailed information about the zone. See Viewing the Configuration of an AP Zone.
AP Group	Name of the AP group to which the AP belongs
IP Address	Internal IP address assigned to the access point
External IP Address	If the device is behind a NAT server, this is the IP address and port number that the controller will use to communicate with the device.
Model	Model number of the Ruckus Wireless access point
AP Firmware	Firmware version that is installed on the access point
Mesh Role	Indicates whether mesh networking is enabled on the access point and the mesh role that is assigned to it. Possible values include: • Disabled: Mesh networking is disabled. • Mesh AP • Root AP • eMesh AP
Mesh Mode	If mesh networking is enabled, this indicates the mesh role (Root AP, Mesh AP, or Disable) of the AP
Channel	Indicates the radio channels used by the AP to provide WLAN services
Status	Indicates whether the access point is currently connected (online) or disconnected (offline)
# of Clients	Indicates the number of wireless clients that are currently associated with the access point. Clicking the number of clients (link, except when zero) loads a page that displays detailed information about the wireless clients. See Viewing a Summary of Wireless Clients.

Table 12. Access point details (Continued)

Column Name	Description
Last Seen	Indicates the date and time when the access point last reported to the controller
Provision Stage	
Administrative State	Shows either *Locked* or *Unlocked*.
Registration State	Shows either *Discovery*, *Approved*, or *Rejected*.
Actions	Icons for actions that you can perform, including: • – Click to view detailed configuration of this access point. • – Click to download the support log from this access point. See Downloading the Support Log from an Access Point. • – Click to run network connectivity tests (PING and traceroute) on this access point. • – Click to restart the access point. • – Click to restart the Cable Modem. • – Click to reset the Cable Modem. • – Click to reset the Cable Modem to the factory default. • – Click to download the support log for this cable modem. • – Click to mark this AP as non-critical.

Exporting the Access Point List to CSV

Follow these steps to export the access point list to a CSV file.

1 Go to *Monitor* > *Access Points*.

2 Click the **Export CSV** button in the content area. The following message appears:

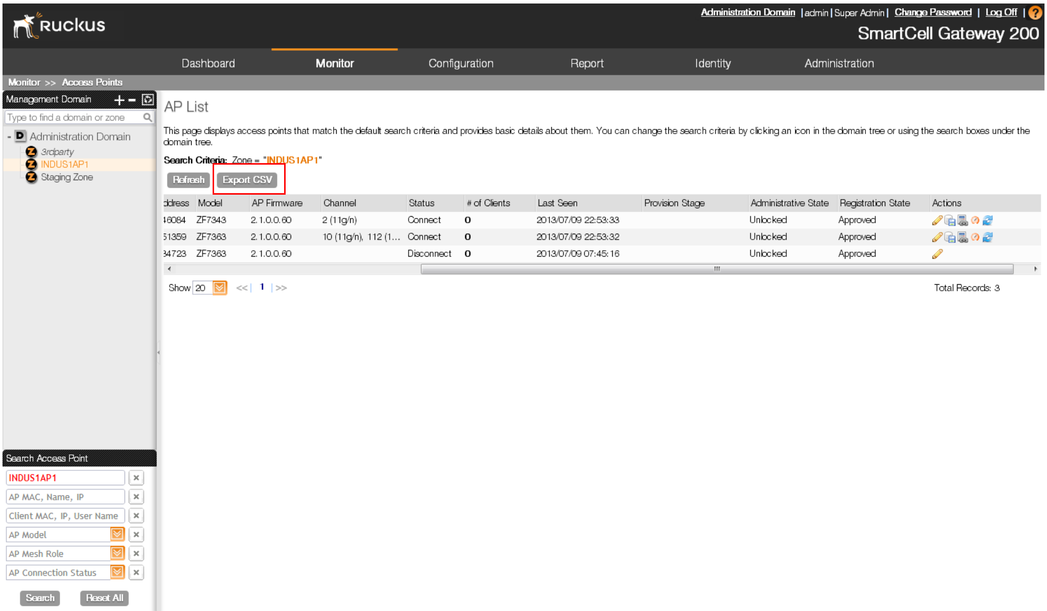
```
Downloading AP Data. Please wait...
```

3 When the message disappears, check the default download folder of your web browser and look for a file named `aps.csv`.

4 Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the access point list to CSV.

Figure 153. Click Export CSV to download the AP list



AP List

This page displays access points that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "INDUS1AP1"

ddress	Model	AP Firmware	Channel	Status	# of Clients	Last Seen	Provision Stage	Administrative State	Registration State	Actions
46084	ZF7343	2.1.0.0.60	2 (11g/n)	Connect	0	2013/07/09 22:53:33		Unlocked	Approved	
51359	ZF7363	2.1.0.0.60	10 (11g/n), 112 (1...	Connect	0	2013/07/09 22:53:32		Unlocked	Approved	
34723	ZF7363	2.1.0.0.60		Disconnect	0	2013/07/09 07:45:16		Unlocked	Approved	

Total Records: 3

INDUS1AP1

Viewing the Configuration of an Access Point

Follow these steps to view the configuration of an access point.

1 Go to *Monitor* > *Access Points*.

2 On the *AP List* page, locate the access point whose details you want to view.

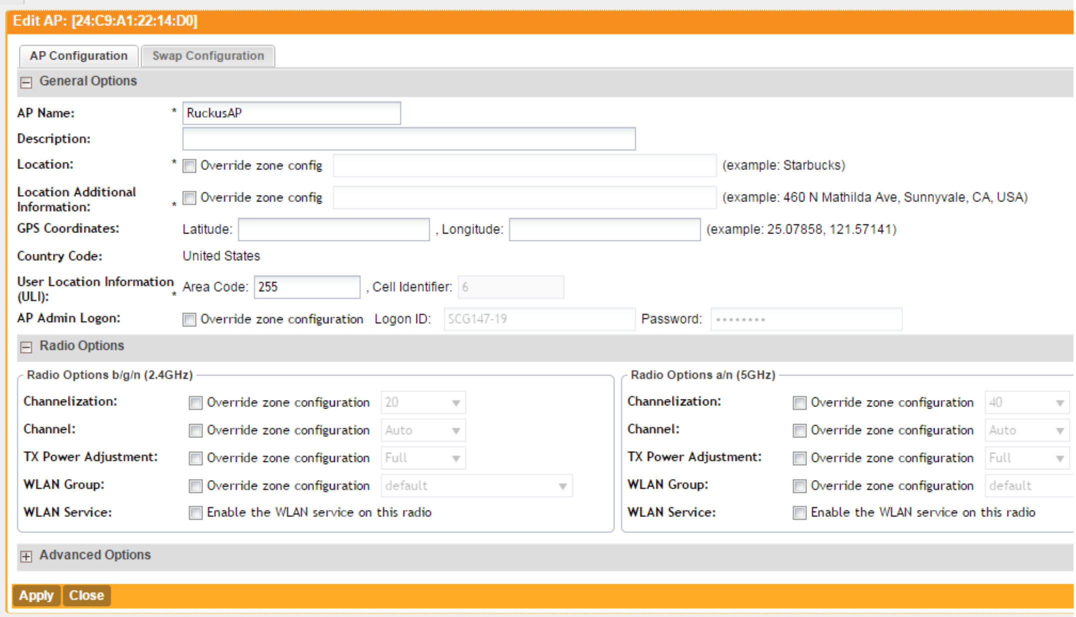
3 Click the AP MAC address to view the AP status information, which includes:

- General AP information
- Status summary
- Radio information
- WLANs
- LAN port status
- Outstanding alarms: For information on how to clear or acknowledge alarms, see Clearing AlarmsClearing Alarms.
- Events

4 To edit the AP configuration details, click **View AP Configuration**.

The page refreshes and displays the AP zone configuration details (shown in Figure 154).

Figure 154. The AP Configuration tab shows the access point’s configuration details



Edit AP: [24:C9:A1:22:14:D0]

AP Configuration | Swap Configuration

⊟ General Options

AP Name: * RuckusAP

Description:

Location: * □ Override zone config (example: Starbucks)

Location Additional Information: * □ Override zone config (example: 460 N Mathilda Ave, Sunnyvale, CA, USA)

GPS Coordinates: Latitude: , Longitude: (example: 25.07858, 121.57141)

Country Code: United States

User Location Information (ULI): * Area Code: 255 , Cell Identifier: 6

AP Admin Logon: □ Override zone configuration Logon ID: SCG147-19 Password: ••••••••

⊟ Radio Options

Radio Options b/g/n (2.4GHz)

Channelization:	□ Override zone configuration	20
Channel:	□ Override zone configuration	Auto
TX Power Adjustment:	□ Override zone configuration	Full
WLAN Group:	□ Override zone configuration	default
WLAN Service:	□ Enable the WLAN service on this radio	

Radio Options a/n (5GHz)

Channelization:	□ Override zone configuration	40
Channel:	□ Override zone configuration	Auto
TX Power Adjustment:	□ Override zone configuration	Full
WLAN Group:	□ Override zone configuration	default
WLAN Service:	□ Enable the WLAN service on this radio	

⊞ Advanced Options

Apply | Close

Downloading the Support Log from an Access Point

If you are experiencing issues with an access point, Ruckus Wireless Support may request you to download the support log from the access point. The support log contains important technical information that may be help Ruckus Wireless Support troubleshoot the issue with the access point.

Follow these steps to download the support log from an access point.

1 Go to *Monitor* > *Access Points*.

2 On the *AP List* page, locate the access point from which you want to download the support log.

3 Under the *Actions* column, click the icon that is in the same row as the MAC address of the access point. The following message appears:

```
Downloading support log file. Please wait...
```

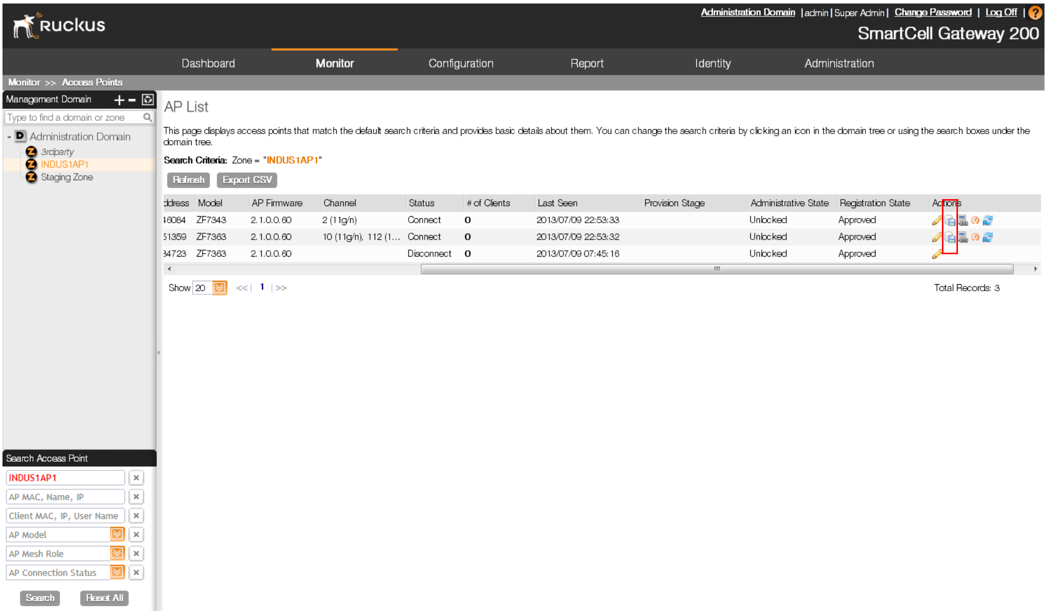
4 When the message disappears, check the default download folder for your web browser and look for a file named `SupportLog_{random-string}.txt`.

5 Use a text editor (for example, Notepad) to view the contents of the text file.

6 Send the support log file to Ruckus Wireless Support, along with your support request.

You have completed downloading the support log from an access point.

Figure 155. Click the icon for downloading the support log



AP List

This page displays access points that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "INDUS1AP1"

ddress	Model	AP Firmware	Channel	Status	# of Clients	Last Seen	Provision Stage	Administrative State	Registration State	Actions
16084	ZF7343	2.1.0.0.60	2 (11g/n)	Connect	0	2013/07/09 22:53:33		Unlocked	Approved	
51359	ZF7363	2.1.0.0.60	10 (11g/n), 112 (1...	Connect	0	2013/07/09 22:53:32		Unlocked	Approved	
34723	ZF7363	2.1.0.0.60		Disconnect	0	2013/07/09 07:45:16		Unlocked	Approved	

Total Records: 3

INDUS1AP1

Restarting an Access Point Remotely

Follow these steps to restart an access point remotely from the web interface.

1 Go to *Monitor* > *Access Points*.

2 On the *AP List* page, locate the access point that you want to restart.

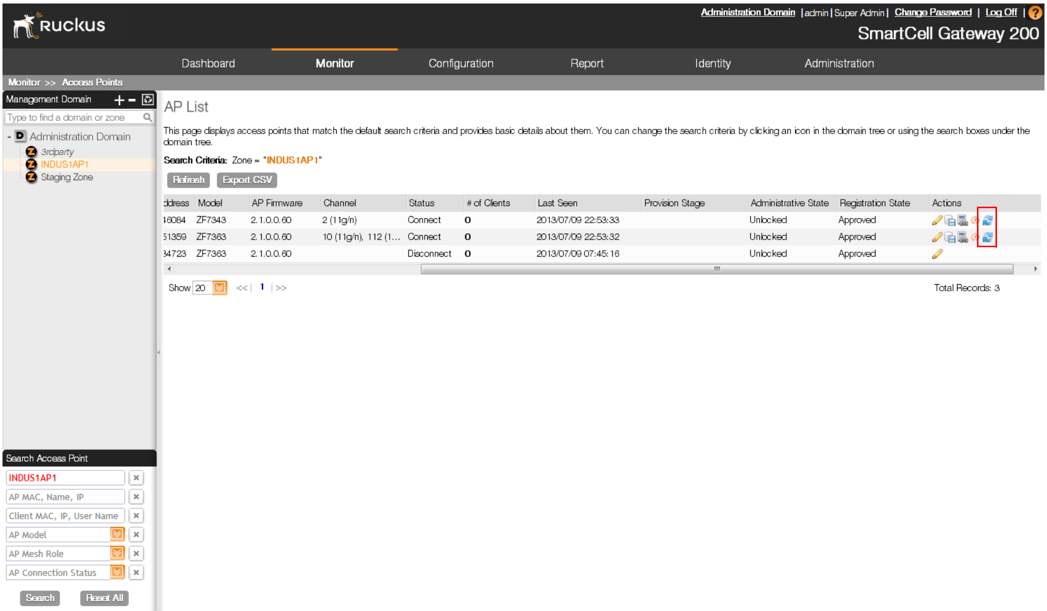
3 Click the 🔄 icon that is in the same row as the MAC address of the access point. The following confirmation message appears:

```
Are you sure you want to restart this AP?
```

4 Click **OK**. The controller sends a restart command to the access point, and then the access point restarts itself.

You have completed restarting an access point remotely.

Figure 156. The restart buttons for restarting access points remotely



AP List

This page displays access points that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "INDUS1AP1"

ddress	Model	AP Firmware	Channel	Status	# of Clients	Last Seen	Provision Stage	Administrative State	Registration State	Actions
46084	ZF7343	2.1.0.0.60	2 (11g/n)	Connect	0	2013/07/09 22:53:33		Unlocked	Approved	
51359	ZF7363	2.1.0.0.60	10 (11g/n), 112 (1...	Connect	0	2013/07/09 22:53:32		Unlocked	Approved	
34723	ZF7363	2.1.0.0.60		Disconnect	0	2013/07/09 07:45:16		Unlocked	Approved	

Total Records: 3

INDUS1AP1

Running Ping and Traceroute on an Access Point

The controller web interface provides two commonly used tools – ping and traceroute – that allow you to diagnose connectivity issues on managed access points.

Follow these steps to run the ping and traceroute on an access point.

1 Go to *Monitor* > *Access Points*.

2 On the *AP List* page, locate the access point on which you want to run the ping or traceroute tool.

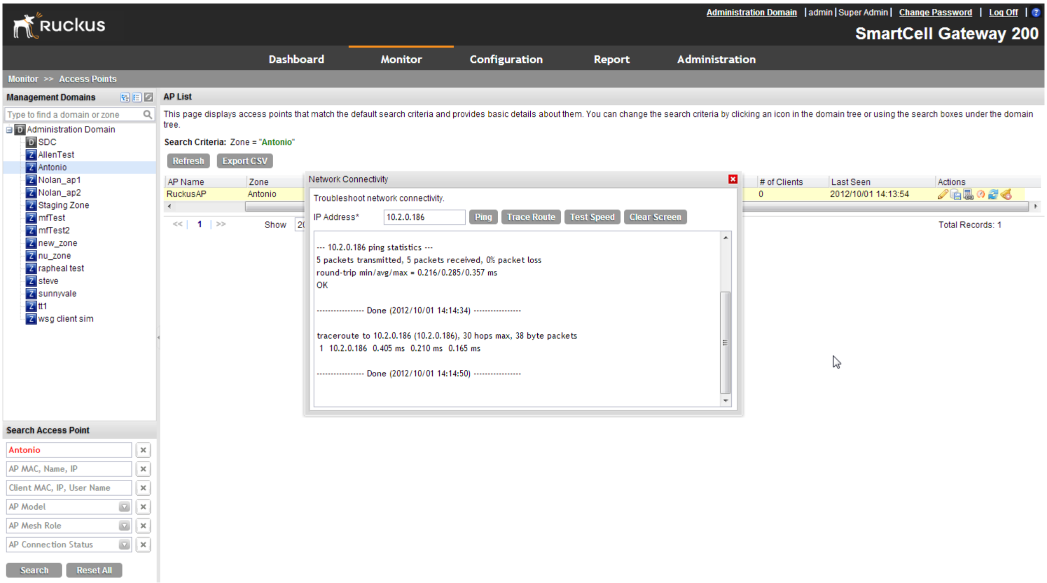
3 Click the 🖥 icon that is in the same row as the MAC address of the access point. The Network Connectivity window appears.

4 In *IP Address*, type an IP address to check whether the access point can connect to it. For example, type `199.238.178.36` if you want to check if the access point can connect to the Ruckus Wireless website.

5 Click either **Ping** or **Trace Route** (depending on which test you want to run). The blank box below is populated with the test results.

You have completed running a ping or traceroute test.

Figure 157. The Network Connectivity window showing both ping and traceroute results



This page displays access points that match the default search criteria and provides basic details about them. You can change the search criteria by clicking an icon in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "Antonio"

AP Name	Zone	# of Clients	Last Seen
RuckusAP	Antonio	0	2012/10/01 14:13:54

Search Access Point: Antonio

Troubleshoot network connectivity.

IP Address* 10.2.0.186

```
--- 10.2.0.186 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.216/0.285/0.357 ms
OK

---------------- Done (2012/10/01 14:14:34) ----------------

traceroute to 10.2.0.186 (10.2.0.186), 30 hops max, 38 byte packets
 1  10.2.0.186  0.405 ms  0.210 ms  0.165 ms

---------------- Done (2012/10/01 14:14:50) ----------------
```

Monitoring Wireless Clients

This section provides information on how to monitor and view information about wireless clients that associate with the managed access points. Topics covered include:

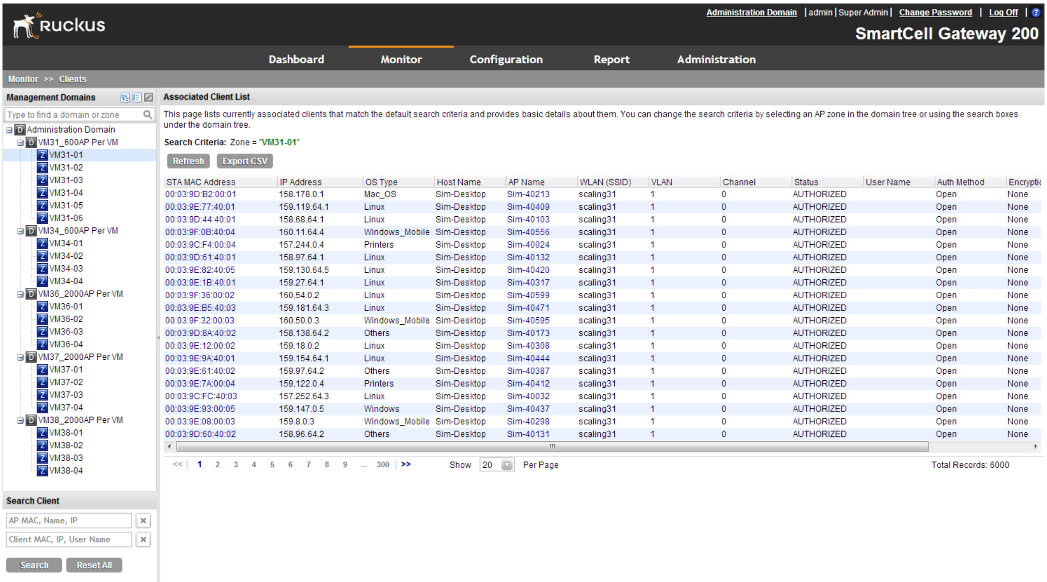
- Viewing a Summary of Wireless Clients
- Exporting the Wireless Client List to CSV
- Viewing Information About a Wireless Client

Viewing a Summary of Wireless Clients

Follow these steps to view a summary of wireless clients that are currently associated with the managed access points.

Go to *Monitor* > *Clients*. The *Associated Clients List* page appears and displays a table that lists all access points that are currently associated with the managed access points.

Figure 158. Select an AP zone in the domain tree to view all wireless clients associated with the APs that belong to the zone



Associated Client List

This page lists currently associated clients that match the default search criteria and provides basic details about them. You can change the search criteria by selecting an AP zone in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "VM31-01"

STA MAC Address	IP Address	OS Type	Host Name	AP Name	WLAN (SSID)	VLAN	Channel	Status	User Name	Auth Method	Encryptio
00:03:9D:B2:00:01	158.178.0.1	Mac_OS	Sim-Desktop	Sim-40213	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:77:40:01	159.119.64.1	Linux	Sim-Desktop	Sim-40409	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:44:40:01	158.68.64.1	Linux	Sim-Desktop	Sim-40103	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:0B:40:04	160.11.64.4	Windows_Mobile	Sim-Desktop	Sim-40556	scaling31	1	0	AUTHORIZED		Open	None
00:03:9C:F4:00:04	157.244.0.4	Printers	Sim-Desktop	Sim-40024	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:61:40:01	158.97.64.1	Linux	Sim-Desktop	Sim-40132	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:82:40:05	159.130.64.5	Linux	Sim-Desktop	Sim-40420	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:1B:40:01	159.27.64.1	Linux	Sim-Desktop	Sim-40317	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:36:00:02	160.54.0.2	Linux	Sim-Desktop	Sim-40599	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:B5:40:03	159.181.64.3	Linux	Sim-Desktop	Sim-40471	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:32:00:03	160.50.0.3	Windows_Mobile	Sim-Desktop	Sim-40595	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:8A:40:02	158.138.64.2	Others	Sim-Desktop	Sim-40173	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:12:00:02	159.18.0.2	Linux	Sim-Desktop	Sim-40308	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:9A:40:01	159.154.64.1	Linux	Sim-Desktop	Sim-40444	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:61:40:02	159.97.64.2	Others	Sim-Desktop	Sim-40387	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:7A:00:04	159.122.0.4	Printers	Sim-Desktop	Sim-40412	scaling31	1	0	AUTHORIZED		Open	None
00:03:9C:FC:40:03	157.252.64.3	Linux	Sim-Desktop	Sim-40032	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:93:00:05	159.147.0.5	Windows	Sim-Desktop	Sim-40437	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:08:00:03	159.8.0.3	Windows_Mobile	Sim-Desktop	Sim-40298	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:60:40:02	158.96.64.2	Others	Sim-Desktop	Sim-40131	scaling31	1	0	AUTHORIZED		Open	None

Total Records: 6000

If you want to view only wireless clients that belong to a particular AP zone (denoted by the Z icon in the domain tree), click the AP zone icon. The table refreshes and displays only the wireless clients that belong to that AP zone.

Table 13 lists the wireless client details that are shown in the table.

Table 13. Wireless client details

Column Name	Description
STA MAC Address	MAC address of the wireless station. Clicking this link loads a page that displays detailed information about the wireless client. See Viewing Information About a Wireless Client.
IP Address	IP address assigned to the wireless client
OS Type	Operating system that the wireless client is using
Host Name	Host name of the wireless client
AP Name	Name assigned to the access point. Clicking this link loads a page that displays detailed information about the access point. See Viewing the Configuration of an Access Point.

Table 13. Wireless client details

Column Name	Description
WLAN (SSID)	Name of the WLAN service or SSID with which the wireless client is associated.
VLAN	VLAN ID assigned to the wireless client
Channel	Radio channel used by the wireless client to access the WLAN service on the access point
Status	Indicates whether the wireless client is authorized or unauthorized to access the WLAN service
User Name	Name of the user logged on to the wireless client
Auth Method	Authentication method used by the access point
Encryption Method	Encryption method used by the access point
Actions	Icons for actions that you can perform, including: • 🗑 – Click to disconnect the wireless client from the access point.

Exporting the Wireless Client List to CSV

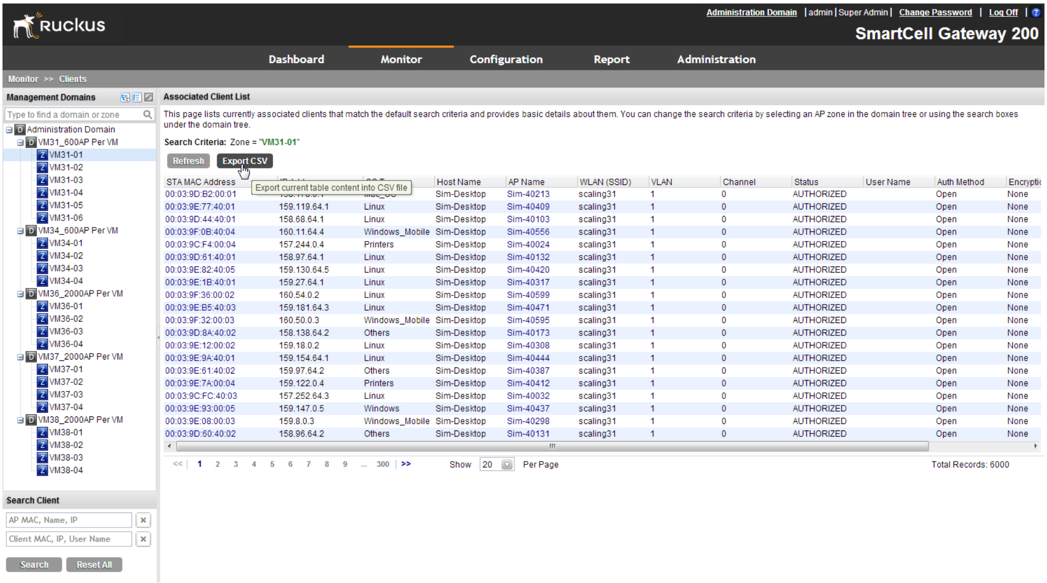
Follow these steps to export the access point list to a CSV file.

1. Go to *Monitor* > *Clients*.
2. Click the **Export CSV** button in the content area. The following message appears:

   Downloading Client Data. Please wait...
3. When the message disappears, check the default download folder for your web browser and look for a file named `clients.csv`.
4. Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the client list to CSV.

Figure 159. A message appears as your browser downloads the CSV file from the controller



This page lists currently associated clients that match the default search criteria and provides basic details about them. You can change the search criteria by selecting an AP zone in the domain tree or using the search boxes under the domain tree.

Search Criteria: Zone = "VM31-01"

STA MAC Address	[illegible]	[illegible]	Host Name	AP Name	WLAN (SSID)	VLAN	Channel	Status	User Name	Auth Method	Encryptic
00:03:9D:B2:00:01	[illegible]	[illegible]	Sim-Desktop	Sim-40213	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:77:40:01	159.119.64.1	Linux	Sim-Desktop	Sim-40409	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:44:40:01	158.68.64.1	Linux	Sim-Desktop	Sim-40103	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:0B:40:04	160.11.64.4	Windows_Mobile	Sim-Desktop	Sim-40556	scaling31	1	0	AUTHORIZED		Open	None
00:03:9C:F4:00:04	157.244.0.4	Printers	Sim-Desktop	Sim-40024	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:61:40:01	158.97.64.1	Linux	Sim-Desktop	Sim-40132	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:82:40:05	159.130.64.5	Linux	Sim-Desktop	Sim-40420	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:1B:40:01	159.27.64.1	Linux	Sim-Desktop	Sim-40317	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:36:00:02	160.54.0.2	Linux	Sim-Desktop	Sim-40599	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:B5:40:03	159.181.64.3	Linux	Sim-Desktop	Sim-40471	scaling31	1	0	AUTHORIZED		Open	None
00:03:9F:32:00:03	160.50.0.3	Windows_Mobile	Sim-Desktop	Sim-40595	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:8A:40:02	158.138.64.2	Others	Sim-Desktop	Sim-40173	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:12:00:02	159.18.0.2	Linux	Sim-Desktop	Sim-40308	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:9A:40:01	159.154.64.1	Linux	Sim-Desktop	Sim-40444	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:61:40:02	159.97.64.2	Others	Sim-Desktop	Sim-40387	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:7A:00:04	159.122.0.4	Printers	Sim-Desktop	Sim-40412	scaling31	1	0	AUTHORIZED		Open	None
00:03:9C:FC:40:03	157.252.64.3	Linux	Sim-Desktop	Sim-40032	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:93:00:05	159.147.0.5	Windows	Sim-Desktop	Sim-40437	scaling31	1	0	AUTHORIZED		Open	None
00:03:9E:08:00:03	159.8.0.3	Windows_Mobile	Sim-Desktop	Sim-40298	scaling31	1	0	AUTHORIZED		Open	None
00:03:9D:60:40:02	158.96.64.2	Others	Sim-Desktop	Sim-40131	scaling31	1	0	AUTHORIZED		Open	None

Total Records: 6000

Viewing Information About a Wireless Client

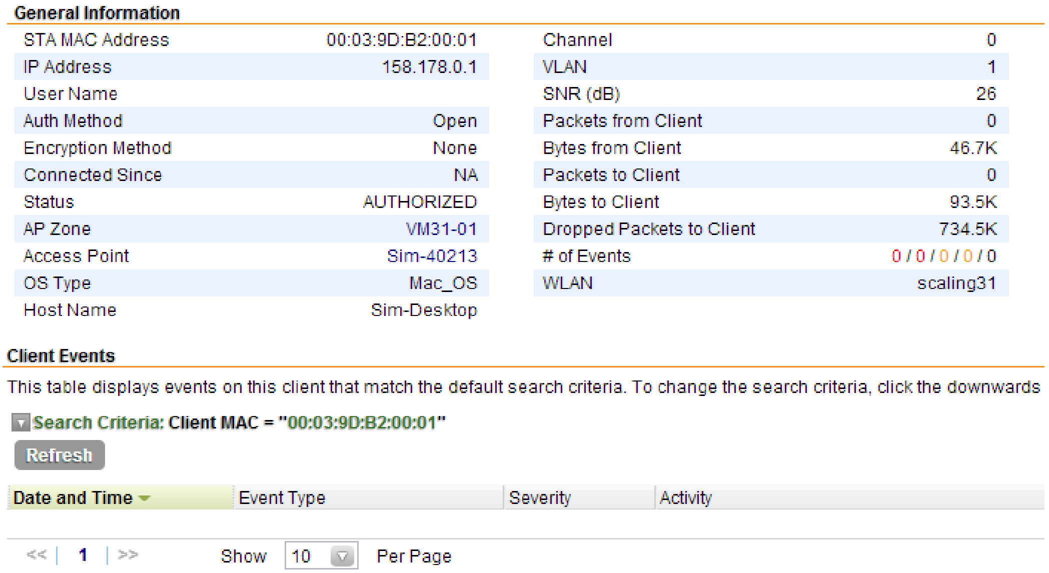
Follow these steps to view information about a wireless client.

1 One the *Clients List* page, locate the wireless client whose details you want to view.

2 Under the *STA MAC Address* column, click the MAC address of the wireless client.

The page refreshes and displays general information about the wireless client, including its MAC address, IP address, authentication method, encryption method, connection details, operating system, and traffic statistics, among others. Recent connectivity events that occurred on the wireless client are displayed in the *Events* section at the bottom of the page.

Figure 160. Page showing the wireless client information



General Information

STA MAC Address	00:03:9D:B2:00:01	Channel	0
IP Address	158.178.0.1	VLAN	1
User Name		SNR (dB)	26
Auth Method	Open	Packets from Client	0
Encryption Method	None	Bytes from Client	46.7K
Connected Since	NA	Packets to Client	0
Status	AUTHORIZED	Bytes to Client	93.5K
AP Zone	VM31-01	Dropped Packets to Client	734.5K
Access Point	Sim-40213	# of Events	0 / 0 / 0 / 0 / 0
OS Type	Mac_OS	WLAN	scaling31
Host Name	Sim-Desktop		

Client Events

This table displays events on this client that match the default search criteria. To change the search criteria, click the downwards

Search Criteria: Client MAC = "00:03:9D:B2:00:01"

Refresh

Date and Time	Event Type	Severity	Activity

Measuring Wireless Network Throughput with SpeedFlex

SpeedFlex is a wireless performance tool included in the controller that you can use to measure the downlink throughput between the controller and an AP. When performing a site survey, you can use SpeedFlex to help find the optimum location for APs on the network with respect to user locations.

NOTE: SpeedFlex is unable to measure the throughput between two devices if those two devices are not on the same VLAN or the same subnet.

Follow these steps to measure the throughput of an AP from the controller web interface.

1. Find out the MAC address of the AP that you want to use for this test procedure.
2. Log on to the controller web interface.
3. If you want to test AP throughput, click *Monitor* > *Access Points*.
4. On the list of APs, look for the MAC address of the AP that you want to test, and then click (SpeedFlex icon) that is in the same row. The SpeedFlex Wireless Performance Test interface loads, showing a speedometer and the IP address of the AP that you want to test.

5 In *Protocol*, select **UDP**.

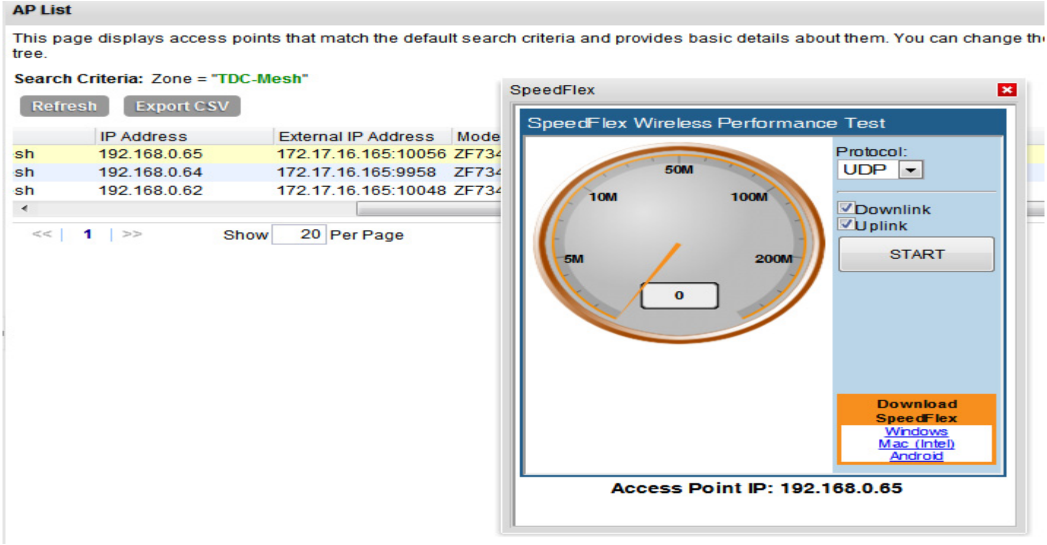
If you are testing AP throughput, you have the option to test both *Downlink* and *Uplink* throughput. Both options are selected by default. If you only want to test one of them, clear the check box for the option that you do not want to test.

6 Click the **Start** button.

A progress bar appears below the speedometer as SpeedFlex generates traffic to measure the downlink or uplink throughput. One throughput test typically runs for 10-30 seconds. If you are testing AP throughput and you selected both the *Downlink* and *Uplink* options, both tests should take about one minute to complete.

When the tests are complete, the results appear below the **Start** button. Information that is shown includes the downlink/uplink throughput and the packet loss percentage during the tests.

Figure 161. The SpeedFlex page



AP List

This page displays access points that match the default search criteria and provides basic details about them. You can change th tree.

Search Criteria: Zone = "TDC-Mesh"

	IP Address	External IP Address	Mode
sh	192.168.0.65	172.17.16.165:10056	ZF734
sh	192.168.0.64	172.17.16.165:9958	ZF734
sh	192.168.0.62	172.17.16.165:10048	ZF734

Show 20 Per Page

SpeedFlex

SpeedFlex Wireless Performance Test

Protocol: UDP

☑ Downlink
☑ Uplink

Access Point IP: 192.168.0.65

Monitoring the System, Alarms, Events, and Administrator Activity 13

In this chapter:

- Monitoring the Controller System
- Viewing Alarms
- Viewing Events
- Viewing Administrator Activity

Monitoring the Controller System

This section provides information on how to view information about the status of the controller system, including its cluster planes and cluster events. It also describes how to use the chassis view and to start the cluster monitor.

Topics covered include:

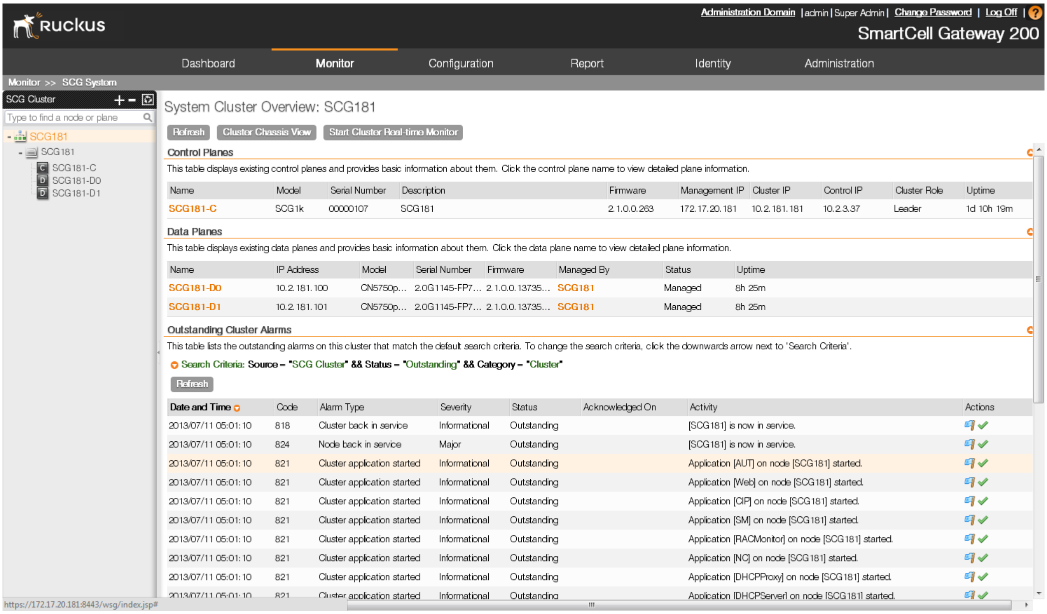
- Viewing the System Cluster Overview
- Displaying the Chassis View of Cluster Nodes
- Starting the Cluster Real-time Monitor

Viewing the System Cluster Overview

The system cluster overview provides summary information about the control planes and data planes on the controller appliance, any outstanding cluster alarms, and the latest cluster events.

To view the system cluster overview, go to *Monitor* > *System*. The *System Cluster Overview* page appears, as shown in Figure 162.

Figure 162. The System Cluster Overview page



System Cluster Overview: SCG181

Control Planes

This table displays existing control planes and provides basic information about them. Click the control plane name to view detailed plane information.

Name	Model	Serial Number	Description	Firmware	Management IP	Cluster IP	Control IP	Cluster Role	Uptime
SCG181-C	SCG1k	00000107	SCG181	2.1.0.0.263	172.17.20.181	10.2.181.181	10.2.3.37	Leader	1d 10h 19m

Data Planes

This table displays existing data planes and provides basic information about them. Click the data plane name to view detailed plane information.

Name	IP Address	Model	Serial Number	Firmware	Managed By	Status	Uptime
SCG181-D0	10.2.181.100	CN5750p...	2.0G1145-FP7...	2.1.0.0.13735...	SCG181	Managed	8h 25m
SCG181-D1	10.2.181.101	CN5750p...	2.0G1145-FP7...	2.1.0.0.13735...	SCG181	Managed	8h 25m

Outstanding Cluster Alarms

This table lists the outstanding alarms on this cluster that match the default search criteria. To change the search criteria, click the downwards arrow next to 'Search Criteria'.

Search Criteria: Source = "SCG Cluster" && Status = "Outstanding" && Category = "Cluster"

Date and Time	Code	Alarm Type	Severity	Status	Acknowledged On	Activity	Actions
2013/07/11 05:01:10	818	Cluster back in service	Informational	Outstanding		[SCG181] is now in service.	✓
2013/07/11 05:01:10	824	Node back in service	Major	Outstanding		[SCG181] is now in service.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [AUT] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [Web] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [CIP] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [SM] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [RACMonitor] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [NC] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [DHCPProxy] on node [SCG181] started.	✓
2013/07/11 05:01:10	821	Cluster application started	Informational	Outstanding		Application [DHCPServer] on node [SCG181] started.	✓

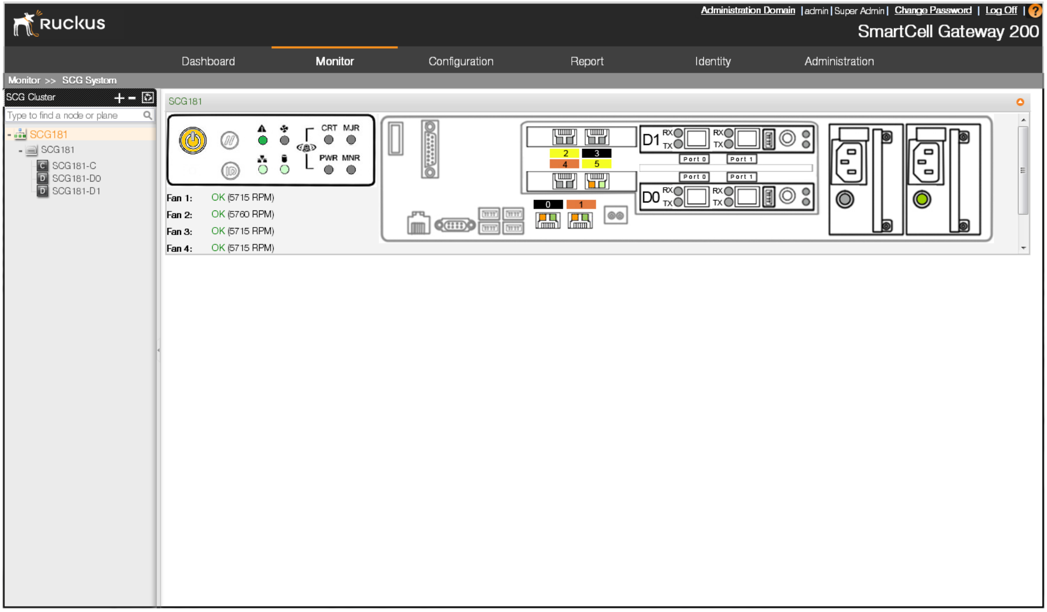
Displaying the Chassis View of Cluster Nodes

The chassis view provides a graphical representation of the control panel (on the front panel of the controller) and the rear panel of each controller node, including their LEDs. Use the LEDs to check the status of the ports and power supplies on the controller. Fan status is also displayed on the chassis view.

To view the chassis of the cluster node, click **Cluster Chassis View** on the *System Cluster Overview* page.

NOTE: The information on the chassis view updates automatically every 30 seconds. This polling frequency is not configurable.

Figure 163. The chassis view page displaying the chassis of all nodes in the cluster



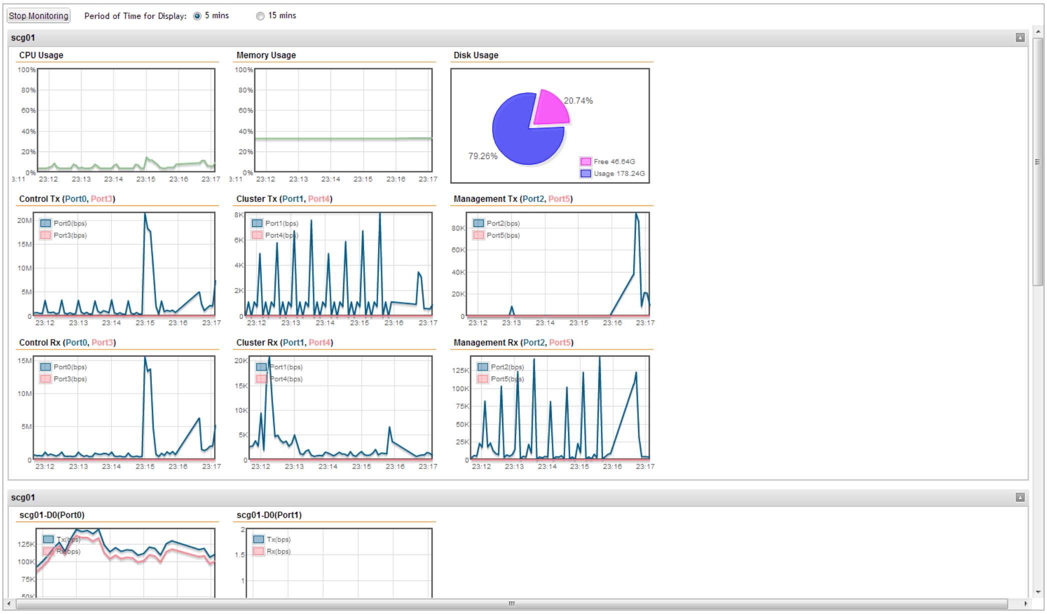
Fan 1: OK (5715 RPM)
Fan 2: OK (5760 RPM)
Fan 3: OK (5715 RPM)
Fan 4: OK (5715 RPM)

Starting the Cluster Real-time Monitor

The Cluster Real-time Monitor displays graphs and charts of the controller system resources. Use this monitor to understand how system resources on the cluster nodes are being used.

To start the cluster real-time monitor, click **Start Cluster Real-time Monitor** on the *System Cluster Overview* page. A new browser page or tab appears (depending on your browser settings), and then the *Cluster Real-time Monitor* page appears.

Figure 164. The Cluster Real-time Monitor page



The resource graphs and charts that are shown on the Cluster Real-time Monitor page include:

- CPU Usage
- Memory Usage
- Disk Usage
- Control Tx (Port0, Port 3)
- Cluster Tx (Port1, Port 4)
- Management Tx (Port2, Port 5)
- Control Rx (Port0, Port 3)
- Cluster Rx (Port1, Port 4)
- Management Rx (Port2, Port5)

To stop the Cluster Real-time Monitor, click the **Stop Monitoring** button on the upper-left part of the page.

Monitoring Rogue Access Points

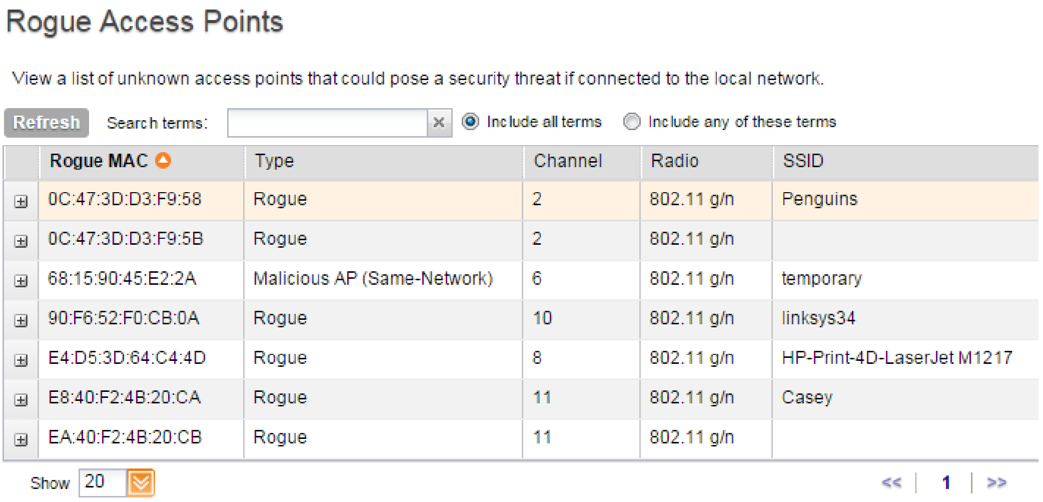
“Rogue” (or unauthorized) APs pose problems for a wireless network in terms of airtime contention, as well as security. Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to other LAN resources. This would potentially allow even more unauthorized users to access your corporate LAN - posing a security risk. Rogue APs also interfere with nearby Ruckus Wireless APs, thus degrading overall wireless network coverage and performance.

The controller’s rogue AP detection options include identifying the presence of a rogue AP, categorizing it as either a known neighbor AP or as a malicious rogue.

If you enabled rogue AP detection when you create an AP zone (see Creating an AP Zone), click *Monitor > Rogue Access Points*. The *Rogue Access Points* page displays all rogue APs that the controller has detected on the network, including the following information:

- *Rogue MAC*: MAC address of the rogue AP.
- *Type*: Type of rogue AP detected. Possible values include:
  - *Rogue*: A normal rogue AP. This rogue AP has not yet been categorized as malicious or non-malicious.
  - *Malicious AP (SSID-spoof)*: A malicious rogue AP that uses the same SSID as a controller-managed AP (also known as an Evil-twin AP).
  - *Malicious AP (MAC-spoof)*: A malicious rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by the controller.
  - *Malicious AP (Same-Network)*: A malicious rogue AP that is connected to the same wired network.
  - *Malicious AP (User-Blocked)*: A rogue AP that has been marked as malicious by the user.
- *Channel*: Radio channel used by the rogue AP.
- *Radio*: WLAN standards with which the rogue AP complies.
- *SSID*: WLAN name that the rogue AP is broadcasting.
- *Encryption*: Indicates whether the wireless signal is encrypted or not.
- *Last Detected*: Date and time when the rogue AP was last detected by the controller.

Figure 165. View a list of rogue APs on the Monitor > Rogue Access Points page



Rogue Access Points

View a list of unknown access points that could pose a security threat if connected to the local network.

Rogue MAC	Type	Channel	Radio	SSID
0C:47:3D:D3:F9:58	Rogue	2	802.11 g/n	Penguins
0C:47:3D:D3:F9:5B	Rogue	2	802.11 g/n	
68:15:90:45:E2:2A	Malicious AP (Same-Network)	6	802.11 g/n	temporary
90:F6:52:F0:CB:0A	Rogue	10	802.11 g/n	linksys34
E4:D5:3D:64:C4:4D	Rogue	8	802.11 g/n	HP-Print-4D-LaserJet M1217
E8:40:F2:4B:20:CA	Rogue	11	802.11 g/n	Casey
EA:40:F2:4B:20:CB	Rogue	11	802.11 g/n	

Viewing Alarms

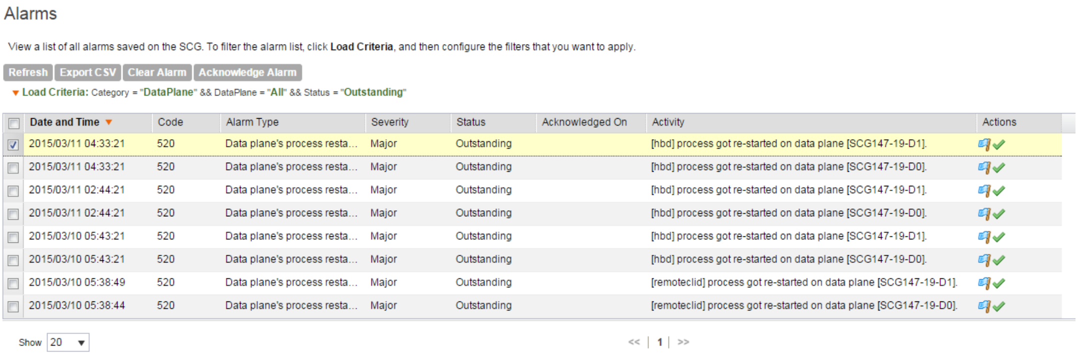
Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and the controller system (control plane and data plane).

