March 2004

# WLAN Product Guide Alcatel OmniAccess Wireless System 2.0



# Welcome to the Alcatel OmniAccess Wireless Product Guide!

Alcatel OmniAccess Wireless System 2.0: Last Updated March 17, 2004



Refer to the <u>OVERVIEWS</u> section to see a big picture view of Alcatel products and features.



See the <u>SOLUTIONS</u> section to look through real-world network and application-specific solutions to real-world problems.



Go to the <u>TASKS</u> section to find detailed instructions on how to install, configure, use, and troubleshoot Alcatel products and supported 802.11 networks.



Visit the <u>REFERENCES</u> section to see technical information, such as the Alcatel Omni-Access Wireless Access Point Site Survey Guide, Quick Installation Guides, Web Browser Online Help files, and Release Notes.

FCC Statements for Alcatel OmniAccess Switches and Appliances

FCC Statements for OmniAccess APs

**Legal Information** 

Alcatel Technical Support

Alcatel OmniAccess Wireless System Release Notes

ACS Software Release Notes

# **Legal Information**

This section includes the following legal information:

- Limited Warranty
- Software License Agreement
- SSH Source Code Statement
- OpenSSL Project License Statements
- Trademarks and Service Marks

# **Limited Product Warranty**

The following describes the Alcatel Internetworking, Inc. standard Product Warranty for End Customers.

#### **Products**

- OmniAccess Wireless Switch (40XX) Family
- OmniAccess Wireless Appliance (4102) Family
- Alcatel OmniAccess Wireless Access Point (1200) Family

# **Limited Warranty**

Alcatel standard warranty for hardware is one (1) year. Alcatel warrants software materials to be defect free for 90 Days from time of purchase. Alcatel requires purchasing the software subscription if a customer would like to receive new OmniAccess Wireless Switch, OmniAccess Wireless Appliance, ACS, or Site Survey software. This limited warranty extends only to you the original purchaser of the Product.

#### **Exclusive Remedy**

Your sole remedy under the limited warranty described above is, at Alcatel's sole option and expense, the repair or replacement of the non-conforming Product or refund of the purchase price