Follow these steps to view recent alarms that have been generated.

Go to *Monitor* > *Alarms*. The *Alarms* page displays the 20 most recent alarms.

NOTE: By default, the Alarms page displays up to 20 event entries per page. You can change the number of alarms to display per page by selecting a number in **Show**. Options range from 10 to 250 entries per page. Alternatively, you can click the >> (next) link to display the next 20 alarms on another page.

Figure 166. The Alarm page, displaying alarms in the “DataPlane” category



Alarms

View a list of all alarms saved on the SCG. To filter the alarm list, click **Load Criteria**, and then configure the filters that you want to apply.

▾ **Load Criteria:** Category = "**DataPlane**" && DataPlane = "**All**" && Status = "**Outstanding**"

□	**Date and Time** ▾	Code	Alarm Type	Severity	Status	Acknowledged On	Activity	Actions
☑	2015/03/11 04:33:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D1].	✓
□	2015/03/11 04:33:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D0].	✓
□	2015/03/11 02:44:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D1].	✓
□	2015/03/11 02:44:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D0].	✓
□	2015/03/10 05:43:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D1].	✓
□	2015/03/10 05:43:21	520	Data plane's process resta...	Major	Outstanding		[hbd] process got re-started on data plane [SCG147-19-D0].	✓
□	2015/03/10 05:38:49	520	Data plane's process resta...	Major	Outstanding		[remoteclid] process got re-started on data plane [SCG147-19-D1].	✓
□	2015/03/10 05:38:44	520	Data plane's process resta...	Major	Outstanding		[remoteclid] process got re-started on data plane [SCG147-19-D0].	✓

Table 14 lists the alarm details that are displayed on the *Alarms* page.

Table 14. Alarm details

Column Name	**Description**
Date and Time	Date and time when the alarm was triggered
Code	Alarm code (see the *Alarm and Reference Guide* for your controller platform for more information)
Alarm Type	Type of alarm event that occurred (for example, AP reset to factory settings)
Severity	Severity level assigned to the alarm. Possible values include (from most severe to least severe): • Critical • Major • Minor • Warning
Status	Indicates whether the alarm has already been cleared or still outstanding
Acknowledged On	Date and time when you or another administrator acknowledge the alarm
Activity	Displays additional details about the alarm, including (if available) the specific access point, control plane, or data plane that triggered the alarm

Table 14. Alarm details (Continued)

Column Name	Description
Actions	Icons for actions that you can perform, including: • 🚩 – Click this to take ownership of issue. Acknowledging an alarm lets other administrators know that someone is already looking into the issue. • ✓ – Click this to clear the alarm. You may clear an alarm to let other administrators know that you have already resolved the issue. When you click this icon, a text box appears where you can enter comments or notes about the resolved issue. Click **Clear** when done.

Using the Search Criteria Section

By default, the controller displays alarms triggered on all access points (using `All APs` as the search criteria) when you load the *Alarms* page. If you want to filter the alarms that are displayed on the page (for example, you want to display only critical alarms), use the *Search Criteria* section.

Follow these steps to filter alarms.

1. Click the gray down button next to *Search Criteria* to expand the section.
2. In the *Source* filter, select source from which to search alarms. Options include **Access Point** and **System**.
3. Click the ➕ icon to add another filter. Available filters include (in the order that they appear when you click the ➕ icon):
   - Severity
   - Triggered Time
   - Status
   - Acknowledge Time
   - Type

NOTE: You do not need to use all these filters. To remove a filter from the search criteria, click the ➖ icon next to the filter that you want to delete.

4. Define the filters that you want to use. For example, if you want to view all critical alarms on all access points, select **Access Point** in *Source*, and then select **Critical** in *Severity*.

5 Click **Search**. The page refreshes and displays the alarms that match the search criteria that you defined.

Exporting the Alarm List to CSV

Follow these steps to export the alarm list to a CSV file.

1 Go to *Monitor* > *Alarms*.

2 Click the **Export CSV** button in the content area. The following message appears:

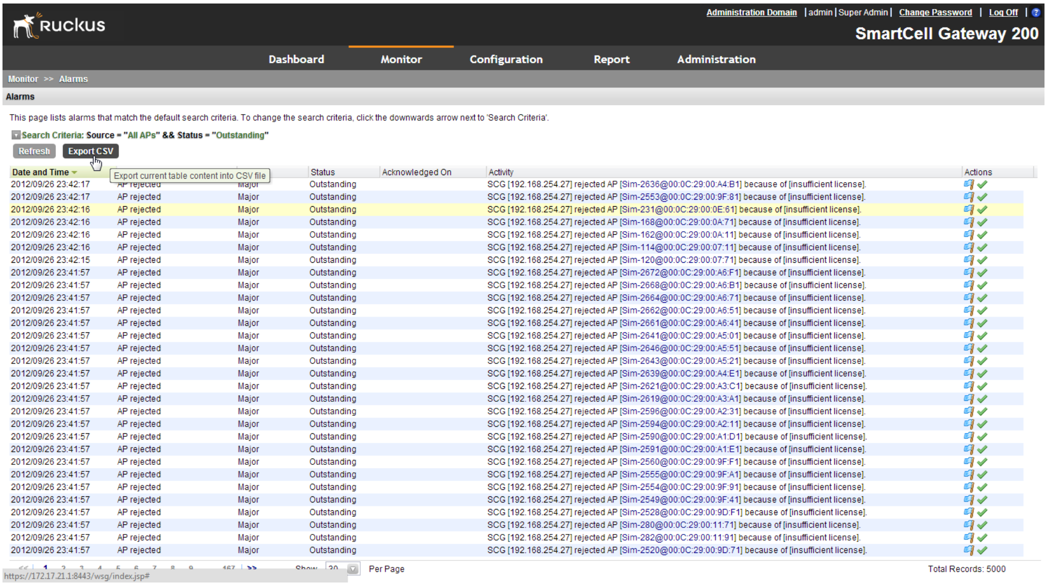
```
Downloading Alarms Data. Please wait...
```

3 When the message disappears, check the default download folder of your web browser and look for a file named `alarms.csv`.

4 Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the alarm list to CSV.

Figure 167. A message appears as your browser downloads the CSV file from the controller


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Administration
Monitor >> Alarms
Alarms
Refresh
Export CSV
Export current table content into CSV file

This page lists alarms that match the default search criteria. To change the search criteria, click the downwards arrow next to 'Search Criteria'.

Search Criteria: Source = "All APs" && Status = "Outstanding"

Date and Time			Status	Acknowledged On	Activity	Actions
2012/09/26 23:42:17	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2636@00:0C:29:00:A4:B1] because of [insufficient license].	✓
2012/09/26 23:42:17	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2553@00:0C:29:00:9F:81] because of [insufficient license].	✓
2012/09/26 23:42:16	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-231@00:0C:29:00:0E:61] because of [insufficient license].	✓
2012/09/26 23:42:16	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-168@00:0C:29:00:0A:71] because of [insufficient license].	✓
2012/09/26 23:42:16	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-162@00:0C:29:00:0A:11] because of [insufficient license].	✓
2012/09/26 23:42:16	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-114@00:0C:29:00:07:11] because of [insufficient license].	✓
2012/09/26 23:42:15	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-120@00:0C:29:00:07:71] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2672@00:0C:29:00:A6:F1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2668@00:0C:29:00:A6:B1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2664@00:0C:29:00:A6:71] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2662@00:0C:29:00:A6:51] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2661@00:0C:29:00:A6:41] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2641@00:0C:29:00:A5:01] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2646@00:0C:29:00:A5:51] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2643@00:0C:29:00:A5:21] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2639@00:0C:29:00:A4:E1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2621@00:0C:29:00:A3:C1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2619@00:0C:29:00:A3:A1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2596@00:0C:29:00:A2:31] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2594@00:0C:29:00:A2:11] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2590@00:0C:29:00:A1:D1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2591@00:0C:29:00:A1:E1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2560@00:0C:29:00:9F:F1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2555@00:0C:29:00:9F:A1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2554@00:0C:29:00:9F:91] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2549@00:0C:29:00:9F:41] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2528@00:0C:29:00:9D:F1] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-280@00:0C:29:00:11:71] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-282@00:0C:29:00:11:91] because of [insufficient license].	✓
2012/09/26 23:41:57	AP rejected	Major	Outstanding		SCG [192.168.254.27] rejected AP [Sim-2520@00:0C:29:00:9D:71] because of [insufficient license].	✓

<< 1 2 3 4 5 6 7 8 9 ... 167 >> Show 30 Per Page Total Records: 5000

https://172.17.21.1:8443/wsg/index.jsp#

Clearing Alarms

Clearing an alarm removes the alarm from the list but keeps it on the controller's database. Do one of the following to clear a single alarm or multiple alarms.

- To clear a single alarm, select the check box that is in the same row as the alarm, and then click **Clear Alarm**. Alternatively, click the ✓ icon.
- To clear multiple alarms, select the check boxes for the alarm that you want to clear, and then click **Clear Alarm**.
- To clear all alarms that are currently displayed on the page, click the check box before the *Date and Time* column, and then click **Clear Alarm**.

Acknowledging Alarms

Acknowledging an alarm lets other administrators know that you have examined the alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it. Do one of the following to acknowledge a single alarm or multiple alarms.

- To acknowledge a single alarm, select the check box that is in the same row as the alarm, and then click **Acknowledge Alarm**. Alternatively, click the 🏳 icon.
- To acknowledge multiple alarms, select the check boxes for the alarm that you want to clear, and then click **Acknowledge Alarm**.
- To acknowledge all alarms that are currently displayed on the page, click the check box before the *Date and Time* column, and then click **Acknowledge Alarm**.

Viewing Events

An event is an occurrence or the detection of certain conditions in and around the network. An AP being rebooted, an AP changing its IP address, and a user updating an AP's configuration are all examples of events.

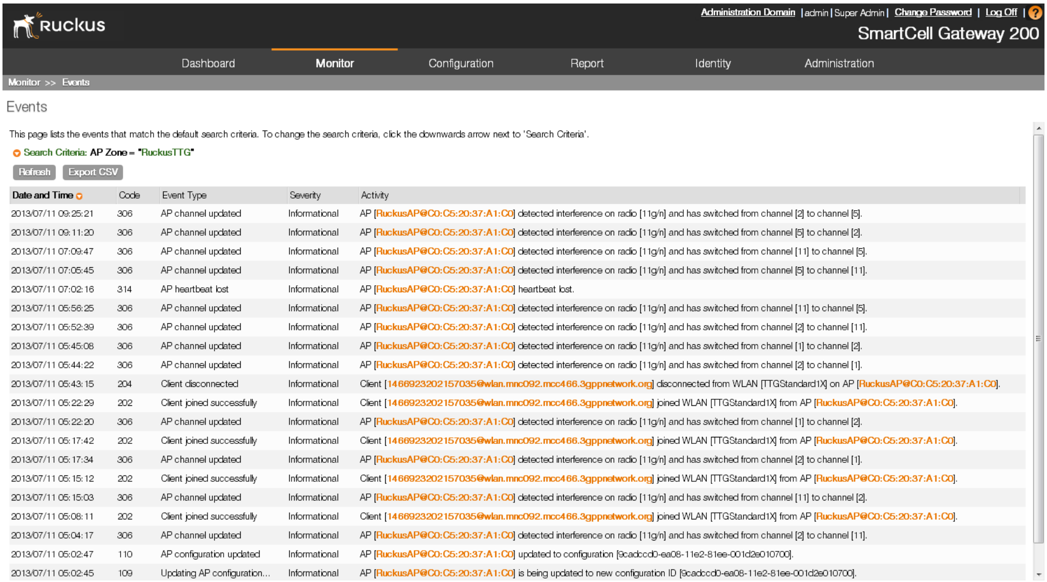
NOTE: Events that require your attention are called *alarms*. For information on alarms, refer to Viewing Alarms.

Follow these steps to view recent events that have been detected by the controller.

Go to *Monitor* > *Events*. The *Events* page appears and displays the 20 most recent events that have occurred.

NOTE: By default, the *Events* page displays up to 20 event entries per page. You can change the number of events to display per page by selecting a number in **Show**. Options range from 10 to 250 entries per page. Alternatively, you can click the **>>** (next) link to display the next 20 events on another page.

Figure 168. The Events page lists the most recent events that have occurred



This page lists the events that match the default search criteria. To change the search criteria, click the downwards arrow next to 'Search Criteria'.

Search Criteria: AP Zone = "RuckusTTG"

Date and Time	Code	Event Type	Severity	Activity
2013/07/11 09:25:21	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [5].
2013/07/11 09:11:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [2].
2013/07/11 07:09:47	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 07:05:45	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [11].
2013/07/11 07:02:16	314	AP heartbeat lost	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] heartbeat lost.
2013/07/11 05:56:25	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 05:52:39	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [11].
2013/07/11 05:45:08	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:44:22	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:43:15	204	Client disconnected	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] disconnected from WLAN [TTGStandard1X] on AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:29	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:17:42	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:17:34	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:15:12	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:15:03	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [2].
2013/07/11 05:08:11	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:04:17	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [11].
2013/07/11 05:02:47	110	AP configuration updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] updated to configuration [9cadccd0-ea08-11e2-81ee-001d2e010700].
2013/07/11 05:02:45	109	Updating AP configuration...	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] is being updated to new configuration ID [9cadccd0-ea08-11e2-81ee-001d2e010700].

Table 15 lists the event details that are displayed on the *Events* page.

Table 15. Event details

Column Name	Description
Date and Time	Date and time when the event occurred
Code	Event code (see the *Alarm and Event Reference Guide* for your controller platform more information)
Event Type	Type of event that occurred (for example, AP configuration updated)

Table 15. Event details

Column Name	Description
Severity	Severity level assigned to the event. Possible values include (from most severe to least severe): • Critical • Major • Minor • Warning
Activity	Displays additional details about the event, including (if available) the specific access point, control plane, or data plane that triggered the event

Using the Search Criteria Section

By default, the controller displays all events that occurred on the first access point that is listed in the domain tree. If you want to filter the events that are displayed on the page (for example, you want to display events on a client or the controller system), use the *Search Criteria* section.

Follow these steps to filter events.

1 Click the gray down button next to *Search Criteria* to expand the section.

2 In the *Source* filter, select source from which to search alarms. Options include **Access Point**, **Client**, and **SCG System**.

3 Click the + icon to add another filter. Available filters include (in the order that they appear when you click the + icon):

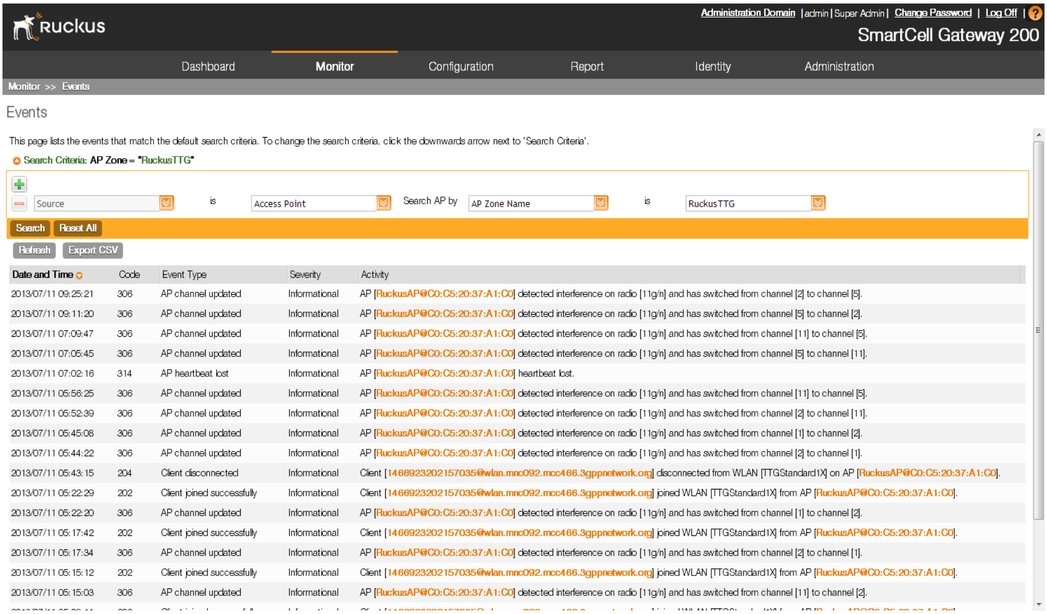
- Date and Time
- Severity
- Type

NOTE: You do not need to use all these filters. To remove a filter from the search criteria, click the − icon next to the filter that you want to delete. The search criteria are case-sensitive.

4 Define the filters that you want to use. For example, if you want to view all critical events on all access points, select **Access Point** in *Source*, leave *Search Plane by* blank, and then select **Critical** in *Severity*.

5 Click **Search**. The page refreshes and displays the events that match the search criteria that you defined.

Figure 169. Define the filters that you want to use to search for events



Events

This page lists the events that match the default search criteria. To change the search criteria, click the downwards arrow next to 'Search Criteria'.

Search Criteria: AP Zone = "RuckusTTG"

Source is Access Point Search AP by AP Zone Name is RuckusTTG

Date and Time	Code	Event Type	Severity	Activity
2013/07/11 09:25:21	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [5].
2013/07/11 09:11:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [2].
2013/07/11 07:09:47	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 07:05:45	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [11].
2013/07/11 07:02:16	314	AP heartbeat lost	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] heartbeat lost.
2013/07/11 05:56:25	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 05:52:39	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [11].
2013/07/11 05:45:08	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:44:22	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:43:15	204	Client disconnected	Informational	Client [14669232021157035@wlan.mnc092.mcc466.3gppnetwork.org] disconnected from WLAN [TTGStandard1X] on AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:29	202	Client joined successfully	Informational	Client [14669232021157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:17:42	202	Client joined successfully	Informational	Client [14669232021157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:17:34	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:15:12	202	Client joined successfully	Informational	Client [14669232021157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:15:03	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [2].

Exporting the Event List to CSV

Follow these steps to export the event list to a CSV file.

1 Go to *Monitor* > *Events*.

2 Click the **Export CSV** button in the content area. The following message appears:

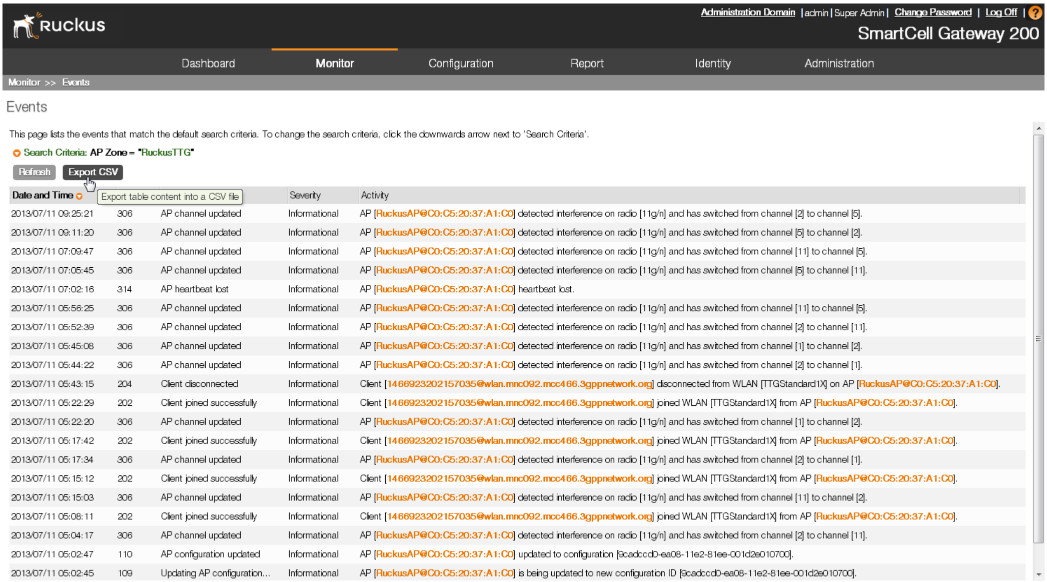
```
Downloading Events Data. Please wait...
```

3 When the message disappears, check the default download folder of your web browser and look for a file named `events.csv`.

4 Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the event list to CSV.

Figure 170. Exporting the event list to CSV



Events

This page lists the events that match the default search criteria. To change the search criteria, click the downwards arrow next to 'Search Criteria'.

Search Criteria: AP Zone = "RuckusTTG"

Date and Time			Severity	Activity
2013/07/11 09:25:21	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [5].
2013/07/11 09:11:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [2].
2013/07/11 07:09:47	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 07:05:45	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [5] to channel [11].
2013/07/11 07:02:16	314	AP heartbeat lost	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] heartbeat lost.
2013/07/11 05:56:25	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [5].
2013/07/11 05:52:39	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [11].
2013/07/11 05:45:08	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:44:22	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:43:15	204	Client disconnected	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] disconnected from WLAN [TTGStandard1X] on AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:29	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:22:20	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [1] to channel [2].
2013/07/11 05:17:42	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:17:34	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [1].
2013/07/11 05:15:12	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:15:03	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [11] to channel [2].
2013/07/11 05:08:11	202	Client joined successfully	Informational	Client [1466923202157035@wlan.mnc092.mcc466.3gppnetwork.org] joined WLAN [TTGStandard1X] from AP [RuckusAP@C0:C5:20:37:A1:C0].
2013/07/11 05:04:17	306	AP channel updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] detected interference on radio [11g/n] and has switched from channel [2] to channel [11].
2013/07/11 05:02:47	110	AP configuration updated	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] updated to configuration [9cadccd0-ea08-11e2-81ee-001d2e010700].
2013/07/11 05:02:45	109	Updating AP configuration...	Informational	AP [RuckusAP@C0:C5:20:37:A1:C0] is being updated to new configuration ID [9cadccd0-ea08-11e2-81ee-001d2e010700].

Viewing Administrator Activity

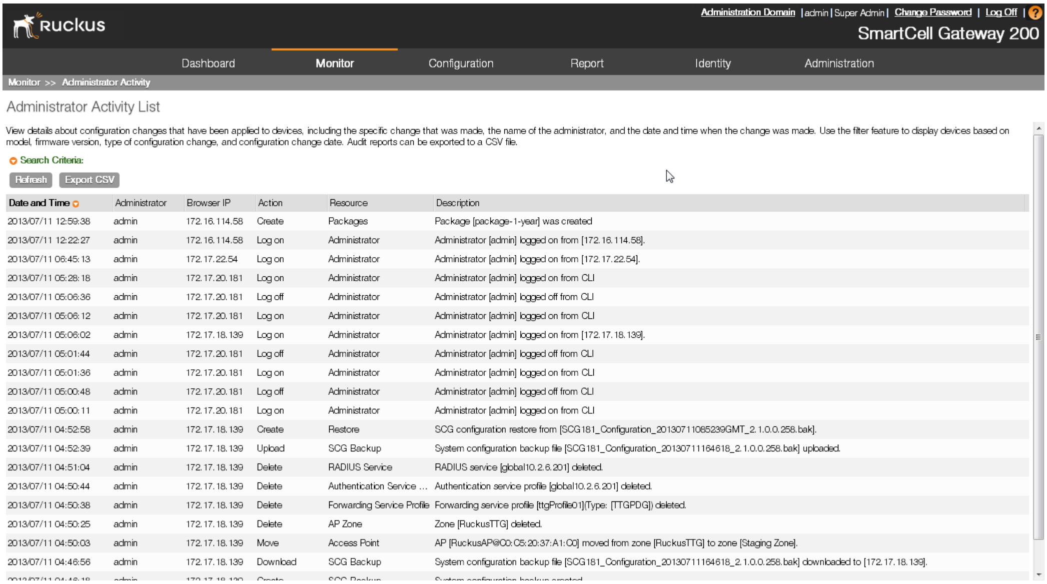
The controller keeps a record of all actions and configuration changes that administrators perform on the server. This feature enables you and other administrators in the organization to determine what changes were made to the controller and by whom.

Follow these steps to view a record of actions that were performed by administrators.

Go to *Monitor > Administrator Activity.* The *Administrator Activity List* page displays the 20 most recent administrator actions.

NOTE: By default, the *Administrator Activity List* page displays up to 20 administrator actions per page. You can change the number of administrator actions to display per page by selecting a number in **Show**. Options range from 10 to 250 entries per page. Alternatively, you can click the **>>** (next) link to display the next 20 administrator actions on another page.

Figure 171. The Administrator Activity List displays the most recent administrator actions


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Monitor >> Administrator Activity

Administrator Activity List

View details about configuration changes that have been applied to devices, including the specific change that was made, the name of the administrator, and the date and time when the change was made. Use the filter feature to display devices based on model, firmware version, type of configuration change, and configuration change date. Audit reports can be exported to a CSV file.

Date and Time	Administrator	Browser IP	Action	Resource	Description
2013/07/11 12:59:38	admin	172.16.114.58	Create	Packages	Package [package-1-year] was created
2013/07/11 12:22:27	admin	172.16.114.58	Log on	Administrator	Administrator [admin] logged on from [172.16.114.58].
2013/07/11 06:45:13	admin	172.17.22.54	Log on	Administrator	Administrator [admin] logged on from [172.17.22.54].
2013/07/11 05:28:18	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:36	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:06:12	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:02	admin	172.17.18.139	Log on	Administrator	Administrator [admin] logged on from [172.17.18.139].
2013/07/11 05:01:44	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:01:36	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:00:48	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:00:11	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 04:52:58	admin	172.17.18.139	Create	Restore	SCG configuration restore from [SCG181_Configuration_20130711085239GMT_2.1.0.0.258.bak].
2013/07/11 04:52:39	admin	172.17.18.139	Upload	SCG Backup	System configuration backup file [SCG181_Configuration_20130711164618_2.1.0.0.258.bak] uploaded.
2013/07/11 04:51:04	admin	172.17.18.139	Delete	RADIUS Service	RADIUS service [global10.2.6.201] deleted.
2013/07/11 04:50:44	admin	172.17.18.139	Delete	Authentication Service ...	Authentication service profile [global10.2.6.201] deleted.
2013/07/11 04:50:38	admin	172.17.18.139	Delete	Forwarding Service Profile	Forwarding service profile [ttgProfile01](Type: [TTGPDG]) deleted.
2013/07/11 04:50:25	admin	172.17.18.139	Delete	AP Zone	Zone [RuckusTTG] deleted.
2013/07/11 04:50:03	admin	172.17.18.139	Move	Access Point	AP [RuckusAP@C0:C5:20:37:A1:C0] moved from zone [RuckusTTG] to zone [Staging Zone].
2013/07/11 04:46:56	admin	172.17.18.139	Download	SCG Backup	System configuration backup file [SCG181_Configuration_20130711164618_2.1.0.0.258.bak] downloaded to [172.17.18.139].
2013/07/11 04:46:18	admin	172.17.18.139	Create	SCG Backup	System configuration backup created

Table 16 lists the administrator activity details that are displayed on the *Administrator Activity List* page.

Table 16. Administrator activity details

Column Name	Description
Date and Time	Date and time when the alarm was triggered
Administrator	Name of the administrator who performed the action
Browser IP	IP address of the browser that the administrator used to log on to the controller
Action	Action performed by the administrator
Resource	Target of the action performed by the administrator. For example, if the action is `Create` and the object is `hotspot portal`, this means that the administrator created a new hotspot portal.
Description	Displays additional details about the action. For example, if the administrator created a new hotspot portal, this column may show the following: `Hotspot [company_hotspot] created`

Using the Search Criteria Section

By default, the controller displays the 30 most recent administrator actions when you load the *Administrator Activity List* page. If you want to filter the actions that are displayed on the page (for example, you want to display only actions that were performed by a particular admin), use the *Search Criteria* section.

1 Click the gray down button next to *Search Criteria* to expand the section.

2 Click the ➕ icon to add a filter. Available filters include (in the order that they appear when you click the ➕ icon:

- Date/Time
- Administrator
- Browser IP
- Object

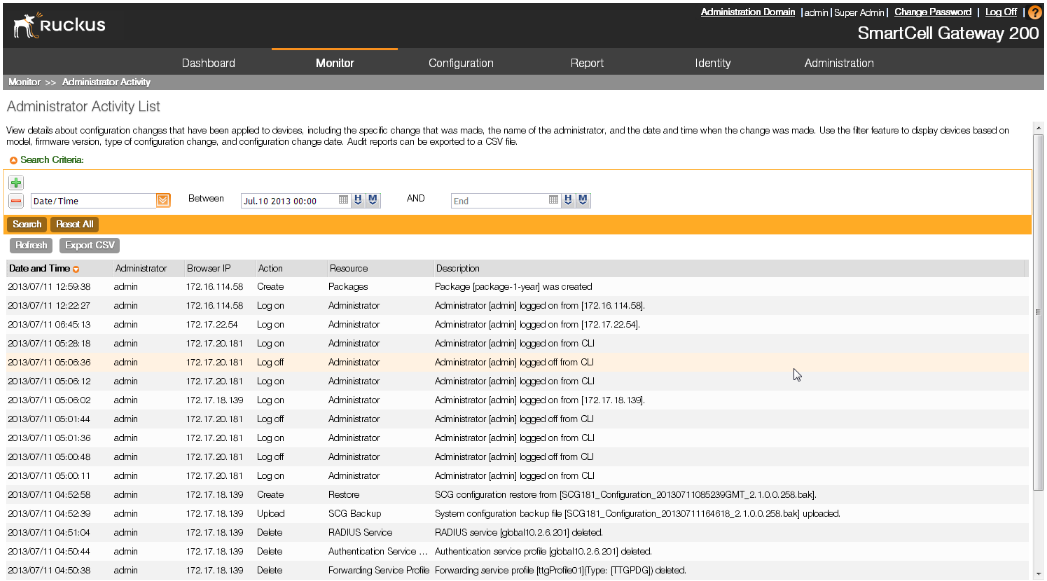
NOTE: You do not need to use all these filters. To remove a filter from the search criteria, click the ➖ icon next to the filter that you want to delete. The search criteria are case-sensitive.

---

3 Define the filters that you want to use. For example, if you want to view all actions performed by a particular administrator for the past month, define the date and time, and then select the name of the administrator in *Administrator*.

4 Click **Search**. The page refreshes and displays the administrator actions that match the search criteria that you defined.

Figure 172. Define the filters that you want to use to search for administrator actions


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Monitor >> Administrator Activity

Administrator Activity List

View details about configuration changes that have been applied to devices, including the specific change that was made, the name of the administrator, and the date and time when the change was made. Use the filter feature to display devices based on model, firmware version, type of configuration change, and configuration change date. Audit reports can be exported to a CSV file.

Search Criteria:

Date/Time Between Jul.10 2013 00:00 AND End

Date and Time	Administrator	Browser IP	Action	Resource	Description
2013/07/11 12:59:38	admin	172.16.114.58	Create	Packages	Package [package-1-year] was created
2013/07/11 12:22:27	admin	172.16.114.58	Log on	Administrator	Administrator [admin] logged on from [172.16.114.58].
2013/07/11 06:45:13	admin	172.17.22.54	Log on	Administrator	Administrator [admin] logged on from [172.17.22.54].
2013/07/11 05:28:18	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:36	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:06:12	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:02	admin	172.17.18.139	Log on	Administrator	Administrator [admin] logged on from [172.17.18.139].
2013/07/11 05:01:44	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:01:36	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:00:48	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:00:11	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 04:52:58	admin	172.17.18.139	Create	Restore	SCG configuration restore from [SCG181_Configuration_20130711085239GMT_2.1.0.0.258.bak].
2013/07/11 04:52:39	admin	172.17.18.139	Upload	SCG Backup	System configuration backup file [SCG181_Configuration_20130711164618_2.1.0.0.258.bak] uploaded.
2013/07/11 04:51:04	admin	172.17.18.139	Delete	RADIUS Service	RADIUS service [global10.2.6.201] deleted.
2013/07/11 04:50:44	admin	172.17.18.139	Delete	Authentication Service ...	Authentication service profile [global10.2.6.201] deleted.
2013/07/11 04:50:38	admin	172.17.18.139	Delete	Forwarding Service Profile	Forwarding service profile [ttgProfile01](Type: [TTGPDG]) deleted.

Exporting the Administrator Activity List to CSV

Follow these steps to export the administrator activity list to a CSV file.

1 Go to *Monitor > Administrator Activity.*

2 Click the **Export CSV** button in the content area. The following message appears:

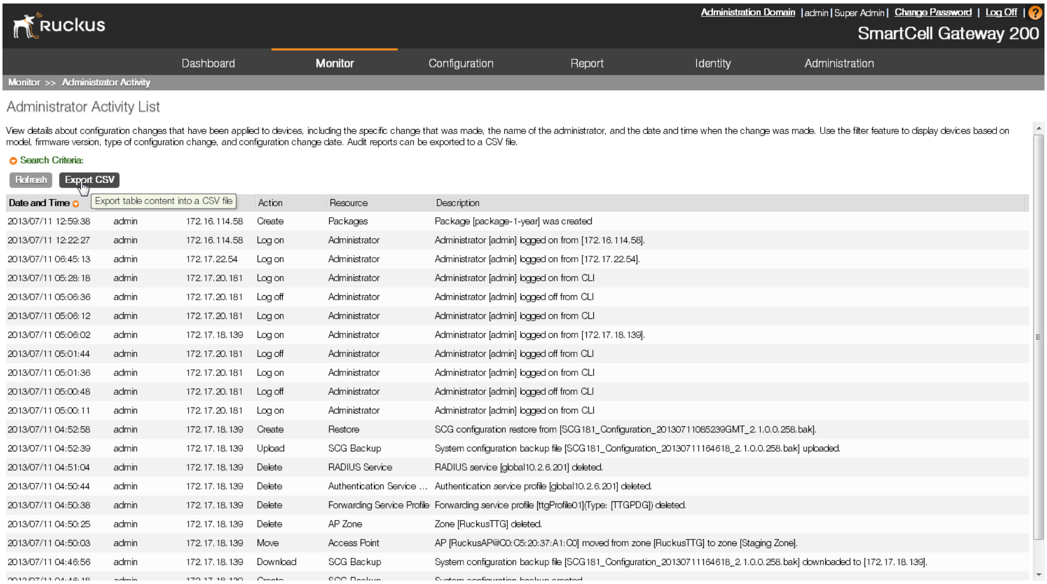
```
Downloading Administrator Data. Please wait...
```

3 When the message disappears, check the default download folder for your web browser and look for a file named `auditLog.csv`.

4 Use a spreadsheet application (for example, Microsoft™ Excel™) to view the contents of the CSV file.

You have completed exporting the administrator activity list to CSV.

Figure 173. Click the Export CSV button to download a CSV file that contains details of administrator activity


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Monitor >> Administrator Activity

Administrator Activity List

View details about configuration changes that have been applied to devices, including the specific change that was made, the name of the administrator, and the date and time when the change was made. Use the filter feature to display devices based on model, firmware version, type of configuration change, and configuration change date. Audit reports can be exported to a CSV file.

Date and Time			Action	Resource	Description
2013/07/11 12:59:38	admin	172.16.114.58	Create	Packages	Package [package-1-year] was created
2013/07/11 12:22:27	admin	172.16.114.58	Log on	Administrator	Administrator [admin] logged on from [172.16.114.58].
2013/07/11 06:45:13	admin	172.17.22.54	Log on	Administrator	Administrator [admin] logged on from [172.17.22.54].
2013/07/11 05:28:18	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:36	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:06:12	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:06:02	admin	172.17.18.139	Log on	Administrator	Administrator [admin] logged on from [172.17.18.139].
2013/07/11 05:01:44	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:01:36	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 05:00:48	admin	172.17.20.181	Log off	Administrator	Administrator [admin] logged off from CLI
2013/07/11 05:00:11	admin	172.17.20.181	Log on	Administrator	Administrator [admin] logged on from CLI
2013/07/11 04:52:58	admin	172.17.18.139	Create	Restore	SCG configuration restore from [SCG181_Configuration_20130711085239GMT_2.1.0.0.258.bak].
2013/07/11 04:52:39	admin	172.17.18.139	Upload	SCG Backup	System configuration backup file [SCG181_Configuration_20130711164618_2.1.0.0.258.bak] uploaded.
2013/07/11 04:51:04	admin	172.17.18.139	Delete	RADIUS Service	RADIUS service [global10.2.6.201] deleted.
2013/07/11 04:50:44	admin	172.17.18.139	Delete	Authentication Service ...	Authentication service profile [global10.2.6.201] deleted.
2013/07/11 04:50:38	admin	172.17.18.139	Delete	Forwarding Service Profile	Forwarding service profile [ttgProfile01](Type: [TTGPDG]) deleted.
2013/07/11 04:50:25	admin	172.17.18.139	Delete	AP Zone	Zone [RuckusTTG] deleted.
2013/07/11 04:50:03	admin	172.17.18.139	Move	Access Point	AP [RuckusAP@C0:C5:20:37:A1:C0] moved from zone [RuckusTTG] to zone [Staging Zone].
2013/07/11 04:46:56	admin	172.17.18.139	Download	SCG Backup	System configuration backup file [SCG181_Configuration_20130711164618_2.1.0.0.258.bak] downloaded to [172.17.18.139].
2013/07/11 04:46:18	admin	172.17.18.139	Create	SCG Backup	System configuration backup created

Working with Reports 14

In this chapter:

- Types of Reports
- Creating a New Report
- Viewing a List of Existing Reports
- Deleting a Report

Types of Reports

The controller provides the following types of reports:

- Active TTG Sessions Report
- Client Number Report
- Client Number vs Airtime Report
- Continuously Disconnected APs Report
- Failed Client Associations Report
- New Client Associations Report
- System Resource Utilization Report
- TX/RX Bytes Report

NOTE: If you download a CSV report created by SCG, the file naming convention is as follows:

<report title>-YYYY-MM-DD_HH-MM-SS-MS_ZZ

where

MS stands for three-digit milliseconds.

ZZ is a random number to avoid the file name conflict when a user subscribes to several reports but based on the same filter. ZZ ranges between 00-99.

For example: New_Client-2015-11-17_08-00-16-031_59.csv

Active TTG Sessions Report

The Active TTG Sessions report shows a historical view of the number of active TTG sessions established in the controller. The active TTG session report can be shown in different time intervals for a specified duration. The report can be generated based on specific control planes or GGSN IP addresses.

Client Number Report

This Client Number Report shows a historical view of the maximum and minimum number of clients connect to the system. Client number can be shown in different time intervals for a specified duration. The report can be generated based on specific management domain, AP zone, AP, SSID, or radio type.

Client Number vs Airtime Report

This Client Number vs Airtime Report shows a historical view of the average number of clients connected to the system and the corresponding airtime (TX, RX, Busy). Client number and airtime can be shown in different time intervals for a specified duration. The report can be generated based on a specific management domain, AP zone, AP, SSID, or radio type.

Continuously Disconnected APs Report

The Continuously Disconnected APs Report shows the list of access points disconnected with specified time range. The report can be generated based on specific management domain and AP zone.

Failed Client Associations Report

The Failed Client Associations Report shows a historical view of the number of failed client associations. Failed client associations can be shown in different time intervals for a specified duration. The report can be generated based on specific management domain, AP zone, AP, SSID, or radio type.

New Client Associations Report

The New Client Associations Report shows a historical view of the number of new client associations. New client Associations can be shown in different time intervals for a specified duration. The report can be generated based on specific management domain, AP zone, AP, SSID, or radio type.

System Resource Utilization Report

The System Resource Utilization Report shows a historical view of the CPU and memory usage of the system. The CPU and memory usage can be shown in different time intervals for a specific duration. The report can be generated based on specific blade.

TX/RX Bytes Report

This TX/RX Bytes Report shows a historical view of the transmitted (TX) and received (RX) bytes of the system. The transmitted and received bytes can be shown in different time intervals for a specified duration. The report can be generated based on a specific management domain, AP zone, AP, SSID or radio type.

Creating a New Report

Follow these steps to create a new report.

1. On the *Saved Reports List* page, click **Create New**. The *Create New Report* form appears.
2. Perform the following steps to create a new report:

   Step 1: Define the General Report Details
   Step 2: Define the Resource Filter Criteria
   Step 3: Define the Time Filter
   Step 4: Define the Report Generation Schedule
   Step 5: Enable Email Notifications (Optional)
   Step 7: Save the Report

Step 1: Define the General Report Details

Follow these steps to define the general details of the report that you are creating in the *General Information* section.

1. In *Title*, type a name for the report that you are creating.
2. In *Description*, type a brief description for the report.
3. In *Report Type*, select the type of report that you want to create. For detailed description of the various report types, refer to Types of Reports.
4. In *Output Format*, select one or both of the following check boxes:

- **CSV**: A comma-separated version of the report. You will need a spreadsheet application (for example, Microsoft™ Excel™) to view the report in CSV format.
- **PDF**: A portable document format version of the report. You will need a PDF reader (for example, Adobe™ Acrobat™) to view the report in PDF.

5 Continue to Step 2: Define the Resource Filter Criteria.

Step 2: Define the Resource Filter Criteria

Follow these steps to define the resources upon which the report that you are creating will be generated. These resources can be defined in the *Resource Filter Criteria* section.

1 Select the resources upon which to generate the report. Resources include:

- **Device**: Select one of the following device resources:
  - **Management Domain**: If you base the report upon this device resource, you must select at least one management domain from the drop-down list. If you want to include multiple management domains in the report, select the management domains from the drop-down list one at a time. To delete a management domain that you selected previously, click the ✖ icon next to the management domain name.
  - **AP Zone**: If you base the report upon this device resource, you must select at least one AP zone from the drop-down list. If you want to include multiple AP zones in the report, select the AP zones from the drop-down list one at a time. To delete an AP zone that you selected previously, click the ✖ icon next to the management domain name.
  - **Access Point**: If you base the report upon this device resource, you must select the name of the specific access point from the drop-down list. You can only select one access point to include in the report.
- **SSID**: Select the SSID or SSIDs that you want to include in the report. If you want to include multiple SSIDs in the report, select the SSIDs from the drop-down list one at a time. To delete an SSID that you selected previously, click the ✖ icon next to the SSID.

  If you do not select an SSID, all existing SSIDs that belong to the device resource you selected in **Device** will be included in the report.
- **Radio**: Select the radio (2.4G or 5G) that you want to include in the report. If you do not select a radio, both 2.4G and 5G radios belong to the device resource you selected in **Device** will be included in the report.

NOTE: You must select at least one resource. You can also select and define all three available resources.

2 Continue to Step 3: Define the Time Filter.

Step 3: Define the Time Filter

Follow these steps to define the time filter to use in generating the report. The time filter can be defined in the *Time Filter* section.

1 In *Time Interval*, select the interval at which to generate the report. Available time interval options include:

- 15 Minutes
- Hourly
- Daily
- Monthly

2 In *Time Filter*, select the time or date period for which to generate the report. Depending on the time interval that you set above, available periods include:

- Hours
- Days
- Months

NOTE: The controller uses this time interval-time filter combination to determine the period from which to generate the report and how often to generate it.

3 Continue to Step 4: Define the Report Generation Schedule.

Step 4: Define the Report Generation Schedule

Follow these steps to define the report generation schedule. This schedule can be defined in the *Schedules* section.

1 In the *Schedules* section, click **Add New**.

2 In *Interval*, select one of the following time intervals:

- **Monthly**: If you select this interval, select the day of the month in **Every** when the controller will generate the report.
- **Weekly**: If you select this interval, select the day of the week in **Every** when the controller will generate the report.
- **Daily**
- **Hourly**

3 In *@Hour* (except when **Hourly** interval is selected above), select the hour of the day when the controller will generate the report. The controller uses the 24-hour clock format.

4 In *Minute*, select the minute of the hour when the controller will generate the report. This minute setting will be used in conjunction with the hour setting that you selected above (except when Hourly interval is selected).

5 If you want to add more schedules, click the **Add New** button again, and then repeat steps 2-4. You can create as many schedules as required. Schedules may overlap if needed.

6 Continue to Step 5: Enable Email Notifications (Optional).

Step 5: Enable Email Notifications (Optional)

Follow these steps to enable the controller to send email notifications when a report has been generated.

NOTE: Make sure you configure the SMTP settings (see Configuring the SMTP Server Settings). If the SMTP settings are not configured, the controller will be unable to send out email notifications even if you enable this feature in this section.

1 In the *Email Notification* section, click the **Enable** button.

2 In the text box below, type the email address to which to send the notification.

3 To add another email address, click **Add New**, and then type the second email address in the text box that appears.

NOTE: You can add as many email addresses as needed by clicking the Add New button, and then typing an additional email address. Note, though, that you must only type a single email address in each text box.

4 Continue to Step 6: Export the Report to an FTP Server (Optional).

Step 6: Export the Report to an FTP Server (Optional)

Follow these steps to automatically export a copy of the report to an FTP server whenever it is generated.

1 In *Export Report Results*, click **Enable**.

2 In *FTP Server*, select the FTP server to which you want to automatically export the reports. The FTP server options that appear here are those that you created in Configuring FTP Services.

3 Continue to Step 7: Save the Report

Step 7: Save the Report

After you complete steps 1 through 5, review the settings that you have configured to make sure they are correct. To save the report, click **OK** at the bottom of the page. The page refreshes, and the report that you created appears in the *Saved Report List* page.

You have completed creating a report.

Viewing a List of Existing Reports

Follow these steps to view a list of reports that have been configured.

Go to **Report** > **Saved Reports**. The *Saved Report List* page appears, displaying a summary of all reports that have been configured. Summary details include:

- Title
- Description
- Report Template
- Time Filter
- Resource Filter
- Schedule
- Status
- Actions that you can perform

To view a report, click the 🔍 icon that is in the same row as the report name. The *Report Result* page appears, displaying versions of the report that have been generated based on the time interval defined in the report schedule. To download and view a comma-separated value (CSV) version of the report, click the **CSV** link that is in the same row as the version that you want to view.

Deleting a Report

Follow these steps to delete an existing report.

1. Go to **Report** > **Saved Reports**. The *Saved Report List* page appears, displaying a summary of all reports that have been configured.
2. From the list of reports, locate the report that you want to delete.
3. Once you locate the report, click the 🗑 icon that is under the *Actions* column. A confirmation message appears.

4 Click **OK**. The list of reports refreshes, and then the report that you deleted disappears from the list.

You have completed deleting a report.

Working with Local, Guest, and Remote Users 15

In this chapter:

- Working with Local, Guest, and Remote Users
- Working with User Roles
- Managing Subscription Packages

Working with Local, Guest, and Remote Users

The controller supports the following types of user accounts:

- Local users: Also known as registered users, these are users who have existing accounts on the controller database. See Working with Local Users.
- Guest users: These are temporary users for whom guest passes have been generated. See Working with Guest Users.
- Remote users: Also known as Bring Your Own Device (BYOD) users, these are users who bring and connect their own devices to the network. See Working with Remote Users.

Working with Local Users

A local user in the controller refers to a registered user who may be given access to the controller hotspot. A user account contains a user's personal information, logon information, and the subscription package that he or she has been assigned.

This section describes the following tasks:

- Creating a Local User Account
- Editing a Local User Account

Creating a Local User Account

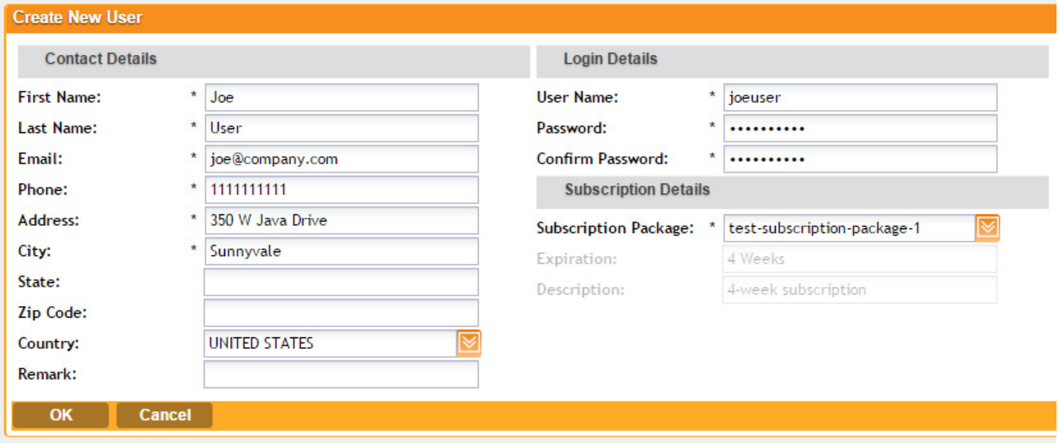
NOTE: When you create a user account, you will be required to assign a subscription package to the user. Before creating a user account, Ruckus Wireless recommends creating at least one subscription package. See Creating a Package for more information.

Follow these steps to create a user account.

1. Go to *Configuration* > *Identity* > *Users*.
2. Click **Create New**.
3. In the *Contact Details* section, fill out the following boxes:
    - First Name
    - Last Name
    - Email
    - Phone
    - Country
    - City
    - Street
    - Zip Code
    - State: Select **Enabled** to enable this user profile or select **Disabled**.
    - Remark
4. In the *Login Details* section, fill out the following boxes to create the logon credentials of this user:
    - *User Name*: Type a name for this user. The user name is not case-sensitive and will always be displayed in lowercase characters.
    - *Password*: Type a password for this user. The password must be at least eight characters in length.
    - *Confirm Password*: Retype the password above.
5. In the *Subscription Details* section, select a subscription package that you want to assign to this user (see Managing Subscription Packages).
6. Click **OK**.

You have completed creating a user account.

Figure 174. Creating a user account



Create New User

Contact Details

First Name:	*	Joe
Last Name:	*	User
Email:	*	joe@company.com
Phone:	*	1111111111
Address:	*	350 W Java Drive
City:	*	Sunnyvale
State:		
Zip Code:		
Country:		UNITED STATES
Remark:		

Login Details

User Name:	*	joeuser
Password:	*	••••••••••
Confirm Password:	*	••••••••••

Subscription Details

Subscription Package:	*	test-subscription-package-1
Expiration:		4 Weeks
Description:		4-week subscription

Editing a Local User Account

Follow these steps to edit an existing local user account.

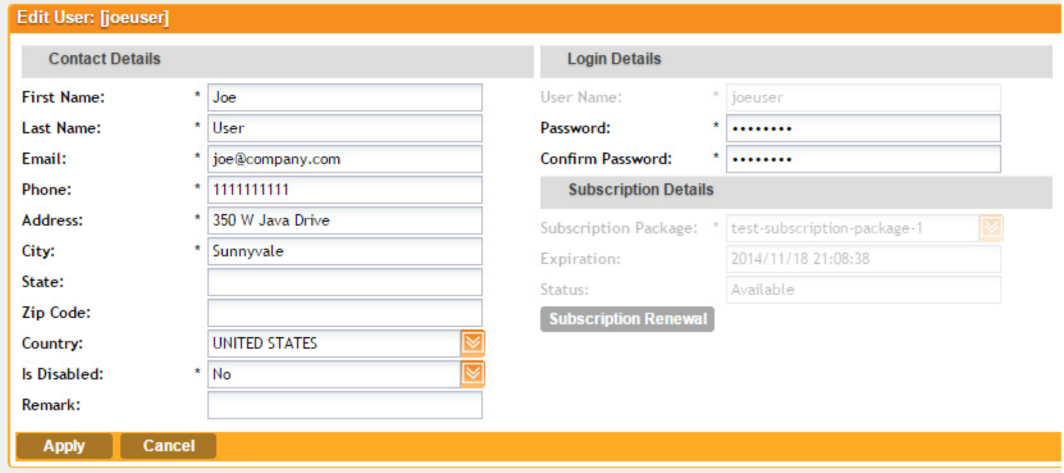
1 Go to *Configuration* > *Identity* > *Users*.

2 Locate the user account that you want to edit, and then click the user name. The *Edit User: [{User Name}]* form appears.

3 Edit the user account by updating the fields in the *Contact Details* and *Login Details* sections.

4 Click **OK**.

Figure 175. Editing a user account



Edit User: [joeuser]

Contact Details

First Name:	*	Joe
Last Name:	*	User
Email:	*	joe@company.com
Phone:	*	1111111111
Address:	*	350 W Java Drive
City:	*	Sunnyvale
State:		
Zip Code:		
Country:		UNITED STATES
Is Disabled:	*	No
Remark:		

Login Details

User Name:	*	joeuser
Password:	*	••••••••
Confirm Password:	*	••••••••

Subscription Details

Subscription Package:	*	test-subscription-package-1
Expiration:		2014/11/18 21:08:38
Status:		Available

Working with Guest Users

Similar to local user accounts (see Working with Local Users), guest user accounts in the controller allow users to gain access to the controller hotspots. However, unlike local user accounts, guest users are not required to provide personal information to access the controller hotspots and can, therefore, remain anonymous.

Generating Guest Passes

Guest users require guest passes, which are credentials that allow temporary access to the controller hotspots and are generated for specific WLANs only – guest pass users will only be able to gain access to the WLANs for which the guest pass was generated.

Generating guest passes involves the following steps:

Step 1: Create a Guest Access Portal

Step 2: Create a Guest Access WLAN

Step 3: Generate a Guest Pass

NOTE: If you want to send the guest pass to guest users via Short Message Service (SMS), make sure you add the SMS server to the controller before starting the next procedure. For information on how to add an SMS server to the controller, see Configuring an SMS Server.

Step 1: Create a Guest Access Portal

1. Create an AP zone that you want to use to provide hotspot access to guest users. See Creating an AP Zone for instructions on how to create one.
2. After you have created an AP zone, go to *Configuration* > *AP Zones*.
3. On the *AP Zone List* page, click the name of the AP zone that you have created to go to its configuration page. The configuration page for that AP zone appears.
4. On the sidebar, click **Guest Access**. The *Guest Access* page appears.
5. Click **Create New**. The *Create New Guest Access Portal* form appears.
6. In *General Options*, configure the following:
   - Portal Name
   - Portal Description
   - Language

7 In *Start Page* under *Redirection*, set where users will be redirected after they log in successfully:

- **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
- **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).

8 In *Guest Access*, configure the following:

- *Guest Pass SMS Gateway*: If you want to send the guest pass to users using SMS and you configured an SMS server earlier, select the SMS server. Otherwise, select Disabled.
- *Terms and Conditions*: To require users to read and accept your terms and conditions prior to use, **Show Terms And Conditions** check box. The box below, which contains the default Terms of Use text, becomes editable. Edit the text or leave it unchanged to use the default text.
- *Web Portal Logo*: By default, the guest hotspot logon page displays the Ruckus Wireless logo. To use your own logo, click the **Upload** button, select your logo (recommended size is 138 x 40 pixels, maximum file size is 20KB), and then click **Upload**.
- *Web Portal Title*: Type your own guest hotspot welcome text or accept the default welcome text ("Welcome to the Guest Access login page").

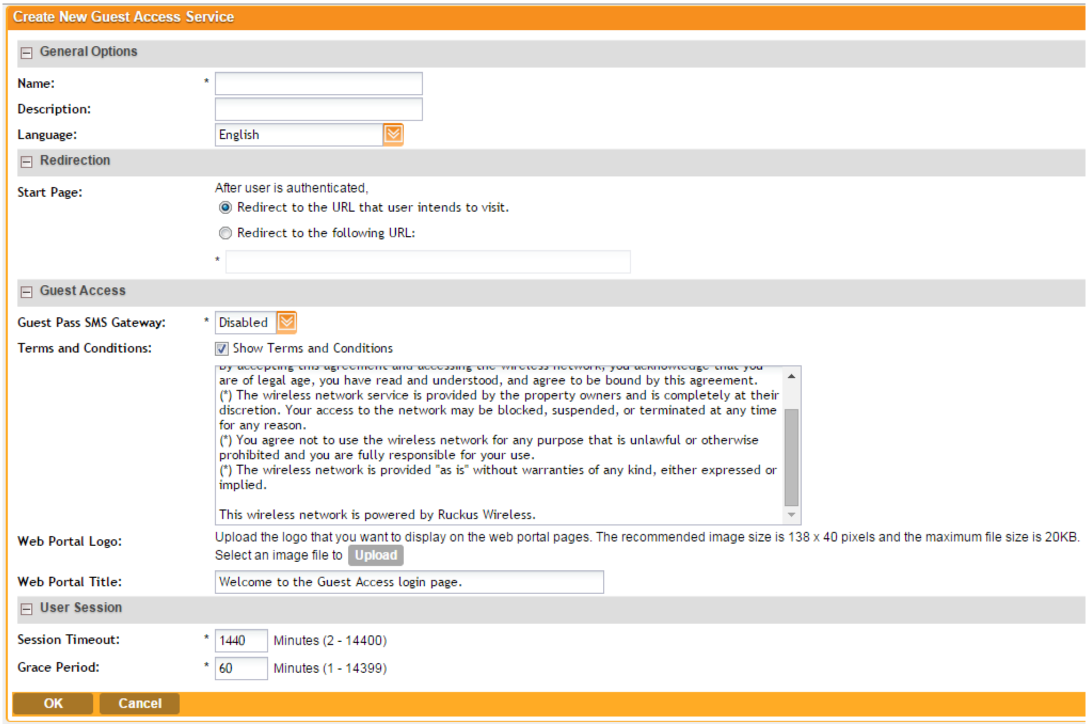
9 In *User Session*, configure the following:

- *Session Timeout*: Specify a time limit after which users will be disconnected and required to log on again.
- *Grace Period*: Set the time period during which clients will not need to re-authenticate after getting disconnected from the hotspot. Enter a number (in minutes) between 1 and 14399.

10 Click **OK**.

You have completed creating a guest access portal. You may now continue to Step 2: Create a Guest Access WLAN.

Figure 176. The Create New Guest Access Portal form



Create New Guest Access Service

⊟ General Options

Name:	*	
Description:		
Language:		English

⊟ Redirection

Start Page:

After user is authenticated,

● Redirect to the URL that user intends to visit.

○ Redirect to the following URL:

*

⊟ Guest Access

Guest Pass SMS Gateway:	*	Disabled
Terms and Conditions:		☑ Show Terms and Conditions

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
(*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.
(*) The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

This wireless network is powered by Ruckus Wireless.

Web Portal Logo: Upload the logo that you want to display on the web portal pages. The recommended image size is 138 x 40 pixels and the maximum file size is 20KB.
Select an image file to Upload

Web Portal Title: Welcome to the Guest Access login page.

⊟ User Session

Session Timeout:	*	1440	Minutes (2 - 14400)
Grace Period:	*	60	Minutes (1 - 14399)

Step 2: Create a Guest Access WLAN

In this step, you will create a WLAN for the AP zone that you created in Step 1: Create a Guest Access Portal.

1 Create a new WLAN. Follow the instructions in Working with WLANs and WLAN Groups.

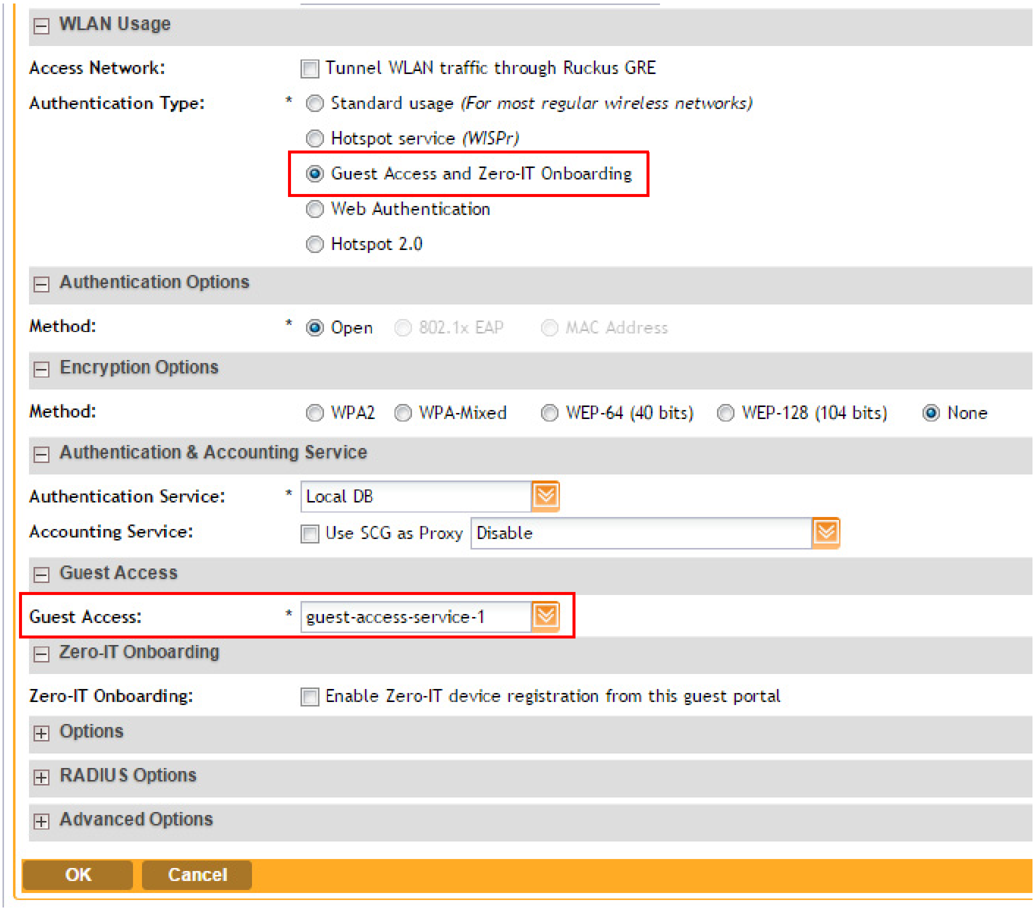
2 Make sure though that you configure *Authentication Type* and *Hotspot (WISPr) Service* exactly as described below.

- In *Authentication Type,* click **Guest Access and Zero-IT Onboarding**.
- In *Guest Access*, select the guest access portal that you created earlier in Step 1: Create a Guest Access Portal.

3 Click **Create New**.

You have completed creating a guest access WLAN. Continue to Step 3: Generate a Guest Pass.

Figure 177. Select Guest Access and Zero-IT Onboarding in Authentication Type, and then select the guest access portal you created earlier in Guest Access



⊟ WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
○ Hotspot service *(WISPr)*
● Guest Access and Zero-IT Onboarding
○ Web Authentication
○ Hotspot 2.0

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method: ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

⊟ Authentication & Accounting Service

Authentication Service: * Local DB

Accounting Service: □ Use SCG as Proxy Disable

⊟ Guest Access

Guest Access: * guest-access-service-1

⊟ Zero-IT Onboarding

Zero-IT Onboarding: □ Enable Zero-IT device registration from this guest portal

Step 3: Generate a Guest Pass

Follow these steps to generate a guest pass.

1 Click *Identity* > *Users*. The *Users* page appears.

2 Click *Guest Pass* > *Guest Pass Service*. The *Guest Pass* page appears.

3 Click *Generate Guest Pass*, and then click **Next**.

4 Configure the following options:

- *Guest Name*: Type a name that you want to assign to the guest user.

- *Guest WLAN*: Select the guest WLAN that you created in Step 2: Create a Guest Access WLAN.
- *Number of Passes*: Type the number of guest passes that you want to generate.
- *Pass Valid For*: Set the validity period for the guest pass by filling in the two boxes. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.

5 Configure the advanced options:

- *Pass Generation*: Select the **Auto Generate** check box if you want the controller to generate the guest pass key automatically. If you want to generate the guest pass manually, clear the **Auto Generate** check box.

NOTE: If you are generating more than one guest pass, the Auto Generate check box is selected automatically and is not configurable.

- *Pass Effective Since*: Set the guest pass validity period by selecting one of the following options:
  - **Effective from the creation time**: This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
  - **Effective from first use**: This type of guest pass is valid from the time the user uses it to authenticate with controller until the specified expiration time. An additional parameter (A Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
  - **Expire guest pass if not used within [ ] days**: If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
- *Max Devices Allowed*: Set the number of users that can share this guest pass.
  - **Limited to [ ]**: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
  - **Unlimited**: If you want an unlimited number of users to share this guest pass, click this option.

- *Session Duration*: If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

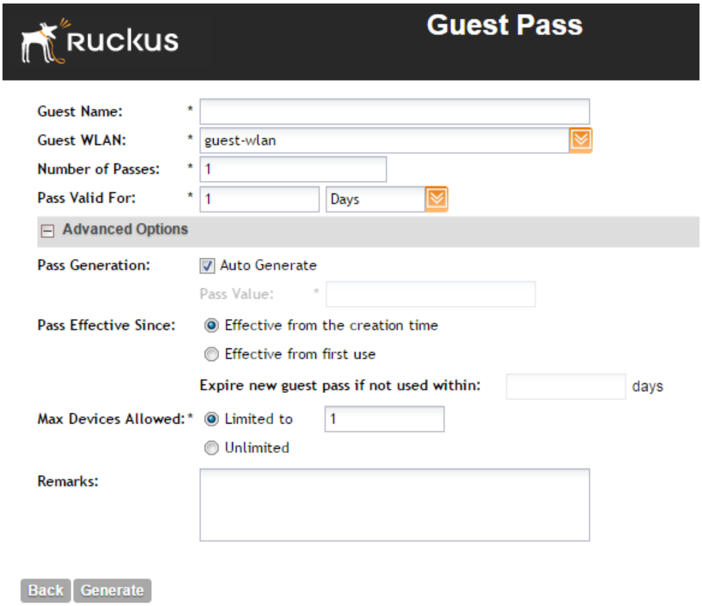
- In *Remarks* (optional), type your notes about this guest pass, if any.

6 Click **Generate**. The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

7 Click **OK** to close the pop-up message.

You have completed generating a guest pass. You are now ready to send the guest pass to guest users. See Step 4: Send Guest Passes to Guest Users for information.

Figure 178. Generating a guest pass



Guest Pass

Guest Name: *

Guest WLAN: * guest-wlan

Number of Passes: * 1

Pass Valid For: * 1 Days

⊟ Advanced Options

Pass Generation: ☑ Auto Generate

Pass Value: *

Pass Effective Since: ● Effective from the creation time
○ Effective from first use

Expire new guest pass if not used within: days

Max Devices Allowed:* ● Limited to 1
○ Unlimited

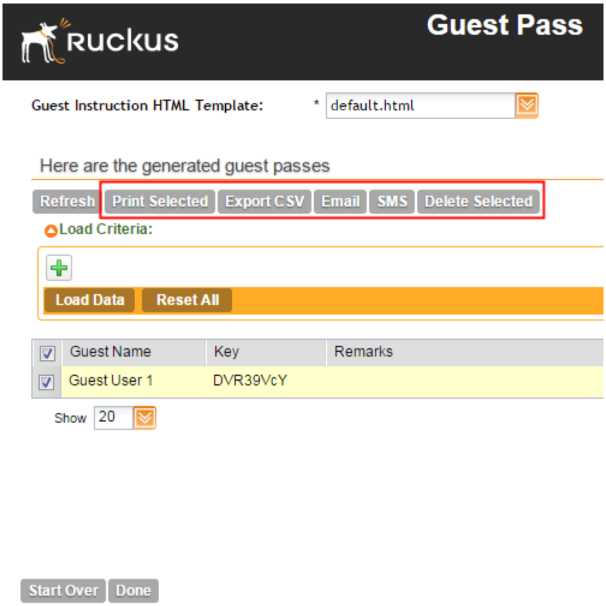
Remarks:

Step 4: Send Guest Passes to Guest Users

On the page that appears after you generate a guest pass are options for delivering the guest pass to guest users (see Figure 179). These delivery options include:

- *Print Selected*: See Printing the Guest Pass.
- *Export CSV*: See Exporting the Guest Pass to CSV.
- *Email*: See Sending the Guest Pass via Email.
- *SMS*: See Sending the Guest Pass via SMS.

Figure 179. Options for delivering guest passes to guest users



Guest Pass

Guest Instruction HTML Template: * default.html

Here are the generated guest passes

☑	Guest Name	Key	Remarks
☑	Guest User 1	DVR39VcY	

Printing the Guest Pass

NOTE: If your browser is blocking pop-ups, make you temporarily disable the pop-up blocker so you can view and print the guest pass.

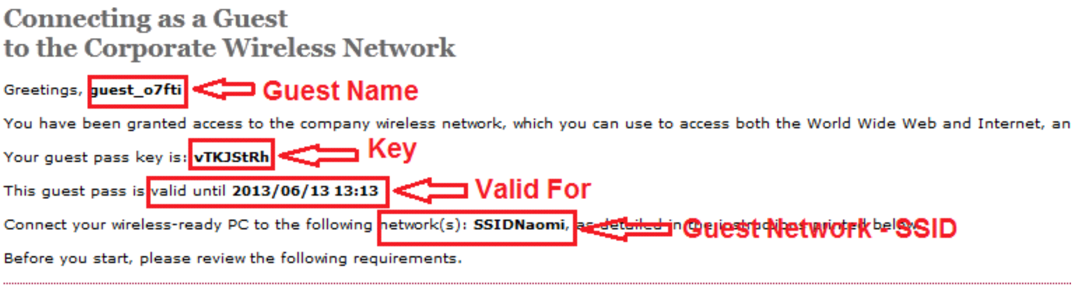
After you generate the guest pass, you can print the guest pass information, which contains the guest user information and instructions on how to connect to the hotspot, and give it to the guest user.

Follow these steps to print a guest pass.

1. Select the guest passes that you want to print by selecting the check boxes before them.
2. In *Guest Instruction HTML Template*, select a printout template to use. The default printout template (`default.html`) is selected by default. If you created custom printout templates (see Creating a Guest Pass Printout Template), they will appear in the drop-down menu.
3. Click **Print Selected**. A new browser page appears, which displays the guest pass and available printing options.
4. Configure your printer settings, and then print the guest passes.

You have completed printing the guest passes.

Figure 180. What a guest pass printout looks like



Connecting as a Guest
to the Corporate Wireless Network

Greetings, **guest_o7fti**

You have been granted access to the company wireless network, which you can use to access both the World Wide Web and Internet, an

Your guest pass key is: **vTKJStRh**

This guest pass is valid until **2013/06/13 13:13**

Connect your wireless-ready PC to the following network(s): **SSIDNaomi**, as detailed in the instructions printed below.

Before you start, please review the following requirements.

Exporting the Guest Pass to CSV

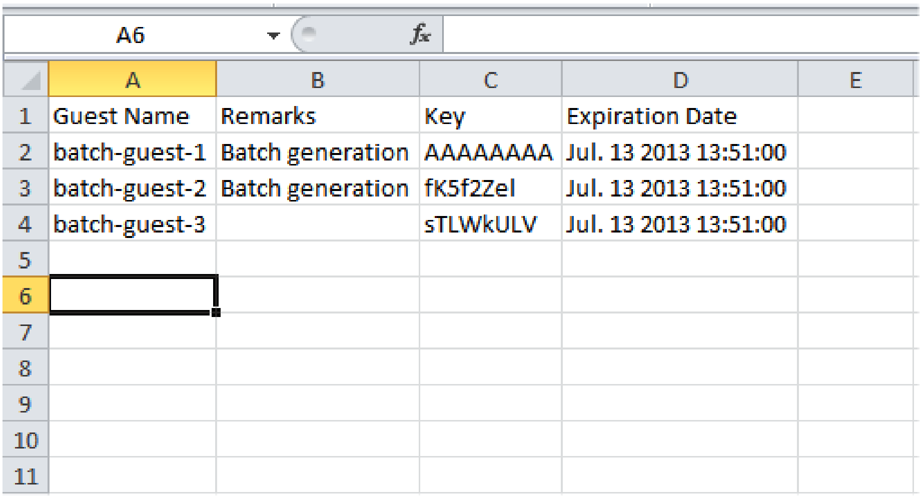
Follow these steps to export the last generated guest passes to a comma-separated value (CSV) file.

1. Select the guest passes that you want to export to CSV by selecting the check boxes before them.
2. Click **Export CSV**. Your web browser downloads the CSV file to its default download location.
3. Go to your web browser's default download location and look for a file named `guestpass[number].csv`.
4. Using Microsoft Excel or a similar application, open the CSV file. The CSV file displays the details of the guest passes, including:
   - Guest Name
   - Remarks
   - Key

- Expiration Date

You have completed exporting the last generated guest passes to CSV.

Figure 181. A sample CSV of generated guest passes when opened in Excel



	A	B	C	D	E
1	Guest Name	Remarks	Key	Expiration Date	
2	batch-guest-1	Batch generation	AAAAAAAA	Jul. 13 2013 13:51:00	
3	batch-guest-2	Batch generation	fK5f2Zel	Jul. 13 2013 13:51:00	
4	batch-guest-3		sTLWkULV	Jul. 13 2013 13:51:00	
5					
6					
7					
8					
9					
10					
11					

Sending the Guest Pass via Email

NOTE: To send guest passes via email, you must have added an external email server to the controller. See Configuring the SMTP Server Settings for more information.

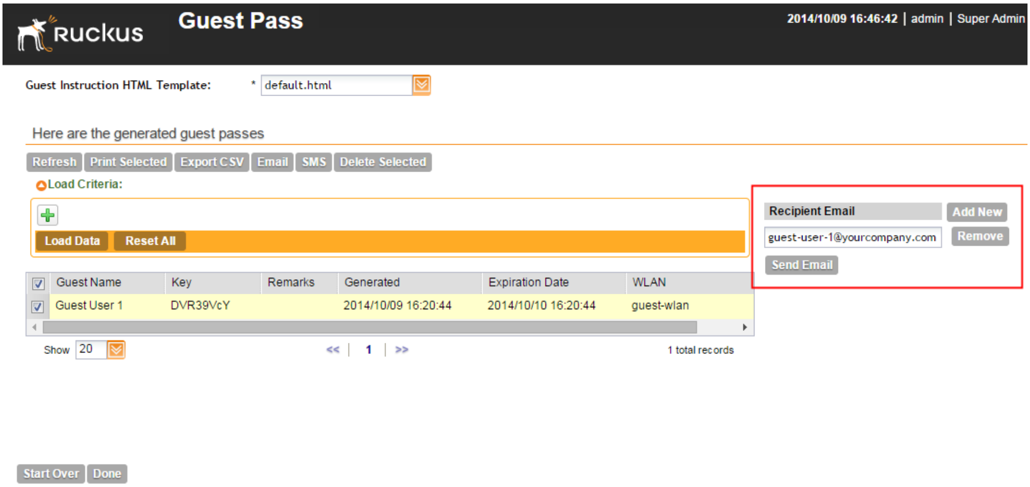
Follow these steps to send the guest pass via email.

1. Select the guest passes that you want to send via email by selecting the check boxes before them.
2. Click **Email**. The *Recipient Email* form appears on the right side of the page (see Figure 182).
3. Click **Add New**.
4. In the box that appears below, type the email address to which you want to send the guest passes.
5. To add another recipient, click **Add New** again, and then type another email address.
6. When you have finished adding all the email recipients, click **Send Email**. A dialog box appears and informs you that the emails have been sent to the message queue successfully

7 Click **OK** to close the dialog box.

You have completed sending guest passes via email.

Figure 182. Use the Recipient Email form to specify who will receive the guest passes via email



2014/10/09 16:46:42 | admin | Super Admin

Guest Instruction HTML Template: * default.html

Here are the generated guest passes

☑	Guest Name	Key	Remarks	Generated	Expiration Date	WLAN
☑	Guest User 1	DVR39VcY		2014/10/09 16:20:44	2014/10/10 16:20:44	guest-wlan

Show 20

1 total records

Recipient Email: guest-user-1@yourcompany.com

Sending the Guest Pass via SMS

NOTE: To send guest passes via email, you must have added an external SMS gateway to the controller. See Configuring an SMS Server for more information.

Follow these steps to send the guest pass via email.

1 Select the guest passes that you want to send via SMS by selecting the check boxes before them.

2 Click **SMS**. SMS options appears on the right side of the page (see Figure 183).

3 In Guest Instruction SMS Template, select the SMS template that you want to use.

4 Click **Add New**.

5 In the box that appears below, type the phone number to which you want to send the guest passes via SMS.

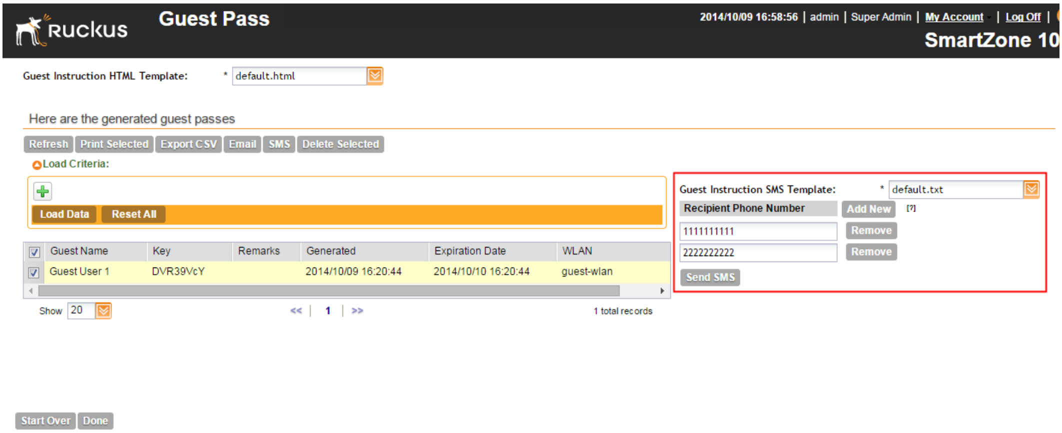
6 To add another SMS recipient, click **Add New** again, and then type another phone number.

7 When you have finished adding all the SMS recipients, click **Send SMS**. A dialog box appears and informs you that the SMS messages have been sent to the message queue successfully

8 Click **OK** to close the dialog box.

You have completed sending guest passes via SMS.

Figure 183. Options for sending guest passes via SMS



Guest Instruction HTML Template: * default.html

Here are the generated guest passes

☑	Guest Name	Key	Remarks	Generated	Expiration Date	WLAN
☑	Guest User 1	DVR39VcY		2014/10/09 16:20:44	2014/10/10 16:20:44	guest-wlan

Show 20 << | 1 | >> 1 total records

Guest Instruction SMS Template: * default.txt

Recipient Phone Number

1111111111

2222222222

Generating Guest Passes from an Imported CSV

You can also manually define the guest passes that you want to generate in a comma-separated value (CSV) file (a sample of which is available for download from the *Guest Pass* page).

Follow these steps to generate guest passes from an imported CSV file.

1 Click *Configuration* > *Identity* > *Users*.

2 Click *Guest Pass* > *Guest Pass Service*. The *Guest Pass* page appears.

3 Click **Import Guest Pass**, and then click **Next**.

4 Look for the following text under **Browse**:

```
To download a sample guest pass, click here.
```

5 Click the `here` link to download the sample CSV file.

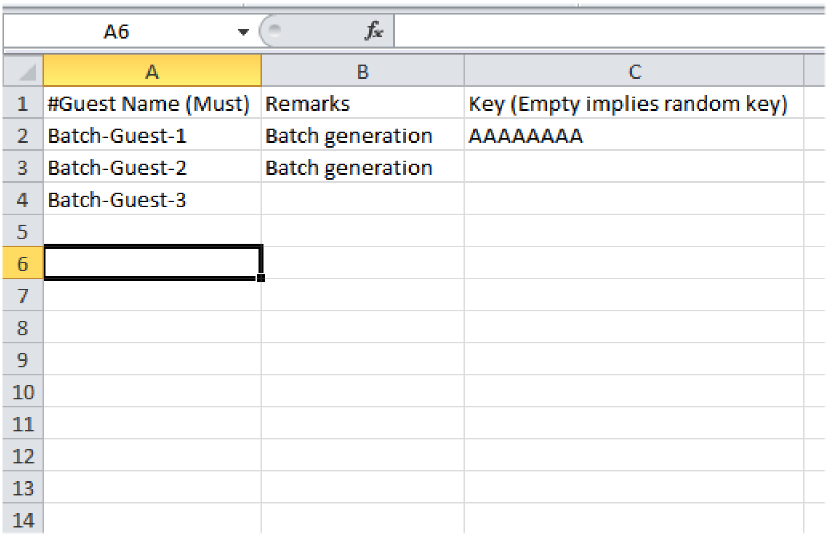
6 Using Microsoft Excel or a similar application, open the CSV file.

7 In the CSV file, fill out the following columns:

- *#Guest Name (Must)*: Assign a user name to the guest pass user.
- Remarks (Optional): Add some notes or comments about this guest pass.

- *Key*: Enter a guest pass key or leave it blank so the controller can generate the key automatically.

Figure 184. The sample CSV file when opened in Excel



	A	B	C
1	#Guest Name (Must)	Remarks	Key (Empty implies random key)
2	Batch-Guest-1	Batch generation	AAAAAAAA
3	Batch-Guest-2	Batch generation	
4	Batch-Guest-3		
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

8 Save the CSV file.

9 Go back to the Guest Pass page, and then configure the following settings on the Common Guest Pass Settings:

- *Guest WLAN*: Select the guest WLAN that you created in Step 2: Create a Guest Access WLAN.
- *Pass Valid For*: Set the validity period for the guest pass by filling in the two boxes. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.

10 Configure the advanced options:

- *Pass Effective Since*: Set the guest pass validity period by selecting one of the following options:
  - **Effective from the creation time**: This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.

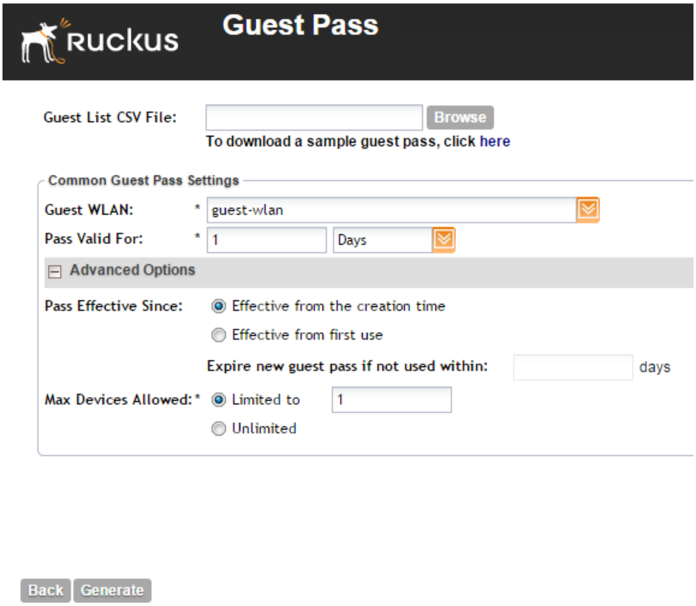
  - **Effective from first use**: This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (A Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
  - **Expire guest pass if not used within [ ] days**: If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
- *Max Devices Allowed*: Set the number of users that can share this guest pass.
  - **Limited to [ ]**: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
  - **Unlimited**: If you want an unlimited number of users to share this guest pass, click this option.
  - *Session Duration*: If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

11 In *Guest List CSV File* (at the top of the page), click **Browse**, and then select the CSV file you edited earlier. The page refreshes, and the number of guest passes that the controller has identified in the CSV file appears below the **Browse** button.

12 Click **Generate**. The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

You have completed generating a guest pass. You are now ready to send the guest pass to guest users. See Step 4: Send Guest Passes to Guest Users for information.

Figure 185. The Guest Pass page for importing a CSV file



Guest List CSV File: [ ] Browse
To download a sample guest pass, click here

Common Guest Pass Settings

Guest WLAN: * guest-wlan

Pass Valid For: * 1 Days

⊟ Advanced Options

Pass Effective Since: ● Effective from the creation time
○ Effective from first use
Expire new guest pass if not used within: [ ] days

Max Devices Allowed:* ● Limited to 1
○ Unlimited

Viewing the List of Guest Users

Follow these steps to view guest users that currently exist on the controller.

1 Click *Configuration* > *Identity* > *Users*.

2 Click the *User Type* column to sort all existing user accounts by user type.

All users of the user type “Guest” are guest users.

You have completed view the list of guest users.

Deleting Guest Users

Follow these steps to delete guest users.

1 Click *Configuration* > *Identity* > *Users*.

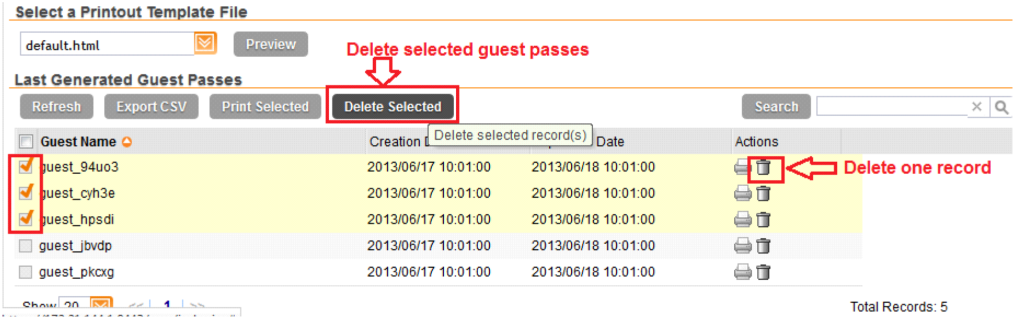
2 Select the check boxes before the guest user accounts that you want to delete. Click **Delete Selected**. A confirmation message appears.

3 Click **Yes** to confirm. The page refreshes, and the guest user accounts that you deleted disappears from the list.

NOTE: To delete a single guest pass, click the 🗑 (delete) icon that is in the same row as the guest pass name.

You have completed deleting a guest pass or guest passes.

Figure 186. Deleting a single guest pass or multiple guest passes


Select a Printout Template File
default.html
Preview
Last Generated Guest Passes
Refresh
Export CSV
Print Selected
Delete Selected
Delete selected record(s)
Search

Delete selected guest passes

Delete one record

□	Guest Name	Creation D	Date	Actions
☑	guest_94uo3	2013/06/17 10:01:00	2013/06/18 10:01:00	🖶 🗑
☑	guest_cyh3e	2013/06/17 10:01:00	2013/06/18 10:01:00	🖶 🗑
☑	guest_hpsdi	2013/06/17 10:01:00	2013/06/18 10:01:00	🖶 🗑
□	guest_jbvdp	2013/06/17 10:01:00	2013/06/18 10:01:00	🖶 🗑
□	guest_pkcxg	2013/06/17 10:01:00	2013/06/18 10:01:00	🖶 🗑

Show 20 << 1 >>

Total Records: 5

Creating a Guest Pass Printout Template

A guest pass printout template contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), as well as the actual instructions for connecting to the WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

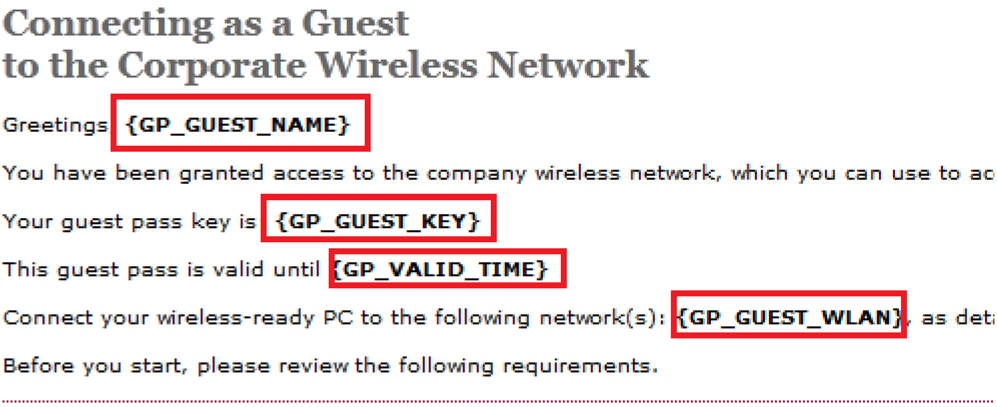
1 Go to *Configuration* > *Identity* > *Users*.

2 Click *Guest Pass* > *Manage Templates*. The *Manage Guest Instruction Templates* page appears.

3 Using an HTML editor, create a new HTML or text file.

4 Add content to the file. Typically, a printout template contains instructions for connecting to the controller hotspot. See Figure 187 for the content of the default printout template.

Figure 187. Content of the default printout template



Connecting as a Guest
to the Corporate Wireless Network

Greetings {GP_GUEST_NAME}

You have been granted access to the company wireless network, which you can use to ac

Your guest pass key is {GP_GUEST_KEY}

This guest pass is valid until {GP_VALID_TIME}

Connect your wireless-ready PC to the following network(s): {GP_GUEST_WLAN}, as det

Before you start, please review the following requirements.

5 Insert the following variables into the content of your template:
   - {GP_GUEST_NAME}: This is the guest pass user name.
   - {GP_GUEST_KEY}: This is the guest pass key.
   - {GP_VALID_TIME}: This is the expiration date and time of the guest pass.
   - {GP_GUEST_WLAN}: This is the WLAN with which the guest user can associate using the guest name and guest key.

6 Save the file.

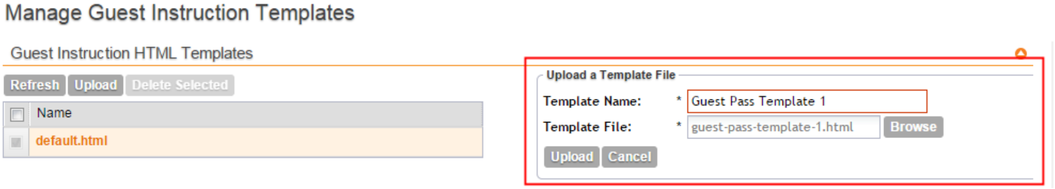
7 On the *Manage Guest Instruction Templates* page, click the appropriate Upload button for the template that you are creating. The Upload a Template File form appears on the right side of the page.

8 Configure the *Upload a Template File* options:
   - *Template Name*: Type a name for the template that you are uploading.
   - *Template File*: Click **Browse**, and then select the template file you created.

9 Click **Upload**. An information message box appears and informs you that the template file has been uploaded successfully.

10 Click **OK**. The template file you uploaded now appears on the list of templates.

Figure 188. The Upload a Template File form



Manage Guest Instruction Templates

Guest Instruction HTML Templates

□	Name
□	default.html

Upload a Template File

Template Name: * Guest Pass Template 1

Template File: * guest-pass-template-1.html

Working with Remote Users

Remote users are users who bring and connect their own devices (for example, smart phones, laptops, tablets, etc.) to the network. They are also known as Bring Your Own Device (BYOD) users. Using a process called “onboarding,” you can make enable these remote users to connect their devices to network.

How Onboarding Works

The following describes how the onboarding process works.

1 The user equipment (UE) associates with the onboarding WLAN and authenticates itself with an external authentication server (for example, Active Directory).

2 The AP that provides the onboarding WLAN sends a JavaScript Object Notation (JSON) request to the identity management (IDM) module on the controller. This JSON request contains the UE’s user name, group name, MAC address, and WLAN.

3 The IDM module retrieves the role that has been mapped to the UE’s group name, gets role mapping, and checks the device limit.

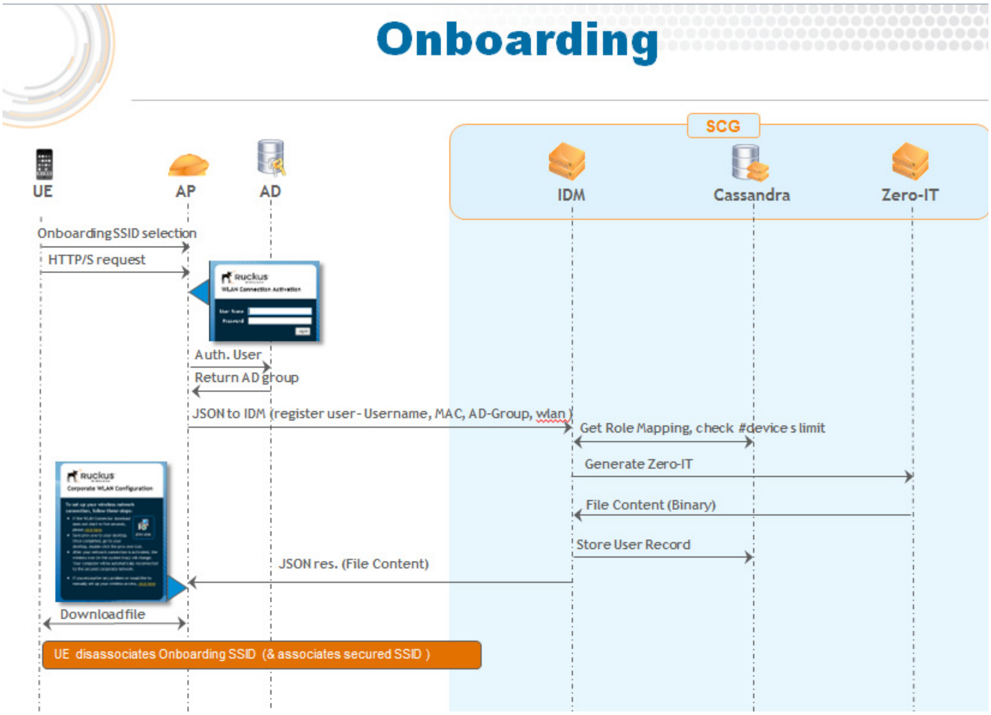
4 The IDM module triggers the Zero-IT service on the AP to generate the Zero-IT binary file.

5 The AP prompts the user of the UE to download and install the Zero-IT binary file.

6 After the user installs the Zero-IT binary file on the UE, the UE disassociates from the onboarding WLAN, and then associates with the standard WLAN that has been set up for remote users.

At this point, the onboarding process is complete and the UE is now able to access the wireless network.

Figure 189. Overview of the onboarding process


Onboarding
SCG
UE
AP
AD
IDM
Cassandra
Zero-IT
Onboarding SSID selection
HTTP/S request
Auth. User
Return AD group
JSON to IDM (register user- Username, MAC, AD-Group, wlan)
Get Role Mapping, check #device s limit
Generate Zero-IT
File Content (Binary)
Store User Record
JSON res. (File Content)
Download file
UE disassociates Onboarding SSID (& associates secured SSID)

Before You Begin

Before you begin creating the onboarding and standard WLANs for remote users, make sure that:

- The authentication server that you will use to authenticate remote users exists on the network. You only need one authentication server and you will use the same authentication server for both the onboarding and standard WLANs.
- You have added the authentication server to the controller. If you have not yet added the authentication server to the controller, see Creating an AAA Server.
- The remote users have existing accounts on the authentication server.
- You have created a guest access portal to use for the onboarding WLAN. If you have not yet created a guest access portal for the onboarding WLAN, see Creating a Guest Access Portal.

Step 1: Create the Onboarding Guest WLAN for Remote Users

Follow these steps to create an onboarding guest WLAN.

1 Click **Configuration** > **AP Zones**.

2 On the *AP Zone List* page, click the AP zone for which you want to create the onboarding guest WLAN.

3 On the sidebar, click **WLAN**. The *WLAN Configuration* page appears.

4 In the *WLAN Configuration* section, click **Create New**. The form for creating a new WLAN service appears.

5 In the *General Options* section, configure the following options.

- *Name/SSID*: Type a short name (two to 32 alphanumeric characters) for this WLAN.
- *Description*: Type a brief description of the qualifications/purpose for this WLAN (for example, Onboarding WLAN).

6 In *Authentication Type* under *WLAN Usage*, click **Guest Access + Hotspot 2.0 Onboarding**.

7 In the *Guest Access Portal* section, configure the following:

- *Guest Portal Service*: Select the guest access portal that you created earlier for this onboarding WLAN.
- *Bypass CNA*: Select the **Enable** check box if you want to bypass the Apple CNA feature on iOS and OS X devices that connect to this WLAN. See Bypassing Apple CNA for more information.
- *Guest Authentication*: Select **Guest** to require users to enter their guest credentials, or select **Always Accept** to allow users without guest credentials to authentication.

8 In the *Online Signup/Onboarding Services* ection, configure the following:

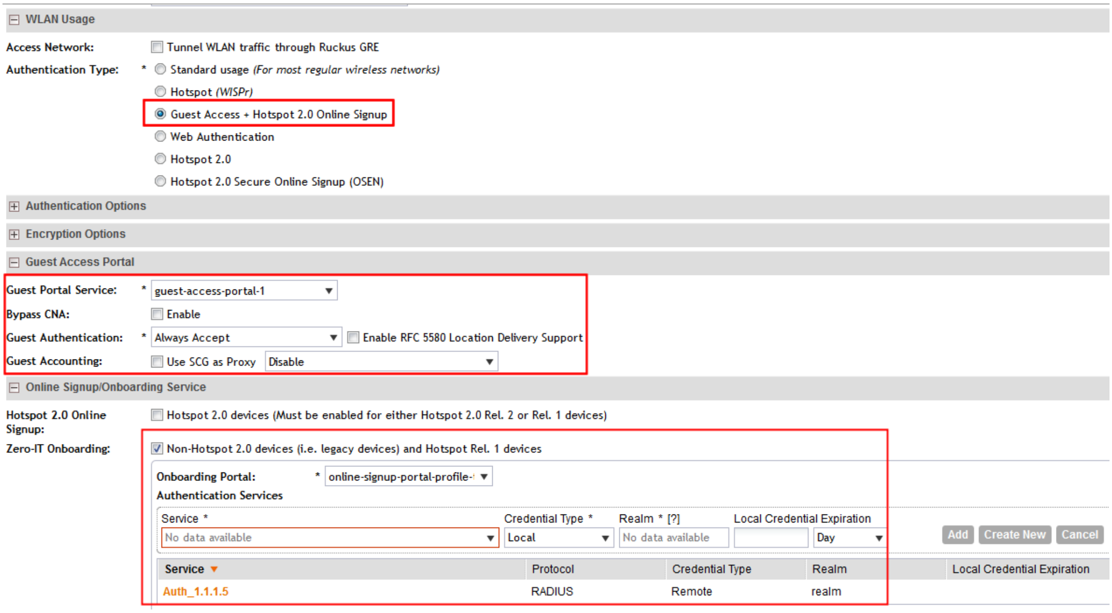
- Select the **Non-Hotspot 2.0 devices (i.e., legacy devices) and Hotspot Rel 1 devices** check box.
- *Onboarding Portal*: Select the portal signup profile that you want this guest WLAN to use.
- *Authentication Services*: Select the authentication server that you previously added to the controller.

9 Configure the other settings in the form as needed.

10 Click **OK** at the bottom of the form.

You have completed creating the onboarding WLAN.

Figure 190. Settings that you need to configure to create the onboarding guest WLAN



⊟ WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
● Guest Access + Hotspot 2.0 Online Signup
○ Web Authentication
○ Hotspot 2.0
○ Hotspot 2.0 Secure Online Signup (OSEN)

⊞ Authentication Options

⊞ Encryption Options

⊟ Guest Access Portal

Guest Portal Service: * guest-access-portal-1

Bypass CNA: □ Enable

Guest Authentication: * Always Accept □ Enable RFC 5580 Location Delivery Support

Guest Accounting: □ Use SCG as Proxy Disable

⊟ Online Signup/Onboarding Service

Hotspot 2.0 Online Signup: □ Hotspot 2.0 devices (Must be enabled for either Hotspot 2.0 Rel. 2 or Rel. 1 devices)

Zero-IT Onboarding: ☑ Non-Hotspot 2.0 devices (i.e. legacy devices) and Hotspot Rel. 1 devices

Onboarding Portal: * online-signup-portal-profile-

Authentication Services

Service *	Credential Type *	Realm * [?]	Local Credential Expiration	
No data available	Local	No data available		Day

Service	Protocol	Credential Type	Realm	Local Credential Expiration
Auth_1.1.1.5	RADIUS	Remote	realm	

Step 2: Create a Standard WLAN with Zero-IT Activation Enabled

Follow these steps to create the standard WLAN with which user devices will associate after they pass authentication and install the Zero-IT binary file.

1 Click **Configuration** > **AP Zones**.

2 On the *AP Zone List* page, click the AP zone for which you want to create the standard WLAN.

3 On the sidebar, click **WLAN**. The *WLAN Configuration* page appears.

4 In the *WLAN Configuration* section, click **Create New**. The form for creating a new WLAN service appears.

5 In the *General Options* section, configure the following options.

- *Name/SSID*: Type a short name (two to 32 alphanumeric characters) for this WLAN.
- *Description*: Type a brief description of the qualifications/purpose for this WLAN (for example, Onboarding WLAN).

6 In *Authentication Method*, click **802.1x EAP**.

7 In *Authentication Service*, select the authentication server that you added earlier to authenticate remote users.

NOTE: This authentication server must be the same server that you selected when you created the onboarding WLAN.

---

8 In *Authentication Type* under *WLAN Usage*, click **Standard usage (For most regular wireless networks)**.

9 In *Zero-IT Activation* under *Options*, select the **Enable Zero-IT Activation** check box. With this option selected, the remote user will be prompted by the AP to install the Zero-IT binary file, which will automatically configure the device's wireless settings and allow it to connect to the wireless network.

10 Click **OK** at the bottom of the form.

You have completed creating the standard WLAN for remote users.

Working with User Roles

Use user roles to limit user access to certain WLANs, to allow them to log on with non-standard client devices, or to grant permission to generate guest passes.

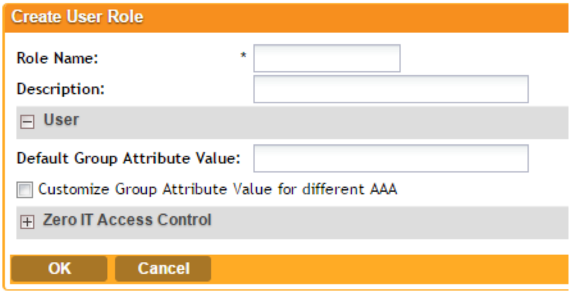
Creating a User Role

Follow these steps to create a user role.

1. Go to *Identity* > *Roles*.
2. Click **Create New**. The *Create User Role* form appears.
3. Configure the options in the *Create User Role* form.
   - *Name*: Type a name for this user role.
   - *Description*: Type a description for this user role.
   - *Default Group Attribute Value*: (Fill in this field only if you are creating a user role based on group attributes extracted from an Active Directory or LDAP server.) Enter the User Group name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.
   - *WLANS*: Specify whether this role will have access to all WLAN or to specific WLANs only.
     - **Allow Zero IT Access to All WLANs**: Click this to allow this user role access to all WLANs.
     - **Allow Zero IT Access to Selected WLANs Only**. Click to allow this user role access to specific WLANs only. You must select the WLAN to which this user role will have access.
   - *Max Devices Allowed*: Set the number of users that can share this role.
     - **Limited to [ ]**: If you want a limited number of users to share this role pass, click this option, and then type the number in the box.
     - **Unlimited**: If you want an unlimited number of users to share this role, click this option.
4. Click **OK**.

You have completed creating a user role.

Figure 191. Creating a user role



Create User Role

Role Name: *

Description:

⊟ User

Default Group Attribute Value:

☐ Customize Group Attribute Value for different AAA

⊞ Zero IT Access Control

Managing Subscription Packages

A subscription package defines the characteristics of a subscription that has been created for a registered user (see Working with Local Users). These characteristics include the expiration date of the subscription.

NOTE: If the user is connected at the time when his or her subscription expires, the user will get disconnected from the AP and any attempts to reauthenticate will fail.

This section covers:

- Viewing a List of Subscription Packages
- Creating a Subscription Package
- Editing a Subscription Package
- Deleting a Subscription Package

Viewing a List of Subscription Packages

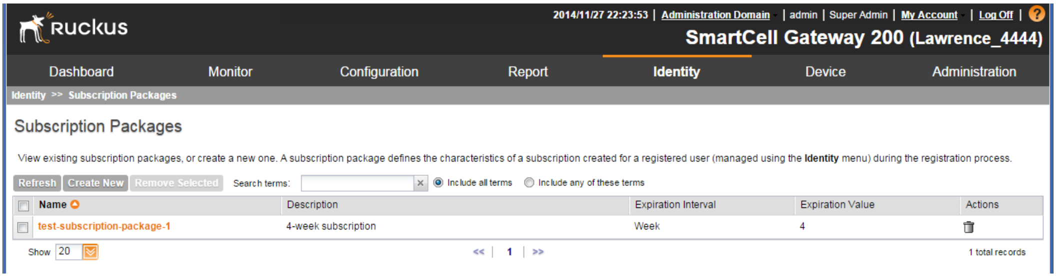
Follow these steps to view a list of existing packages.

Go to *Identity* > *Subscription Packages*. The *Subscription Packages* page displays a table of existing packages along with their basic details, including:

- *Name*: The name of the package.
- *Description*: A brief description of the package.
- *Expiration Time*: The time unit used in conjunction with *Expiration Value* to define when the package will expire.
- *Expiration Value*: The value used in conjunction with *Expiration Time* to define when the package will expire.

- *Actions*: A list of actions that you can perform. In this release, the only action available is **Delete Packages** (see Deleting a Subscription Package).

Figure 192. Viewing existing subscription packages


Ruckus
2014/11/27 22:23:53 | Administration Domain | admin | Super Admin | My Account | Log Off | ?
SmartCell Gateway 200 (Lawrence_4444)
Dashboard
Monitor
Configuration
Report
Identity
Device
Administration
Identity >> Subscription Packages
Refresh
Create New
Remove Selected
Search terms:
● Include all terms
○ Include any of these terms
Show 20
<< | 1 | >>
1 total records

Subscription Packages

View existing subscription packages, or create a new one. A subscription package defines the characteristics of a subscription created for a registered user (managed using the **Identity** menu) during the registration process.

□	Name	Description	Expiration Interval	Expiration Value	Actions
□	test-subscription-package-1	4-week subscription	Week	4	🗑

Creating a Subscription Package

Follow these steps to create a package.

1 Go to *Identity* > *Subscription Packages*. The *Subscription Packages* page appears.

2 Click **Create New**.

3 In *Package Name*, type a name for the subscription package that you are creating.

4 In *Description*, type a description for the package. This is an optional field.

5 In *Expiration Time*, set the time unit to use for the package expiration. Options available include:

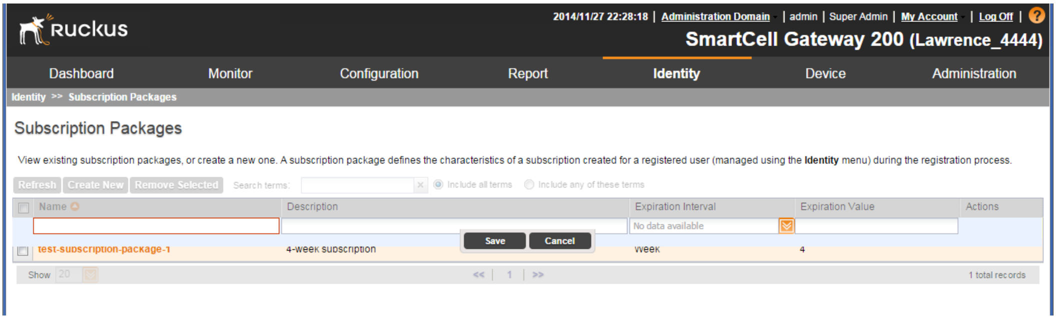
   - Hour
   - Day
   - Week
   - Month
   - Year
   - Never

6 In *Expiration Value*, set the actual value to use in combination with the Expiration Time. For example, if you selected **Day** in *Expiration Time* and you typed **7** in *Expiration Value*, the package will expire 7 days after it is assigned to a user.

7 Click **Save**.

The page refreshes, and the package that you created appears in the view list.

Figure 193. Creating a subscription package


Ruckus
2014/11/27 22:28:18 | Administration Domain | admin | Super Admin | My Account | Log Off |
SmartCell Gateway 200 (Lawrence_4444)
Dashboard
Monitor
Configuration
Report
Identity
Device
Administration
Identity >> Subscription Packages
Refresh
Create New
Remove Selected
Search terms:
Include all terms
Include any of these terms
Save
Cancel
Show 20
<< | 1 | >>
1 total records

Subscription Packages

View existing subscription packages, or create a new one. A subscription package defines the characteristics of a subscription created for a registered user (managed using the **Identity** menu) during the registration process.

	Name	Description	Expiration Interval	Expiration Value	Actions
			No data available		
□	test-subscription-package-1	4-week subscription	Week	4	

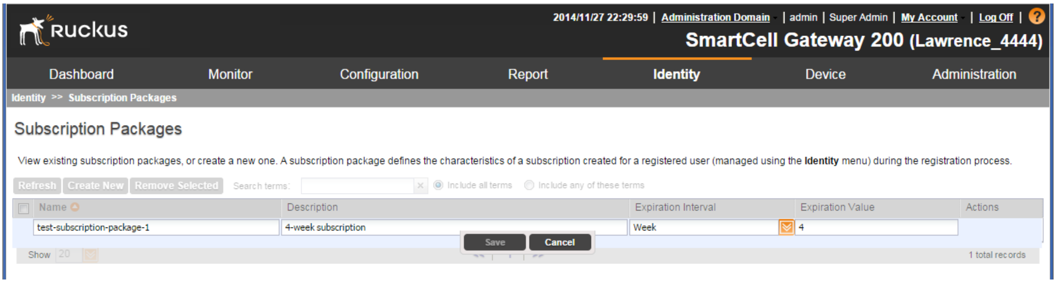
Editing a Subscription Package

You can change or update the package settings anytime. Follow these steps to edit an existing package.

1. Go to *Identity* > *Subscription Packages*. The *Subscription Packages* page appears.
2. Locate the package that you want to edit.
3. Under the *Name* column, click the name of the package that you want to edit. The entire row becomes editable.
4. Edit the profile by changing any of the following options:
   - Name
   - Description
   - Expiration Interval
   - Expiration Value
5. Click **Save**.

You have completed editing a package.

Figure 194. Editing a subscription package


Ruckus
2014/11/27 22:29:59 | Administration Domain | admin | Super Admin | My Account | Log Off |
SmartCell Gateway 200 (Lawrence_4444)
Dashboard
Monitor
Configuration
Report
Identity
Device
Administration
Identity >> Subscription Packages
Refresh
Create New
Remove Selected
Search terms:
Include all terms
Include any of these terms
Save
Cancel
Show 20
1 total records

Subscription Packages

View existing subscription packages, or create a new one. A subscription package defines the characteristics of a subscription created for a registered user (managed using the **Identity** menu) during the registration process.

	Name	Description	Expiration Interval	Expiration Value	Actions
	test-subscription-package-1	4-week subscription	Week	4	

Deleting a Subscription Package

Follow these steps to delete a subscription package.

1 Go to *Identity* > *Subscription Packages*. The *Subscription Packages* page appears.

2 Locate the package that you want to delete.

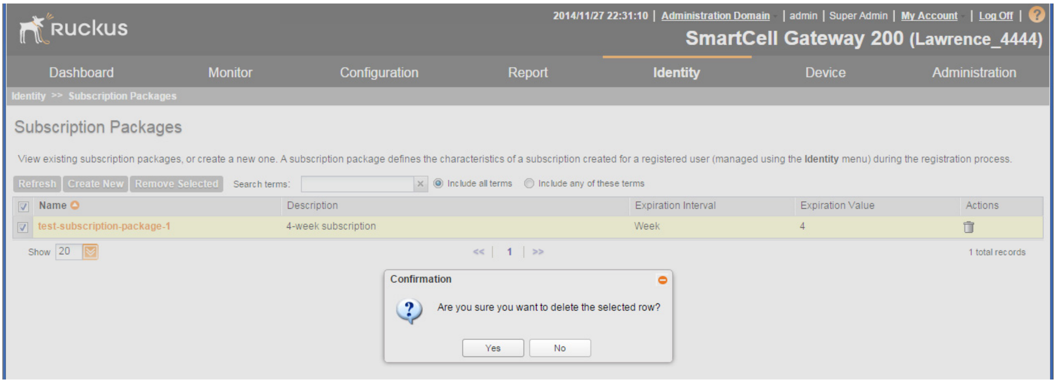
3 Under the *Actions* column, click the 🗑 icon that is in the same row as the package name. The following confirmation message appears:

```
Are you sure you want to delete the selected row?
```

4 Click **Yes**. The page refreshes, and the package that you deleted disappears from the table.

You have completed deleting a package.

Figure 195. Deleting a subscription package



Ruckus
2014/11/27 22:31:10 | Administration Domain | admin | Super Admin | My Account | Log Off |
SmartCell Gateway 200 (Lawrence_4444)
Dashboard
Monitor
Configuration
Report
Identity
Device
Administration
Identity >> Subscription Packages
Refresh
Create New
Remove Selected
Search terms:
Include all terms
Include any of these terms
Show 20
<< | 1 | >>
1 total records
Yes
No

Subscription Packages

View existing subscription packages, or create a new one. A subscription package defines the characteristics of a subscription created for a registered user (managed using the **Identity** menu) during the registration process.

☑	Name	Description	Expiration Interval	Expiration Value	Actions
☑	test-subscription-package-1	4-week subscription	Week	4	🗑

Confirmation

Are you sure you want to delete the selected row?

Performing Administrative Tasks 16

In this chapter:

- Backing Up and Restoring Clusters
- Backing Up and Restoring the Controller's Network Configuration from an FTP Server
- Backing Up and Restoring System Configuration
- Resetting a Node to Factory Settings
- Upgrading the Controller
- Working with Logs
- Managing License Files

Backing Up and Restoring Clusters

Back up the controller cluster periodically to ensure that you can restore the control plane, data plane, and AP firmware versions as well as the system configuration in the cluster if is a system failure occurs.

This section covers the following topics:

- Creating a Cluster Backup
- Restoring a Cluster Backup
- Deleting a Cluster Backup

NOTE: You can also perform these procedures from the SCG-200 command line interface. Note, however, that you will need to execute the commands on each node. For more information, see the *SmartCell Gateway 200 Command Line Interface Reference Guide* for this release.

Creating a Cluster Backup

Follow these steps to back up an entire controller cluster.

1 Take note of the current system time. You can view the *General System Settings* page under *Configuration* > *System*. For more information, see Setting the System Time.

2 Go to *Administration* > *Cluster Backup and Restore*.

3 Click **Back Up Entire Cluster**. The following confirmation message appears:

```
Are you sure you want to back up the cluster?
```

4 Click **Yes**. The following message appears:

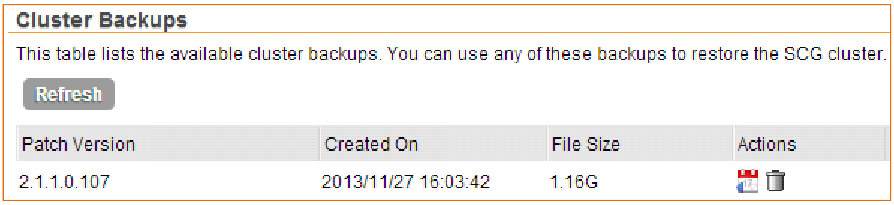
```
The cluster is in maintenance mode. Please wait a few
minutes.
```

When the cluster backup process is complete, a new entry appears in the *Cluster Backups* section with a *Created On* value that is approximate to the time when you started the cluster backup process.

CAUTION! If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

You have completed backing up the controller cluster.

Figure 196. A new entry appears in the Cluster Backups section



Cluster Backups

This table lists the available cluster backups. You can use any of these backups to restore the SCG cluster.

Patch Version	Created On	File Size	Actions
2.1.1.0.107	2013/11/27 16:03:42	1.16G	📅 🗑

Restoring a Cluster Backup

Follow these steps to restore a cluster backup.

CAUTION! You must perform the restore procedure on the exact same node where you generated the cluster backup.

---

1. Go to **Administration** > **Cluster Backup and Restore**.
2. In the *Cluster Backups* section, locate the cluster backup that you want to restore.
3. Click the 📅 icon that is in the same row as the cluster backup. The following confirmation message appears:

   ```
   Are you sure you want to restore the cluster?
   ```

4. Click **Yes**. The page refreshes, and then the following message appears:

   ```
   System is restoring! Please wait...
   ```

NOTE: The cluster restore process may take several minutes to complete.

When the restore process is complete, the controller logs you off the web interface automatically.

CAUTION! Do not refresh the controller web interface while the restore process is in progress. Wait for the restore process to complete successfully.

---

5. Log back on to the controller web interface.

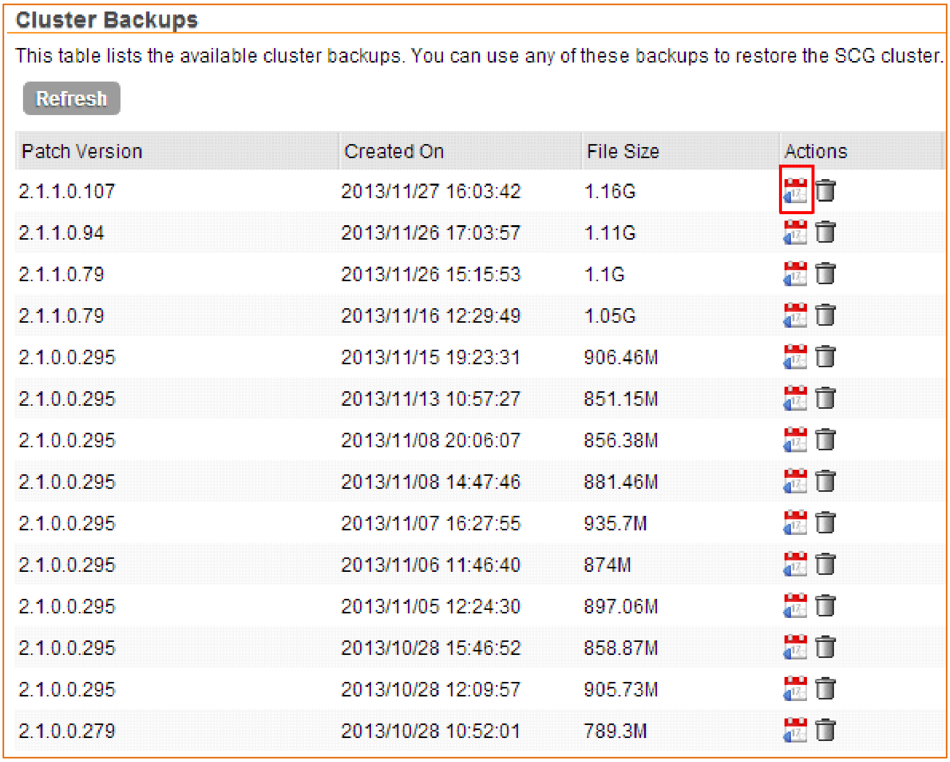
NOTE: If the web interface displays the message "`Cluster is out of service. Please try again in a few minutes.`" appears after you log on to the controller web interface, wait for about three minutes. The dashboard will appear shortly. The message appears because the controller is still initializing its processes.

---

6. Go to **Administration** > **Upgrade**, and then check the *Current System Information* section and verify that all nodes in the cluster have been restored to the previous version and are all in service.
7. Go to **Administration** > **Diagnostics**, and then click **Application Logs & Status** on the sidebar. Check the *Health Status* column and verify that all of the controller processes are online (see Figure 198).

You have completed restoring the cluster backup.

Figure 197. Under Actions, click the calendar icon to start the cluster restore process

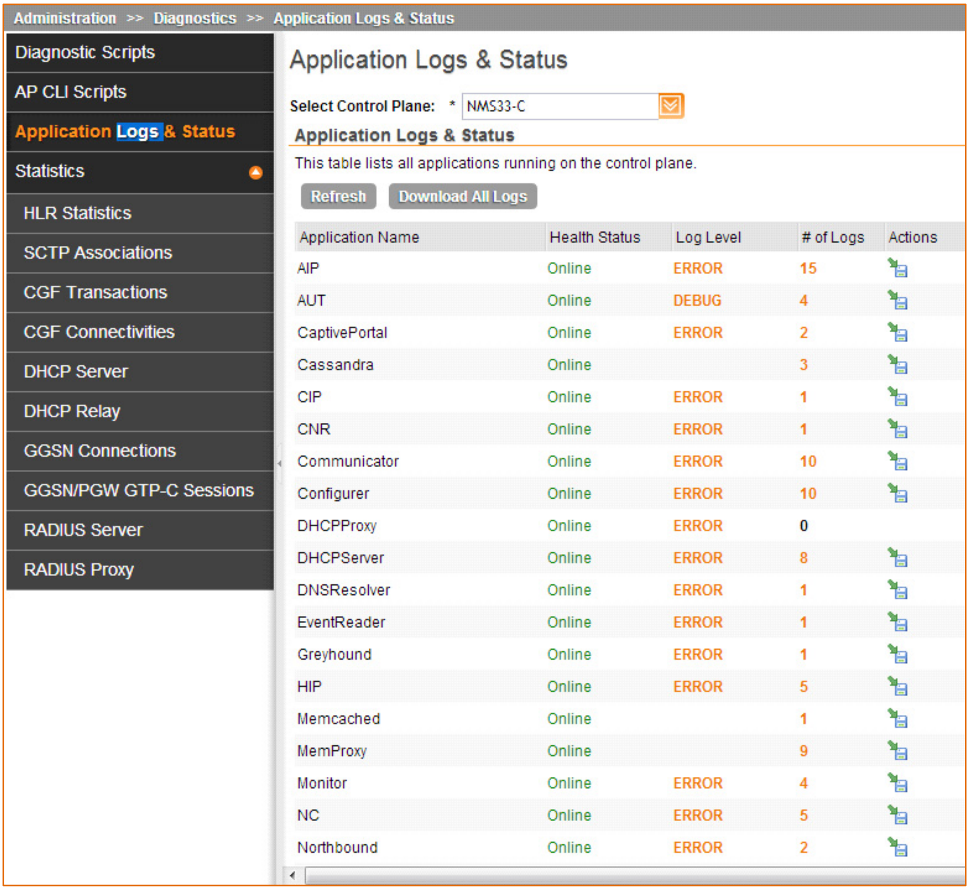


Cluster Backups

This table lists the available cluster backups. You can use any of these backups to restore the SCG cluster.

Patch Version	Created On	File Size	Actions
2.1.1.0.107	2013/11/27 16:03:42	1.16G	📅 🗑
2.1.1.0.94	2013/11/26 17:03:57	1.11G	📅 🗑
2.1.1.0.79	2013/11/26 15:15:53	1.1G	📅 🗑
2.1.1.0.79	2013/11/16 12:29:49	1.05G	📅 🗑
2.1.0.0.295	2013/11/15 19:23:31	906.46M	📅 🗑
2.1.0.0.295	2013/11/13 10:57:27	851.15M	📅 🗑
2.1.0.0.295	2013/11/08 20:06:07	856.38M	📅 🗑
2.1.0.0.295	2013/11/08 14:47:46	881.46M	📅 🗑
2.1.0.0.295	2013/11/07 16:27:55	935.7M	📅 🗑
2.1.0.0.295	2013/11/06 11:46:40	874M	📅 🗑
2.1.0.0.295	2013/11/05 12:24:30	897.06M	📅 🗑
2.1.0.0.295	2013/10/28 15:46:52	858.87M	📅 🗑
2.1.0.0.295	2013/10/28 12:09:57	905.73M	📅 🗑
2.1.0.0.279	2013/10/28 10:52:01	789.3M	📅 🗑

Figure 198. After the upgrade is complete, go to the Application Logs & Status page and verify that all of the controller processes are online



Application Logs & Status

Select Control Plane: * NMS33-C

Application Logs & Status

This table lists all applications running on the control plane.

Application Name	Health Status	Log Level	# of Logs	Actions
AIP	Online	ERROR	15	⬇
AUT	Online	DEBUG	4	⬇
CaptivePortal	Online	ERROR	2	⬇
Cassandra	Online		3	⬇
CIP	Online	ERROR	1	⬇
CNR	Online	ERROR	1	⬇
Communicator	Online	ERROR	10	⬇
Configurer	Online	ERROR	10	⬇
DHCPProxy	Online	ERROR	0	
DHCPServer	Online	ERROR	8	⬇
DNSResolver	Online	ERROR	1	⬇
EventReader	Online	ERROR	1	⬇
Greyhound	Online	ERROR	1	⬇
HIP	Online	ERROR	5	⬇
Memcached	Online		1	⬇
MemProxy	Online		9	⬇
Monitor	Online	ERROR	4	⬇
NC	Online	ERROR	5	⬇
Northbound	Online	ERROR	2	⬇

Deleting a Cluster Backup

Follow these steps to delete a cluster backup.

1 Go to **Administration** > **Cluster Backup and Restore**.

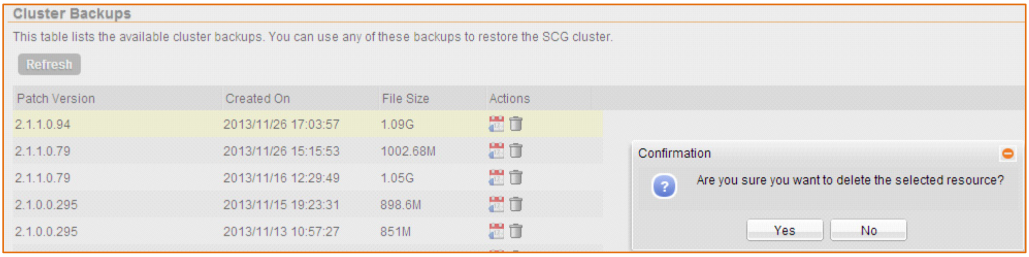
2 In the *Cluster Backups* section, locate the cluster backup that you want to delete.

3 Click the 🗑 icon that is in the same row as the cluster backup. The following confirmation message appears:

```
Are you sure you want to delete the selected resource?
```

4 Click **Yes**. The page refreshes and the row is deleted from the *Cluster Backups* list.

Figure 199. A confirmation message appears after you click the trash bin icon



Cluster Backups

This table lists the available cluster backups. You can use any of these backups to restore the SCG cluster.

Refresh

Patch Version	Created On	File Size	Actions
2.1.1.0.94	2013/11/26 17:03:57	1.09G	📅 🗑
2.1.1.0.79	2013/11/26 15:15:53	1002.68M	📅 🗑
2.1.1.0.79	2013/11/16 12:29:49	1.05G	📅 🗑
2.1.0.0.295	2013/11/15 19:23:31	898.6M	📅 🗑
2.1.0.0.295	2013/11/13 10:57:27	851M	📅 🗑

Confirmation

Are you sure you want to delete the selected resource?

Backing Up and Restoring the Controller's Network Configuration from an FTP Server

In addition to backing up and restoring the controller's network configuration from its own database, the controller supports backup and restore of its network configuration from an FTP server using the CLI. This section describes the requirements for backing up and restoring the controller's network configuration from an FTP server, the information that is included in the backup file, and how to perform the backup and restore process.

Requirements

To back up and restore the controller's network configuration from an FTP server, the controller must have already been set up and in service. In case of a multi-node cluster, all the nodes in the cluster must be in service.

What Information Is Backed Up

Table 17 lists the network configuration that is backed up from the control and data planes when you perform a backup procedure to an FTP server.

Table 17. Information that is backed up to the FTP server

Control Plane	Data Plane
• Control interface • Cluster interface • Management interface • Static routes • User-defined interfaces	• Primary interface • Static routes • Internal subnet prefix

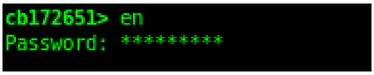
Backing Up to an FTP Server

Follow these steps to back up the controller network configuration to an FTP server.

1 Log on to the controller from the CLI. See Accessing the Command Line Interface for more information.

2 At the prompt, enter **en** to enable privileged mode.

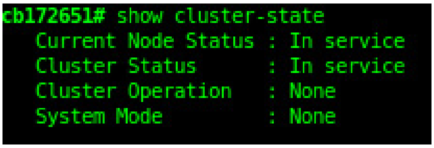
Figure 200. Enable privileged mode



```
cb172651> en
Password: *********
```

3 Enter **show cluster-state** to display the statuses of the node and the cluster. Before continuing to the next step, verify that both the node and the cluster are in service.

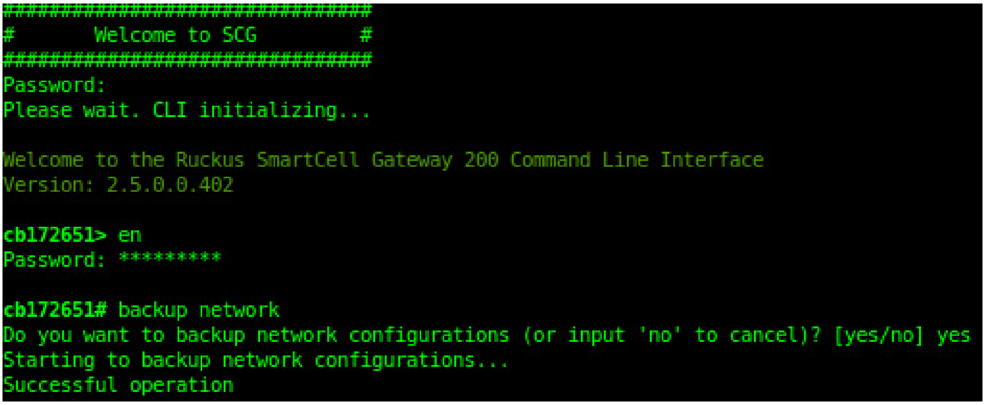
Figure 201. Verify that both the node and the cluster are in service



```
cb172651# show cluster-state
   Current Node Status : In service
   Cluster Status      : In service
   Cluster Operation   : None
   System Mode         : None
```

4 Enter **backup network** to back up the controller network configuration, including the control plane and data plane information. The controller creates a backup of its network configuration on its database.

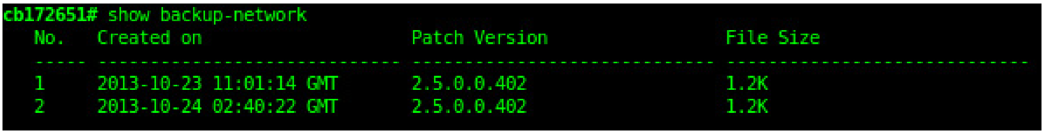
Figure 202. Run "backup network"



```
################################
#       Welcome to SCG         #
################################
Password:
Please wait. CLI initializing...

Welcome to the Ruckus SmartCell Gateway 200 Command Line Interface
Version: 2.5.0.0.402

cb172651> en
Password: *********

cb172651# backup network
Do you want to backup network configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup network configurations...
Successful operation
```

5 Enter **`show backup-network`** to view a list of backup files that have been created. Verify that the *Created On* column displays an entry that has a time stamp that is approximate to the time you started the backup.

Figure 203. Enter the "show backup-network" command



```
cb172651# show backup-network
   No.   Created on                    Patch Version                 File Size
   ----- ----------------------------- ----------------------------- -----------------------------
   1     2013-10-23 11:01:14 GMT       2.5.0.0.402                   1.2K
   2     2013-10-24 02:40:22 GMT       2.5.0.0.402                   1.2K
```

6 Enter **`copy backup-network {ftp-url}`**, where `{ftp-url}` (remove the braces) is the URL or IP address of the FTP server to which you want to back up the cluster configuration.

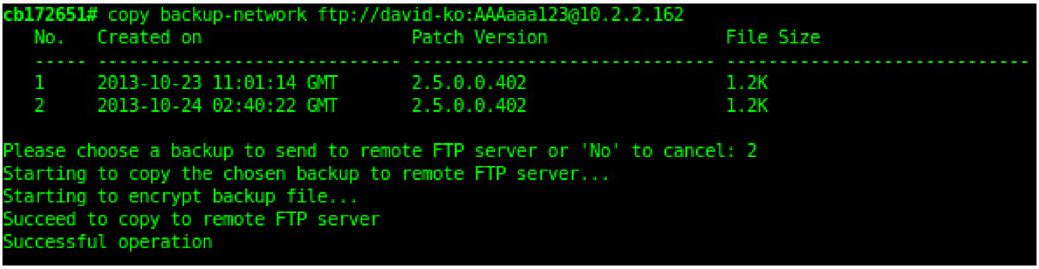
The CLI prompts you to choose the number that corresponds to the backup file that you want to export to the FTP server.

7 Enter the number of the backup file that you want to export to the FTP server.

The controller encrypts the backup file, and then exports it to the FTP server. When the export process is complete, the following message appears on the CLI:

```
Succeed to copy to remote FTP server
Successful operation
```

Figure 204. "Succeed to copy to remote FTP server" indicates that you have exported the backup file to the FTP server successfully



```
cb172651# copy backup-network ftp://david-ko:AAAaaa123@10.2.2.162
   No.   Created on                    Patch Version                 File Size
   ----- ----------------------------- ----------------------------- -----------------------------
   1     2013-10-23 11:01:14 GMT       2.5.0.0.402                   1.2K
   2     2013-10-24 02:40:22 GMT       2.5.0.0.402                   1.2K

Please choose a backup to send to remote FTP server or 'No' to cancel: 2
Starting to copy the chosen backup to remote FTP server...
Starting to encrypt backup file...
Succeed to copy to remote FTP server
Successful operation
```

8 Using an FTP client, log on to the FTP server, and then verify that the backup file exists. The file format of the backup file is

`network_<YYYYMMDDHHmmss>_<controller-version>.bak`.

For example, if you created the backup file on October 24th 2013 at 02:40:22 and the controller version is 2.5.0.0.402, you should see a file named
`network_20131024024022_2.5.0.0.402.bak`
on the FTP server.

You have completed backing up the controller to an FTP server.

Restoring from an FTP Server

Before you continue, take note of the following limitations with restoring a backup file of the controller network configuration from an FTP server:

- Only release 2.1 and later support restoring from an FTP server.
- In this current release, restoring the entire cluster from an FTP server is unsupported. The restore process must be performed on one node at a time.
- Restoring from an FTP server can only be performed using the CLI.

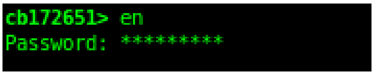
CAUTION! Restoring a backup file to the controller requires restarting all of the controller services.

Follow these steps to restore a backup file of the controller's network configuration that you previously uploaded to an FTP back to the controller.

1 Log on to the controller from the CLI. See Accessing the Command Line Interface for more information.

2 At the prompt, enter **en** to enable privileged mode.

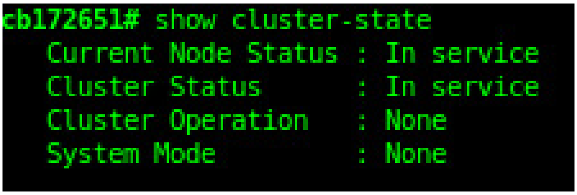
Figure 205. Enable privileged mode



```
cb172651> en
Password: *********
```

3 Enter **show cluster-state** to display the statuses of the node and the cluster. Before continuing to the next step, verify that both the node and the cluster are in service.

Figure 206. Verify that both the node and the cluster are in service



```
cb172651# show cluster-state
   Current Node Status : In service
   Cluster Status      : In service
   Cluster Operation   : None
   System Mode         : None
```

4 Enter the following command to log on to the FTP server and check for available backup files that can be copied to the controller:

```
copy <ftp-url> backup-network
```

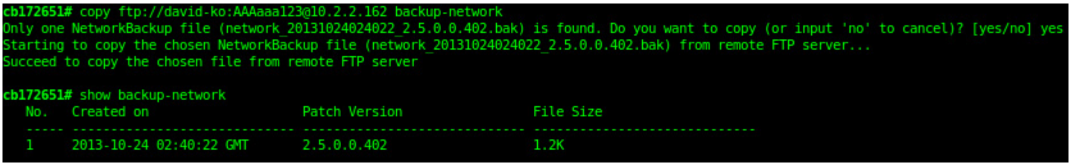
5 If multiple backup files exist on the FTP server, the CLI prompts you to select the number that corresponds to the file that you want to copy back to the controller. If a single backup file exists, the CLI prompts you to confirm that you want to copy the existing backup file to the controller.

When the controller finishes copying the selected backup file from the FTP server back to the controller, the following message appears:

```
Succeed to copy the chosen file from the remote FTP server
```

6 Enter `show backup-network` to verify that the backup file was copied back to the controller successfully.

Figure 207. Verify that the backup file was copied to the controller successfully



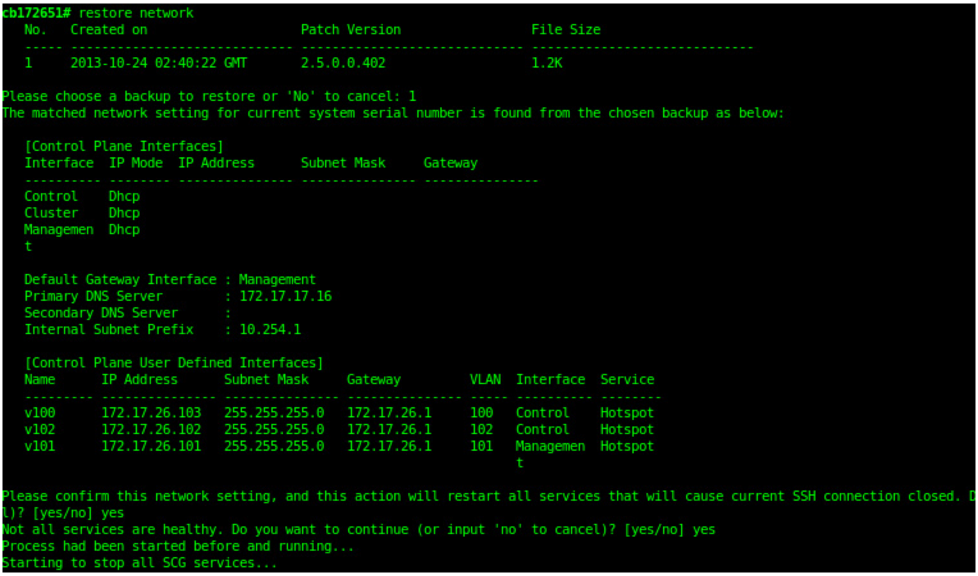
```
cb172651# copy ftp://david-ko:AAAaaa123@10.2.2.162 backup-network
Only one NetworkBackup file (network_20131024024022_2.5.0.0.402.bak) is found. Do you want to copy (or input 'no' to cancel)? [yes/no] yes
Starting to copy the chosen NetworkBackup file (network_20131024024022_2.5.0.0.402.bak) from remote FTP server...
Succeed to copy the chosen file from remote FTP server

cb172651# show backup-network
   No.   Created on                    Patch Version                 File Size
   ----- ----------------------------- ----------------------------- -----------------------------
   1     2013-10-24 02:40:22 GMT       2.5.0.0.402                   1.2K
```

7 Run **`restore network`** to start restoring the contents of the backup file to the current controller. The CLI displays a list of backup files, and then prompts you to select the backup file that you want to restore to the controller.

8 Enter the number that corresponds to the backup file that you want to restore. The CLI displays the network configuration that the selected backup file contains.

If the serial number of the current controller matches the serial number contained in one of the backup files, the CLI automatically selects the backup file to restore and displays the network configuration that it contains.

Figure 208. Enter the number that corresponds to the backup file that you want to restore



```
cb172651# restore network
   No.   Created on                   Patch Version                File Size
   ----- ---------------------------- ---------------------------- ----------------------------
   1     2013-10-24 02:40:22 GMT      2.5.0.0.402                  1.2K

Please choose a backup to restore or 'No' to cancel: 1
The matched network setting for current system serial number is found from the chosen backup as below:

   [Control Plane Interfaces]
   Interface  IP Mode  IP Address      Subnet Mask     Gateway
   ---------- -------- --------------- --------------- --------------
   Control    Dhcp
   Cluster    Dhcp
   Managemen  Dhcp
   t

   Default Gateway Interface : Management
   Primary DNS Server        : 172.17.17.16
   Secondary DNS Server      :
   Internal Subnet Prefix    : 10.254.1

   [Control Plane User Defined Interfaces]
   Name      IP Address      Subnet Mask     Gateway         VLAN  Interface  Service
   --------- --------------- --------------- --------------- ----- ---------- --------
   v100      172.17.26.103   255.255.255.0   172.17.26.1     100   Control    Hotspot
   v102      172.17.26.102   255.255.255.0   172.17.26.1     102   Control    Hotspot
   v101      172.17.26.101   255.255.255.0   172.17.26.1     101   Managemen  Hotspot
                                                                   t

Please confirm this network setting, and this action will restart all services that will cause current SSH connection closed. D
l)? [yes/no] yes
Not all services are healthy. Do you want to continue (or input 'no' to cancel)? [yes/no] yes
Process had been started before and running...
Starting to stop all SCG services...
```

9 Type **`yes`** to confirm that you want to restore the selected backup file. The controller starts the restore process and performs the following steps:

a Stop all services.

b Back up the current network configuration. This will enable the controller to roll back to the current configuration, in case there is an issue with the restore process.

c Clean up the current network configuration. The controller deletes its previous network configuration, including static routes, name server, user defined interfaces, etc.

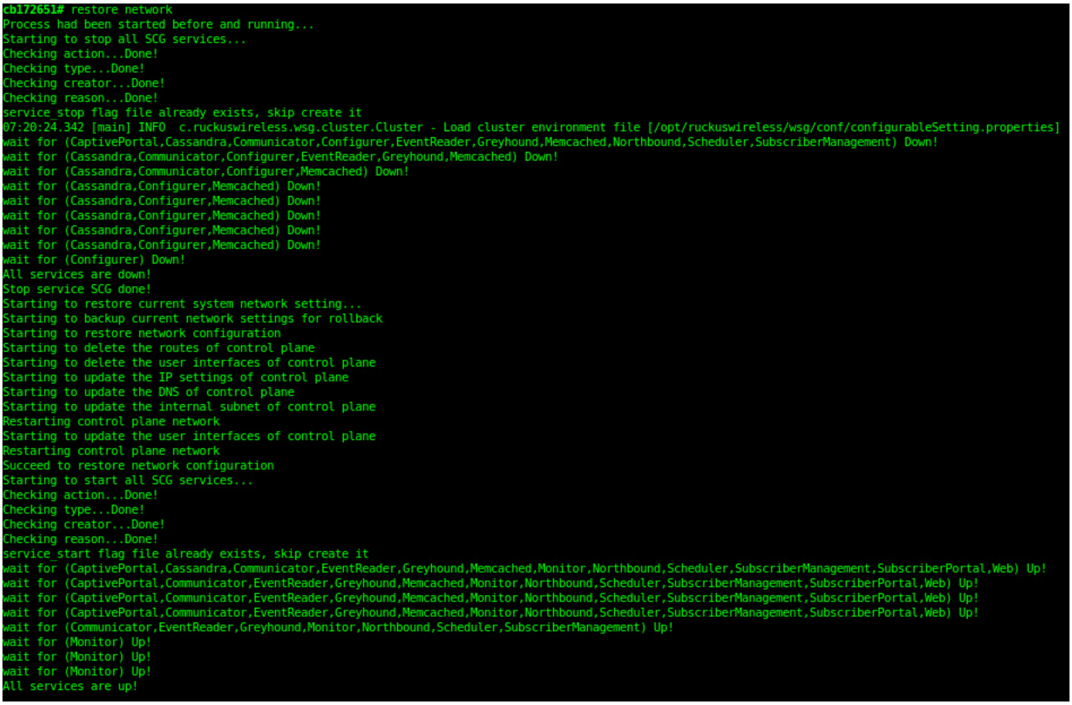
d Restore the network configuration contained in the selected backup file.

e Restart all services.

When the restore process is complete, the following message appears on the CLI:

```
All services are up!
```

Figure 209. The controller performs several steps to restore the backup file

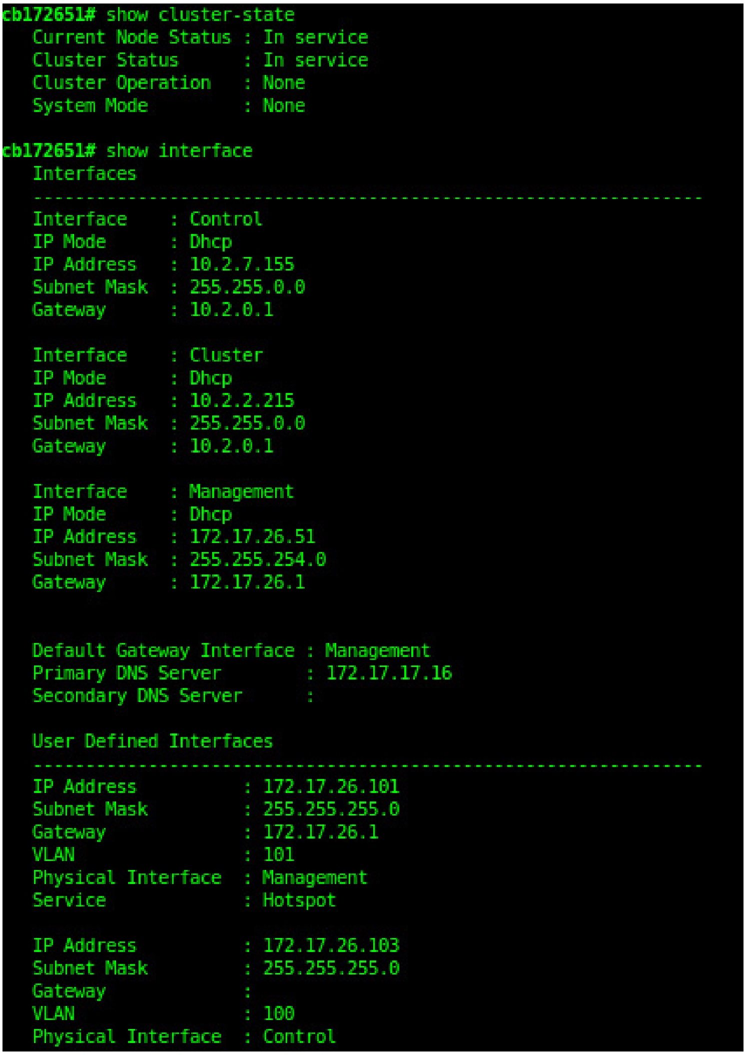


```
cb172651# restore network
Process had been started before and running...
Starting to stop all SCG services...
Checking action...Done!
Checking type...Done!
Checking creator...Done!
Checking reason...Done!
service_stop flag file already exists, skip create it
07:20:24.342 [main] INFO  c.ruckuswireless.wsg.cluster.Cluster - Load cluster environment file [/opt/ruckuswireless/wsg/conf/configurableSetting.properties]
wait for (CaptivePortal,Cassandra,Communicator,Configurer,EventReader,Greyhound,Memcached,Northbound,Scheduler,SubscriberManagement) Down!
wait for (Cassandra,Communicator,Configurer,EventReader,Greyhound,Memcached) Down!
wait for (Cassandra,Communicator,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Configurer) Down!
All services are down!
Stop service SCG done!
Starting to restore current system network setting...
Starting to backup current network settings for rollback
Starting to restore network configuration
Starting to delete the routes of control plane
Starting to delete the user interfaces of control plane
Starting to update the IP settings of control plane
Starting to update the DNS of control plane
Starting to update the internal subnet of control plane
Restarting control plane network
Starting to update the user interfaces of control plane
Restarting control plane network
Succeed to restore network configuration
Starting to start all SCG services...
Checking action...Done!
Checking type...Done!
Checking creator...Done!
Checking reason...Done!
service_start flag file already exists, skip create it
wait for (CaptivePortal,Cassandra,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (Communicator,EventReader,Greyhound,Monitor,Northbound,Scheduler,SubscriberManagement) Up!
wait for (Monitor) Up!
wait for (Monitor) Up!
wait for (Monitor) Up!
All services are up!
```

10 Do the following to verify that the restore process was completed successfully:

- Run **`show cluster-state`** to verify that the node and the cluster are back in service.
- Run **`show interface`** to verify that all of the network configuration settings have been restored.

Figure 210. Verify that the node and cluster are back in service and that the network configuration has been restored successfully



```
cb172651# show cluster-state
   Current Node Status : In service
   Cluster Status      : In service
   Cluster Operation   : None
   System Mode         : None

cb172651# show interface
   Interfaces
   ----------------------------------------------------------------
   Interface    : Control
   IP Mode      : Dhcp
   IP Address   : 10.2.7.155
   Subnet Mask  : 255.255.0.0
   Gateway      : 10.2.0.1

   Interface    : Cluster
   IP Mode      : Dhcp
   IP Address   : 10.2.2.215
   Subnet Mask  : 255.255.0.0
   Gateway      : 10.2.0.1

   Interface    : Management
   IP Mode      : Dhcp
   IP Address   : 172.17.26.51
   Subnet Mask  : 255.255.254.0
   Gateway      : 172.17.26.1


   Default Gateway Interface : Management
   Primary DNS Server        : 172.17.17.16
   Secondary DNS Server      :

   User Defined Interfaces
   ----------------------------------------------------------------
   IP Address          : 172.17.26.101
   Subnet Mask         : 255.255.255.0
   Gateway             : 172.17.26.1
   VLAN                : 101
   Physical Interface  : Management
   Service             : Hotspot

   IP Address          : 172.17.26.103
   Subnet Mask         : 255.255.255.0
   Gateway             :
   VLAN                : 100
   Physical Interface  : Control
```

You have completed importing and applying the network configuration backup from the FTP server to the controller.

Backing Up and Restoring System Configuration

Ruckus Wireless strongly recommends that you back up the controller database periodically. This will help ensure that you can restore the system configuration settings easily if the database becomes corrupted for any reason.

Table 18 lists the information that is included in the system configuration backup file.

Table 18. What's backed up in the system configuration backup file

Configuration Data	Administration Data	Report Data	Identity Data
• AP zones • 3rd party AP zones • Services and profiles • Packages • System settings • Management domains • Administrator accounts • Mobile virtual network operator accounts	• Cluster backups • System configuration backups • Upgrade settings and history • Uploaded system diagnostic scripts • Installed licenses	• Saved reports • Historical client statistics • Network tunnel statistics	• Created profiles • Generated guest passes •

CAUTION! A system configuration backup does not include control plane settings, data plane settings, and user-defined interface settings.

NOTE: In addition to the web interface, you can also perform system configuration backup and restore from the command line interface of the SCG-200. For more information, see the *SmartCell Gateway 200 Command Line Interface Reference Guide* for this release.

Creating a System Configuration Backup

Follow these steps to create a backup of the controller database.

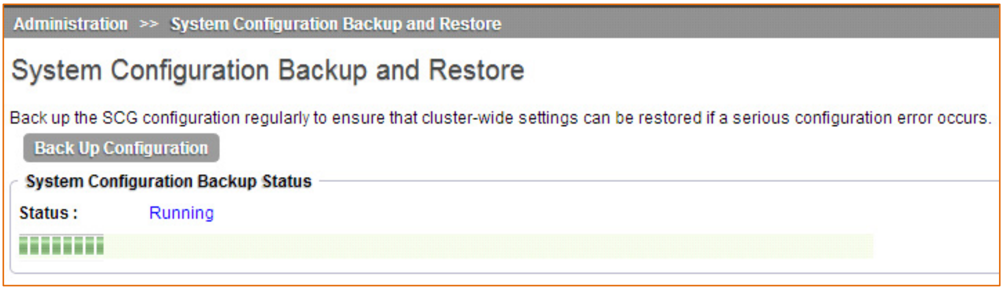
1 Go to **Administration** > **System Configuration Backup and Restore**.

2 Click **Back Up Configuration**. The following confirmation message appears:

```
Are you sure you want to back up the controller's
configuration?
```

3 Click **OK**. A progress bar appears as the controller creates a backup of the its database.

Figure 211. A progress bar appears as the controller backs up its database



Administration >> System Configuration Backup and Restore

System Configuration Backup and Restore

Back up the SCG configuration regularly to ensure that cluster-wide settings can be restored if a serious configuration error occurs.

System Configuration Backup Status

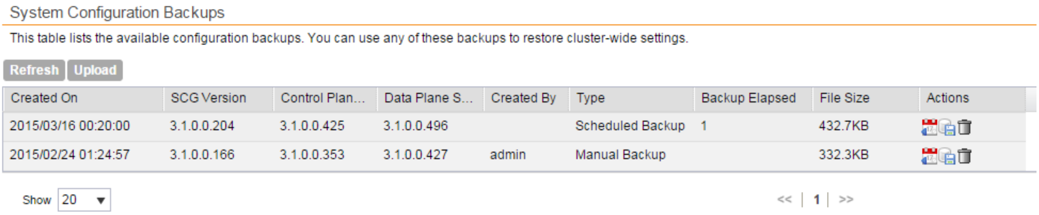
Status : Running

When the backup process is complete, the progress bar disappears, and the *Configuration Backup Status* section appears and shows the following information:

- *Latest backup started*: Date and time when configuration backup was initiated
- *Finished at*: Date and time when configuration backup was completed
- *Status*: Shows either `Successful` or `Failed`
- *Progress Status: Shows the current status of the backup process*

The backup file appears under the *Configuration Backups* section.

Figure 212. The backup file appears in the System Configuration Backups section



System Configuration Backups

This table lists the available configuration backups. You can use any of these backups to restore cluster-wide settings.

Created On	SCG Version	Control Plan...	Data Plane S...	Created By	Type	Backup Elapsed	File Size	Actions
2015/03/16 00:20:00	3.1.0.0.204	3.1.0.0.425	3.1.0.0.496		Scheduled Backup	1	432.7KB	📅 💾 🗑
2015/02/24 01:24:57	3.1.0.0.166	3.1.0.0.353	3.1.0.0.427	admin	Manual Backup		332.3KB	📅 💾 🗑

Exporting the Configuration Backup to an FTP Server Automatically

In addition to backing up the configuration file manually, you can configure the controller to export the configuration file to an FTP server automatically whenever you click **Back Up Configuration**.

Follow these steps to back up the configuration file to an FTP server automatically.

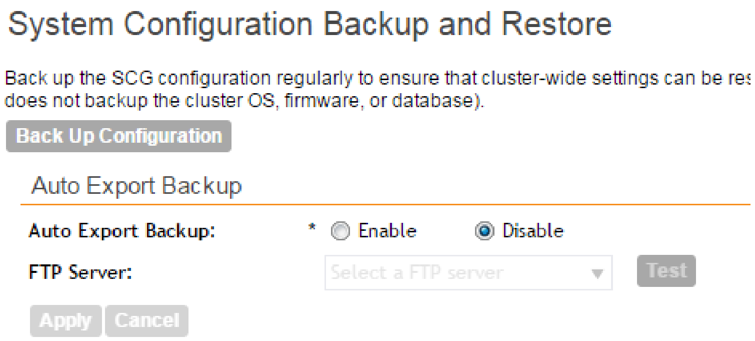
1. Go to **Administration** > **System Configuration Backup and Restore**.
2. Go to the *Auto Export Backup* section.
3. In *Auto Export Backup*, click **Enable**.
4. In *FTP Server,* select the FTP server to which you want to export the backup file. The FTP server options that appear here are those that you created in Configuring FTP Services.
5. Click **Test**. The controller attempts to establish connection to the FTP server using the user name and password that you supplied. If the connection attempt is successful, the following message appears:

   ```
   FTP server connection established successfully.
   ```

   If the connection attempt is unsuccessful, verify that the FTP server details (including the user name and password) are correct, and then click **Test** again.
6. After you verify the controller is able to connect to the FTP server successfully, click **Apply** to save the FTP server settings.

You have completed configuring the controller to export the configuration backup file to an FTP server. When you click the **Back Up Configuration** button (see Creating a System Configuration Backup), a copy of the configuration backup will be uploaded to the FTP server automatically.

Figure 213. Configure the FTP server settings in the Auto Export Backup section



System Configuration Backup and Restore

Back up the SCG configuration regularly to ensure that cluster-wide settings can be res
does not backup the cluster OS, firmware, or database).

Auto Export Backup

Auto Export Backup: * ○ Enable ● Disable

FTP Server: Select a FTP server ▾

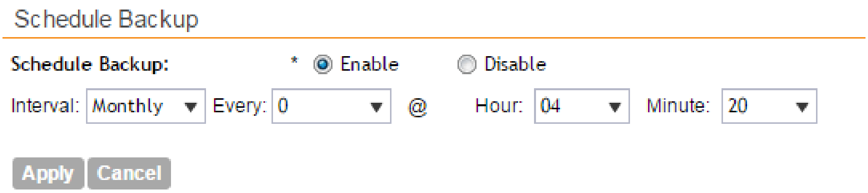
Scheduling a Configuration Backup

You also have the option to configure the controller to backup its configuration automatically based on a schedule you specify. Follow these steps to schedule a configuration backup.

1. Go to *Administration* > *System Configuration Backup and Restore*.
2. Scroll down to the *Schedule Backup* section.
3. In *Schedule Backup*, click **Enable**.
4. In *Interval*, set the schedule when the controller will automatically create a backup of its configuration. Options include:
   - Daily
   - Weekly
   - Monthly
5. Define the schedule further by configuring the following options:
   - Every: If you selected **Weekly** in the previous step, select the day of the week when the controller will generate the backup. If you selected **Monthly**, select the day of the month.
   - Hour: Select the hour of the day when the controller will generate the backup.
   - Minute: Select the minute of the hour.
6. Click **Apply**.

You have completed configuring the controller to create a backup automatically. When a scheduled configuration backup is generated, it appears in the *System Configuration Backups* section.

Figure 214. Configure the schedule in the Schedule Backup section



Schedule Backup

Schedule Backup: * ◉ Enable ○ Disable

Interval: Monthly Every: 0 @ Hour: 04 Minute: 20

Downloading a Copy of the Configuration Backup

After you create a configuration backup, you have the option to download the backup file from the *System Configuration Backups* section. Follow these steps to download the backup file to the computer that you are using to access the controller web interface.

1 Go to *Administration* > *System Configuration Backup and Restore.*

2 Scroll down to the *System Configuration Backups* section.

3 Locate the entry for the backup file that you want to download. If multiple backup files appear on the list, use the date when you created the backup to find the backup entry that you want.

4 Click the 💾 icon that is in the same row as the backup file that you want to download.

Your web browser downloads the backup file to its default download folder.

NOTE: When your web browser completes downloading the backup file, you may see a notification at the bottom of the page, similar to what is shown in Table 215.

---

5 Check the default download folder for your web browser and look for a file that resembles the following naming convention:

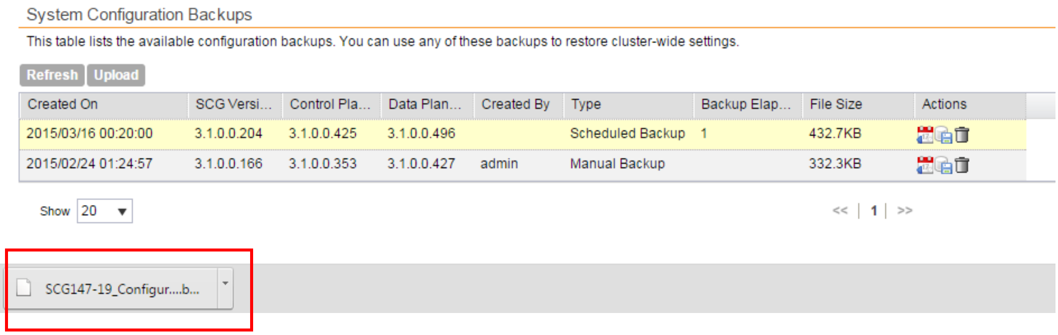
```
{Cluster Name}_Backup-
Conf_{MMdd}_db_{MM}_{dd}_{HH}_{mm}.bak
```

For example, if the controller cluster is named `ClusterA` and you created the configuration backup on September 7 at 11:08 AM, the backup file name will be:

```
ClusterA_BackupConf_0907_db_09_07_11_08.bak
```

You have completed downloading a copy of the configuration backup.

Figure 215. When your browser completes downloading the backup file, you may see a notification at the bottom of the web page



System Configuration Backups

This table lists the available configuration backups. You can use any of these backups to restore cluster-wide settings.

Created On	SCG Versi...	Control Pla...	Data Plan...	Created By	Type	Backup Elap...	File Size	Actions
2015/03/16 00:20:00	3.1.0.0.204	3.1.0.0.425	3.1.0.0.496		Scheduled Backup	1	432.7KB	📅 ⧉ 🗑
2015/02/24 01:24:57	3.1.0.0.166	3.1.0.0.353	3.1.0.0.427	admin	Manual Backup		332.3KB	📅 ⧉ 🗑

Restoring a System Configuration Backup

Follow these steps to restore a backup controller database.

1 Go to **Administration** > **System Configuration Backup and Restore**.

2 In the *System Configuration Backups* section, locate the backup file that you want to restore.

3 Once you locate the backup file, click the 📅 icon that is in the same row as the backup file. A confirmation message appears.

NOTE: Take note of the backup version that you are using. At the end of this procedure, you will use the backup version to verify that the restore process was completed successfully.

4 Click **Yes**. The following message appears:

```
System is restoring. Please wait...
```

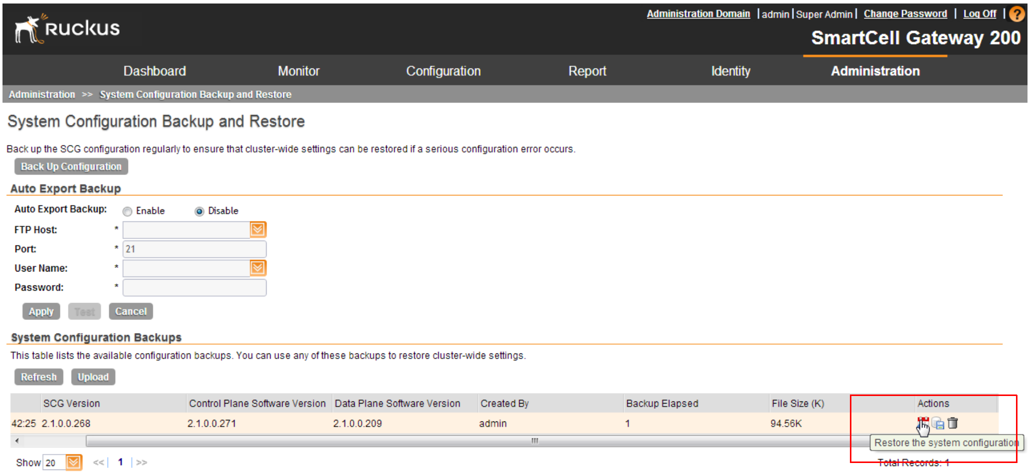
When the restore process is complete, the controller logs you off the web interface automatically.

5 Log on to the controller web interface.

6 Check the web interface pages (for example, Configuration, Report, and Identity) and verify that the setting and data contained in the backup file have been restored successfully to the controller.

You have completed restoring a system configuration backup file.

Figure 216. Under the Actions column, click the configuration restore icon


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Administration >> System Configuration Backup and Restore

System Configuration Backup and Restore

Back up the SCG configuration regularly to ensure that cluster-wide settings can be restored if a serious configuration error occurs.

Back Up Configuration

Auto Export Backup

Auto Export Backup: ○ Enable ● Disable

FTP Host: *

Port: * 21

User Name: *

Password: *

Apply Test Cancel

System Configuration Backups

This table lists the available configuration backups. You can use any of these backups to restore cluster-wide settings.

Refresh Upload

	SCG Version	Control Plane Software Version	Data Plane Software Version	Created By	Backup Elapsed	File Size (K)	Actions
42:25	2.1.0.0.268	2.1.0.0.271	2.1.0.0.209	admin	1	94.56K	

Restore the system configuration

Show 20 << | 1 | >>

Total Records: 1

Deleting a Configuration Backup

Follow these steps to delete a backup of the controller database

1 Go to **Administration** > **System Configuration Backup and Restore**.

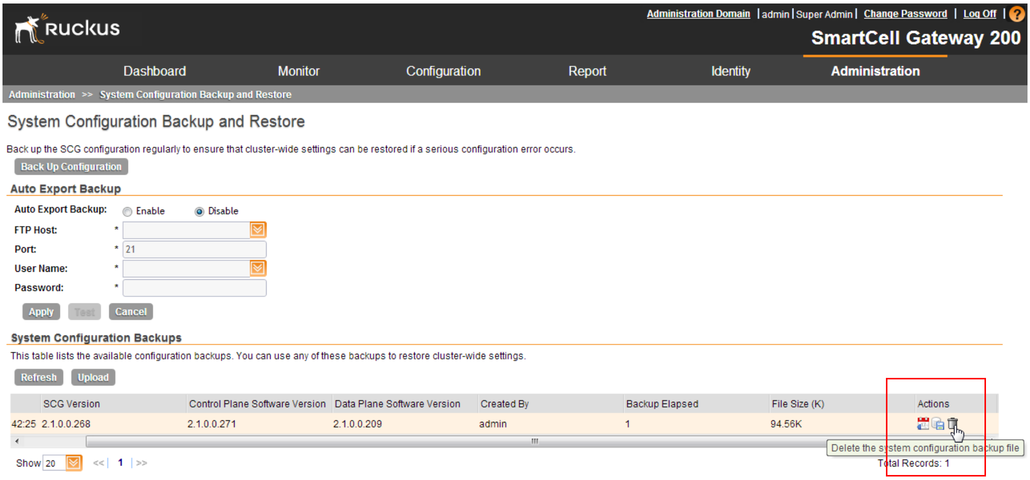
2 In the *System Configuration Backups* section, locate the backup version that you want to delete.

3 Once you locate the backup file, click the 🗑 icon under the *Actions* column. A confirmation message appears.

4 Click **Yes**. The page refreshes, and the backup file that you deleted disappears from the *System Configuration Backups* section.

You have completed deleting a backup file.

Figure 217. Under the Actions column, click the trash bin icon


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Administration >> System Configuration Backup and Restore

System Configuration Backup and Restore

Back up the SCG configuration regularly to ensure that cluster-wide settings can be restored if a serious configuration error occurs.

Back Up Configuration

Auto Export Backup

Auto Export Backup: ○ Enable ● Disable
FTP Host: *
Port: * 21
User Name: *
Password: *

Apply Test Cancel

System Configuration Backups

This table lists the available configuration backups. You can use any of these backups to restore cluster-wide settings.

Refresh Upload

	SCG Version	Control Plane Software Version	Data Plane Software Version	Created By	Backup Elapsed	File Size (K)	Actions
42:25	2.1.0.0.268	2.1.0.0.271	2.1.0.0.209	admin	1	94.56K	

Delete the system configuration backup file

Show 20 << | 1 | >>

Total Records: 1

Resetting a Node to Factory Settings

NOTE: The information in this section only applies to the SCG-200.

You can reset a node in a cluster to factory settings by removing it from the cluster. When you reset a node to factory settings, all of its system configuration settings are completely erased and its IP address reverts to 192.168.2.2.

There are two methods to reset a node to factory settings:

- Using the Web Interface
- Using the CLI

CAUTION! Resetting a node to factory settings will erase all of its system configuration settings, backup files, and cluster settings. Before resetting a node to factory settings, Ruckus Wireless strongly recommends that you export all of the backup files on the controller to an FTP server using either the web interface or CLI.

What Happens After Reset to Factory Settings

Before resetting a node to factory settings, consider the following notes:

- All of the system configuration settings of the node will be erased. This includes all of the domain, AP zone, user, and system settings, as well as all of the controller backups.
- The node will revert to its default IP address – 192.168.2.2.
- The controller software version will not be reset to its original software version when you first set it up. It will keep the existing software version at the time you reset it to factory settings.

Using the Web Interface

To remove a node from a cluster, it must be a follower node. If the node that you want to remove from the cluster is the leader node, make sure you demote it to a follower node first before continuing with this procedure.

Follow these steps to remove a node from the cluster and reset it to factory settings.

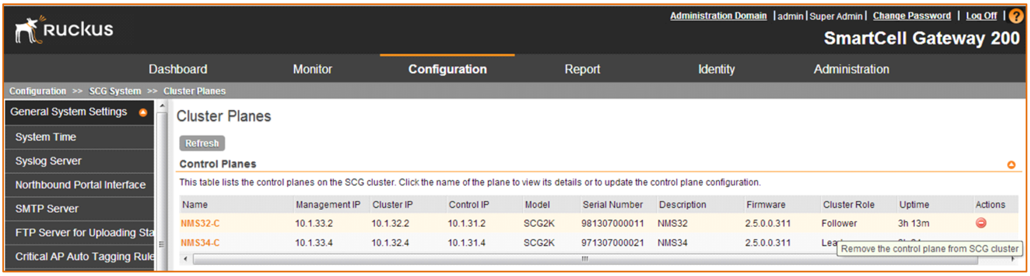
1. Log on to the controller web interface of the leader node.
2. Go to *Configuration* > *System* > *Cluster Planes*. The *Cluster Planes* page appears.
3. In the *Control Planes* table, locate the node that you want to reset to factory settings.
4. Click the ⊖ icon that is in the same row as the node that you want to reset to factory settings. A confirmation message appears.
5. Click **Yes**. The page refreshes, and then the node that you deleted disappears from the *Control Plane* table.

You have completed removing a node from the cluster and resetting it to factory settings.

NOTE: To set up this controller again, access the controller setup wizard `http://192.168.2.2:8080`. See the *SCG-200 Getting Started Guide* for more information.

NOTE: After the controller is reset to factory settings, the controller allows the data blade interface IP address and gateway address to be on different subnets.

Figure 218. Click the delete icon


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Identity
Administration
Configuration >> SCG System >> Cluster Planes
General System Settings
System Time
Syslog Server
Northbound Portal Interface
SMTP Server
FTP Server for Uploading Sta
Critical AP Auto Tagging Rule
Refresh
Remove the control plane from SCG cluster

Cluster Planes

Control Planes

This table lists the control planes on the SCG cluster. Click the name of the plane to view its details or to update the control plane configuration.

Name	Management IP	Cluster IP	Control IP	Model	Serial Number	Description	Firmware	Cluster Role	Uptime	Actions
NMS32-C	10.1.33.2	10.1.32.2	10.1.31.2	SCG2K	981307000011	NMS32	2.5.0.0.311	Follower	3h 13m	⊖
NMS34-C	10.1.33.4	10.1.32.4	10.1.31.4	SCG2K	971307000021	NMS34	2.5.0.0.311	Lea		

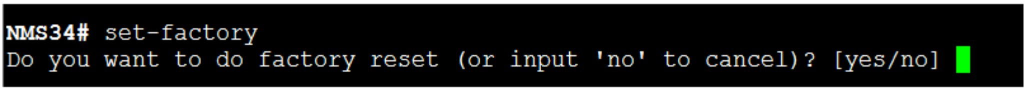
Using the CLI

You can also use the command line interface to remove a node from a cluster and reset it to factory settings. See Accessing the Command Line Interface for information on how to gain access to the CLI.

After you log on to the CLI of the node, follow these steps to reset a node to factory settings.

1 At the prompt, enter **set-factory**. A confirmation message appears.

Figure 219. Enter set-factory to reset the node to factory settings



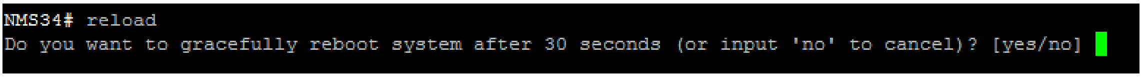
```
NMS34# set-factory
Do you want to do factory reset (or input 'no' to cancel)? [yes/no]
```

2 Enter **yes** to confirm.

3 Enter **reload**. This command is required to trigger the factory reset process. A confirmation message appears.

4 Enter **yes** to confirm. The controller reboots, and then triggers the factory reset process.

Figure 220. Enter reload to trigger the factory reset process



```
NMS34# reload
Do you want to gracefully reboot system after 30 seconds (or input 'no' to cancel)? [yes/no]
```

The controller reboots. You have completed resetting the node to factory default settings.

Upgrading the Controller

Ruckus Wireless may periodically release controller software updates that contain new features, enhancements, and fixes for known issues. These software updates may be made available on the Ruckus Wireless support website or released through authorized channels.

This section covers the following topics:

- Performing the Upgrade
- Verifying the Upgrade
- Rolling Back to a Previous Software Version

CAUTION! Although the software upgrade process has been designed to preserve all controller settings, Ruckus Wireless strongly recommends that you back up the controller cluster before performing an upgrade. Having a cluster backup will ensure that you can easily restore the controller system if the upgrade process fails for any reason. For information on how to back up the controller cluster, refer to Creating a Cluster Backup.

CAUTION! Ruckus Wireless strongly recommends that you ensure that all interface cables are intact during the upgrade procedure.

CAUTION! Ruckus Wireless strongly recommends that you ensure that the power supply is not disrupted during the upgrade procedure.

NOTE: If you are managing an SCG-200, you can also perform system configuration backup, restore, and upgrade from the controller command line interface. For more information, see the *SmartCell Gateway 200 Command Line Interface Reference Guide*.

Performing the Upgrade

Follow these steps to upgrade the controller software.

CAUTION! Ruckus Wireless strongly recommends backing up the controller cluster before performing the upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster. See Backing Up and Restoring Clusters.

NOTE: Before starting this procedure, you should have already obtained a valid controller software upgrade file from Ruckus Wireless Support or an authorized reseller.

1 Copy the software upgrade file that you received from Ruckus Wireless to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.

2 Go to **Administration** > **Upgrade**.

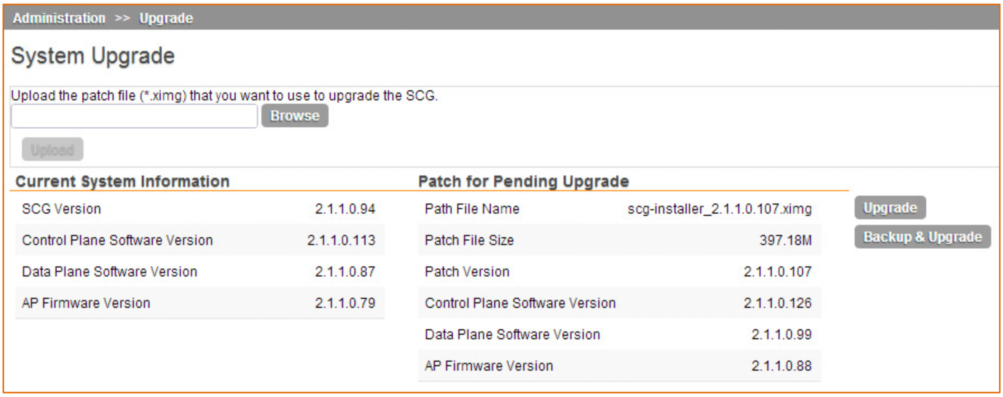
3 In the *Patch File Upload* section, click the **Browse** button, and then browse to the location of the software upgrade file. Typically, the file name of the software upgrade file is
`scg-installer_{version}.ximg.`

4 Select the software upgrade file, and then click **Open**.

5 Click **Upload** to upload the software upgrade file. The controller uploads the file to its database, and then performs file verification.

After the file is verified, the *Upgrade Pending Patch Information* section is populated with information about the upgrade file. The **Upgrade** and **Backup & Upgrade** buttons also appear in this section.

Figure 221. The “Upgrade” and “Backup & Upgrade” button appear on the right side



System Upgrade

Upload the patch file (*.ximg) that you want to use to upgrade the SCG.

Current System Information

SCG Version	2.1.1.0.94
Control Plane Software Version	2.1.1.0.113
Data Plane Software Version	2.1.1.0.87
AP Firmware Version	2.1.1.0.79

Patch for Pending Upgrade

Path File Name	scg-installer_2.1.1.0.107.ximg
Patch File Size	397.18M
Patch Version	2.1.1.0.107
Control Plane Software Version	2.1.1.0.126
Data Plane Software Version	2.1.1.0.99
AP Firmware Version	2.1.1.0.88

6 Start the upgrade process by clicking one of the following buttons:

- **Upgrade**: Click this button to start the upgrade process without backing up the current controller cluster or its system configuration.

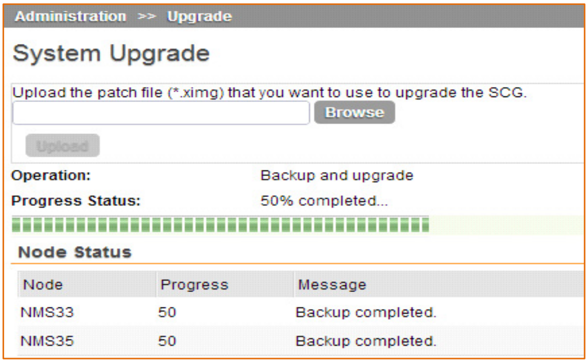
- **Backup & Upgrade**: Click this button to back up the controller cluster and system configuration before performing the upgrade.

CAUTION! Ruckus Wireless strongly recommends usage of backup and upgrade icon while performing the upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster. See Backing Up and Restoring Clusters.

A confirmation message appears.

7 Click **Yes**. The controller starts the process that you selected. The screens that appear next will depend on the process that you selected to upgrade immediately or to back up and then upgrade the controller.

Figure 222. “Backup completed” status if you selected Backup & Upgrade



System Upgrade

Upload the patch file (*.ximg) that you want to use to upgrade the SCG.

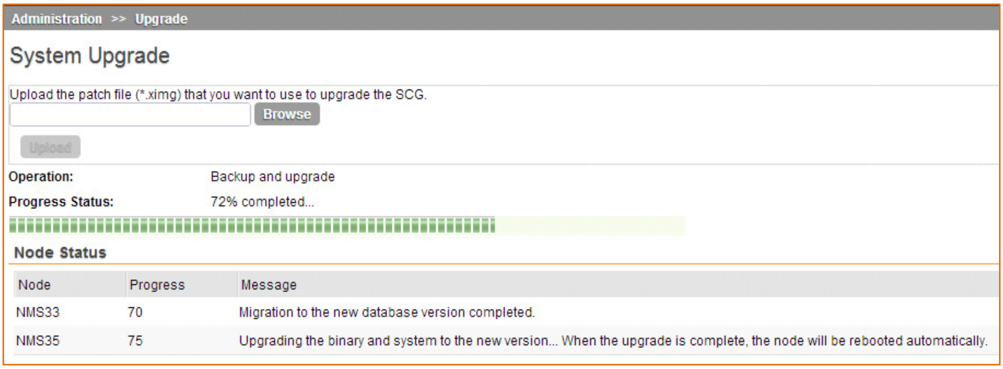
Operation: Backup and upgrade

Progress Status: 50% completed...

Node Status

Node	Progress	Message
NMS33	50	Backup completed.
NMS35	50	Backup completed.

Figure 223. The System Upgrade page displays the status of the upgrade process



System Upgrade

Upload the patch file (*.ximg) that you want to use to upgrade the SCG.

Operation: Backup and upgrade

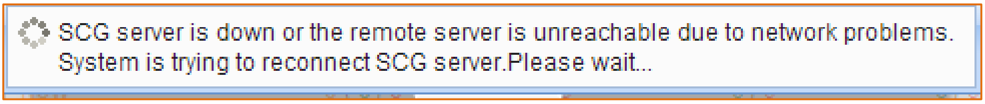
Progress Status: 72% completed...

Node Status

Node	Progress	Message
NMS33	70	Migration to the new database version completed.
NMS35	75	Upgrading the binary and system to the new version... When the upgrade is complete, the node will be rebooted automatically.

When the upgrade (or backup-and-upgrade) process is complete, the controller logs you off the web interface automatically. The controller web interface may display the message shown in Figure 224 as it completes the upgrade process. Wait for a few minutes until the web interface log on page appears.

Figure 224. The controller web interface may display the following message as it completes the upgrade process



SCG server is down or the remote server is unreachable due to network problems. System is trying to reconnect SCG server.Please wait...

When the controller log on page appears again, you have completed upgrading the controller. Continue to Verifying the Upgrade to check if the upgrade was completed successfully.

Verifying the Upgrade

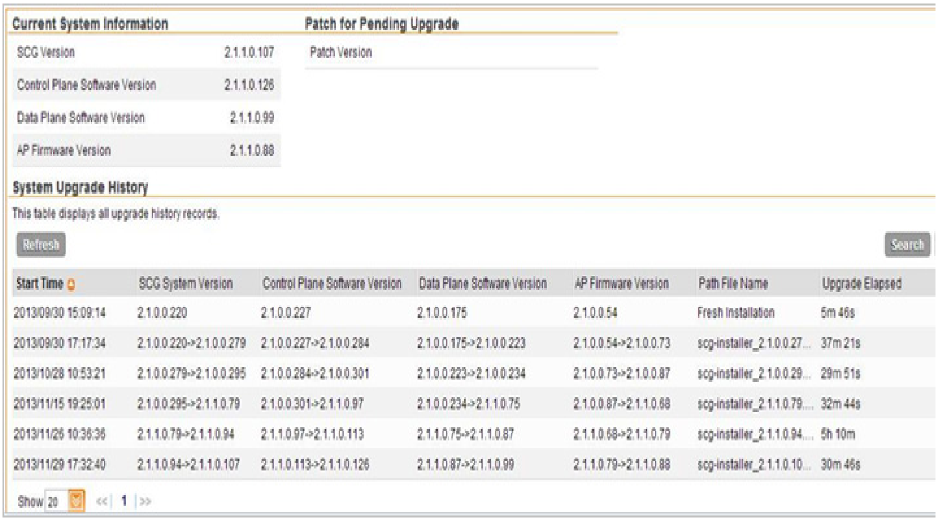
Follow these steps to verify that the controller upgrade was completed successfully.

1 Log on to the controller web interface.

2 Go to **Administration** > **Upgrade**.

3 In the *Current System Information* section, check the value for *Controller Version*. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

Figure 225. Check the value for controller Version



Current System Information

SCG Version	2.1.1.0.107
Control Plane Software Version	2.1.1.0.126
Data Plane Software Version	2.1.1.0.99
AP Firmware Version	2.1.1.0.88

Patch for Pending Upgrade

Patch Version

System Upgrade History

This table displays all upgrade history records.

Start Time	SCG System Version	Control Plane Software Version	Data Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2013/09/30 15:09:14	2.1.0.0.220	2.1.0.0.227	2.1.0.0.175	2.1.0.0.54	Fresh Installation	5m 46s
2013/09/30 17:17:34	2.1.0.0.220->2.1.0.0.279	2.1.0.0.227->2.1.0.0.284	2.1.0.0.175->2.1.0.0.223	2.1.0.0.54->2.1.0.0.73	scg-installer_2.1.0.0.27...	37m 21s
2013/10/28 10:53:21	2.1.0.0.279->2.1.0.0.295	2.1.0.0.284->2.1.0.0.301	2.1.0.0.223->2.1.0.0.234	2.1.0.0.73->2.1.0.0.87	scg-installer_2.1.0.0.29...	29m 51s
2013/11/15 19:25:01	2.1.0.0.295->2.1.1.0.79	2.1.0.0.301->2.1.1.0.97	2.1.0.0.234->2.1.1.0.75	2.1.0.0.87->2.1.1.0.68	scg-installer_2.1.1.0.79....	32m 44s
2013/11/26 10:36:36	2.1.1.0.79->2.1.1.0.94	2.1.1.0.97->2.1.1.0.113	2.1.1.0.75->2.1.1.0.87	2.1.1.0.68->2.1.1.0.79	scg-installer_2.1.1.0.94....	5h 10m
2013/11/29 17:32:40	2.1.1.0.94->2.1.1.0.107	2.1.1.0.113->2.1.1.0.126	2.1.1.0.87->2.1.1.0.99	2.1.1.0.79->2.1.1.0.88	scg-installer_2.1.1.0.10...	30m 46s

Rolling Back to a Previous Software Version

There are two scenarios in which you may want to roll back the controller software to a previous version:

1 You encounter issues during the software upgrade process and the controller cannot be upgraded successfully. In this scenario, you can only perform the software rollback from the CLI using the `restore local` command. If you have a two-node controller cluster, run the `restore local` command on each of the nodes to restore them to the previous software before attempting to upgrade them again.

2 You prefer a previous software version to the newer version to which you have upgraded successfully. For example, you feel that the controller does not operate normally after you upgraded to the newer version and you want to restore the previous software version, which was more stable. In this scenario, you can perform the software rollback either from the web interface or the CLI. If you have a two-node controller cluster, you must have cluster backup on both of the nodes.

To ensure that you will be able to roll back to a previous version, Ruckus Wireless strongly recommends the following before attempting to upgrade the controller software:

- Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully. See Creating a Cluster Backup for the local backup instructions. If you have a local backup and you want to roll back the controller to a previous software version, follow the same procedure described in Restoring a Cluster Backup.
- If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server. See Backing Up to an FTP Server for remote backup instructions and Restoring from an FTP Server for remote restore instructions.

Recovering a Cluster from an Unsuccessful Upgrade

If an issue occurs during the upgrade process (for example, a power outage occurs or one of the interfaces goes down), you can recover the cluster if the controller has either a local configuration backup or a remote (FTP) configuration backup.

If the Controller Has Local Configuration Backup

Follow these steps to recover a cluster when the controller has a configuration backup stored locally.

1. Unplug the cluster interface cables of each node in the cluster to isolate each individual node.
2. On each of the nodes in the cluster, perform the following:
   a. Log on to the CLI, and then execute `restore local`. This command will restore the system configuration of the node from a local backup.
   b. When the CLI indicates that the `restore local` command has been completed successfully, plug in the cluster interface cable.

You have completed recovering the controller cluster using a local configuration backup.

If the Controller Has an FTP Backup

Follow these steps to recover a cluster when the controller has a configuration backup on a remote FTP server. See Backing Up to an FTP Server for more information.

You must perform steps on each of the nodes in the cluster.

1. Log on to the CLI of each of the nodes.

2 Execute the **`set-factory`** command to reset the node to factory settings.

NOTE: See Resetting a Node to Factory Settings for more information.

3 Using the CLI, set up the controller as a standalone unit.

4 Copy the cluster configuration backup from the FTP server to the controller.

5 Execute the `restore local` command from the CLI.

6 When the CLI indicates that the `restore local` command has been completed successfully, plug in the cluster interface cable.

Repeat the same procedure until you have restore the cluster configuration backup from the FTP server to all of the nodes in the cluster.

You have completed recovering the controller cluster using an FTP backup.

Working with Logs

This section describes the logs that are available in the controller and how to download them.

- Available System Log Types
- Downloading All Logs
- Downloading Snapshot Logs Generated from the CLI

Available System Log Types

The controller generates logs for all the applications that are running on the server. Table 19 lists the controller applications that are running.

Table 19. Controller applications and log types

Application	Description
AIP	Handles the accounting messages for TTG sessions
CaptivePortal	Performs portal redirect for clients and manages the walled garden and blacklist
Cassandra	The controller's database server that stores most of the run-time information and statistical data
Cassandra client	Used as the interface between processes of the TTG-modules and Cassandra (Persistent Database)
CIP	The Charging Interface module, which handles the Ga interface towards CGF server
CNR	
Communicator	Communicates with access points and retrieves statuses, statistics, and configuration updates
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
DHCPProxy	The DHCP process in SCG-D that proxies DHCP messages to the DHCP server
DHCPServer	The DHCP server in SCG-C TTG module, receives DHCP messages from DHCP relay in d-blade
eAUT	Manages the sessions the SCG-C TTG module
EventReader	Receives event messages from access points and saves the information into the database

Table 19. Controller applications and log types (Continued)

Application	Description
FreeRadius	Relays the access points' RADIUS authentication and accounting requests to the external server
Greyhound	The interface between the SCG-C TTG module and the AP interface, used to send and receive proprietary messages for AP association and disassociation
GTP Stack SM	Module for managing the interfaces towards operator GGSNs and PGWs
HIP	Module with SIGTRAN stack and interface to operator HLR(s)
Kennel	Diagnostic script service that runs the diagnostic scripts in the controller
Memcached	The controller's memory cache that stores client authentication information for fast authentication or roaming
Memcached client	Memcached client used as the interface between processes of TTG-modules and Memcached (Shared memory)
Memproxy	Replicates MemCached entries to other cluster nodes
Monitor	Monitors the health of cluster processes and communicates cluster state changes to the cluster node
NC	The Node Controller, which monitors all SCG-C TTG processes
Net-SNMP	SNMP service
Northbound API	Performs UE authentication and handles approval or denial of UEs to AP
Ntpd	Enables APs to synchronize their time with the parent controller and synchronizes time with an external NTP server and internal controller nodes in the same cluster.
RAC	The RADIUS Authentication module, used for processing RADIUS messages from the AP and the AAA server (CoA,DM)
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
RepCached	Replicates client authentication information to each MemCached server in each cluster node
Resolver	Used by the GTP stack for DNS resolution, retrieves the IP addresses of GGSN and PGW

Table 19. Controller applications and log types (Continued)

Application	Description
Scheduler	Performs task scheduling and aggregates statistical data
SM	
SNMPAgent	Configures SNMP settings and sends SNMP traps
SSHD	The SSD server that establishes sshtunnel and controls port forwarding with AP in the sshtunnel
SubscriberManagement	Maintains local user credentials for WISPr authentication.
SubscriberPortal	Internal portal page for WISPr (hotspot)
Syslog-ng	Collects and sends log information from all processes
Web	Runs the controller management web server
Zapd	Perform SpeedFlex testing

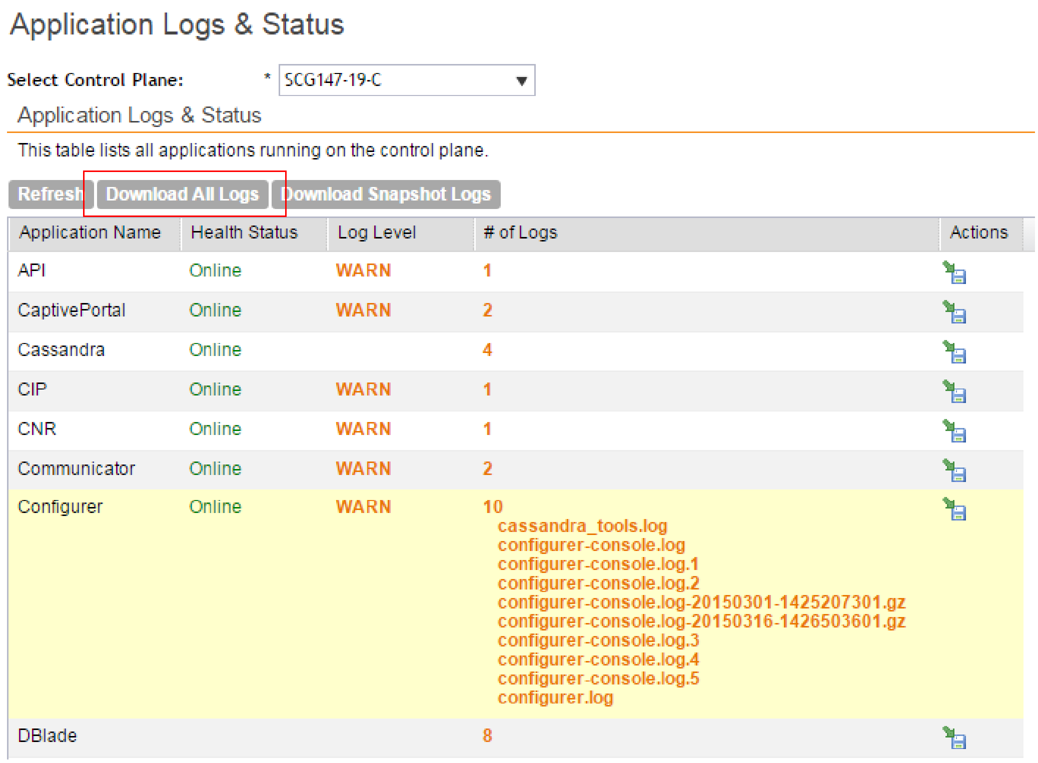
Downloading All Logs

Follow these steps to download all available logs from the controller.

1. Go to **Administration** > **Diagnostics**.
2. On the sidebar, click **Application Logs & Status**.
3. In *Select Control Plane*, select the control plane from which you want to download logs.
4. Click the **Download All Logs** button. Your web browser downloads the logs in GZIP Compressed Tar Archive (with .TGZ extension) to its default download location.
5. Go to your web browser’s default download location and verify that the TGZ file was downloaded successfully.
6. Use your preferred compression/decompression program to extract the log files from the TGZ file.
7. When the log files are extracted (for example, `adminweb.log`, `cassandra.log`, `communicator.log`, etc.), use a text editor to open and view the log contents.

You have completed downloading all the controller logs.

Figure 226. Click the Download All Logs button



Application Logs & Status

Select Control Plane: * SCG147-19-C

Application Logs & Status

This table lists all applications running on the control plane.

Application Name	Health Status	Log Level	# of Logs	Actions
API	Online	WARN	1	💾
CaptivePortal	Online	WARN	2	💾
Cassandra	Online		4	💾
CIP	Online	WARN	1	💾
CNR	Online	WARN	1	💾
Communicator	Online	WARN	2	💾
Configurer	Online	WARN	10 cassandra_tools.log configurer-console.log configurer-console.log.1 configurer-console.log.2 configurer-console.log-20150301-1425207301.gz configurer-console.log-20150316-1426503601.gz configurer-console.log.3 configurer-console.log.4 configurer-console.log.5 configurer.log	💾
DBlade			8	💾

Downloading Snapshot Logs Generated from the CLI

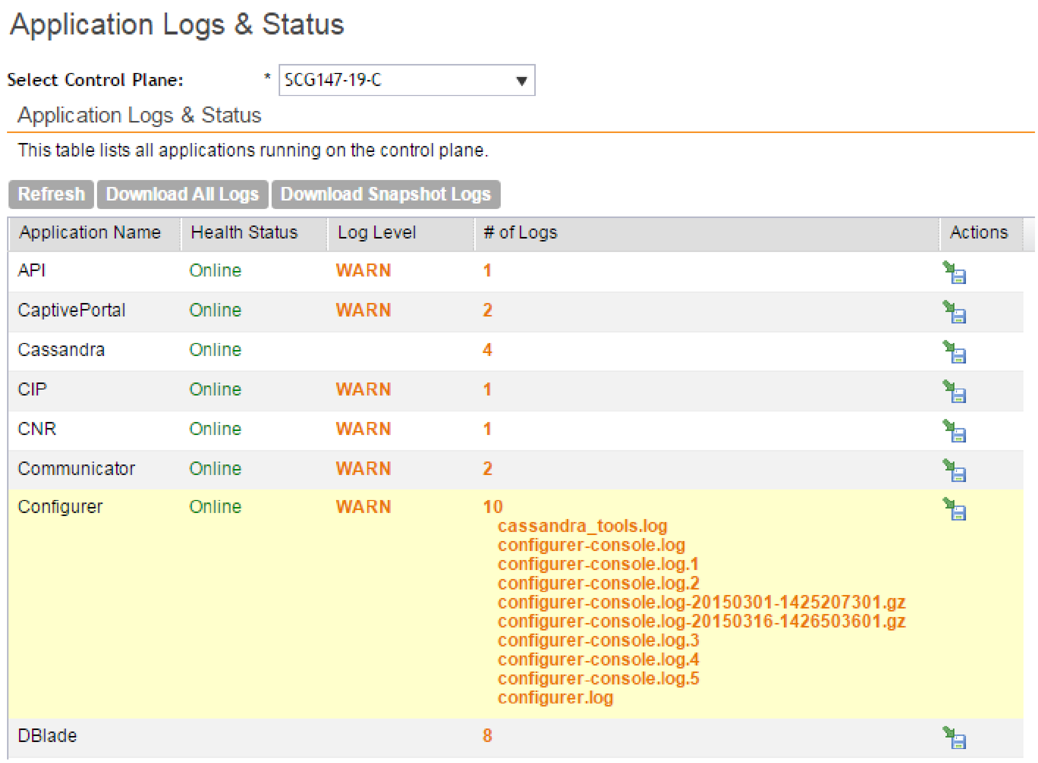
Snapshot logs contain system and configuration information, such as the AP list, configurations settings, event list, communicator logs, SSH tunnel lists, etc. If you triggered the controller to generate a snapshot from the CLI, you have the option to download snapshot logs from the web interface.

Follow these steps to download the CLI-generated snapshot logs from the web interface.

1. On the CLI, trigger the controller to generate a snapshot.
2. Log on to the web interface.
3. Go to *Administration* > *Diagnostics*.
4. On the sidebar, click **Application Logs & Status**.
5. Click **Download Snapshot Logs**. Your web browser downloads a tar (.TGZ) file that contains all available snapshot logs.
6. Go to your browser’s default download folder, and then verify that the snapshot log file or files have been downloaded successfully.
7. Extract the contents of the tar file.

You have completed downloading snapshot logs from the controller.

Figure 227. Click Download Snapshot Logs to download all available snapshot logs



Application Logs & Status

Select Control Plane: * SCG147-19-C

Application Logs & Status

This table lists all applications running on the control plane.

Application Name	Health Status	Log Level	# of Logs	Actions
API	Online	WARN	1	
CaptivePortal	Online	WARN	2	
Cassandra	Online		4	
CIP	Online	WARN	1	
CNR	Online	WARN	1	
Communicator	Online	WARN	2	
Configurer	Online	WARN	10 cassandra_tools.log configurer-console.log configurer-console.log.1 configurer-console.log.2 configurer-console.log-20150301-1425207301.gz configurer-console.log-20150316-1426503601.gz configurer-console.log.3 configurer-console.log.4 configurer-console.log.5 configurer.log	
DBlade			8	

Managing License Files

The maximum number of access points that the controller can manage is controlled by the license file that came with the controller. If the number of access points on the network exceeds the limit in the license file, you will need to obtain an additional license file and upload it to the controller.

NOTE: For information on obtaining additional license files, contact Ruckus Wireless Support or an authorized Ruckus Wireless reseller.

The maximum number of access points that a license supports depends on its stock-keeping unit (SKU). For more information, refer to License SKUs.

This section covers the following topics:

- Uploading a License File

- Viewing License Details
- License SKUs

Uploading a License File

Follow these steps to upload a license file to the controller.

1 Copy the license file that you obtained from Ruckus Wireless to a computer or network location that you can access from the controller web interface.

2 Go to **Administration** > **Licenses**.

3 In the *Upload License* section, click **Browse**. The *Open* dialog box appears.

4 Browse to the location where you saved the license file.

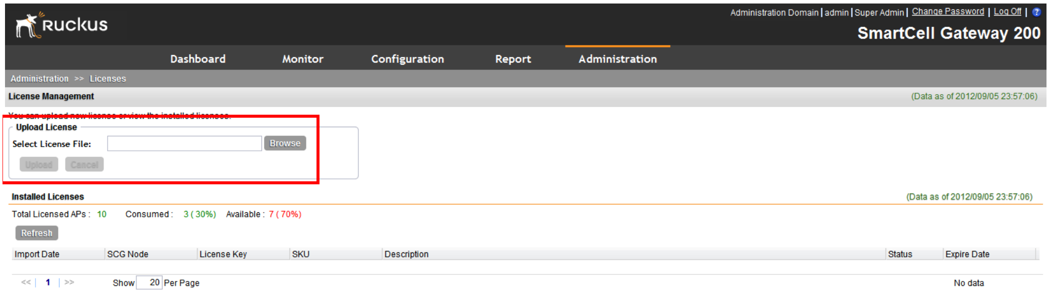
5 Select the license file (with `.LIC` extension), and then click **Open**.

6 Click **Upload**. The controller uploads the license file. When the process is complete, the following message appears:

```
License uploaded successfully.
```

You have completed uploading a license file to the controller.

Figure 228. In the Upload License section, click Browse, and then select the license file



License Management (Data as of 2012/09/05 23:57:06)

You can upload new license or view the installed licenses.

Upload License

Select License File:

Installed Licenses (Data as of 2012/09/05 23:57:06)

Total Licensed APs : 10 Consumed : 3 (30%) Available : 7 (70%)

Import Date	SCG Node	License Key	SKU	Description	Status	Expire Date

No data

Viewing License Details

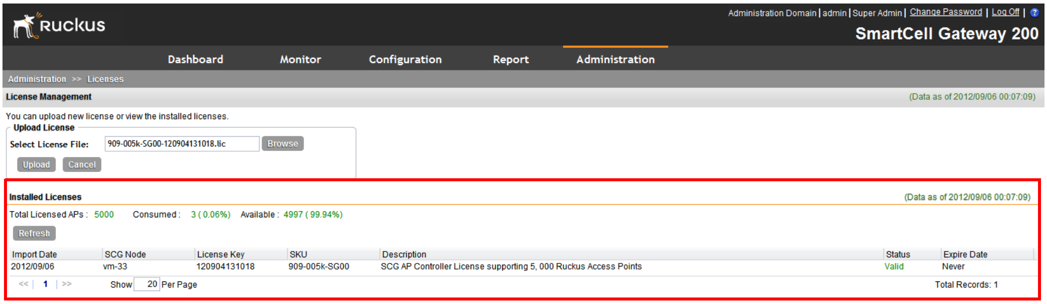
The details of all the licenses that you have uploaded to the controller appear in the *Installed Licenses* section. Details available include:

- *Total Licensed AP*s: The maximum number of access points that can be supported by all the licenses that have been uploaded to the controller.
- *Consumed*: The number of license seats that have been used. One access point uses up one license seat. For example, if three access points have registered with the controller, the *Consumed* field will show `3`.
- *Available*: The number of license seats remaining. For example, if all your licenses support up to 5000 access points, and the controller has used up three licenses so far, the Available field will show `4997`.

Below the **Refresh** button is a table that displays details about the individual license files that you have uploaded to the controller. Details available include:

- *Import Date*: The date when you uploaded the license file to the controller
- *Node*: The specific node (either a control plane or data plane) for which the license file was generated
- *License Key*: The key associated with the license file
- *SKU*: The stock-keeping unit code of the license file. Refer to License SKUs for more information.
- *Description*: Shows the type of license and the number of Ruckus Wireless access points that is supported by the license file
- *Status*: Shows the status of the license file. `Valid` indicates that the controller recognizes that the license file.
- *Expire Date*: The date when the license file expires. You will need to renew the license (or obtain a new one) for the controller to continue managing the access points on the network.

Figure 229. Go to the Installed Licenses section to view the license details


Ruckus
Administration Domain | admin | Super Admin | Change Password | Log Off | ?
SmartCell Gateway 200
Dashboard
Monitor
Configuration
Report
Administration
Administration >> Licenses
Browse
Upload
Cancel
Refresh

License Management (Data as of 2012/09/06 00:07:09)

You can upload new license or view the installed licenses.

Upload License

Select License File: 909-005k-SG00-120904131018.lic

Installed Licenses (Data as of 2012/09/06 00:07:09)

Total Licensed APs : 5000 Consumed : 3 (0.06%) Available : 4997 (99.94%)

Import Date	SCG Node	License Key	SKU	Description	Status	Expire Date
2012/09/06	vm-33	120904131018	909-005k-SG00	SCG AP Controller License supporting 5, 000 Ruckus Access Points	Valid	Never

<< | 1 | >> Show 20 Per Page Total Records: 1

License SKUs

The number of access point that a single license file supports depends on its SKU. Refer to Table 20 for the different license SKUs available and the number of access points that they support.

Table 20. Controller license SKUs

License SKU	Description
909-010K-SG00	Supports up to 10,000 Ruckus Wireless access points
909-005K-SG00	Supports up to 5,000 Ruckus Wireless access points
909-001K-SG00	Supports up to 1,000 Ruckus Wireless access points
909-0500-SG00	Supports up to 500 Ruckus Wireless access points
909-0100-SG00	Supports up to 100 Ruckus Wireless access points

Accessing the Command Line Interface

A

NOTE: The information in this appendix only applies to the SCG-200.

In this appendix:

- About the Command Line Interface
- What You Will Need
- Step 1: Connect the Administrative Computer to the Controller
- Step 2: Start and Configure the SSH Client
- Step 3: Log On to the CLI
- Changing the Management IP Address from the CLI

About the Command Line Interface

The controller has a built-in command line interface (CLI) that you can use to configure controller settings and manage access points. This section describes the requirements and the procedure for accessing the controller CLI.

NOTE: For a complete list of commands that the controller command line interface supports, refer to the *SmartCell Gateway 200 Command Line Interface Reference Guide*.

What You Will Need

To access the controller CLI, you will need the following:

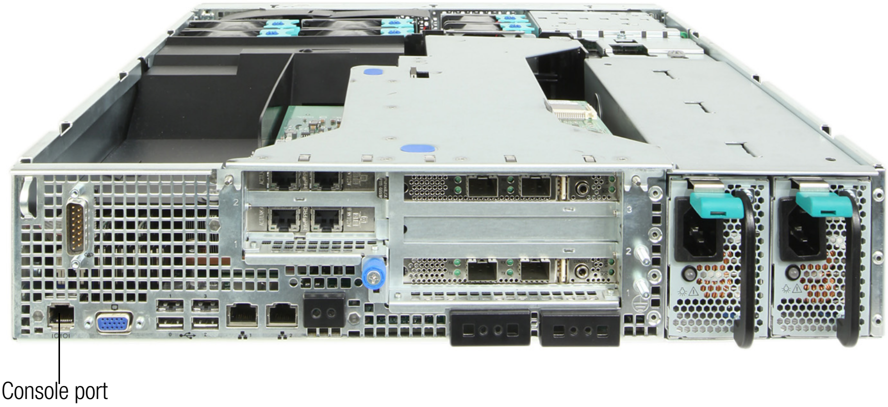
- A computer that you want to designate as administrative computer
- A network connection to the controller (if you want to use an SSH connection) or an RS-232 serial to RJ45 cable (if you want to use a serial connection)
- An SSH (secure shell) client

Step 1: Connect the Administrative Computer to the Controller

Connect the administrative computer to the controller either through the network or directly using an RS-232 serial to RJ45 cable.

- If you want to use an SSH connection, connect the administrative computer to the same subnet or broadcast domain as the controller interface (management or control) to which you want to connect.
- If you want to use a serial connection, make sure that both the administrative computer and the controller are both powered on. And then, do the following:
  - **a** Connect the RJ45 end of the cable to the port labeled **|O|O|** (console port) on the controller. See Figure 230 for the location of the console port.
  - **b** Connect the RS-232 end of the cable to a COM port on the administrative computer.

Figure 230. Console port location



Step 2: Start and Configure the SSH Client

Before starting this procedure, make sure that the SSH client is already installed on the administrative computer.

NOTE: The following procedure describes how to use PuTTY, a free and open source telnet/SSH client, to access the controller CLI. If you are using a different SSH client, the procedure may be slightly different (although the connection settings should be the same). For more information on PuTTY, visit `www.putty.org`.

See the following sections depending on your connection method:

- Using an SSH Connection
- Using a Serial Connection

Using an SSH Connection

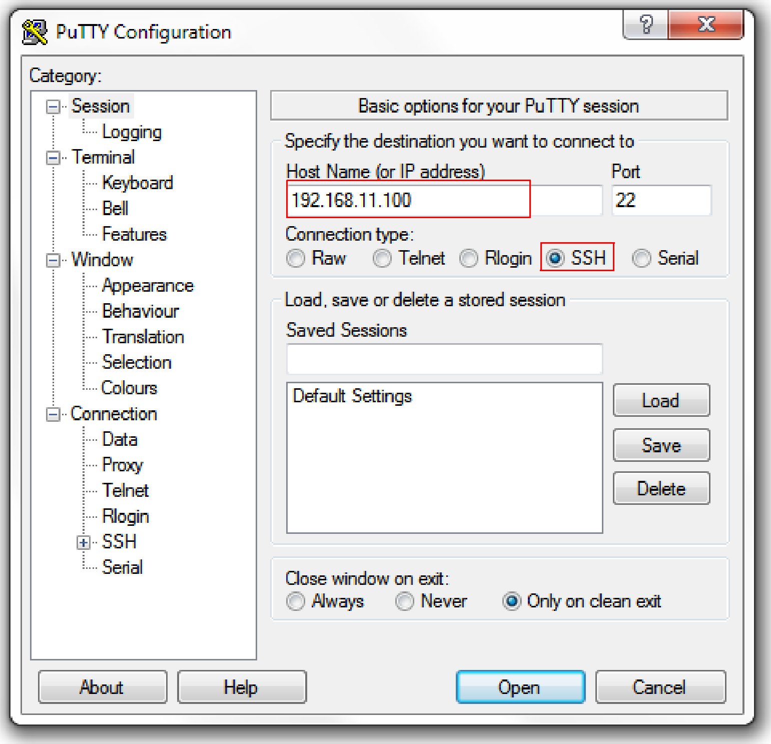
If you connected the administrative computer to the same subnet or broadcast domain as the Management (Web) interface of the controller, follow these steps to start and configure the SSH client.

1 Start PuTTY. The PuTTY Configuration dialog box appears, showing the *Session* screen.

2 In *Connection type*, select **SSH**.

3 Enter the IP address of the Management (Web) interface of the controller in the **Host Name (or IP address)** field.

Figure 231. Select SSH as the connection type and enter the IP address of the management interface



Specify the destination you want to connect to

Host Name (or IP address): 192.168.11.100

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

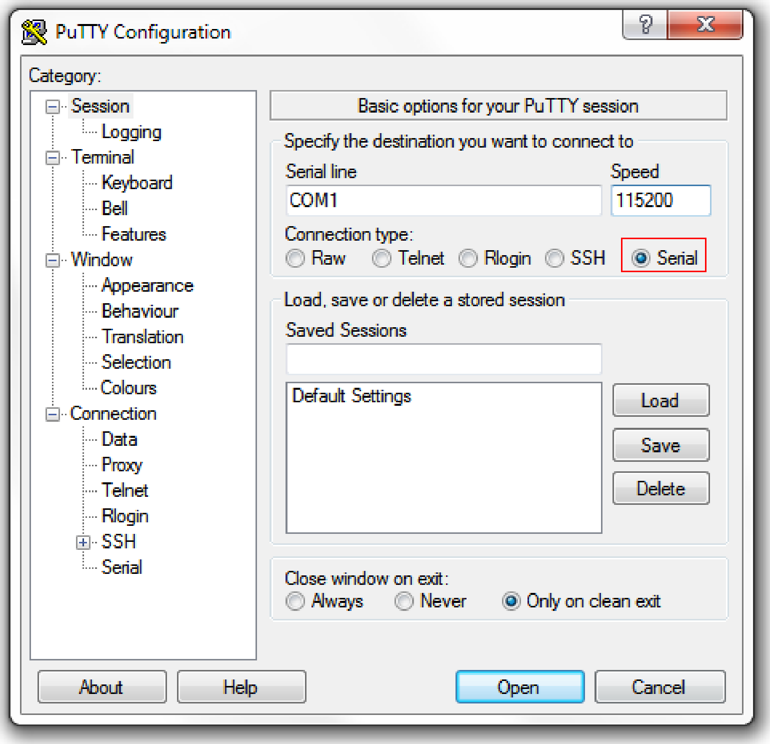
4 Click **Open.** The PuTTY console appears and displays the login prompt.

Using a Serial Connection

If you connected the administrative computer to the console port on the controller using an RS-232 serial to RJ45 cable, follow these steps to start and configure the terminal session.

1. Start PuTTY. The PuTTY Configuration dialog box appears, showing the *Session* screen.
2. In *Connection type*, select **Serial** if you are connecting via serial cable.

Figure 232. Selecting Serial as the connection type



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

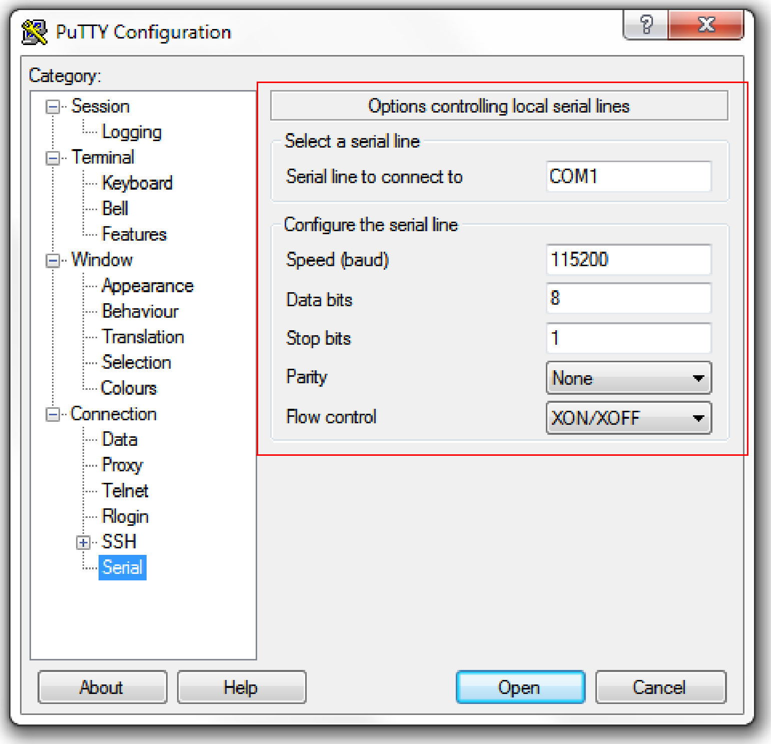
Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Under *Category*, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings.

Figure 233. PuTTY's default serial connection settings



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

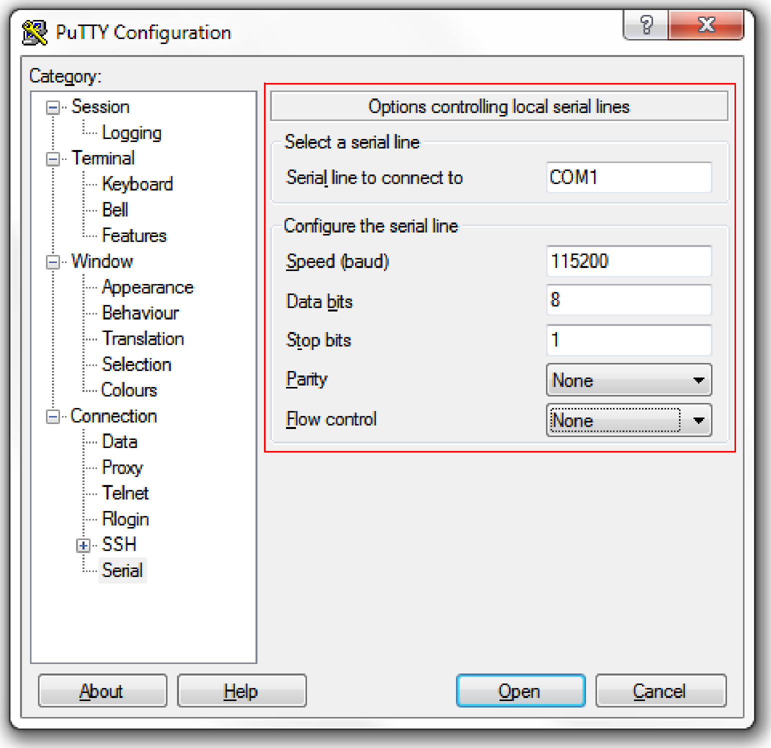
Parity: None

Flow control: XON/XOFF

4 Configure the serial connection settings as follows:

- *Serial line to connect to*: Type the COM port name to which you connected the RS-232 cable.
- *Bits per second*: 115200
- *Data bits*: 8
- *Stop bits*: 1
- *Parity*: None
- *Flow control*: None

Figure 234. PuTTY's serial connection settings for connecting to the controller



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

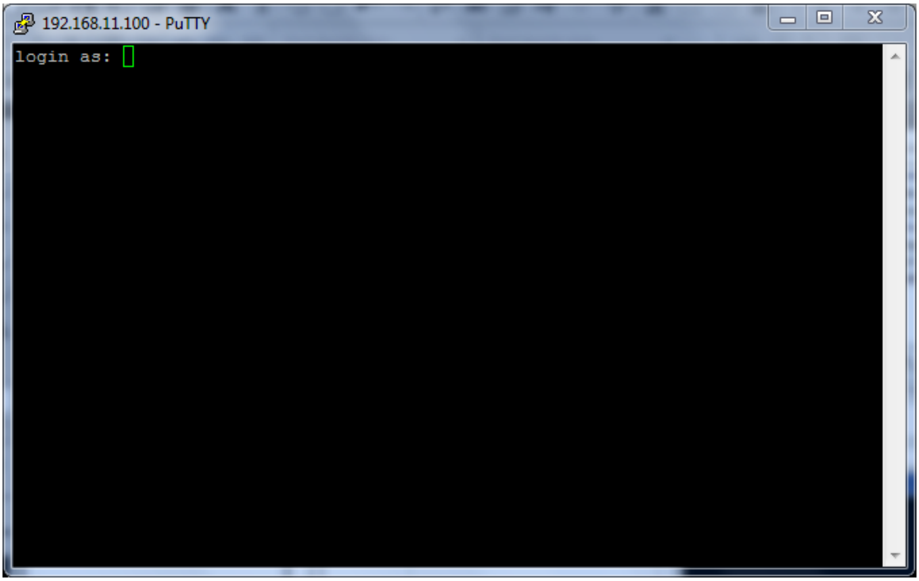
Stop bits: 1

Parity: None

Flow control: None

5 Click **Open.** The PuTTY console appears and displays the login prompt.

Figure 235. The PuTTY console displaying the login prompt



```
login as: 
```

You have completed configuring the SSH client to connect to the controller CLI.

Step 3: Log On to the CLI

1 At the `login as` prompt, press `<Enter>` once.

2 At the `Please login` prompt, type **`admin`**, and then press `<Enter>`.

3 At the `Password` prompt, type the password that you set during the controller setup, and then press **`<Enter>`**. The CLI welcome message and the `ruckus` prompt appears.

You are now logged into the controller CLI as a user with limited privileges. If you want to run more commands, you can switch to privileged mode by entering **`enable`** at the prompt, and then

To view a list of commands that are available, enter **`help`** or **`?`** (question mark).

NOTE: You can tell if you are logged into the CLI in limited or privileged mode by looking at the `ruckus` prompt. If you are in limited mode, the prompt appears as `ruckus>` (with a *greater than* sign). If you are in privileged mode, the prompt appears as `ruckus#` (with a pound sign).

Changing the Management IP Address from the CLI

The controller also supports changing the management IP address (the IP address you use to access the controller web interface) from the command line interface. Follow these steps to change the IP address from the CLI.

1. Log on to the CLI.
2. At the `ruckus#` prompt, enter **`config`** to enter the configuration mode.
3. At the `ruckus(config)#` prompt, enter **`interface management`**.
4. At the `ruckus(config-if)#` prompt, enter the following command:

   `ip address {ip-address} {subnet-mask} {gateway}`

   Where:

   - {ip-address} is the IP address that you want to assign to the management interface
   - {subnet-mask} is the subnet mask
   - {gateway} is the gateway IP address (optional)

   Separate the IP address, subnet mask, and gateway IP address values with a space.
5. At the `ruckus(config)#` prompt, enter **`exit`** to save your changes.

This example shows how to update the management interface IP address:

```
ruckus(config)# interface management
ruckus(config-if)# ip address   10.0.0.2   255.255.255.0
10.0.0.1
This command will reload all SCG services. Do you want to
continue (or input 'no' to
cancel)? [yes/no]
ruckus(config-if)# yes
ruckus(config-if)# exit
```

You have completed updating the management interface IP address.

Working with the Captive Portal

B

In this appendix:

- Overview of the Captive Portal
- Configuring the Captive Portal
- Captive Portal Workflows and VSA

Overview of the Captive Portal

The controller supports tunneling of captive portal user traffic to the 3G/4G/5G core network. During hotspot authentication, the controller either routes user traffic to the packet core or directly breaks the traffic out to the Internet, depending on authentication method used by the UE. Users who are authenticating via the 802.1x method can either be routed to the GGSN or through local breakout to Internet based on certain configurations. For users authenticated via captive portal, integration with packet core is not supported and traffic is always routed to Internet from the controller.

By routing traffic directly to the Internet, the operator loses control and visibility over Wi-Fi traffic. Since the controller does not support Policy and Charging Rule Function (PCRF) integration for retrieving policy for user and LI integration, QoS and LI cannot be applied to traffic that is directly routed to the Internet.

Smart Wi-Fi system is an enhancement that allows user traffic integration with GGSN for user authentication via a captive portal. Multiple schemes are supported for captive portal based authentication, such as:

- User name and password
- Voucher
- One-time password based on MSISDN
- Creating virtual account and adding credits

Smart Wi-Fi System allows packet core integration for all users irrespective of the authentication scheme used. Decision to either integrate user traffic to packet core or directly to Internet is based on the configuration setup.

To establish data traffic tunnel to core network (GGSN/PGW), the controller receives associated IMSI and MSISDN user identities from the AAA server preconfigured with the required credentials to map following identifiers:

- User name
- MAC address
- IMSI value
- MSISDN value

When the user accesses the controller's WLAN through the captive portal registration, it interfaces with the AAA server to register the user device's MAC address. Upon successful authentication, the captive portal disassociates the user and re-associates it with the controller's WLAN using the registered device MAC address. This functionality is supported as part of the MAC bypass feature with Ruckus Wireless APs.

When a user reconnects to a WLAN, the Ruckus Wireless AP triggers MAC-based authentication. Upon a successful authentication, the AAA server returns the associated identifiers of IMSI and MSISDN along with the flag (Ruckus VSA - see: Captive Portal Workflows and VSA) indicating that the TTG tunnel is established. The controller returns the TTG session type to the AP used by the data plane to trigger the TTG establishment when *DHCP DISCOVER* is received.

Configuring the Captive Portal

This section describes the configuration procedures required to set up the captive portal.

- Configuring the GGSN/PGW Service
- Configuring an Authentication Profile
- Configuring Accounting Profile
- Configuring TTG+PDG Forwarding Profiles
- Configuring WISPr (Hotspot) Services of the AP Zone
- AP Zone WLAN Services & Group

Configuring the GGSN/PGW Service

The controller has 3GPP-defined Tunnel Terminating Gateway (TTG) functionality, which enables it to act as a gateway between the UE (southbound) and the telecom core (northbound) to tunnel traffic between the UE (User Equipment, such as mobile phones) and controller gateway terminates the tunnel and then transfers the data over to GGSN (Gateway GPRS Serving Node) implementing the Gn’ interface via GTPv1 (Release 6).

The Gn interface is used in controlling the signal between controller and GGSN as well as for tunneling end user data payload within the backbone network between both the nodes.

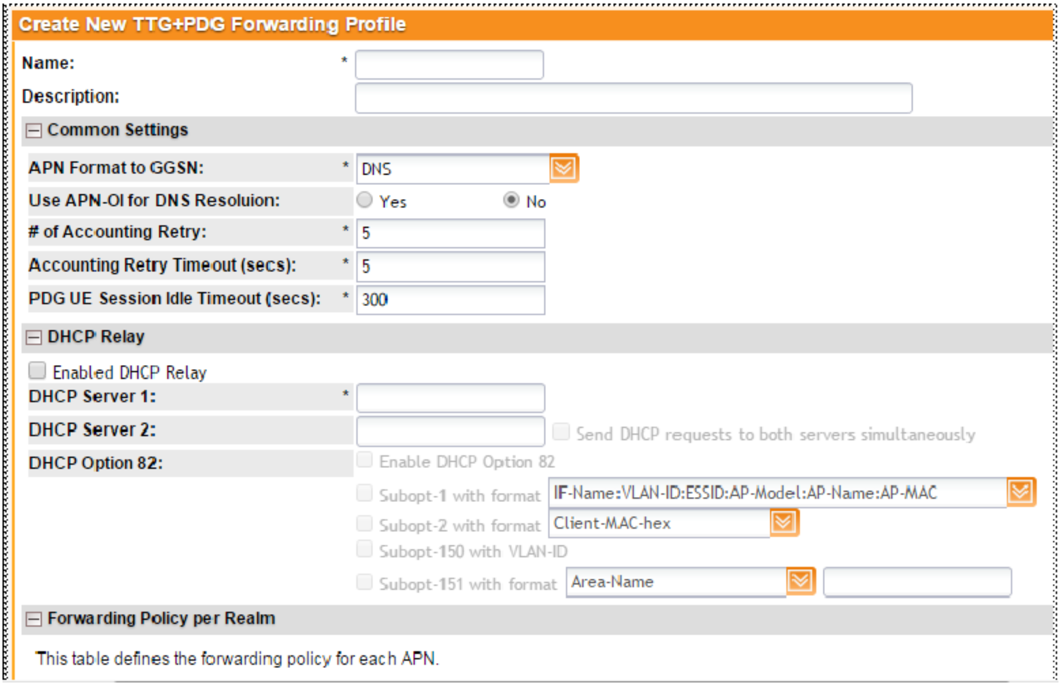
GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between controller and GGSN. A GTP tunnel is established between controller and GGSN for a data session initiated from UE.

A GTP tunnel is identified by a pair of IP addresses and a pair of GTP Tunnel End Point Identifiers (TEIDs), where one IP address and TEID is for the SGSN and the other is for GGSN. TEID is a session identifier used by GTP protocol entities in SGSN and GGSN.

GTP separates signaling from payload. Traffic is sorted onto a control plane (GTP-C) for signaling and a user plane (GTP-U) for user data. GTP-C is a tunnel control and management protocol and is used to create, modify and delete tunnels. GTP-U is a tunneling mechanism that provides a service for carrying user data packets.

Clicking **Configuration** > **Services & Profiles** on the main menu displays a sidebar on the left side of the page, which includes *GGSN Services*. Figure 236 shows the GGSN Service configuration page.

Figure 236. The GGSN/PGW Services configuration page



Create New TTG+PDG Forwarding Profile

Name:	*	
Description:		

⊟ **Common Settings**

APN Format to GGSN:	*	DNS
Use APN-OI for DNS Resoluion:		○ Yes ● No
# of Accounting Retry:	*	5
Accounting Retry Timeout (secs):	*	5
PDG UE Session Idle Timeout (secs):	*	300

⊟ **DHCP Relay**

□ Enabled DHCP Relay

DHCP Server 1:	*	
DHCP Server 2:		□ Send DHCP requests to both servers simultaneously
DHCP Option 82:		□ Enable DHCP Option 82 □ Subopt-1 with format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC □ Subopt-2 with format Client-MAC-hex □ Subopt-150 with VLAN-ID □ Subopt-151 with format Area-Name

⊟ **Forwarding Policy per Realm**

This table defines the forwarding policy for each APN.

Follow these steps to configure the GGSN/PGW service.

1 Go to **Configuration** > **Services & Profiles**.

2 On the sidebar (under *Services*), click **GGSN/PGW**.

3 In the *GTP Common Configuration* section, configure the following options:

- *Response Timer*: Define the response expected from GGN server from the drop down list, which ranges from 2 to 5 seconds. The controller will attempt to contact the GGSN during call establishment.
- *Number of Retries*: Define the number of times that controller will attempt to contact the GGSN. If all attempts fail, the relevant alarm is raised to confirm the failure of the GGSN path. For example, if the response timer is 3 and the number of retries is 5, it means that for each retry, controller will for 3 seconds.

- *Echo Request Timer*: Define number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure.
- *DNS Response Time*: Specify the maximum time that DNS waits for a response from a signaling request message.
- *DNS # Retry*: specify the maximum number of times that the DNS attempts to send a signaling request.

4 In the *DNS Servers* section, click **Add Server** to add a DNS IP address. If you're adding multiple DNS IP addresses, you can set their priority by clicking the **Move Up** and **Move Down** buttons. DNS servers that are higher up on the list of servers are given higher priority.

5 In the *APN Resolution* section, click **Create New** to define the IP address of the GGSN that should serve the AP. Configure the following options:

- **Domain Name**: Type the GGSN domain name.
- **IP Address**: Type the GGSN IP address.

6 Click **Apply**.

You have completed configuring the GGSN service.

Configuring an Authentication Profile

An authentication profile defines the authentication policy when the controller is used as a RADIUS proxy service for WLAN. RADIUS protocol is used for interfacing between Access Points (AP) and the controller as well as between the controller and a third party AAA (Authentication, Authorization and Accounting) server. The controller acts as RADIUS proxy for authentication and authorization and as a RADIUS client for accounting.

Follow these steps to create an authentication profile.

1 Go to **Configuration** > **Services & Profiles**.

2 On the sidebar under *Profiles*, click **Authentication**. The *Authentication Profiles* page appears.

3 Click **Create New**. The *Create New Authentication Profile* form appears.

4 In *Name*, type a name for the authentication profile that you are adding.

5 In *Friendly Name*, type a name that will be displayed as the authentication profile that you are adding

6 In *Description*, type a brief description of the profile. This is an optional field.

7 In *Service Protocol,* choose RADIUS setting. This is the default setting.

8 *RFC 5580 Out of Band Local Delivery*: Select the **Enable for Ruckus APs Only** is check box if you want AP location information for Ruckus Wireless APs to be included in RADIUS accounting messages. AP location information can be retrieved from the APs if their location information was entered statically (for APs without GPS) or automatically acquired (for APs with GPS).

9 In the *Primary Server* section, configure the settings of the primary RADIUS server.

- *IP Address*: Type the IP address of the AAA server.
- *Port*: Type the port number of the AAA server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

10 In the *Secondary Server* section, configure the settings of the secondary RADIUS server.

NOTE: The *Secondary Server* section is only visible if you selected the **Enable backup RADIUS server** check box earlier.

- *IP Address*: Type the IP address of the secondary AAA server.
- *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

11 Configure the *Health Check Policy* options. These options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

- *Response Window*: Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the “zombie period” (see below). If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server. Note that the zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus ¼ of the configured Zombie Period. The default Response Window is 20 seconds.

- *Zombie Period*: Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable. An AAA server that is marked “zombie” (inactive or unreachable) will be used for proxying with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server. The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is proxied to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.
- *Revive Interval*: Set the time (in seconds) after which, if no RADIUS messages are proxied to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.
- *No Response Fail*: Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.

CAUTION! To ensure that the RADIUS failover mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For information on configuring the RADIUS NAS request timeout and max number of retries, see Administrator Guide. For 3rd party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at 3rd party controller/ AP.

12 Configure the *Rate Limiting* options.

- *Maximum Outstanding Requests (MOR)*: Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096. When the MOR value is reached, RADIUS messages are dropped and a corresponding event is triggered.

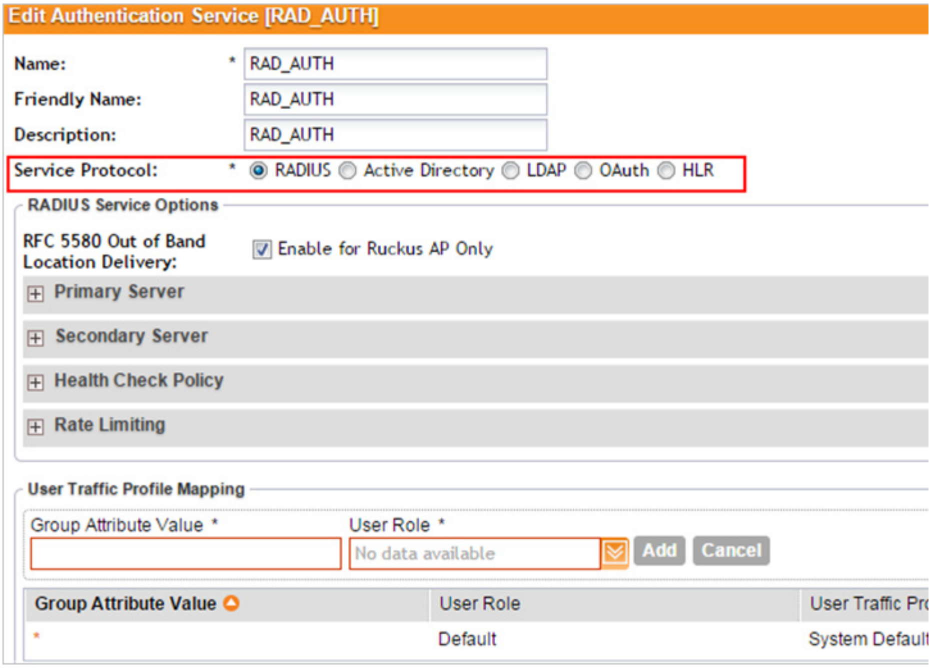
- *Threshold (% of MOR)*: Set a percentage value of the MOR at which (when reached) the controller will generate an event. For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.
- *Sanity Timer*: Set a timer (in seconds) that the controller will use to assert event 1301. When the load condition drops below the configured *Threshold* value (above), the controller will wait for the sanity timer to elapse before asserting event 1301.

13 *Group Traffic Profile Mapping*: Fill in this field only if you are creating a user role based on Group attributes extracted from an Active Directory or LDAP server Enter the User Group name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.

14 Click **OK** at the bottom of the form.

You have completed adding an authentication profile.

Figure 237. Authentication Profile form



Edit Authentication Service [RAD_AUTH]

Name: *	RAD_AUTH
Friendly Name:	RAD_AUTH
Description:	RAD_AUTH
Service Protocol: *	● RADIUS ○ Active Directory ○ LDAP ○ OAuth ○ HLR

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: ☑ Enable for Ruckus AP Only

⊞ Primary Server

⊞ Secondary Server

⊞ Health Check Policy

⊞ Rate Limiting

User Traffic Profile Mapping

Group Attribute Value * | User Role * No data available | Add | Cancel

Group Attribute Value	User Role	User Traffic Pr
*	Default	System Default

Configuring Accounting Profile

An accounting profile defines the accounting policy when the controller is used as a RADIUS proxy for WLAN services.

Follow these steps to create an accounting profile.

1 Go to **Configuration** > **Services & Profiles**.

2 On the sidebar under *Profiles*, click **Accounting**. The *Accounting Profiles* page appears.

3 Click **Create New**. The *Create New Accounting Profile* form appears.

4 In *Name*, type a name for the authentication profile that you are adding.

5 In *Description*, type a brief description of the profile. This is an optional field.

6 In *Service Protocol,* choose RADIUS setting. This is the default setting.

7 In the *Primary Server* section, configure the settings of the primary RADIUS server.

- *IP Address*: Type the IP address of the AAA server.
- *Port*: Type the port number of the AAA server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

8 In the *Secondary Server* section, configure the settings of the secondary RADIUS server.

NOTE: The *Secondary Server* section is only visible if you selected the **Enable backup RADIUS server** check box earlier.

- *IP Address*: Type the IP address of the secondary AAA server.
- *Port*: Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the shared secret to confirm.

9 Configure the *Health Check Policy* options. These options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

- *Response Window*: Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the “zombie period” (see below). If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server. Note that the zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus ¼ of the configured Zombie Period. The default Response Window is 20 seconds.
- *Zombie Period*: Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable. An AAA server that is marked “zombie” (inactive or unreachable) will be used for proxying with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server. The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is proxied to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.
- *Revive Interval*: Set the time (in seconds) after which, if no RADIUS messages are proxied to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.
- *No Response Fail*: Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.

CAUTION! To ensure that the RADIUS failover mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For information on configuring the RADIUS NAS request timeout and max number of retries, see Administrator Guide. For 3rd party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at 3rd party controller/ AP.

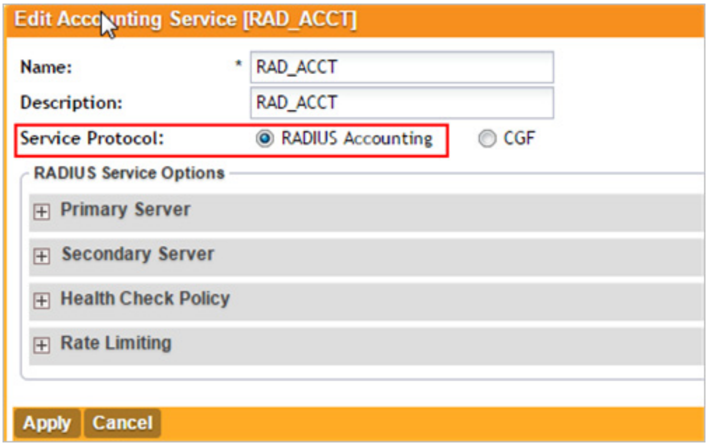
10 Configure the *Rate Limiting* options.

- *Maximum Outstanding Requests (MOR)*: Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096. When the MOR value is reached, RADIUS messages are dropped and a corresponding event is triggered.
- *Threshold (% of MOR)*: Set a percentage value of the MOR at which (when reached) the controller will generate an event. For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.
- *Sanity Timer*: Set a timer (in seconds) that the controller will use to assert event 1301. When the load condition drops below the configured *Threshold* value (above), the controller will wait for the sanity timer to elapse before asserting event 1301.

11 Click **OK** at the bottom of the form.

You have completed adding an accounting profile.

Figure 238. Accounting Profile form



Edit Accounting Service [RAD_ACCT]

Name: *	RAD_ACCT
Description:	RAD_ACCT
Service Protocol:	● RADIUS Accounting ○ CGF

Configuring TTG+PDG Forwarding Profiles

A TTG+PDG forwarding profile defines the gateway and tunnel configurations for core network GTP tunnels and LBO configurations. Follow these steps to add a TTG+PDG profile.

1. On the *TTG+PDG Forwarding Profiles* page, click **Create New**. The *Create New TTG+PDG Forwarding Profile* form appears.
2. In *Name*, type a name for the TTG+PDG Profile that you are adding.
3. In *Description*, give a brief description of the profile created. This is an optional field.
4. In *Common Settings,* configure the following:
   - *APN Format to GSN*: Select either **DNS** or **String** from the drop-down list.
   - *APN-OI for DNS Resolution:* Specify if the APN-OI is required.
   - *# of Accounting Retry*: Specify the interval (in minutes) at which the controller will recheck the primary TTG+PDG RADIUS profile, if it is available. The default interval is 5 minutes.
   - *Accounting Retry Timeout (secs)*: Type the timeout period (in seconds) after which an expected response message is considered to have failed.
   - *PDG UE Session Idle Timeout (secs):* Type the timeout period (in seconds) after which an expected response message is considered to have failed.
5. In *DHCP Relay*, configure the following options to enable the DHCP relay agent in the controller:
   - *Enable DHCP Relay*: Select this check box to enable the DHCP relay agent in the controller.
   - *DHCP Server 1*: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
   - *DHCP Server 2*: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
   - *DHCP Option 82*: Select this check box If you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub options by selecting the corresponding check boxes:
     - *Subopt-1 with format*: You can customize sub option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is:

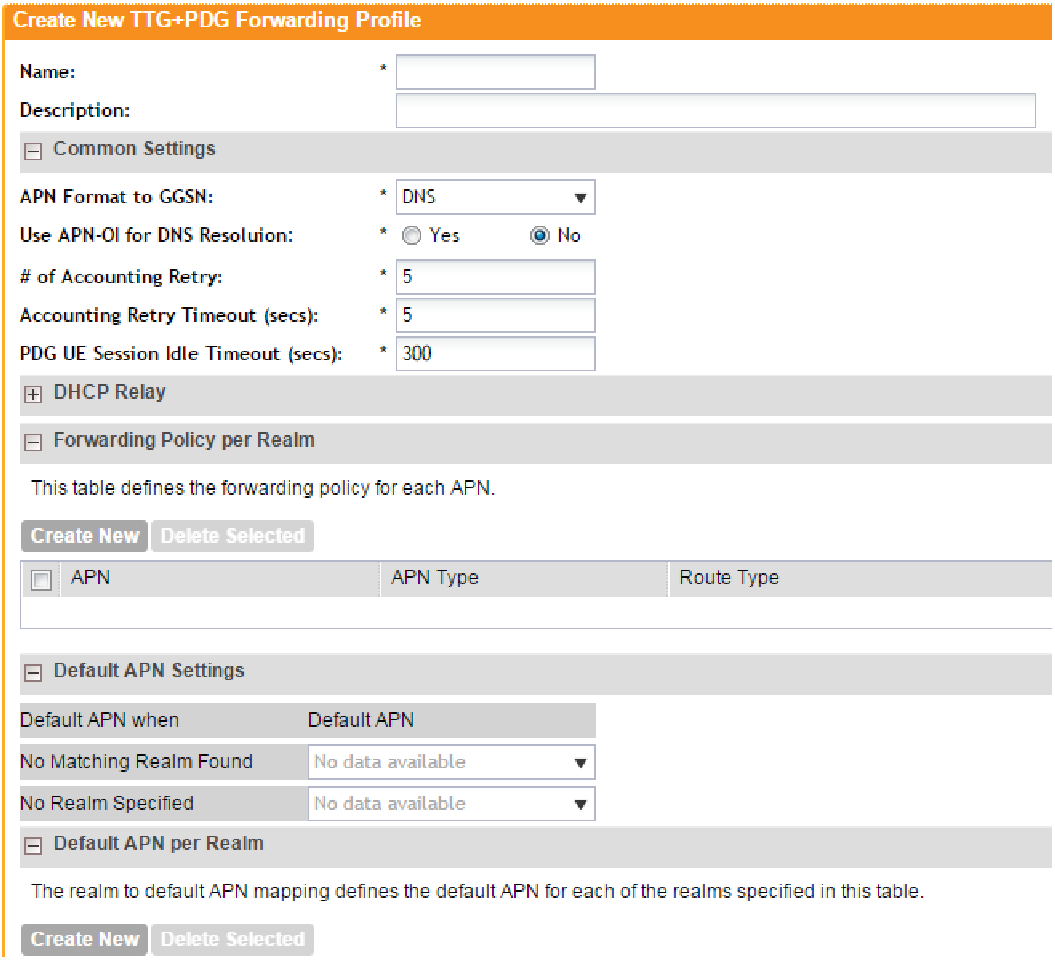
```
IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC
```

- Subopt 2 with format: You can customize sub option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
- *Subopt-150 with VLAN ID*: This sub option encapsulates the VLAN ID.
- *Subopt-151 with format*: This sub option can encapsulate either the ESSID or a configurable Area Name.

6. In *Forwarding Policy Per Realm*, specify the forwarding policy for each realm in the table. Configure the following:
   - APN
   - APN Type
   - Route Type
   - Profile Name
7. In *Default APN Settings*, configure the following:
   - No Matching Realm Found
   - No Realm Specified
8. Click **Create New**.

You have completed adding a TTG+PDG profile.

Figure 239. Creating a TTG+PDG Profile



Create New TTG+PDG Forwarding Profile

Name: *

Description:

⊟ Common Settings

APN Format to GGSN: * DNS ▼

Use APN-OI for DNS Resoluion: * ○ Yes ● No

# of Accounting Retry: * 5

Accounting Retry Timeout (secs): * 5

PDG UE Session Idle Timeout (secs): * 300

⊞ DHCP Relay

⊟ Forwarding Policy per Realm

This table defines the forwarding policy for each APN.

□	APN	APN Type	Route Type

⊟ Default APN Settings

Default APN when	Default APN
No Matching Realm Found	No data available ▼
No Realm Specified	No data available ▼

⊟ Default APN per Realm

The realm to default APN mapping defines the default APN for each of the realms specified in this table.

Configuring WISPr (Hotspot) Services of the AP Zone

Follow these steps to configure the hotspot service of the zone template.

1. Click **Configuration** > **AP Zones**.
2. On the *AP Zone List* page, click the AP zone for which you want to create a hotspot service.
3. On the sidebar, click **WISPr (Hotspot)**. The *WISPr (Hotspot) Services* page appears.
4. Click **Create New**. The form for creating a new hotspot service appears.
5. In the *General Options* section, configure the following options:
   - *Name*: Type a name for the hotspot service.
   - *Description*: Type a description for the hotspot service.
   - *Type*: Click **Registered Users** if you want only users with existing profiles on the controller to be able to connect to this hotspot. Click **Guest-Access** if you want guest users to be able to connect to this hotspot.
6. In the *Redirection* section, configure the following options:
   - *Smart Client Support*: Select one of the following options:
     - **None**: Select this option to disable Smart Client support on the hotspot service.
     - **Enable**: Selection this option to enable Smart Client support.
     - **Only Smart Client Allowed**: Select this option to allow only Smart Clients to connect to the hotspot service.

     For more information, see Configuring Smart Client Support.
   - *Logon URL*: Type the URL of the subscriber portal (the page where hotspot users can log in to access the service). For more information, see Configuring the Logon URL.
   - *Start Page*: Set where users will be redirected after they log in successfully:
     - **Redirect to the URL that user intends to visit**: You could redirect users to the page that they want to visit.
     - **Redirect to the following URL**: You could set a different page where users will be redirected (for example, your company website).
7. In the *User Session* section, configure the following options:
   - *Session Timeout*: Set a time limit (in minutes) after which users will be disconnected from the hotspot service and will be required to log on again.

- *Grace Period*: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log on again.

8 In the *Location Informatio*n section, configure the following options:

- *Location ID*: Type the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The required code includes:
  - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
  - network

  The following is an example of what the Location ID entry should look like: isocc=us,cc=1,ac=408,network=RuckusWireless
- *Location Name*: Type the name of the location of the hotspot service.

9 In *Walled Garden*, click **Create New** to add a walled garden. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account.

In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:

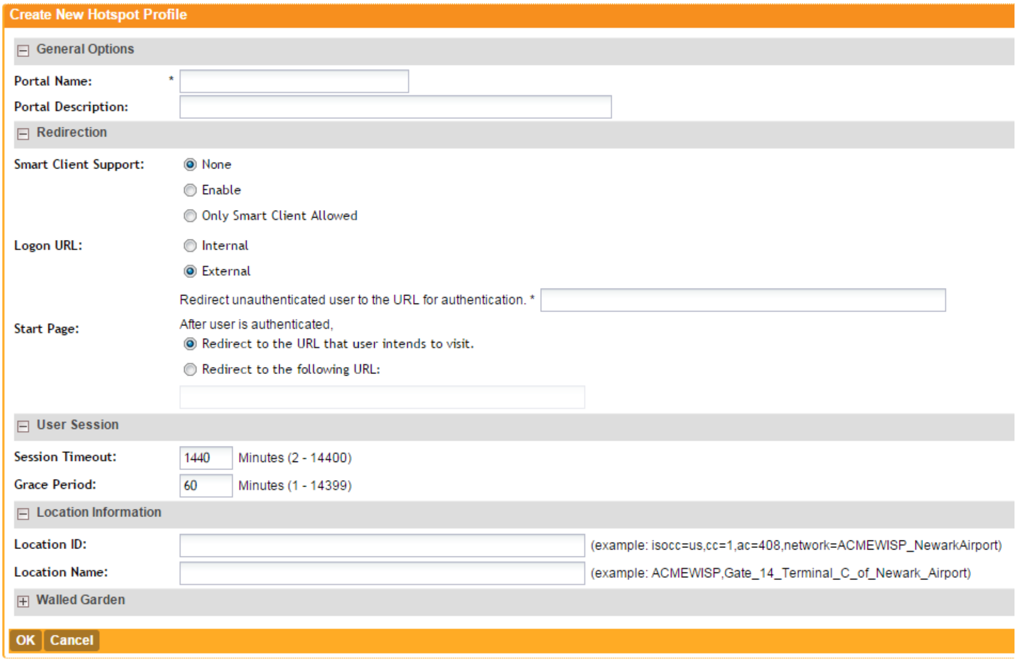
- IP address (for example, 10.11.12.13)
- Exact website address (for example, www.ruckuswireless.com)
- Website address with regular expression (for example, *.ruckuswireless.com, *.com, *)

After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to re-authenticate when they navigate through the page.

10 Click **Create New**.

You have completed configuring a hotspot service of the AP zone.

Figure 240. The Create New Hotspot Profile form



Create New Hotspot Profile

⊟ General Options

Portal Name: *

Portal Description:

⊟ Redirection

Smart Client Support:
● None
○ Enable
○ Only Smart Client Allowed

Logon URL:
○ Internal
● External

Redirect unauthenticated user to the URL for authentication. *

Start Page:
After user is authenticated,
● Redirect to the URL that user intends to visit.
○ Redirect to the following URL:

⊟ User Session

Session Timeout: 1440 Minutes (2 - 14400)

Grace Period: 60 Minutes (1 - 14399)

⊟ Location Information

Location ID: (example: isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)

Location Name: (example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

⊞ Walled Garden

OK Cancel

AP Zone WLAN Services & Group

Follow these steps to configure tunneling combination for Captive Portal.

NOTE: There is only 1configuration combination allowed for usage of this feature.

1. Click **Configuration** > **AP Zones > WLAN**.
2. On the *AP Zone List* page, select the AP zone in the WLAN Services & Group page.
3. In *WLAN Usage* options*:*
   - *Access Network* - Enable *Tunnel WLAN traffic through Ruckus GRE.*
   - *Core Network* **-** Enable *Bridge option*
   - *Authentication Type* **-** Enable *Hotspot (WISPr)*
4. In *Authentication options:*
   - *Method***-** Enable *MAC Address)*
5. In *Hotspot Portal options:*

- *Hotspot (WISPr) Portal* - Choose the portal as hotspot
- *Authentication Service* - Enable using RADIUS authentication as the controller proxy
- *Accounting Service* - Enable using RADIUS authentication as the controller proxy

6 In *Forwarding Profile options:*

- *Forwarding Policy* - Choose the forwarding policy as TTG.
- Enable WISPr TTG support

7 In *Advanced options:*

- *User Traffic Profile* - Choose the forwarding policy as Bridge.
- Enable WISPr TTG support

8 Click **Apply**.

You have completed configuring WLAN for Captive Portal. With this you have completed configuration for Captive Portal.

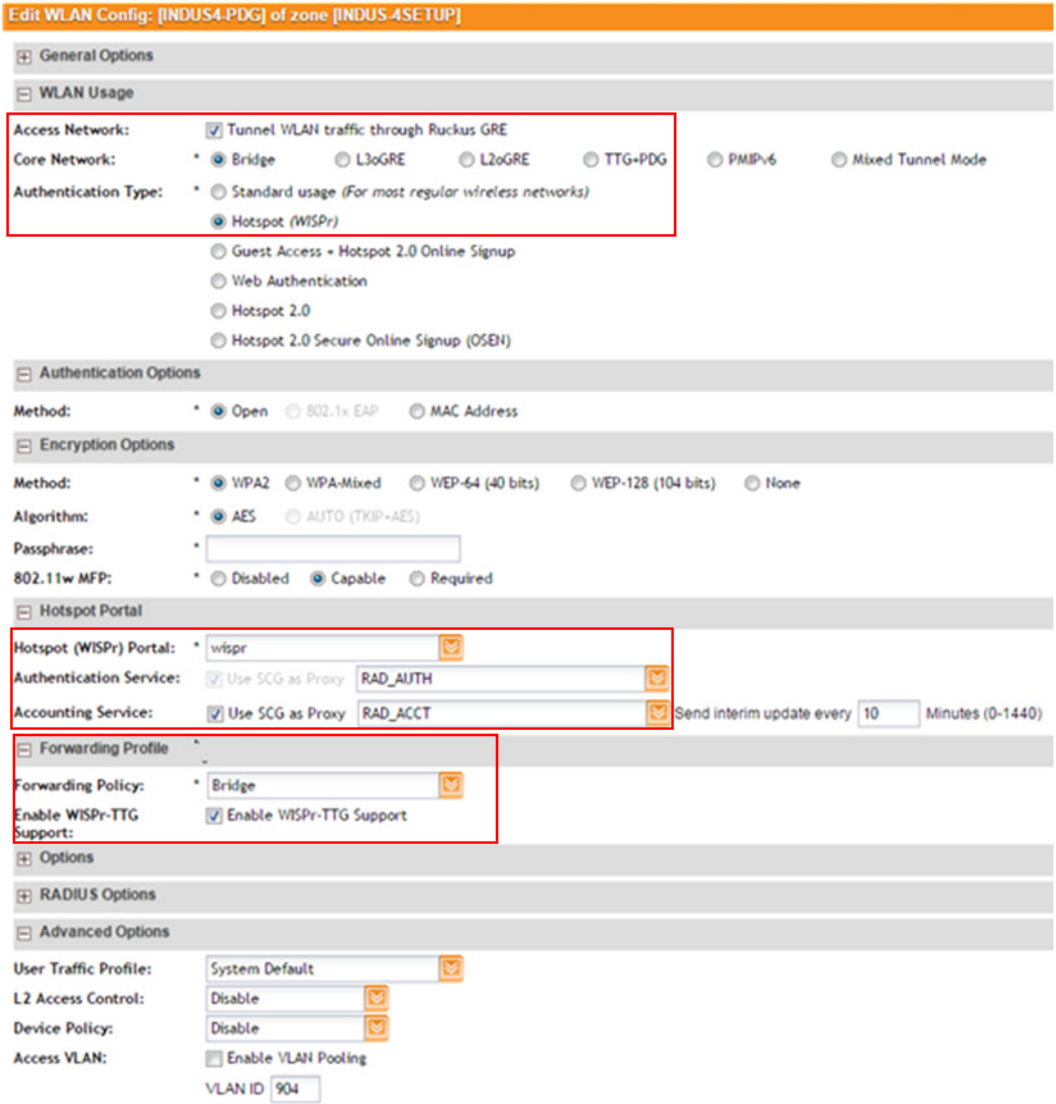


Figure 241. Configuring WLAN

Edit WLAN Config: [INDUS4-PDG] of zone [INDUS-4SETUP]

⊞ General Options

⊟ WLAN Usage

Access Network: ☑ Tunnel WLAN traffic through Ruckus GRE

Core Network: * ● Bridge ○ L3oGRE ○ L2oGRE ○ TTG+PDG ○ PMIPv6 ○ Mixed Tunnel Mode

Authentication Type: * ○ Standard usage *(For most regular wireless networks)*
● Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Online Signup
○ Web Authentication
○ Hotspot 2.0
○ Hotspot 2.0 Secure Online Signup (OSEN)

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method: * ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Algorithm: * ● AES ○ AUTO (TKIP+AES)

Passphrase: *

802.11w MFP: * ○ Disabled ● Capable ○ Required

⊟ Hotspot Portal

Hotspot (WISPr) Portal: * wispr

Authentication Service: ☑ Use SCG as Proxy RAD_AUTH

Accounting Service: ☑ Use SCG as Proxy RAD_ACCT Send interim update every 10 Minutes (0-1440)

⊟ Forwarding Profile *

Forwarding Policy: * Bridge

Enable WISPr-TTG Support: ☑ Enable WISPr-TTG Support

⊞ Options

⊞ RADIUS Options

⊟ Advanced Options

User Traffic Profile: System Default

L2 Access Control: Disable

Device Policy: Disable

Access VLAN: □ Enable VLAN Pooling

VLAN ID 904

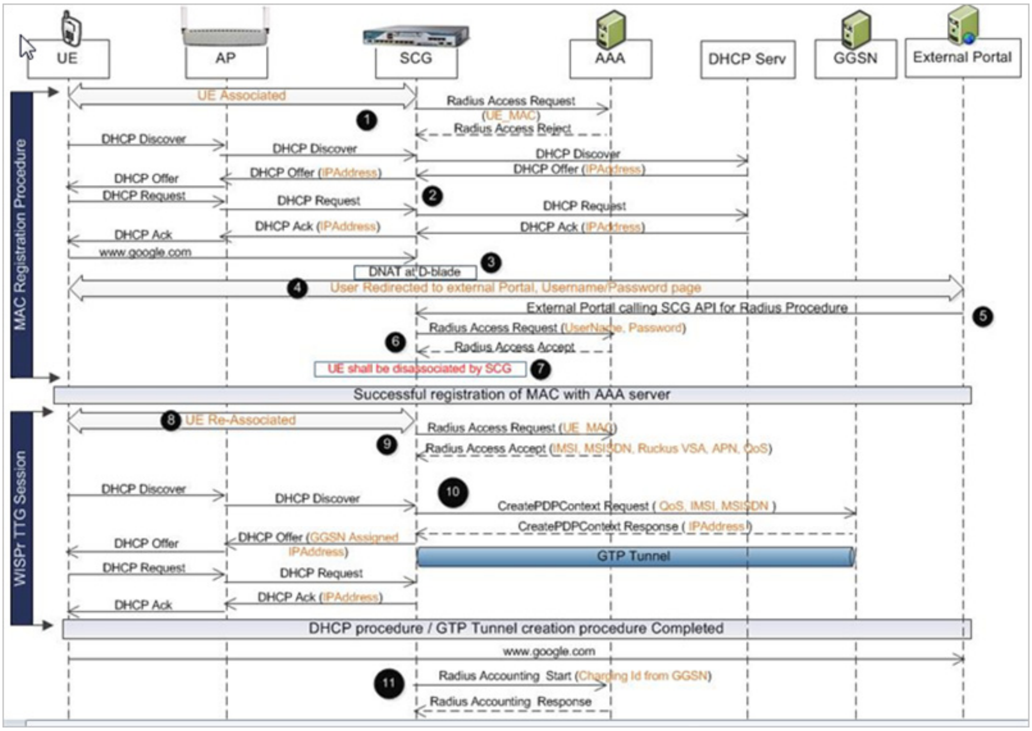
Captive Portal Workflows and VSA

This section describes the workflow of the captive portal and VSA.

Successful Captive Portal Authentication

Figure 242 describes the workflow where the external portal sends a message to the controller to initiate the RADIUS authentication to complete the portal authentication procedure.

Figure 242. Captive portal authentication workflow


UE
AP
SCG
AAA
DHCP Serv
GGSN
External Portal
MAC Registration Procedure
UE Associated
Radius Access Request (UE_MAC)
1
Radius Access Reject
DHCP Discover
DHCP Discover
DHCP Discover
DHCP Offer (IPAddress)
DHCP Offer (IPAddress)
DHCP Offer
DHCP Request
2
DHCP Request
DHCP Request
DHCP Ack (IPAddress)
DHCP Ack (IPAddress)
DHCP Ack
www.google.com
DNAT at D-blade
3
4
User Redirected to external Portal, Username/Password page
External Portal calling SCG API for Radius Procedure
5
Radius Access Request (UserName, Password)
6
Radius Access Accept
UE shall be disassociated by SCG
7
Successful registration of MAC with AAA server
WISPr TTG Session
8
UE Re-Associated
Radius Access Request (UE_MAC)
9
Radius Access Accept (IMSI, MSISDN, Ruckus VSA, APN, QoS)
DHCP Discover
DHCP Discover
10
CreatePDPContext Request (QoS, IMSI, MSISDN)
CreatePDPContext Response (IPAddress)
DHCP Offer
DHCP Offer (GGSN Assigned IPAddress)
GTP Tunnel
DHCP Request
DHCP Request
DHCP Ack
DHCP Ack (IPAddress)
DHCP procedure / GTP Tunnel creation procedure Completed
www.google.com
11
Radius Accounting Start (Charging Id from GGSN)
Radius Accounting Response

1 The UE associated controller triggers MAC based authentication, which is rejected by the AAA server since the UE MAC is not registered.

2 A DHCP procedure is triggered and the IP address is allocated from the DHCP server.

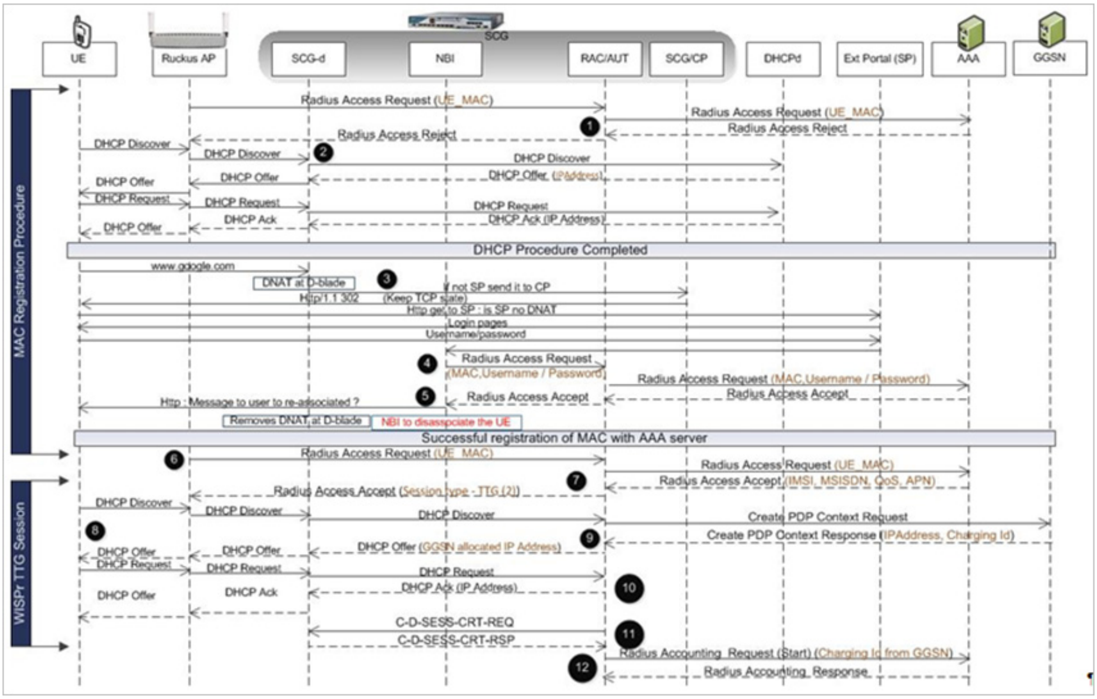
3 When the UE tries to browse a DNAT procedure is performed at the data plane since the user is not yet authenticated.

4. The user is redirected to login page of the external portal.
5. On user entering his login credentials the external portal calls the controller’s API (NBI API) to complete the authentication procedure
6. The controller triggers the RADIUS CHAP authentication towards the AAA server.
7. On successful authentication the user is disassociated. This complete the UE registration procedure with external AAA server.
8. The UE re-associates to the AP.
9. MAC authentication is triggered by the controller. The AAA server responds with access accept with IMSI, MSISDN, QoS (optional) and APN (optional).
10. DHCP procedure is initiated by UE. During this procedure the controller establishes GTP tunnel and DHCP offer is sent with GGSN to the assigned IP address.
11. On completion of the DHCP procedure the user continues with the data session. The controller also triggers the accounting message towards the AAA accounting server.

Successful GTP Tunnel Establishment

Figure 243 shows the workflow of successful GTP tunnel establishment for WISPr authentication and RADIUS CHAP from the controller.

Figure 243. Successful GTP tunnel establishment



1 The UE associated controller triggers MAC based authentication, which is rejected by the AAA server since the UE MAC is not registered.

2 A DHCP procedure is triggered and the IP address is allocated from the DHCP server.

3 When the UE tries to browse a DNAT procedure is performed at the data plane since the user is not yet authenticated.

4 The user is redirected to login page of the external portal.

5 On user entering his login credentials the external portal calls the controller's API (NBI API) to complete the authentication procedure

6 The controller triggers the RADIUS CHAP authentication towards the AAA server.

7 On successful authentication the user is disassociated. This complete the UE registration procedure with external AAA server.

8 The UE re-associates to the AP.

9 MAC authentication is triggered by the controller. The AAA server responds with access accept with IMSI, MSISDN, QoS (optional) and APN (optional).

10 DHCP procedure is initiated by UE. During this procedure, the controller establishes a GTP tunnel and a DHCP offer is sent with GGSN to the assigned IP address.

11 Upon completion of the DHCP procedure, the user continues with the data session.

12 The controller also triggers the accounting message towards the AAA accounting server.

Ruckus VSA for Captive Portal

Table 21 lists the values of the new Ruckus VSA - *Ruckus-WISPr-Redirect-Policy,* included by the AAA server in RADIUS access accept messages*.*

Table 21. Ruckus VSA

Ruckus VSA	**APN Resolution**	**Controller Behavior/Action**
REDIRECT-AFTER-GTP	GTPv1	- GTP tunnel with GGSN - Ruckus VSA Ruckus-Session-Type = TTG in Access Accept to AP
REDIRECT-AFTER-GTP	GTPv2	- GTP tunnel with PGW - Ruckus VSA Ruckus-Session-Type = TTG in Access Accept to AP
REDIRECT-AFTER-GTP	PDG	- Non-TTG session or VANILLA-REDIRECT - No Ruckus VSA Ruckus-Session-Type (125) in Access Accept
NULL (No VSA received from AAA)	GTPv1	- GTP tunnel with GGSN - Ruckus VSA Ruckus-Session-Type = TTG in Access Accept to AP
NULL (No VSA received from AAA)	GTPv2	- GTP tunnel with PGW - Ruckus VSA Ruckus-Session-Type = TTG in Access Accept to AP

Table 21. Ruckus VSA

Ruckus VSA	APN Resolution	Controller Behavior/Action
NULL (No VSA received from AAA)	PDG	- Non-TTG session or VANILLA-REDIRECT - No Ruckus VSA Ruckus-Session-Type (125) in Access Accept
VANILLA-REDIRECT	GTPv1	- Non-TTG session or VANILLA-REDIRECT - No Ruckus VSA Ruckus-Session-Type (125) in Access Accept
VANILLA-REDIRECT	GTPv2	- Non-TTG session or VANILLA-REDIRECT - No Ruckus VSA Ruckus-Session-Type (125) in Access Accept
VANILLA-REDIRECT	PDG	- Non-TTG session or VANILLA-REDIRECT - No Ruckus VSA Ruckus-Session-Type (125) in Access Accept

Statistics Files the Controller Exports to an FTP Server

C

This appendix describes the content of the statistics files that the controller exports to an FTP server (if configured).

- AP Inventory
- Control Plane Statistics
- Mobility Zone Inventory
- Zone Statistics
- AP Statistics
- Zone Time Radio Statistics
- Zone Time WLAN Statistics
- AP Time Radio Statistics
- AP Time WLAN Statistics
- Control Plane Statistics
- Data Plane Statistics
- Data Plane Ethernet Port Statistics
- AP SoftGRE Tunnel Statistics
- SoftGRE Gateway Statistics
- Tenant Time Radio Statistics
- Tenant Time WLAN Statistics
- Tenant Zone Statistics
- Tenant Zone Radio Statistics

NOTE: The controller statistics files use Unix timestamps in milliseconds (for example, “1.40729E+12” is Unix timestamp for “8/6/2014 2:30:00 AM”). You can use an online timestamp conversion tool to convert Unix timestamps to human-readable timestamps.

NOTE: The file name format of the Statistics file is as follows:
<report title>-YYYY-MM-DD_HH-MM-SS-MS_ZZ
where:
- MS stands for three-digit milliseconds.
- ZZ is a random number to avoid the file name conflict when a user subscribes to several reports but based on the same filter. ZZ ranges between 00-99.
For example: New_Client-2015-11-17_08-00-16-031_59.csv

AP Inventory

The AP inventory file contains detailed information about each AP that the controller was managing at the time the file was uploaded to the FTP.

The default AP inventory file name format is:

`ap_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 22. Attributes in the AP inventory file

Column Name	Description
key	MAC address of the AP
zoneUUID	ID of the zone to which the AP belongs
gpsSource	GPS coordinates (for example, 47.633625,-122.186446)
lastSeen	Unix timestamp of AP's latest connection
fwVersion	Current AP firmware version
meshRole	Mesh role assigned to the AP. Possible values include: • 0: Disabled • 1: RAP • 2: MAP • 3: EMAP • 4: Mesh is down • 5: Mesh role is undefined
location	AP location info
rebootStartTime	Time when AP reboot was started
type	The type of JSON string
deviceName	Device name assigned to the AP
description	Description of the AP
extIp	External IP address assigned to the AP
registrationState	Registration state of the AP. Possible values include: • 0: Pending • 1: Approved • 2: Rejected
gpsInfo	GPS coordinates of the AP's location (if configured)

Table 22. Attributes in the AP inventory file

Column Name	Description
countryCode	Country code assigned to the AP
cableModemInfo	Cable modem info (if the AP has a cable modem component)
enableWlanservice24	Enable 2.4GHz radio
connectionStatus	Current connection status of the AP
heartbeatLost	Time AP heartbeat was lost (if any). If heartbeat has not been lost, the value is “FALSE.”
meshSSID	Mesh SSID used by the AP to form the mesh
extPort	External port
apGroupUUID	Table key assigned to the AP group to which the AP belongs
model	Model of the AP
timeStamp	Timestamp of the record (in Unix timestamp)
wsgWlanIDAndClientCount	Client count of each WLAN
clientCount	Current client count on the AP
hops	Number of devices between this mesh AP and the root AP
bladeId	ID of the control blade
enableWlanservice50	Enable 5GHz radio
approvedTime	Unix timestamp when the AP registration was approved
registrationTime	Unix timestamp when the AP registered with the controller
uptime	Number of minutes elapsed since AP was last rebooted
lastRegistrationInfo	AP registration info
ip	IP address assigned to the AP
dpMac	Data plane MAC address
ap	MAC address of the AP
provisionTag	Tag used to preprovision the AP to its current zone
tagged	Tagged AP is the AP with daily traffic exceed the customized threshold value
channel	Radio channel that the AP is using

Table 22. Attributes in the AP inventory file

Column Name	Description
serial	Serial number of the AP
apMac	MAC address of the AP
provisionStage	Current provision status of the AP
provisionMethod	AP join method (Discovered/Preprovision/Swap)
registrationState	Registration state of the AP. Possible values include: • 0: Pending • 1: Approved • 2: Rejected
adminstrativeState	AP WLAN state. Possible values include 0 (unlocked) and 1 (locked).

Control Plane Statistics

The control plane statistics file contains detailed general information about the control plane. Its default file name format is:

`controlBlade__YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 23. Attributes in the control plane statistics file

Column Name	Description
key	Control plane ID
hostName	Name of the control plane
model	Model of the control plane
serialNumber	Serial number of the control plane
mac	Serial number of the control plane
startTime	Timestamp when the control plane was set up
description	Description of the control plane

Mobility Zone Inventory

The mobility zone inventory file contains detailed information about every zone that existed on the controller at the time the file was uploaded to the FTP server.

The default zone inventory statistics file name format is:

`mobilityZone_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 24. Attributes in the mobility zone inventory file

Column Name	Description
key	ID assigned to the zone
mobilityZoneName	Name assigned to the zone
description	Description of the zone
createdDatetime	Date and time (in Unix timestamp) when the zone was created

Zone Statistics

The zone statistics file contains detailed information on traffic, client associations, and AP uptime at the zone level during the configured period of time. The default file name format depends on the time period specified for uploading the statistics file:

- If the zone statistics file is exported *daily*: `statsZoneDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the zone statistics file is exported *hourly*: `statsZoneHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

NOTE: The term "period" in the following table refers to the time interval (hourly or daily) selected in *Statistics Date Interval* on the web interface.

Table 25. Attributes in the zone statistics file

Column Name	Description
key	ID of the zone
airtime	Total airtime of channel utilization during the period
minNumClients	Minimum number of concurrently connected clients during the period
rxFrames_r	Total number of frames received during the period
txRateKbps	Transmit data rate in kilobits per second for the period
rxRateKbps	Receive data rate in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txBytes_r	Total number of bytes transmitted during the period
rxBytes_r	Total number of bytes received during the period
timeStamp	Data aggregation time (in Unix timestamp)
txFrames_r	Total number of frames transmitted during the period
uptime_r	Percentage of time during which the AP was up during the period. Uptime is computed based on the up and down events that occurred.
avgNumClients	Average number of concurrently connected clients during the period
failedAssoc	Number of failed associated clients during the period

Table 25. Attributes in the zone statistics file

Column Name	Description
maxNumClients	Maximum number of concurrently connected clients during the period

AP Statistics

The AP statistics file contains detailed information on traffic, client associations, and AP uptime at the AP level during the configured period of time.

The default AP statistics file name format depends on the time period specified for uploading the file:

- If the AP statistics file is exported *daily*:
  `statsAPDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the AP statistics file is exported *hourly*:
  `statsAPHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

NOTE: The term “period” in the following table refers to the time interval (hourly or daily) selected in *Statistics Date Interval* on the web interface.

Table 26. Attributes in the AP statistics file

Column Name	Description
key	MAC address of the AP
airtime	Total airtime of channel utilization during the period
minNumClients	Minimum number of concurrently connected clients during the period
txRateKbps	Transmit data rate in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txBytes_r	Total number of bytes transmitted during the period
rxRateKbps	Received data rate in kilobits per second for the period
rxBytes_r	Total number of bytes received during the period
rxFrames_r	Total number of frames received during the period

Table 26. Attributes in the AP statistics file

Column Name	Description
uptime_r	Percentage of time during which the AP was up during the period. Uptime is computed based on the up and down events that occurred.
avgNumClients	Average number of concurrently connected clients during the period
txFrames_r	Total number of frames transmitted during the period
failedAssoc	Number of clients that failed to associate with the AP during the period
maxNumClients	Maximum number of concurrently connected clients during the period
timestamp	Data aggregation time (in Unix timestamp)

Zone Time Radio Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*: `statsZoneTimeRadioDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*: `statsZoneTimeRadioHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 27. Attributes in the zone time radio statistics file

Column Name	Description
key	ID of the zone
airtime	Total airtime of channel utilization during the period
minNumClients	Minimum number of concurrently connected clients during the period
airtimeB	Busy airtime (channel) utilization during the period
txBytes_r	Total number of bytes transmitted during the period
rxFrames_r	Total number of data frames received during the period
newAssoc	Number of newly associated clients during the period
timestamp	Data aggregation time
txFrames_r	Total number of frames transmitted during the period
rxBytes_r	Total number of bytes received during the period
airtimeRx	Total receiving airtime (channel) utilization during the period
avgNumClients	Average number of concurrently connected clients during the period
airtimeTx	Total transmitting airtime (channel) utilization during the period
radioId	Identifies the specific radio used by the AP
failedAssoc	Number of clients that failed to associate with the AP during the period
maxNumClients	Maximum number of concurrently connected clients during the period

Table 27. Attributes in the zone time radio statistics file

Column Name	Description
phyError	Number of PHY errors during the period

Zone Time WLAN Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*: `statsZoneTimeWlanDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*: `statsZoneTimeWlanHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 28. Attributes in the zone time WLAN statistics file

Column Name	Description
key	ID assigned to the zone
tenantId	ID of the MVNO account
minNumClients	Minimum number of concurrently connected clients during the period
txDataFrames_r	Total number of data frames transmitted during the period
txBytes_r	Total number of bytes transmitted during the period
txRateKbps	Transmit data rate in kilobits per second during the period
rxMgmtFrames_r	Total number of management frames received during the period
timestamp	Data aggregation time
txFrames_r	Total number of frames transmitted during the period
wsgWlanId	WLAN ID of the controller
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of concurrently connected clients during the period
txDataBytes_r	Total number of data bytes transmitted during the period
radioId	Identifies the specific radio used by the AP

Table 28. Attributes in the zone time WLAN statistics file

Column Name	Description
ssid	SSID of the WLAN
maxNumClients	Maximum number of concurrently connected clients during the period
rxMgmtBytes_r	Total number of management bytes received during the period
rxDataBytes_r	Total number of data bytes received during the period
wlanId	Identifies the specific WLAN ID on the AP
rxFrames_r	Total number of frames received during the period
rxRateKbps	Receive data rate in kilobits per second during the period
newAssoc	Number of newly associated clients during the period
txMgmtFrames_r	Total number of management frames transmitted during the period
bssid	BSSID of the WLAN
txMgmtBytes_r	Total number of management bytes transmitted during the period
ap	MAC address of the AP
failedAssoc	Number of clients that failed to associate with the AP during the period
channel	Radio channel that the AP is using

AP Time Radio Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*:
  `statsAPTimeRadioDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*:
  `statsAPTimeRadioHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 29. Attributes in the AP time radio statistics file

Column Name	Description
key	ID assigned to the AP
airtime	Total airtime (channel) utilization during the period
minNumClients	Minimum number of concurrently connected clients during the period
airtimeB	Busy airtime (channel) utilization during the period
txBytes_r	Total number of bytes transmitted during the period
rxFrames_r	Total number of data frames received during the period
newAssoc	Number of newly associated clients during the period
timestamp	Data aggregation time
txFrames_r	Total number of data frames transmitted during the period
rxBytes_r	Total number of bytes received during the period
airtimeRx	Total receiving airtime (channel) utilization during the period
avgNumClients	Average number of concurrently connected clients during the period
airtimeTx	Total transmitting airtime (channel) utilization during the period
radioId	Identifies the specific radio used by the AP
failedAssoc	Number of failed associated clients during the period
maxNumClients	Maximum number of concurrently connected clients during the period
phyError	Number of PHY errors during the period

AP Time WLAN Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*:
`statsAPTimeWlanDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*:
`statsAPTimeWlanHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 30. Attributes in the AP time WLAN statistics files

Field name	Description
key	MAC address of the AP
minNumClients	Minimum number of concurrently connected clients during the period
txFail_r	Total number of packets that failed transmission during the period
wlanId	Identifies the specific WLAN ID on the AP
txBytes_r	Total number of bytes transmitted during the period
rxFrames_r	Total number of data frames received during the period
txRateKbps	Transmit data rate in kilobits per second during the period
newAssoc	Number of newly associated clients during the period
timeStamp	Data aggregation time
rxRateKbps	Receive data rate in kilobits per second during the period
txFrames_r	Total number of data frames transmitted during the period
bssid	BSSID of the WLAN
wsgWlanId	Identified the WLAN ID in the controller system
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of concurrently connected clients during the period
ssid	SSID of the WLAN
failedAssoc	Number of clients that failed to associate with the WLAN during the period

Table 30. Attributes in the AP time WLAN statistics files

Field name	Description
maxNumClients	Maximum number of concurrently connected clients during the period
radioId	The radio on the AP used to provide the WLAN service. Possible values include 0 (2.4Ghz radio) and 1 (5GHz radio).
tenantId	ID of the MVNO account

Control Plane Statistics

Control plane statistics describe traffic related information on the control plane. The default control plane statistics file name format depends on the time period specified for uploading the file:

- If the control plane statistics file is exported *daily*: `statsCBladeSysMonDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the control plane statistics file is exported *hourly*: `statsCBladeSysMonHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

NOTE: The term “period” in the following table refers to the time interval (hourly or daily) selected in *Statistics Date Interval* on the web interface.

Table 31. Attributes in the control plane statistics file

Column Name	Description
key	Control plane ID
bond0_rxBytes	Traffic received (in bytes) on bond0
eth1_txBpsMin	Minimum transmitted throughput (in bits per second) on eth1
eth1_txPackets	Number of packets transmitted on eth1
eth2_txBytes	Transmitted traffic (in bytes) on eth2
eth0_rxBps	Received throughput (in bits per second) on eth0
bond1_rxBpsMin	Minimum received throughput (in bits per second) on bond1
eth3_rxBps	Received throughput (in bits per second) on eth3

Table 31. Attributes in the control plane statistics file

Column Name	Description
bond1_rxBpsMax	Maximum received throughput (in bits per second) on bond1
eth0_txBps	Transmitted throughput (in bits per second) on eth0
bond0_txBpsMin	Minimum transmitted throughput (in bits per second) on bond0
eth1_txBpsMax	Maximum transmitted throughput (in bits per second) on eth1
eth5_rxBps	Received throughput (in bits per second) on eth5
bond1_rxDropped	Dropped received packets on bond1
eth3_rxBpsMin	Minimum received throughput (in bits per second) on eth3
eth2_txBpsMax	Maximum transmitted throughput (bps) on eth2
eth5_txBps	Transmitted throughput (bps) on eth5
eth5_txDropped	Dropped transmitted packet on eth5
eth4_rxBpsMin	Minimum transmitted throughput (bps) on eth4
eth0_txPackets	Transmitted packet count on eth0
eth4_rxBpsMax	Maximum received throughput (bps) on eth4
eth5_rxPackets	Received packet count on eth5
eth3_txBps	Transmitted throughput (bps) on eth3
bond2_rxBps	Received throughput (bps) on bond2
diskFreeMax	Maximum free disk space
eth4_rxDropped	Dropped received packets on eth4
diskFreeMin	Minimum free disk space
eth2_txBpsMin	Minimum transmitted throughput (bps) on eth2
eth5_txBpsMin	Minimum transmitted throughput (bps) on eth5
memoryPercMax	Maximum memory percentage
bond2_rxDropped	Dropped received packet on bond2
memoryPercMin	Minimum memory percentage
eth3_txPackets	Transmitted packet count on eth3

Table 31. Attributes in the control plane statistics file

Column Name	Description
eth3_txBytes	Transmitted traffic bytes on eth3
bond0_txBytes	Transmitted traffic bytes on bond0
eth1_rxDropped	Dropped received packets on eth1
eth2_txDropped	Dropped transmitted packet on eth2
eth4_txBpsMin	Minimum transmitted throughput (bps) on eth4
timestamp	UNIX timestamp
eth3_rxDropped	Dropped received packet on eth3
eth4_txBps	Transmitted throughput (bps) on eth4
eth0_rxBpsMax	Maximum received throughput (bps) on eth0
eth1_txDropped	Dropped transmitted packet on eth1
bond1_txPackets	Transmitted packet count on bond1
bond1_rxBps	Received throughput (bps) on bond1
eth0_txDropped	Dropped transmitted packet on eth0
eth4_txBpsMax	Maximum transmitted throughput (bps) on eth4
diskFree	Free disk volume
eth0_rxDropped	Dropped received packets on eth0
bond0_txBpsMax	Maximum transmitted throughput (bps) on bond0
bond0_txBps	Maximum transmitted throughput (bps) on bond0
bond2_txBps	Transmitted throughput (bps) on bond2
eth0_rxBpsMin	Minimum transmitted throughput (bps) on eth0
eth1_rxBps	Received throughput (bps) on eth1
bond2_txBpsMax	Maximum transmitted throughput (bps) on bond2
bond0_txDropped	Dropped transmitted packets on bond0
eth1_rxBpsMax	Maximum received throughput (bps) on eth1
bond2_txBytes	Transmitted traffic bytes on bond2
eth3_rxPackets	Received packet count on eth3
diskTotalMax	Maximum total disk volume

Table 31. Attributes in the control plane statistics file

Column Name	Description
diskTotalMin	Minimum total disk volume
bond2_rxBpsMax	Maximum received throughput (bps) on bond2
diskTotal	Maximum total disk volume
eth0_txBytes	Transmitted traffic bytes on eth0
bond0_rxDropped	Dropped received packets on bond0
eth2_rxBpsMax	Maximum received throughput (bps) on eth2
eth4_rxBps	Received throughput (bps) on eth4
bond2_txBpsMin	Minimum transmitted throughput (bps) on bond2
eth5_rxBpsMin	Minimum transmitted throughput (bps) on eth5
eth1_txBytes	Transmitted traffic bytes on eth1
eth5_txPackets	Transmitted packet count on eth5
eth3_rxBytes	Received traffic bytes on eth3
bond1_txDropped	Dropped transmitted packet on bond1
eth5_txBytes	Transmitted traffic bytes on eth5
bond1_rxBytes	Received traffic bytes on bond1
bond2_txDropped	Dropped transmitted packets on bond2
bond0_txPackets	Transmitted packet count on bond0
eth5_rxDropped	Dropped received packets on eth5
eth1_rxBytes	Received traffic bytes on eth1
bond1_txBps	Minimum transmitted throughput (bps) on bond1
eth2_rxBpsMin	Minimum transmitted throughput (bps) on eth2
eth3_txBpsMin	Minimum transmitted throughput (bps) on eth3
eth5_txBpsMax	Maximum transmitted throughput (bps) on eth5
cpuPercMin	Minimum CPU usage percentage
bond0_rxBps	Received throughput (bps) on bond0
eth5_rxBpsMax	Maximum received throughput (bps) on eth5
bond0_rxBpsMin	Minimum transmitted throughput (bps) on bond0
eth0_txBpsMax	Maximum transmitted throughput (bps) on eth0

Table 31. Attributes in the control plane statistics file

Column Name	Description
memoryPerc	Memory usage percent
eth1_rxBpsMin	Minimum transmitted throughput (bps) on eth1
bond2_txPackets	Transmitted packet count on bond2
eth2_rxBytes	Received traffic bytes on eth2
eth4_txPackets	Transmitted packet count on eth4
eth4_txDropped	Dropped transmitted packet on eth4
eth2_rxDropped	Dropped received packet on eth2
cpuPerc	CPU usage percent
bond1_txBytes	Transmitted traffic bytes on bond1
bond1_rxPackets	Received packet count on bond1
bond0_rxPackets	Received packet count on bond0
eth5_rxBytes	Received traffic bytes on eth5
eth1_rxPackets	Received packet count on eth1
eth0_rxPackets	Received packet count on eth0
cpuPercMax	Maximum CPU usage percentage
eth2_txPackets	Transmitted packet count on eth2
eth4_txBytes	Transmitted traffic bytes on eth4
eth3_rxBpsMax	Maximum received throughput (bps) on eth3
eth4_rxPackets	Received packet count on eth4
bond1_txBpsMin	Minimum transmitted throughput (bps) on bond1
bond0_rxBpsMax	Maximum received throughput (bps) on bond0
eth4_rxBytes	Received traffic bytes on eth4
bond1_txBpsMax	Maximum transmitted throughput (bps) on bond1
eth0_txBpsMin	Minimum transmitted throughput (bps) on eth0
bond2_rxBytes	Received traffic bytes on bond2
eth2_rxBps	Received throughput (bps) on eth2
eth2_rxPackets	Received packet count on eth2
eth2_txBps	Transmitted throughput (bps) on eth2

Table 31. Attributes in the control plane statistics file

Column Name	Description
eth3_txBpsMax	Maximum transmitted throughput (bps) on eth3
eth0_rxBytes	Received traffic bytes on eth0
eth3_txDropped	Dropped transmitted packet on eth3
bond2_rxBpsMin	Minimum transmitted throughput (bps) on bond2
eth1_txBps	Transmitted throughput (bps) on eth1
bond2_rxPackets	Received packet count on bond2

Data Plane Statistics

Data plane statistics describe general information about the data plane. The default data plane statistic file name format is:

```
dp_YYYY_MM_DD_hh_mm_ss_ms.csv
```

where `ms` stands for three-digit milliseconds.

Table 32. Attributes in the data plane statistics file

Column	Description
key	MAC address of the data plane
bladeId	Data plane ID
name	Name of the data plane
model	Model of the data plane
serialNumber	Serial number of the data plane
fwVersion	Current firmware version of the data plane
uptime	Number of minutes elapsed since the data plane was last rebooted
chassisID	Data plane associated with the control plane's MAC address
ip	IP address assigned to the data plane
creationTime	Timestamp when the data plane connected to the controller
lastSeen	Timestamp of the data plane's latest connection

Data Plane Ethernet Port Statistics

Data plane Ethernet port statistics describe traffic related information on the data plane. The default data plane statistic file name format is:

```
dpEthPortStatistics_YYYY_MM_DD_hh_mm_ss_ms.csv
```

where `ms` stands for three-digit milliseconds.

Table 33. Attributes in the data plane Ethernet port statistics file

Column	Description
dBladeId	MAC address of the data plane
portId	Data plane port ID (either 1 or 2)
timeIntervalInMillis	Unix timestamp when these statistics were collected. These statistics are collected at 15-minute intervals (for example, 10:00, 10:15. 10:30).
txRate	The rate at which the data plane was transmitting data at the time the controller generated this report
rxRate	The rate at which the data plane was receiving data at the time the controller generated this report
txPkts	Incremental packet count transmitted during the 15-minute interval
rxPkts	Incremental packet count received during the 15-minute interval
txDrops	Incremental transmitted packet count dropped during the 15-minute interval
rxDrops	Incremental received packet count dropped during the 15-minute interval
txBytes	Incremental bytes transmitted during the 15-minute interval
rxBytes	Incremental bytes received during the 15-minute interval

AP SoftGRE Tunnel Statistics

AP SoftGRE tunnel statistics describe SoftGRE tunnel-related information. The default AP SoftGRE tunnel statistics file name format is:

```
statsAPSoftGRETunnel_YYYY_MM_DD_hh_mm_ss_ms.csv
```

where `ms` stands for three-digit milliseconds.

Table 34. Attributes in the AP SoftGRE tunnel statistics file

Column	Description
gw	IP address or FQDN of the SoftGRE gateway
apMac	MAC address of the AP
apIpAddress	IP address of the AP
timeIntervalInMillis	Unix timestamp when these statistics were collected. These statistics are collected at 15-minute intervals (for example, 10:00, 10:15. 10:30).
accessType	This value is always “SoftGRE.”
zoneId	Zone UUID
txPkts	TX packet count of GRE interface
txBytes	TX byte count of GRE interface
rxPkts	RX packet count of GRE interface
rxBytes	RX byte count of GRE interface
txErrPkts	TX error packet count of GRE interface
rxErrPkts	RX error packet count of GRE interface
txDropPkts	TX drop packet count of GRE interface
rxDropPkts	RX drop packet count of GRE interface
txFragPkts	Oversized packet count
cICMP	ICMP count
cNonICMP	No-reply ICMP count
cDisconnect	Disconnect count

SoftGRE Gateway Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*:
  `statsSoftGREGatewayDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*:
  `statsSoftGREGatewayHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 35. Attributes in the SoftGRE gateway statistics files

Column Name	Description
gw	IP address or FQDN of the SoftGRE gateway
txPkts	MAC address of the AP
txBytes	IP address of the AP
rxPkts	Unix timestamp when these statistics were collected. These statistics are collected at 15-minute intervals (for example, 10:00, 10:15. 10:30).
rxBytes	This value is always “SoftGRE.”
txErrPkts	Zone UUID
rxErrPkts	TX packet count of GRE interface
txDropPkts	TX byte count of GRE interface
rxDropPkts	RX packet count of GRE interface
txFragPkts	RX byte count of GRE interface
cICMP	TX Error packet count of GRE interface
cNonICMP	RX Error packet count of GRE interface
cDisconnect	TX Drop packet count of GRE interface

Tenant Time Radio Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*: `statsTenantTimeRadioDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*: `statsTenantTimeRadioHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 36. Attributes in the tenant time radio statistics file

Column Name	Description
key	Tenant identity
rxDataFrames_r	Total number of data frames received during the period
minNumClients	Minimum number of connected clients (concurrent) during the period
txDataFrames_r	Total number of data frames transmitted during the period
txBytes_r	Total number of bytes transmitted during the period
txRateKbps	Transmitted data rate expressed in kilobits per second for the period
rxMgmtFrames_r	Total number of management frames received during the period
timestamp	Data aggregation time
txFrames_r	Total number of data frames transmitted during the period
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of connected clients (concurrent) during the period
txDataBytes_r	Total number of data bytes transmitted during the period
radioId	Denotes the specific radio within the AP
maxNumClients	Maximum number of connected clients (concurrent) during the period
rxMgmtBytes_r	Total number of management bytes received during the period
rxDataBytes_r	Total number of data bytes received during the period

Table 36. Attributes in the tenant time radio statistics file

Column Name	Description
rxFrames_r	Total number of data frames received during the period
rxRateKbps	Received data rate expressed in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txMgmtFrames_r	Total number of management frames transmitted during the period
txMgmtBytes_r	Total number of management bytes transmitted during the period
ap	MAC address of the AP
failedAssoc	Number of clients that failed to associate during the period
channel	Radio channel that the AP is using

Tenant Time WLAN Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*: `statsTenantTimeWlanDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*: `statsTenantTimeWlanHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 37. Attributes in the tenant time WLAN statistics

Column Name	Description
key	Tenant identity
rxDataFrames_r	Total number of data frames received during the period
minNumClients	Minimum number of connected clients (concurrent) during the period
txDataFrames_r	Total number of data frames transmitted during the period
txBytes_r	Total number of bytes transmitted during the period
txRateKbps	Transmitted data rate expressed in kilobits per second for the period
rxMgmtFrames_r	Total number of management frames received during the period
timestamp	Data aggregation time
txFrames_r	Total number of data frames transmitted during the period
wsgWlanId	Represents the WLAN in the controller system
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of connected clients (concurrent) during the period
txDataBytes_r	Total number of data bytes transmitted during the period
radioId	Denotes the specific radio on the AP
ssid	SSID string of the WLAN
maxNumClients	Maximum number of connected clients (concurrent) during the period

Table 37. Attributes in the tenant time WLAN statistics

Column Name	Description
rxMgmtBytes_r	Total number of management bytes received during the period
rxDataBytes_r	Total number of data bytes received during the period
wlanId	Denotes the specific WLAN on the AP
rxFrames_r	Total number of data frames received during the period
rxRateKbps	Received data rate expressed in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txMgmtFrames_r	Total number of management frames transmitted during the period
bssid	BSSID string of the WLAN
txMgmtBytes_r	Total number of management bytes transmitted during the period
zoneUUID	Zone identity
ap	MAC address of the AP
failedAssoc	Number of clients that failed to associate during the period
channel	Radio channel that the AP is using

Tenant Zone Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*:
  `statsTenantZoneDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*:
  `statsTenantZoneHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 38. Attributes in the tenant zone statistics

Column Name	Description
key	Tenant identity
rxDataFrames_r	Total number of data frames received during the period
minNumClients	Minimum number of connected clients (concurrent) during the period
txDataFrames_r	Total number of data frames transmitted during the period
txBytes_r	Total number of bytes transmitted during the period
txRateKbps	Transmitted data rate expressed in kilobits per second for the period
rxMgmtFrames_r	Total number of management frames received during the period
timestamp	Data aggregation time
txFrames_r	Total number of data frames transmitted during the period
wsgWlanId	Represents the WLAN in the controller system
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of connected clients (concurrent) during the period
txDataBytes_r	Total number of data bytes transmitted during the period
ssid	SSID string of the WLAN
maxNumClients	Maximum number of connected clients (concurrent) during the period
rxMgmtBytes_r	Total number of management bytes received during the period

Table 38. Attributes in the tenant zone statistics

Column Name	Description
rxDataBytes_r	Total number of data bytes received during the period
rxFrames_r	Total number of data frames received during the period
rxRateKbps	Received data rate expressed in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txMgmtFrames_r	Total number of management frames transmitted during the period
txMgmtBytes_r	Total number of management bytes transmitted during the period
zoneUUID	Zone identity
ap	MAC address of the AP
failedAssoc	Number of clients that failed to associate during the period
channel	Radio channel that the AP is using

Tenant Zone Radio Statistics

The default file name format depends on the time period specified for uploading the statistics file:

- If the statistics file is exported *daily*: `statsTenantZoneRadioDay_YYYY_MM_DD_hh_mm_ss_ms.csv`
- If the statistics file is exported *hourly*: `statsTenantZoneRadioHour_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 39. Attributes in the tenant zone radio statistics

Column Name	Description
key	Tenant identity
rxDataFrames_r	Total number of data frames received during the period
minNumClients	Minimum number of connected clients (concurrent) during the period
txDataFrames_r	Total number of data frames transmitted during the period
txBytes_r	Total number of bytes transmitted during the period
txRateKbps	Transmitted data rate expressed in kilobits per second for the period
rxMgmtFrames_r	Total number of management frames received during the period
timestamp	Data aggregation time
txFrames_r	Total number of data frames transmitted during the period
rxBytes_r	Total number of bytes received during the period
avgNumClients	Average number of connected clients (concurrent) during the period
txDataBytes_r	Total number of data bytes received during the period
radioId	Denote the specific radio within the AP
maxNumClients	Maximum number of connected clients (concurrent) during the period
rxMgmtBytes_r	Total number of management bytes received during the period
rxDataBytes_r	Total number of data bytes received during the period

Table 39. Attributes in the tenant zone radio statistics

Column Name	Description
rxFrames_r	Total number of data frames received during the period
rxRateKbps	Received data rate expressed in kilobits per second for the period
newAssoc	Number of newly associated clients during the period
txMgmtFrames_r	Total number of management frames transmitted during the period
txMgmtBytes_r	Total number of management bytes transmitted during the period
zoneUUID	Zone identity
ap	MAC address of the AP
failedAssoc	Number of failed associated clients during the period
channel	Radio channel that the AP is using

Tenant Inventory File

The tenant inventory file contains detailed information about each tenant account that has been created on the controller.

The default tenant inventory file name format is:

`tenant_YYYY_MM_DD_hh_mm_ss_ms.csv`

where `ms` stands for three-digit milliseconds.

Table 40. Attributes in the tenant inventory statistics

Column Name	Description
key	Tenant identity
Phone	Phone number of the tenant
adminUUID	UUID of the creator
createdDatetime	Unix timestamp when the tenant was created
city	City where the tenant is located
address	Address of the tenant
email	Email address of the tenant
description	Description of the account
modifiedDatetime	Unix timestamp when the account was last updated
name	Name of the tenant

Ports to Open for AP-Controller Communication

A

AP-SCG/SZ/vSZ Communication

The table below lists the ports that must be opened on the network firewall to ensure that the SCG/SZ/vSZ (controller), managed APs, and RADIUS servers can communicate with each other successfully.

Table 1. Ports to open for AP-SCG/SZ/vSZ-H communication

Port Number	Layer 4 Protocol	Source	Destination	Configurable from Web Interface?	Purpose
21	TCP	AP	Controller	Yes	FTP upload of reports, statistics, and configuration backups
22	TCP	AP	Controller (control plane)	No	SSH tunnel
49	TCP	TACACS + server	Controller	Yes	TACACS+ based authentication of controller administrators
91	TCP	AP	Controller (control plane)	No	AP firmware upgrade
123	UDP	AP	Controller (control plane)	No	NTP sync up • Not required in 2.1.2, 2.1.3, 2.5.1, 2.6, 3.0 • Required in1.x, 2.1, 2.1.1, 2.5
443	TCP	AP	Controller (control plane)	No	Access to the SCG/SZ/vSZ web interface via HTTPS

Table 1. Ports to open for AP-SCG/SZ/vSZ-H communication

Port Number	Layer 4 Protocol	Source	Destination	Configurable from Web Interface?	Purpose
8443	TCP	Any	Controller	No	Access to the SCG/SZ/vSZ web interface via HTTPS
23232	TCP	AP	SCG (data plane)	No	GRE tunnel
23233	UDP	AP	SCG (data plane)	Yes	GRE tunnel (required only when tunnel mode is GRE over UDP)
12222/ 12223	UDP	AP	Controller	No	LWAPP discovery
1812/1813	UDP	AP	RADIUS	Yes	AAA authentication and accounting
8022	No (SSH)	Any	Management interface	Yes	Management ACL for one-port configuration
8090	TCP	Any	Controller	No	Allows unauthorized UEs to browse to an HTTP website
8099	TCP	Any	Controller	No	Allows unauthorized UEs to browse to an HTTPS website
8100	TCP	Any	Controller	No	Allows unauthorized UEs to browse using a proxy UE
8111	TCP	Any	Controller	No	Allows authorized UEs to browse using a proxy UE
9080	HTTP	Any	Controller	No	Northbound Portal Interface for hotspots
9443	HTTPS	Any	Controller	No	Northbound Portal Interface for hotspots
9998	TCP	Any	Controller	No	Internal WISPr portal

AP-ZD Communication

The table below lists the ports that must be opened on the network firewall to ensure that the ZoneDirector (ZD), its managed APs, and other network devices can communicate with each other successfully.

Table 2. Ports to open for AP-ZoneDirector communication

Port Number	Layer 4 Protocol	Source	Destination	Configurable from Web Interface?	Purpose
21	TCP	AP	ZD	No	AP firmware upgrade (the firewall must be stateful for PASV FTP transfers)
22	TCP	AP	ZD	No	AP statistics reporting (via SSH)
22	TCP	Any	ZD	No	Access to the ZoneDirector CLI (via SSH)
49	TCP	TACACS+ server	ZD	Yes	TACACS+ based authentication of ZoneDirector administrators
80	TCP	Any	ZD	No	Access to the ZoneDirector web interface (via HTTP)
443	TCP	ZD	FlexMaster	No	Registration, inform, firmware upgrade messages
8443	TCP	Any	ZD	No	Access to the ZoneDirector web interface (via HTTPS)
18301	UDP	AP	ZD	No	SpeedFlex
12222/ 12223	UDP	AP	ZD	No	LWAPP discovery
443/33003	TCP	ZD (primary)	ZD (backup)	No	Smart Redundancy

Table 2. Ports to open for AP-ZoneDirector communication

Port Number	Layer 4 Protocol	Source	Destination	Configurable from Web Interface?	Purpose
Varies (specified in FM Inventory 'Device Web Port Number Mapping')	TCP	FlexMaster	ZD	Yes	Access to the ZoneDirector web interface

SoftGRE Support

B

This appendix describes the SoftGRE support that the controller provides and the supported deployment topology. Topics include:

- Overview of SoftGRE Support
- Supported Deployment Scenario
- SoftGRE Packet Format

Overview of SoftGRE Support

There are numerous equipment vendors serving the service provider market today. Among these vendors, the more prominent ones include Alcatel-Lucent (ALU), Ericsson, NSN, Huawei and Cisco. Most of these vendors support different tunneling and mobility management protocols at their packet gateways.

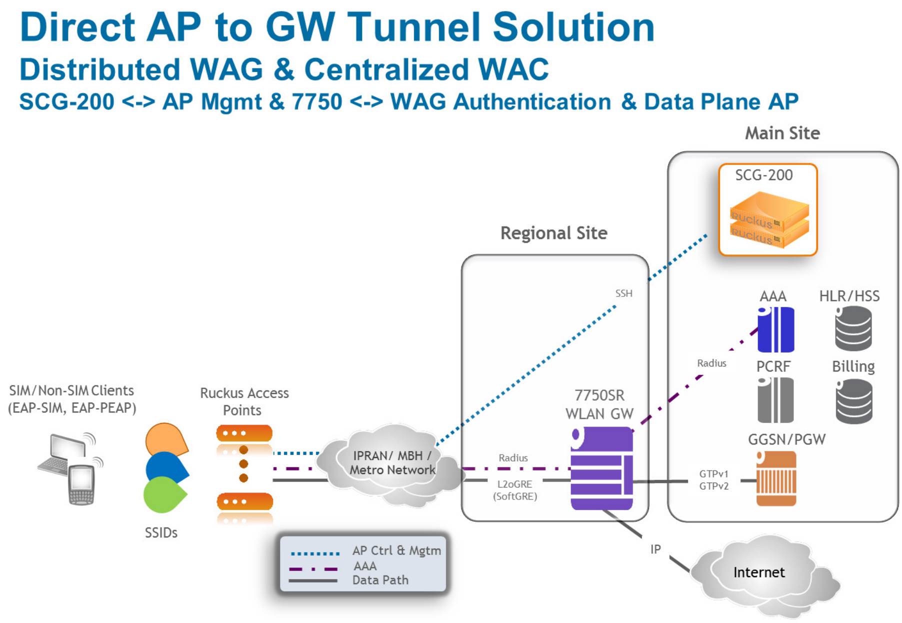
Since most (if not all) of these equipment vendors do not develop access points themselves, they are publishing SoftGRE specifications to enable access point vendors (such as Ruckus Wireless) to support SoftGRE on their devices.

Supported Deployment Scenario

The controller supports SoftGRE in the deployment scenario wherein the controller functions purely as an AP controller. In this deployment topology, the controller only manages the Ruckus Wireless APs and does not perform other functions. All control paths (RADIUS Authentication/Accounting) and data paths (SoftGRE tunnel) terminate on the third party WLAN gateway.

If 802.1x authentication is used, the RADIUS server will be outside of the SoftGRE tunnel. If open, WISPr-based authentication is used, the portal or redirect function will be on the edge router or northbound of the edge router. The controller does not play any role in the control and data path functions (see Figure 1).

Figure 1. The controller as a pure AP controller



Direct AP to GW Tunnel Solution

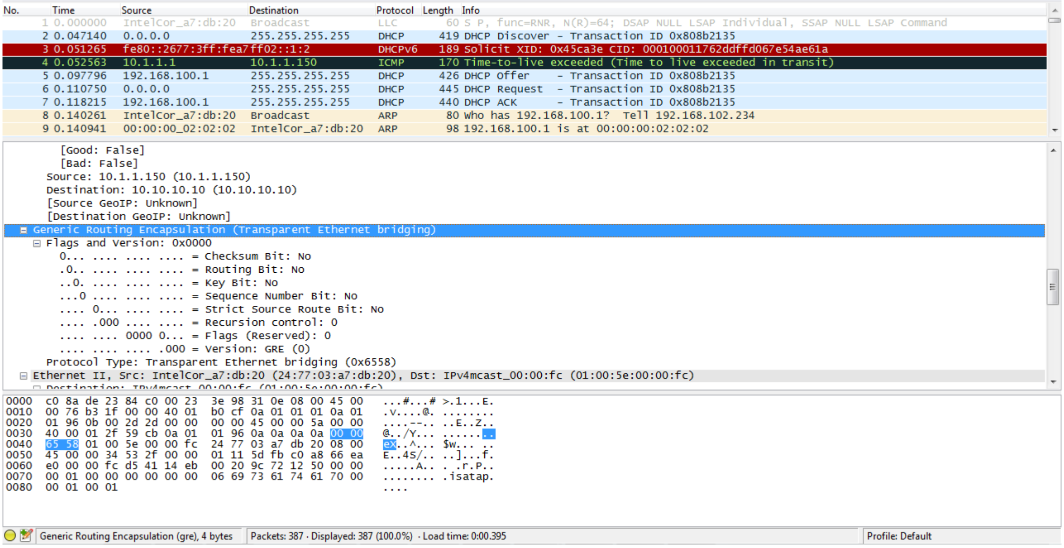
Distributed WAG & Centralized WAC

SCG-200 <-> AP Mgmt & 7750 <-> WAG Authentication & Data Plane AP

SoftGRE Packet Format

Figure displays a screen shot of SoftGRE packet capture data.

Figure 2. Example of SoftGRE packet format



```
No.   Time       Source              Destination       Protocol Length Info
    1 0.000000   IntelCor_a7:db:20   Broadcast         LLC        60 S P, func=RNR, N(R)=64; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    2 0.047140   0.0.0.0             255.255.255.255   DHCP      419 DHCP Discover - Transaction ID 0x808b2135
    3 0.051265   fe80::2677:3ff:fea7ff02::1:2          DHCPv6    189 Solicit XID: 0x45ca3e CID: 000100011762ddffd067e54ae61a
    4 0.052563   10.1.1.1            10.1.1.150        ICMP      170 Time-to-live exceeded (Time to live exceeded in transit)
    5 0.097796   192.168.100.1       255.255.255.255   DHCP      426 DHCP Offer    - Transaction ID 0x808b2135
    6 0.110750   0.0.0.0             255.255.255.255   DHCP      445 DHCP Request  - Transaction ID 0x808b2135
    7 0.118215   192.168.100.1       255.255.255.255   DHCP      440 DHCP ACK      - Transaction ID 0x808b2135
    8 0.140261   IntelCor_a7:db:20   Broadcast         ARP        80 Who has 192.168.100.1?  Tell 192.168.102.234
    9 0.140941   00:00:00_02:02:02   IntelCor_a7:db:20 ARP        98 192.168.100.1 is at 00:00:00:02:02:02
```

```
        [Good: False]
        [Bad: False]
      Source: 10.1.1.150 (10.1.1.150)
      Destination: 10.10.10.10 (10.10.10.10)
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
⊟ Generic Routing Encapsulation (Transparent Ethernet bridging)
  ⊟ Flags and Version: 0x0000
        0... .... .... .... = Checksum Bit: No
        .0.. .... .... .... = Routing Bit: No
        ..0. .... .... .... = Key Bit: No
        ...0 .... .... .... = Sequence Number Bit: No
        .... 0... .... .... = Strict Source Route Bit: No
        .... .000 .... .... = Recursion control: 0
        .... .... 0000 0... = Flags (Reserved): 0
        .... .... .... .000 = Version: GRE (0)
      Protocol Type: Transparent Ethernet bridging (0x6558)
⊟ Ethernet II, Src: IntelCor_a7:db:20 (24:77:03:a7:db:20), Dst: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
  ⊟ Destination: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
```

```
0000  c0 8a de 23 84 c0 00 23  3e 98 31 0e 08 00 45 00   ...#...# >.1...E.
0010  00 76 b3 1f 00 00 40 01  b0 cf 0a 01 01 01 0a 01   .v....@. ........
0020  01 96 0b 00 2d 2d 00 00  00 00 45 00 00 5a 00 00   ....--.. ..E..Z..
0030  40 00 01 2f 59 cb 0a 01  01 96 0a 0a 0a 0a 00 00   @../Y... ........
0040  65 58 01 00 5e 00 00 fc  24 77 03 a7 db 20 08 00   eX..^... $w... ..
0050  45 00 00 34 53 2f 00 00  01 11 5d fb c0 a8 66 ea   E..4S/.. ..]...f.
0060  e0 00 00 fc d5 41 14 eb  00 20 9c 72 12 50 00 00   .....A.. . .r.P..
0070  00 01 00 00 00 00 00 00  06 69 73 61 74 61 70 00   ........ .isatap.
0080  00 01 00 01                                        ....
```

Generic Routing Encapsulation (gre), 4 bytes | Packets: 387 · Displayed: 387 (100.0%) · Load time: 0:00.395 | Profile: Default

Configuring SoftGRE

This section describes the configuration options for the SoftGRE feature.

- Creating an AP Zone That Supports SoftGRE
- Changing the Tunnel Type from SoftGRE

Creating an AP Zone That Supports SoftGRE

For information on how to create an AP zone that supports SoftGRE tunneling, see Working with AP Zones.

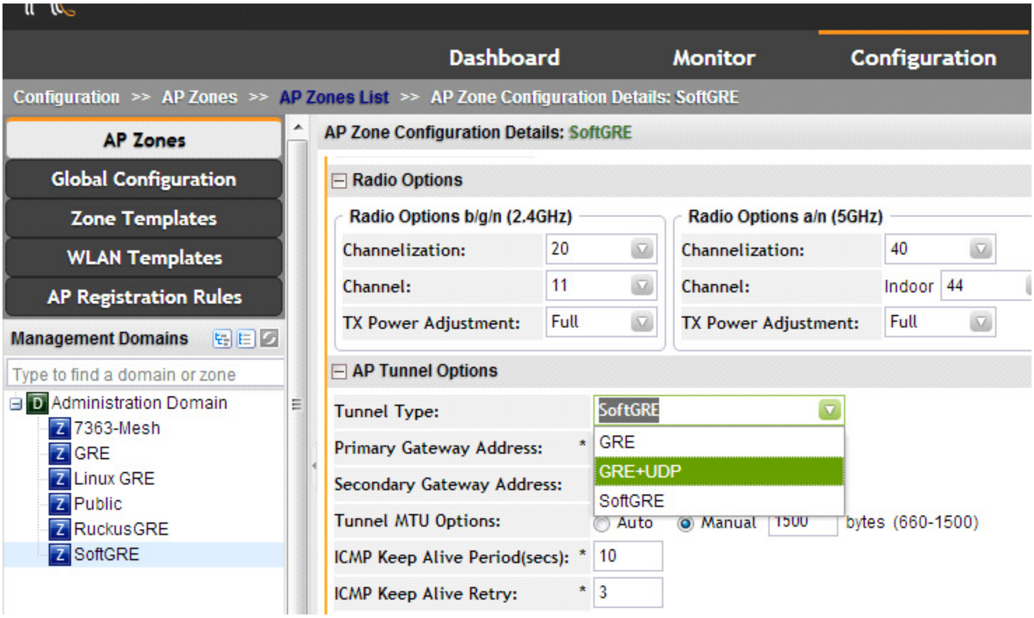
NOTE: MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

Changing the Tunnel Type from SoftGRE

If no tunneled WLANs exist in the zone, you can change the tunnel type from **SoftGRE** to **GRE** or **GRE + UDP**. Follow these steps to change the tunnel type from SoftGRE.

1. Go to **Configuration** > **AP Zones** page.
2. On the *AP Zone List* page, click the name of the zone that you want to edit. The *Zone Configuration* page appears.
3. Click **Edit**.
4. Scroll down to the *AP GRE Tunnel Option* section.
5. In *AP Tunnel Type*, select the tunnel type to which you want to change from **SoftGRE**.
6. Click **Apply**.

Figure 3. Change the tunnel type from SoftGRE to GRE or GRE+UDP



AP Zone Configuration Details: SoftGRE

Radio Options

Radio Options b/g/n (2.4GHz)

Channelization: 20
Channel: 11
TX Power Adjustment: Full

Radio Options a/n (5GHz)

Channelization: 40
Channel: Indoor 44
TX Power Adjustment: Full

AP Tunnel Options

Tunnel Type: SoftGRE
Primary Gateway Address: *
Secondary Gateway Address:
Tunnel MTU Options: ○ Auto ● Manual 1500 bytes (660-1500)
ICMP Keep Alive Period(secs): * 10
ICMP Keep Alive Retry: * 3

If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

```
Unable to update the configuration of the AP zone. Reason: It is
disallowed to change the tunnel type, because it has tunneled WLAN.
```

Monitoring SoftGRE

You can use the *Monitor* pages to view AP SoftGRE statistics. This section describes:

- Checking the AP Tunnel Type of a Zone
- Viewing SoftGRE Traffic Statistics of an AP

Checking the AP Tunnel Type of a Zone

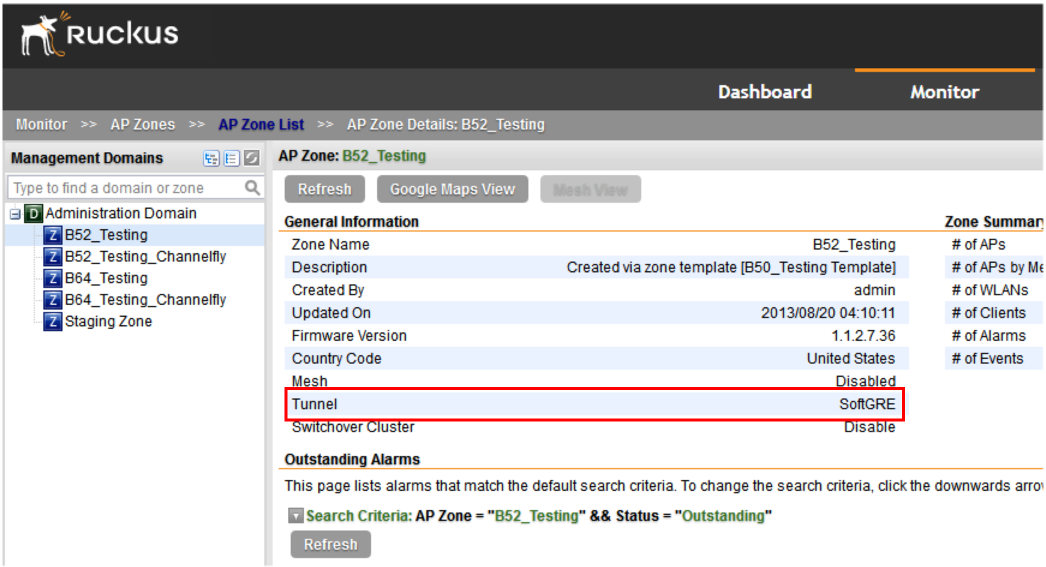
Follow these steps to check if a zone is using SoftGRE tunneling.

1 Go to *Monitor* > *AP Zone*.

2 In the *Administration Domain* tree, click each AP zone name to display their zone information summary.

3 In the *General Information* section, check the value for *Tunnel*. If the value shown is **SoftGRE**, this indicates that the zone is using SoftGRE tunneling.

Figure 4. Check the value for “Tunnel” to verify that a zone is using SoftGRE tunneling



General Information

Zone Name	B52_Testing
Description	Created via zone template [B50_Testing Template]
Created By	admin
Updated On	2013/08/20 04:10:11
Firmware Version	1.1.2.7.36
Country Code	United States
Mesh	Disabled
Tunnel	SoftGRE
Switchover Cluster	Disable

Zone Summar

- # of APs
- # of APs by Me
- # of WLANs
- # of Clients
- # of Alarms
- # of Events

Outstanding Alarms

This page lists alarms that match the default search criteria. To change the search criteria, click the downwards arro

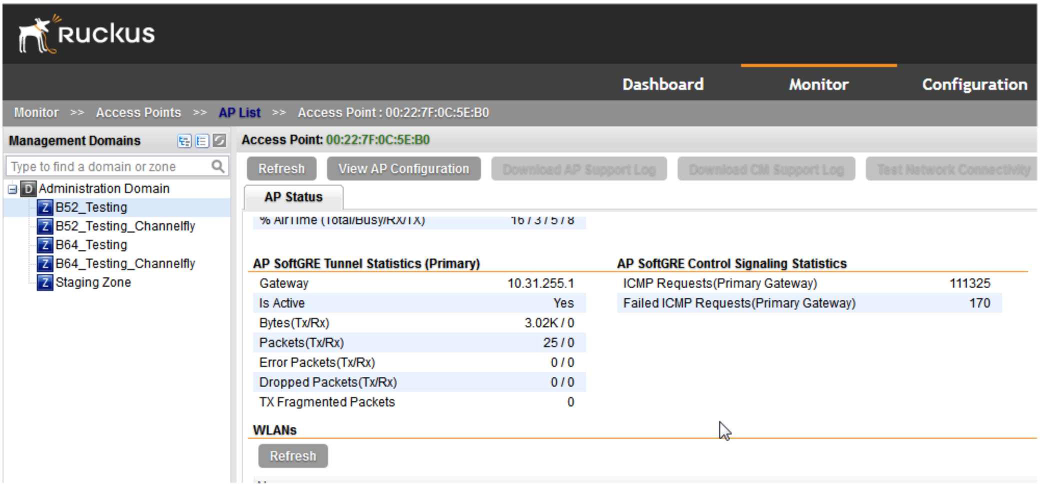
Search Criteria: AP Zone = "B52_Testing" && Status = "Outstanding"

Viewing SoftGRE Traffic Statistics of an AP

Follow these steps to view the SoftGRE tunnel statistics of an AP that belongs to a zone enabled for SoftGRE.

1. Go to *Monitor* > *Access Points*.
2. In the *Administration Domain* tree, click a zone that is enabled for SoftGRE. The APs that appear on the *AP List* page are all using SoftGRE tunneling.
3. Click the MAC address of an AP whose SoftGRE traffic statistics you want to view.
4. On the **AP Status** tab, scroll down to the *AP SoftGRE Tunnel Statistics* section to view the AP SoftGRE statistics. Additional SoftGRE statistics appear in the *AP SoftGRE Control Signaling Statistics* section. Table 3 describes the SoftGRE statistics that appear.

Figure 5. AP SoftGRE statistics on the Monitor page



% AirTime (Total/Busy/RX/TX)	16 / 3 / 5 / 8

AP SoftGRE Tunnel Statistics (Primary)

Gateway	10.31.255.1
Is Active	Yes
Bytes(Tx/Rx)	3.02K / 0
Packets(Tx/Rx)	25 / 0
Error Packets(Tx/Rx)	0 / 0
Dropped Packets(Tx/Rx)	0 / 0
TX Fragmented Packets	0

AP SoftGRE Control Signaling Statistics

ICMP Requests(Primary Gateway)	111325
Failed ICMP Requests(Primary Gateway)	170

Table 3. SoftGRE statistics of an AP

Statistic	Description
Gateway	The IP address of the gateway server
Is Active	• Yes, if the gateway is currently active • No, if the gateway is inactive
Bytes (Tx/Rx)	The number bytes transmitted/received (Tx/Rx) through the SoftGRE tunnel
Packets (Tx/Rx)	The number packets transmitted/received (Tx/Rx) through the SoftGRE tunnel
Error Packets (Tx/Rx)	The number of packets with errors. Tx errors may be caused by any of the following: • No routing entry to destination • Invalid routing entry (routing traffic to tunnel interface itself) • Transmission error in core IP layer of Linux Rx errors may be caused by any of the following: • Bad packets received, checksum does not match (remote peer enables CSUM field in GRE header) • Sequence number does not match (remote peer enables SEQ field in GRE header) • SKB error during GRE decapsulation.
Dropped Packets (Tx/Rx)	The number of packets that have been dropped. • Tx dropped packets may be due to insufficient space in the Linux buffer or insufficient memory when allocating extra buffer for GRE encapsulation. • Rx dropped packets may be due to insufficient space in the Linux buffer.
TX Fragmented Packets	The number of oversized Tx packets.
ICMP Requests	The total number of ICMP requests
Failed ICMP Requests	The total number of failed ICMP requests

You have completed viewing the AP SoftGRE statistics.

This chapter lists the SNMP MIBs, alarms, and events that are related to SoftGRE.

SoftGRE SNMP MIBs

Table 4 lists the SoftGRE related OIDs.

Table 4. OIDs related to SoftGRE

Parent Node	Node Name	OID
ruckusWLANAPInfo	ruckusSCGWLANAPMacAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.1
	ruckusSCGWLANAPSoftGREServer	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.2
	ruckusSCGWLANAPSoftGREGWAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.3
	ruckusSCGWLANAPSoftGREActive	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.4
	ruckusSCGWLANAPSoftGRETxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.5
	ruckusSCGWLANAPSoftGRETxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.6
	ruckusSCGWLANAPSoftGRERxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.7
	ruckusSCGWLANAPSoftGRERxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.8
	ruckusSCGWLANAPSoftGRETxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.9
	ruckusSCGWLANAPSoftGRERxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.10
	ruckusSCGWLANAPSoftGRETxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.11
	ruckusSCGWLANAPSoftGRERxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.12
	ruckusSCGWLANAPSoftGRETxPktsFrag	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.13
	ruckusSCGWLANAPSoftGREICMPTotal	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.14
	ruckusSCGWLANAPSoftGREICMPNoReply	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.15

Table 4. OIDs related to SoftGRE

Parent Node	Node Name	OID
	ruckusSCGWLANAPSoftGREDisconnect	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.16

SoftGRE Alarms and Events

If there is no downstream traffic in the tunnel, APs that belong to the zone configured for SoftGRE send out-of-band ICMP keep-alive messages (interval is configurable) to the active third party WLAN gateway. If an AP does not receive a response from the active WLAN gateway, it triggers an alarm and it automatically creates a SoftGRE tunnel to the standby WLAN gateway.

If the AP does not receive a response from the standby WLAN gateway either, the AP disconnects all tunneled WLAN services. It continues to send keep-alive messages to both the active WLAN gateway (primary GRE remote peer) and standby WLAN gateway (secondary GRE remote peer). If it receives a response from either WLAN gateway, the AP restores all tunneled WLAN services automatically.

There are four types of events that APs send to the controller:

- Failover from primary GRE remote peer to secondary GRE remote peer
- Failover from secondary GRE remote peer to primary GRE remote peer.
- Tunnel disconnected because both primary and secondary GRE remote peers are unreachable
- Tunnel restored because either primary or secondary GRE remote peer is reachable

For the list of alarms and events related to SoftGRE that APs generate, refer to SoftGRE Events and SoftGRE Alarms.

SoftGRE Events

Table 5lists the SoftGRE related events that APs send to the controller.

Table 5. SoftGRE related events that APs send to the controller

Event Code	Event Type	Severity	Event Attributes	Event Description
611	apSoftGRETunnelFailoverPtoS	Warning	"apMac"="xx:xx:xx:xx:xx:xx", "primaryGRE"="xxx.xxx.xxx.xxx", "secondaryGRE"="xxx.xxx.xxx.xxx	"AP [{apname@apMac}] fails over from primaryGRE [{address}] to secondaryGRE [{address}].
612	apSoftGRETunnelFailoverStoP	Warning	"apMac"="xx:xx:xx:xx:xx:xx", "secondaryGRE"="xxx.xxx.xxx.xxx", "primaryGRE"="xxx,xxx.xxx.xxx	"AP [{apname@apMac}] fails over from secondaryGRE [{address }] to primaryGRE [{address}].
613	apSoftGREGatewayReachable	Informational	"apMac"="xx:xx:xx:xx:xx:xx", "softgreGW"="primaryGRE", "softgreGWAddress" = "xxx.xxx.xxx.xxx"	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.
614	apSoftGREGatewayNotReachable	Critical	apMac"="xx:xx:xx:xx:xx:xx", "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"	AP [{apname@apMac}] is unable to reach the following gateways: [{gateway list}]. ?"

SoftGRE Alarms

Table 6 lists the SoftGRE related alarms that APs send to the controller.

Table 6. SoftGRE related alarms that APs send to the controller

Alarm Code	Alarm Type	Default to Trap	Severity	Attributes	Description
611	apSoftGRETunnelFailoverPtoS	true	major	• "apMac"="xx:xx:xx:xx:xx:xx" • "primaryGRE"="xxx.xxx.xxx.xxx" • "secondaryGRE"="xxx.xxx.xxx.xxx	AP[{apname@apMac}] fails over from primaryGRE[{address}] to secondaryGRE[{address}].
612	apSoftGRETunnelFailoverStoP	true	major	• "apMac"="xx:xx:xx:xx:xx:xx" • "secondaryGRE"="xxx.xxx.xxx.xxx" • "primaryGRE"="xxx,xxx.xxx.xxx	AP[{apname@apMac}] fails over from secondaryGRE[{address }] to primaryGRE[{address}].
613	apSoftGREGatewayReachable	true	informational	• "apMac"="xx:xx:xx:xx:xx:xx" • "softgreGW"="primaryGRE" • "softgreGWAddress" = "xxx.xxx.xxx.xxx"	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.
614	apSoftGREGatewayNotReachable	true	major	• “apMac"="xx:xx:xx:xx:xx:xx" • "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"	AP [{apname@apMac }] is unable to reach the following gateways: [{gateway list}].

Replacing Hardware Components C

This appendix describes how to replace hardware components (including hard disk drives, power supply units, and system fans) on the controller.

In this appendix:

- Installing or Replacing Hard Disk Drives
- Replacing PSUs
- Replacing System Fans

Installing or Replacing Hard Disk Drives

You can install up to six hot-swappable SAS or SATA hard disk drives on the controller. The drives go into carriers that connect to the SAS/SATA backplane board once the carriers with drives attached are inserted back into the drive bays. The controller ships with six drive carriers.

CAUTION! If you install fewer than six hard disk drives, the unused drive bays must contain the empty carriers that ship with the server to maintain proper cooling.

Ordering a Replacement Hard Disk

To order a replacement hard disk for the controller, contact your Ruckus Wireless sales representative and place an order for FRU part number 902-0188-0000 (Hard Drive, 600GB, 10K RPM, 64MB Cache 2.5 SAS 6Gb/s, Internal).

CAUTION! Use only FRU part number 902-0188-0000 as replacement hard disk for the controller. Using other unsupported hard disks will render the controller hardware warranty void.

Removing the Front Bezel

You must remove the front bezel to add or replace a hard drive in one of the drive bays. It is not necessary to remove the front chassis cover or to power down the system. The hard drives are hot-swappable.

Follow these steps to remove the front bezel of the controller.

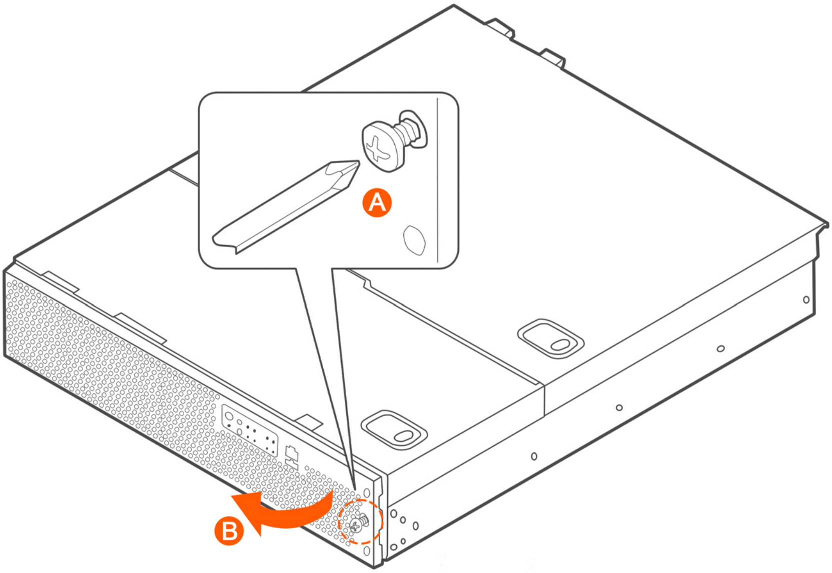
You need to remove the front bezel for tasks such as:

- Installing or removing hard disk drives or an SD flash card
- Observing the individual hard disk drive activity/fault indicators
- Replacing the control panel LED/switch board

The server does not have to be powered down just to remove the front bezel.

1. Loosen the captive bezel retention screw on the right side of the bezel (see A in Figure 6).
2. Rotate the bezel to the left to free it from the pins on the front panel (see B in Figure 6), and then remove it.

Figure 6. Removing the front bezel

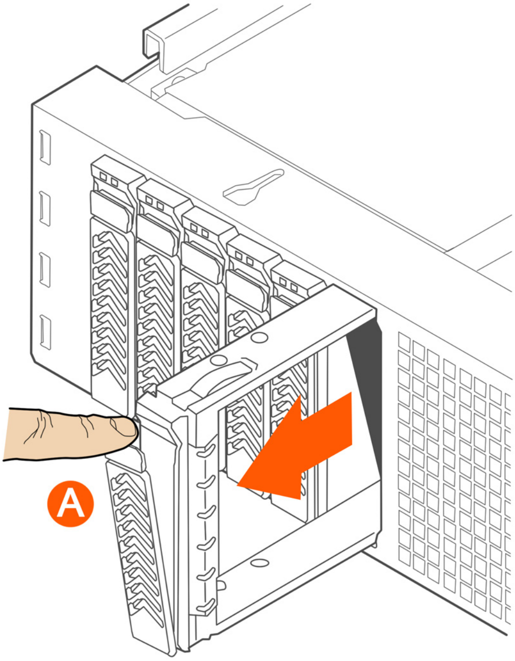


Removing an HDD Carrier from the Chassis

Follow these steps to remove a hard disk drive carrier from the chassis.

1. Remove the front bezel (see Removing the Front Bezel).
2. Select the drive bay where you want to install or replace the drive. Drive bay 0 must be used first, then drive bay 1 and so on. The drive bay numbers are printed on the front panel below the drive bays.
3. Remove the drive carrier by pressing the green button to open the lever (see A in Figure 7).
4. Pull the drive carrier out of the chassis.

Figure 7. Removing the drive carrier

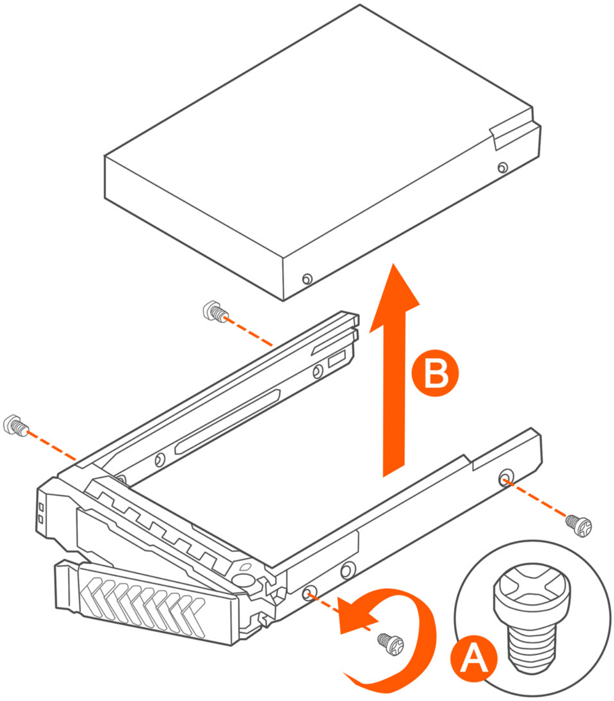


Installing a Hard Drive in a Carrier

Follow these steps to install a hard drive in a drive carrier.

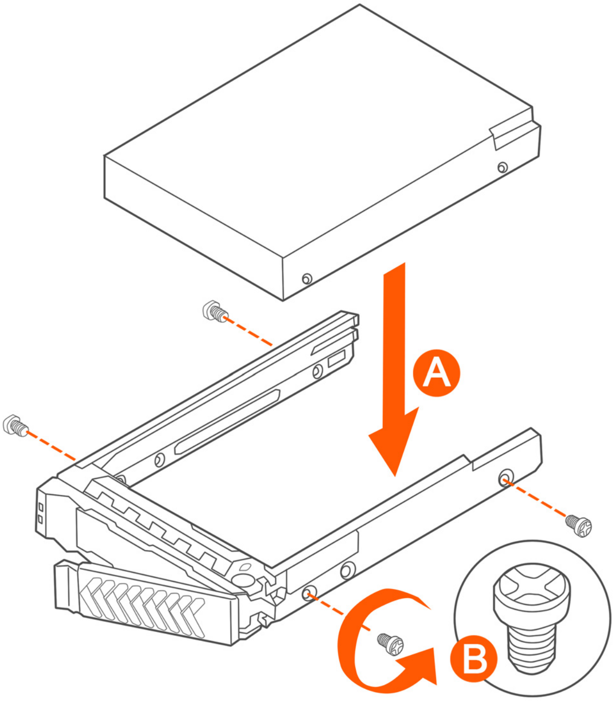
1. If a drive is already installed (that is, if you are replacing the drive), remove it by unfastening the four screws that attach the drive to the drive carrier (see A in Figure 8). Set the screws aside for use with the new drive.
2. Lift the drive out of the carrier (see B in Figure 8).

Figure 8. Removing the hard drive



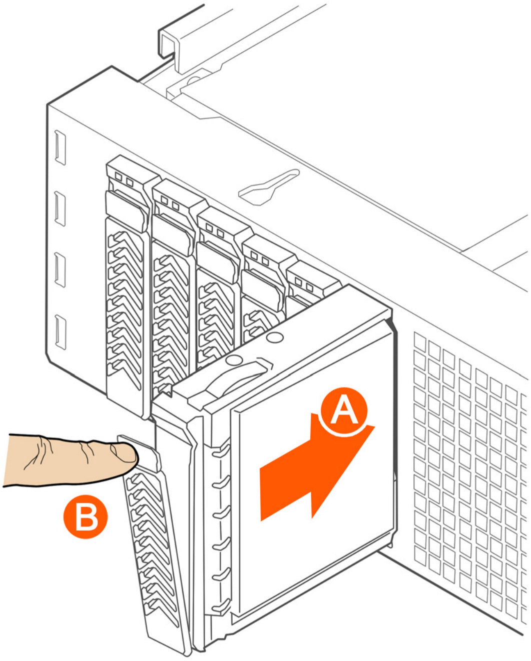
3. Install the new drive in the drive carrier (see A in Figure 9), and then secure the drive with the four screws that come with the carrier (see B).

Figure 9. Installing the hard drive



4 With the drive carrier locking lever fully open, push the hard drive carrier into the drive bay in the chassis until it stops (see A in Figure 10).

Figure 10. Inserting the carrier back into the chassis



5 Press the locking lever until it snaps shut and secures the drive in the bay.

You have completed installing or replacing the hard drive onto the controller.

NOTE: The new hard drive will synchronize automatically with the existing RAID array. During the synchronization process, the HDD LED on the controller will blink amber and green alternately. When the process is complete, the HDD LED will turn off.

Reinstalling the Front Bezel

Follow these steps to reinstall the front bezel on the controller.

1 Insert the tabs on the left side of the bezel into the slots on the front panel of the chassis.

2 Move the bezel toward the right of the front panel and align it on the front panel pins.

3 Snap the bezel into place and tighten the retention screw to secure it.

Replacing PSUs

The controller includes two redundant, hot-swappable power supply units (2 AC PSUs or 2 DC PSUs). No chassis components need to be removed to add or replace a PSU.

Follow these steps to remove and replace a PSU.

1 Identify the faulty PSU by looking at the PSU status LED (red indicates PSU failure, green indicates normal operation).

2 Press and hold the green safety lock downward while grasping the PSU handle.

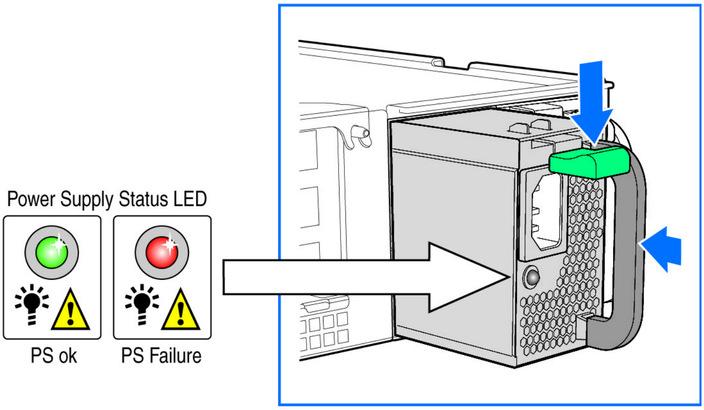
3 Pull outward on the handle, sliding the PSU all the way out of the rear of the machine.

4 Insert the new PSU into the slot and, while holding the green safety lock, slide the PSU into the slot until it locks in place.

The PSU status LED turns green, indicating that the PSU is operating normally.

NOTE: If you are installing a DC power supply, there are two threaded studs for chassis enclosure grounding. A 90° standard barrel, two-hole, compression terminal lug with 5/8-inch pitch suitable for a #14-10 AWG conductor must be used for proper safety grounding. A crimping tool may be needed to secure the terminal lug to the grounding cable.

Figure 11. Replacing a PSU



Replacing System Fans

The controller includes six redundant, hot-swappable system fans (four 80mm fans and two 60mm fans). There are also two fans located inside the power supply units. Redundancy for the two PSU fans is only achieved when both PSUs are installed.

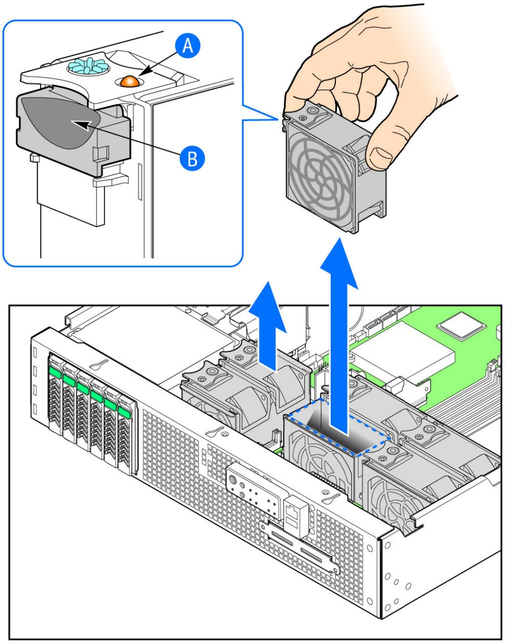
If any of the system fans requires replacement, the replacement procedure is identical.

WARNING! Electrostatic discharge (ESD) can damage internal components such as printed circuit boards and other parts. Ruckus Wireless recommends that you only perform this procedure with adequate ESD protection. At a minimum, wear an anti-static wrist strap attached to the ESD ground strap attachment on the front panel of the chassis.

Follow these steps to replace a system fan.

1. Open the front chassis cover of the controller. It may be necessary to extend the controller into a maintenance position.
2. Identify the faulty fan. Each fan has a “service required” LED that turns amber when the fan is malfunctioning.
3. Remove the faulty fan by grasping both sides of the fan assembly, using the plastic finger guard on the left side and pulling the fan out of the metal fan enclosure.
4. Slide the replacement fan into the same metal fan enclosure. Use the edges of the metal enclosure to align the fan properly and ensure the power connector is seated properly in the header on the side of the enclosure.
5. Apply firm pressure to fully seat the fan.
6. Verify that the (service required) LED on the top of the fan is not lit.
7. Close the front chassis cover and return the controller to its normal position in the rack, if necessary.

Figure 12. Replacing a system fan



Replacing a Controller Node

D

NOTE: The information in this appendix only applies to the SCG-200.

This appendix describes how to back up cluster and configuration data and replace a controller node. Topics include:

- Prerequisites
- Backing Up and Restoring the Cluster
- Backing Up and Restoring Configuration

Prerequisites

The following are required to perform the procedures described in this guide.

1. A remote FTP server with at least 50GB of free disk space. You must create an FTP account (user name and password) before starting these procedures.
2. If you are restoring to a multi node cluster environment, all backup files must be taken around the same time. If the backup files are out-of-sync, the restore process may be unsuccessful.

Backing Up and Restoring the Cluster

Cluster backup creates a backup of the entire cluster. Take note of the following before performing a cluster backup.

- The cluster backup file is typically very large (larger than 1GB).
- Cluster backup cannot be completed successfully if any one of the nodes has less than 50GB of disk space after the backup process.

Step 1: Back Up the Cluster from the Web Interface

For information on how to back up the cluster from the controller web interface, see Creating a Cluster Backup.

Step 2: Back Up the Cluster from the Controller CLI

1. Log on to the controller CLI as a system administrator.
2. Run the **`enable`** command to enable privileged mode on the CLI.

   ```
   ruckus> enable
   Password: ********
   ruckus#
   ```

3. Run the **`show diskinfo`** command to determine the current disk size of the node. To complete the cluster backup successfully, the `/mnt` directory must have at least 50GB (53,687,091,200 in 1K-blocks) of free disk space.

   ```
   ruckus# show diskinfo

   Filesystem           1K-blocks      Used Available Use%
   Mounted on
   rootfs                 4128448   315520   3603216   9% /
   /dev/root              4128448   315520   3603216   9% /
   /dev/sda1           2064208     97208  1862144  5% /boot
   /dev/mapper/vg00-lv00
   41276736   5646756  33533240  15% /mnt
   tmpfs                1048576      696   1047880  1% /tmp
   tmpfs              3066864       0  3066864  0% /dev/shm
   ```

4. Run the **`backup`** command to start the backing up the current cluster.

   ```
   ruckus# backup
   Do you want to backup system in this context (yes/no)? yes
   Backup process starts.
   Backup process has been scheduled to run. You can check
   backup version using 'show backup'.
   ```

5. Run the **`show backup`** command to verify that the cluster backup file has been created successfully.

Step 3: Transfer the Cluster Backup File to an FTP Server

1. Log on to the controller CLI as a system administrator.
2. Enable privileged mode on the CLI.

   ```
   ruckus> enable
   ```

```
Password: ********
ruckus#
```

3. Run the **remote backup** command to copy the cluster backup file to an FTP server.

```
ruckus# remote backup {ftp username} {ftp password} {ftp
server address} {(optional) ftp server port}
idx version date
------------------------------------------
1 1.1.1.0.207 2012-10-16 06:46:07 GMT
2 1.1.1.0.209 2012-10-17 05:20:51 GMT
Please choose a backup version to send to remote FTP: (ex:
1, 2, ...): 2
Remote backup process starts
Remote backup process completed
```

NOTE: The names of the backup files are automatically assigned by the controller based on the timestamp when the backup file was generated and the controller release version. To make it easy for you to identify the backup files, Ruckus Wireless strongly recommends moving each node's backup file to its own directory on the FTP server (for example, `//ftp/node1`) after the backup process is completed.

Step 4: Restoring the Cluster Backup to the Controller

The procedure for restoring the cluster backup to the controller depends on the controller environment – whether it is a single node environment or a multi-node environment.

Restoring to a Single Node Environment

Follow these steps to restore a cluster backup to a single node environment.

1. Prepare the new controller to which you will restore the cluster backup.
   - a Either obtain a new controller or factory reset an existing controller.
   - b Log on to the controller as a system administrator.
   - c Run the setup command to configure the controller's network settings.

```
ruckus> setup
################################################
Start SCG setup process:
```

```
################################################
    :
    :
Setup configuration of ethers...
Network would be restarted. You could connect to SCG
back by using Management port (10.2.2.35)!!
Enter "restart network" to continue... restart network
```

2 Transfer the backup file from the FTP server to the controller.

a Log on to the controller CLI as a system administrator.

b Run the **enable** command to enable privileged mode on the CLI.

```
ruckus> enable
Password: ********
ruckus#
```

c Run the **copy <ftp-url> backup** command to transfer the backup file from the FTP server to the controller.

```
ruckus# copy <ftp-url> backup
```

NOTE: If there is only one backup file on the FTP server, the system will automatically transfer this file to the controller. If there are multiple files, it will show the list of all available files and you will be prompted to select the file that you want to transfer.

3 Run the **restore local** command to restore the backup file to the controller.

```
ruckus# restore local

This action will REBOOT the system. Do you want to only
restore this SCG node (yes/no)? yes
idx  version     date
------------------------------------------
1    1.1.1.0.93  2013-02-01 03:09:27 GMT
2    1.1.1.0.93  2013-02-03 07:21:24 GMT

Please choose a backup version to restore (ex: 1, 2, ...): 2
```

You have completed restoring the backup file to a single node.

Restoring to a Multi Node Environment

If you are restoring to a multi node cluster, you can either replace only one node in the (still-healthy) cluster or replace multiple nodes in the cluster.

Replacing a Single Node in a Cluster

Follow these steps to replace a single node in a cluster backup.

1 If the node that you want to replace is still functioning, follow these steps to remove the node.

- a Choose a controller that will remain in the cluster.
- b Log on to that controller's web interface as an administrator.
- c Go to *Configuration* > *System*.
- d On the sidebar, click **Cluster Planes**.
- e Locate the node that you want to replace.
- f Under the *Actions* column, click the **Delete** button to remove the node from the cluster.

2 If the node that you want to replace is out of service, you will need to shut it down before you can replace it. Follow these steps.

- a On the node that you want to replace, log on to the CLI as a system administrator.
- b Run the **`enable`** command to enable privileged mode on the CLI.

```
ruckus> enable
Password: ********
ruckus#
```

- c (Optional) Back up the current controller system. See Step 2: Back Up the Cluster from the Controller CLI.
- d On the node that you want to replace, run the **`shutdown`** command.

```
ruckus# shutdown
```

- e Log on to the controller web interface as a system administrator.
- f Go to *Configuration* > *System*.
- g On the sidebar, click **Cluster Planes**.
- h Locate the node that you want to replace,
- i Under the *Actions* column, click the delete button to remove the node from the cluster.

j Set up the node as a new controller, and then join the existing cluster. For step by step instructions, see the *SmartCell Gateway 200 Getting Started Guide*.

Replacing Multiple Nodes in a Cluster

If the cluster itself is not healthy anymore or if multiple nodes need to be replaced, you must restore backup files taken around the same time to all of the nodes in the cluster. Follow these steps to restore backups to multiple nodes in a cluster.

CAUTION! Backup files must be taken around the same time. If the backup file of one node is out of sync from the others, the restore process will be unsuccessful.

CAUTION! When restoring to multiple nodes, it is critical that you perform the restore process on all nodes at the same time.

1. Log on to the CLI as a system administrator.
2. Run the **`enable`** command to enable privileged mode on the CLI.

```
ruckus> enable
Password: ********
ruckus#
```

3. Run the **`remote restore`** command to transfer the backup file from the FTP server to the controller.

```
ruckus# remote restore {ftp username} {ftp password} {ftp
server address} {(optional) ftp server port} {directory}
idx version date
------------------------------------------
1 1.1.0.0.207 2012-10-16 06:46:07 GMT
2 1.1.0.0.209 2012-10-17 05:20:51 GMT
Please choose a backup version to get from remote FTP: 2
Remote restore process starts
Remote restore process completed
```

NOTE: If there is only one backup file on the FTP server, the system will automatically transfer this file to the controller. If there are multiple files, it will show the list of all available files and you will be prompted to select the file that you want to transfer. If the backup files are in the root directory, use “/” in {directory}. If the backup files are in a subdirectory, use “/{subdir}/{subdir}” to indicate the subdirectory in which the system should check.

4. After all backup files for all nodes have been transferred from the FTP server to the controller, run the **restore local** command to restore the backup file to the controller.

```
ruckus# restore local

This action will REBOOT the system. Do you want to only
restore this SCG node (yes/no)? yes
idx  version     date
------------------------------------------
1    1.1.1.0.93  2013-02-01 03:09:27 GMT
2    1.1.1.0.93  2013-02-03 07:21:24 GMT

Please choose a backup version to restore (ex: 1, 2, ...): 2
```

5. Verify that the following message appears on each node:

```
Remote restore process completed
```

This indicates that the node is ready for the restore process.

6. Once all nodes are ready for the restore process, run the restore command for all nodes at the same time.

Backing Up and Restoring Configuration

Configuration backup creates a backup of all existing configuration information on the controller. In additional to backing up a different set of information, configuration backup is different from cluster backup in a few ways:

- The configuration backup file is smaller, compared to the cluster backup file.
- The controller can be configured to back up its configuration to an external FTP server automatically.
- Configuration backup does not back up any statistical files or general system configuration.

Backed Up Configuration Information

The following list show which configuration information will be backing up.

- AP zones
- AP zone global configuration
- Zone templates
- WLAN templates

- AP registration rules
- Access point information
- General system settings
- Web certificate
- SNMP agent
- Alarm to SNMP agent
- Cluster planes
- Management interface ACL
- Domain information
- User credentials and information
- Mobile Virtual Network Operators (MVNO) information

Backing Up Configuration

There are two methods you can use to back up the controller configuration:

- Backing Up Configuration from the Web Interface
- Backing Up Configuration from the CLI

Backing Up Configuration from the Web Interface

For information on how to back up the controller configuration to an external FTP server automatically, see Exporting the Configuration Backup to an FTP Server Automatically.

Backing Up Configuration from the CLI

Follow these steps to back up the controller configuration from the CLI.

1 Log on to the controller CLI as a system administrator.

2 Run the **enable** command to enable privileged mode on the CLI.

```
ruckus> enable
Password: ********
ruckus#
```

3 Run the **backup config** command to start backing up and transferring the node configuration to an FTP server.

```
ruckus# backup config {ftp username} {ftp password} {ftp
server address} {(optional) ftp server port}
Do you want to backup configuration (yes/no)? yes
```

```
Backup Configuration process starts
Backup Configuration process has been scheduled to run.
You can check backup version using 'show backup-config'
```

4 Run the **show backup-config** command to verify that the backup file has been created.

You have completed backing up the controller node to an external FTP server.

Restoring Configuration

- Restoring Configuration to a Single Node Environment
- Restoring Configuration to Multi Node Environment

Restoring Configuration to a Single Node Environment

1 Prepare the new controller to which you will restore the cluster backup.

   a Either obtain a new controller or factory reset an existing controller.

   b Log on to the controller as a system administrator.

   c Run the setup command to configure the controller's network settings.

```
ruckus> setup

################################################
Start SCG setup process:
################################################
    :
    :
Setup configuration of ethers...
Network would be restarted. You could connect to SCG back
by using Management port (10.2.2.35)!!
Enter "restart network" to continue... restart network
```

   d Complete the controller setup process from the CLI.

2 After you complete the controller setup, log on to the controller web interface as a system administrator.

3 Go to Administration > Configuration Backup and Restore.

4 In the Configuration Backups section, click the Upload icon.

5 Browse to the location (either on the local computer or on the network) of the configuration backup file that you want to restore.

6 Select the configuration backup file, and then click Upload. When the upload process is complete, the backup file appears in the Configuration Backups section.

7 Restore the configuration backup file to the node, either using the web interface or the CLI.

To use the web interface:

a On the web interface, go to **Administration** > **Configuration Backup and Restore**.

b In *Configuration Backups*, locate the configuration backup file that you want to restore, and then click the restore icon that is in the same row.

c Follow the prompts (if any) to complete the restore process.

To use the CLI:

a Log on to the CLI as a system administrator.

b Run the **`restore config`** command.

```
ruckus# restore config

This action will REBOOT the system. Do you want to only
restore this SCG node (yes/no)? yes
idx  version     date
------------------------------------------
1    1.1.1.0.93  2013-02-01 03:09:27 GMT
2    1.1.1.0.93  2013-02-03 07:21:24 GMT

Please choose a backup version to restore (ex: 1, 2,
...): 2
```

c Follow the prompts (if any) to complete the restore process.

You have completed restoring the configuration to a single node controller.

Restoring Configuration to Multi Node Environment

If you are restoring to a multi node cluster, you can either replace only one node in the (still-healthy) cluster or replace multiple nodes in the cluster.

Restoring Configuration to a Single Node in a Cluster

Follow these steps to replace the configuration of a single node in a cluster.

1. If the node that you want to replace is still functioning, follow these steps to remove the node.
   - a Choose a controller that will remain in the cluster.
   - b Log on to that controller's web interface as an administrator.
   - c Go to *Configuration* > *System*.
   - d On the sidebar, click **Cluster Planes**.
   - e Locate the node that you want to replace.
   - f Under the *Actions* column, click the delete button to remove the node from the cluster.
2. If the node that you want to replace is out of service, you will need to shut down the node before you can replace it. Follow these steps.
   - a On the node that you want to replace, log on to the CLI as a system administrator.
   - b Run the enable command to enable privileged mode on the CLI.

     ```
     ruckus> enable
     Password: ********
     ruckus#
     ```
   - c (Optional) Back up the current controller system. See Step 2: Back Up the Cluster from the Controller CLI.
   - d On the node that you want to replace, run the **`shutdown`** command.

     ```
     ruckus# shutdown
     ```
   - e Log on to the controller web interface as a system administrator.
   - f Go to *Configuration* > *System*.
   - g On the sidebar, click **Cluster Planes**.
   - h Locate the node that you want to replace,
   - i Under the *Actions* column, click the delete button to remove the node from the cluster.
   - j Set up the node as a new controller, and then join the existing cluster. For step by step instructions, see the *SmartCell 200 Getting Started Guide*.

You have completed restoring configuration to a single node in the cluster.

Restoring Configuration to Multiple Nodes in a Cluster

If the cluster itself is not healthy anymore or if multiple nodes need to replaced, you must you must factory reset all remaining nodes to ensure that configuration restore to the cluster will be successful.

1. Prepare the new controller nodes and factory reset all of the existing nodes in the cluster.
2. Complete the setup procedure for one of the controller nodes. For instructions, see the *SmartCell Gateway 200 Getting Started Guide* for this release.
3. After you complete the setup of one node, log on to the web interface of that node as a system administrator.
4. Go to **Administration** > **Configuration Backup and Restore**.
5. In the *Configuration Backups* section, click the upload icon.
6. Locate the configuration backup file that you want to restore.
7. Click **Upload**. After the configuration file is uploaded successfully, it appears in the *Configuration Backups* section.
8. Restore the configuration backup to the node either using the web interface or the CLI.

   To use the web interface:

   a Go to Administration > Configuration Backup and Restore page.

   b In the *Configuration Backups* section, locate the configuration backup file that you want to restore.

   c Click the restore icon that is in the same row.

   d Follow the prompts (if any) to complete the restore process.

   To use the CLI:

   a Log on to the CLI of the node as a system administrator.

   b Run the restore config command.

   ```
   ruckus# restore config

   This action will REBOOT the system. Do you want to only
   restore this SCG node (yes/no)? yes
   idx  version     date
   ------------------------------------------
   1    1.1.1.0.93  2013-02-01 03:09:27 GMT
   ```

```
2    1.1.1.0.93  2013-02-03 07:21:24 GMT

Please choose a backup version to restore (ex: 1, 2,
...): 2
```

c. When the configuration restore process on this node is complete, set up the next node and configure it to join the existing cluster.

You have completed restoring configuration backup to multiple nodes in a cluster.

SSID Syntaxes Supported by Ruckus Wireless Products

E

This appendix describes the SSID syntaxes that Ruckus Wireless products support.

In this appendix:

- SCG SSID Syntax
- ZoneDirector SSID Syntax
- ZoneFlex AP SSID Syntax

SCG SSID Syntax

The following sections describe the supported SSID syntax in the following SCG release versions:

- 1.1. x
- 2.1.x
- 2.5.x

1.1. x

Table 7 describes the SSID syntax that is supported in the 1.1.x release of the SCG.

Table 7. Supported SSID syntax in 1.1.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~(126)
	Supported Characters	_space_!"#$%&'()*+,-./ 0123456789:;<=>?@ABCDEFGHIJKLMNOPQR STUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}
CLI	Length	Unsupported
	Supported Characters	Unsupported

2.1.x

Table 8 describes the SSID syntax that is supported in the 2.1.x release of the SCG.

Table 8. Supported SSID syntax in 2.1.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~(126)
	Supported Characters	_space_!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}
CLI	Length	Between 2 and 32 characters
	Supported Characters	All characters, but the space character cannot be the first or last character in the SSID

2.5.x

Table 9 describes the SSID syntax that is supported in the 2.5.x release of the SCG.

Table 9. Supported SSID syntax in 2.5.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~(126)
	Supported Characters	_space_!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}
CLI	Length	Between 2 and 32 characters
	Supported Characters	All characters

ZoneDirector SSID Syntax

The following sections describe the supported SSID syntax in the following SCG release version:

- 9.8, 9.7
- 9.6

9.8, 9.7

Table 10 describes the SSID syntax that is supported in the 9.8 and 9.7 releases of the ZoneDirector.

Table 10. Supported SSID syntax in ZoneDirector 9.8 and 9.7

Web Interface	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: `can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126).`
CLI	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed by a double quotation mark.

9.6

Table 11 describes the SSID syntax that is supported in the 9.6 release of the ZoneDirector.

Table 11. Supported SSID syntax in ZoneDirector 9.6

Web Interface	Length	Between two and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: `can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126).`
CLI	Length	Between two and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~ (126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed in a double quotation mark (for example, “Ruckus Wireless SSID”).

ZoneFlex AP SSID Syntax

The following sections describe the supported SSID syntax in the following ZoneFlex AP release versions:

- 9.8, 9.7, and 9.6

9.8, 9.7, and 9.6

Table 12 describes the SSID syntax that is supported in the 9.6 release of the ZoneDirector.

Table 12. Supported SSID syntax in ZoneFlex AP 9.8, 9.7, and 9.6

Web Interface	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
CLI	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~ (126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed in a double quotation mark (for example, “Ruckus Wireless SSID”). If the space character is not enclosed in a double quotation mark, the space character and any characters after that will be ignored. For example, if you run the command “`set ssid wlan0` **`ruckus-ap 123`**”, the controller CLI will run the command as “`set ssid wlan0` **`ruckus-ap 123`**”.

Index

Numerics

802.11d 88, 146

A

access network 465
access point
  rebooting 334
  restarting remotely 334
access points
  downloading support log 333
  exporting to CSV 331
  monitoring 328
  viewing a summary 329
  viewing configuration 332
account 464
accounting profile 457
accounting retry 460
accounting retry timeout 460
acknowledge 348
Administration page 26
administrative tasks
  backup 414
  deleting
backup 419
  restore 418
administrator activity 355
  exporting to CSV 358
  filtering 357
administrator password 36
  changing 36
advanced 466
alarm severity 348, 353
alarm types 348, 352
alarms
  exporting to CSV 350
  filtering 349, 353
  severity 348, 353
  types 348, 352
  viewing 347
AP status summary 28
AP zone
  exporting to CSV 324
  monitoring 321
  viewing a summary 321
  viewing configuration 325
  viewing on Google Maps 326
apn format to gsn 460
apn resolution 453
authentication 465
authentication profile 453
authentication type 465

B

backing up
  FTP 406
backup 414
  deleting 419
  restoring 418

C

Captive Portal 303
CLI 440
  logging on 447
client admission control 64
client count summary 28
client fingerprinting 89, 147
client number report 361
client OS type summary widget 30
command line interface 440
common settings 460
communication ports 1
Configuration page 26
content area 26
continuously disconnected APs report 361
controller 453
core network 465
creating
  hotspot 316
  report 362

D

Dashboard page 26
DC power supply 24
default apn settings 461

deleting
  report 367
dhcp discover 450
DHCP Option 82 89, 147, 218, 225, 460
DHCP relay 218, 224, 460
dhcp relay 460
dhcp server 1 460
dhcp server 2 460
dns response time 453
dns retry 453
dns servers 453
domain summary 29
downloading
  system logs 432

E

echo request timer 453
electrostatic discharge 25
enable 463
enable dhcp relay 460
exporting
  access points 331
  alarms 350
  AP zones 324
external portal 468

F

filtering
  alarms 349
firewall ports 1
Force DHCP 89, 146
forwarding policy per realm 461
forwarding profile 460, 466
friendly name 453
front bezel
  reinstalling 23
  removing 19
FRU
  hard disk 18

G

Google Maps 326
grace period 464
grounding cable 24
group traffic profile mapping 456
guest access 463

H

hard disk drive carrier 20
hard drives
  installing 18
HDD replacement 18
health check policy 454, 457
hotspot
  creating 316
hotspot portal 463, 465

I

identifiers 450
inactivity timeout 89, 147
installing
  hard drive 18
IPSec 114

L

LLDP
  attributes 61
location information 464
logging off 37
logging on 22
logon
  CLI 447
logon page 22
logon url 463

M

main menu 25
management port number 22
management protocol 451
maximum outstanding requests 455, 459
mesh role 330
method 465
miscellaneous bar 26
Monitor page 26
monitoring
  access points 328
  AP zones 321

N

network connectivity 335
no response fail 455, 458
none 463
number of retries 452

O

onboarding 390
only smart client allowed 463

P

packet core 449
pages
  Administration 26
  Configuration 26
  Dashboard 26
  Monitor 26
  Report 26
password 23
patch file 424
payload 451
pdg ue session idle timeout 460
ping 335
port 454
portal authentication 468
ports to open 1
power supply unit 24
primary server 454, 457
PSU 24

R

rate limiting 455, 458
rebooting access point 334
reconnects 450
redirection 463
registered users 463
removing
  front bezel 19
replacement hard disk 18
replacing
  hard drive 18
  power supply unit 24
  system fan 25
report notification 366
Report page 26
report schedule 365
reports
  client number 361
  continuously disconnected APs 361
  creating 362
  deleting 367
  email notifications 366
  system resource utilization 362
  TX/RX bytes 362
  types 360
  viewing list 367
response timer 452
response window 454, 458
restarting access point 334
restoring
  backup 418
  FTP 408
revive interval 455, 458
rfc 5580 out of band local delivery 454
RS-232 serial to RJ45 cable 440
ruckus vsa 471

S

sanity timer 456, 459
secondary server 454, 457
serial connection 444
service protocol 453, 457
session identifier 451
session timeout 463
shared secret 454
sidebar 26
smart client support 463
Smart Monitor 46
snapshot 434
software upgrade file 424
SSH client 440, 442
SSH connection 442
start page 463
submenu 26
Subscriber Portal 303
support log 333
supported web browsers 22
system fan 25
system logs
  available logs 430
  downloading 432
system resource utilization report 362
system summary 29

T

TACACS+ 289
threshold 456, 459
traceroute 335
ttg establishment 450
tunnel control 451
tunnel establishment 470
tunnel terminating gateway 451

tunnel traffic 451
tunneling 449, 465
TX/RX bytes report 362

U

user name 23
user session 463
user traffic 449

V

verifying upgrade 426
viewing
  alarms 347
  AP zones 321

W

walled garden 303, 464
Web browser 22
Web interface 22
  Administration 26
  Configuration 26
  Dashboard 26
  features 23
  logging off 37
  logging on 22
  Monitor 26
  password 23
  Report 26
  user name 23
widget slot 34
widget slots 31
widgets 27
  adding a widget to a widget slot 33
  adding to the dashboard 31
  AP status summary 28
  available slots 31
  available widgets 27
  client count summary 28
  client OS type summary 30
  data throughput summary 30
  deleting 35
  displaying a widget in a widget slot 34
  domain summary 29
  moving to another slot 35
  system summary 29
wireless clients
  exporting to CSV 338

monitoring 336
viewing information 339
viewing summary 336
wlan usage 465

Z

zombie period 455, 458
zone template 463

Ruckus®
Simply Better Wireless.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com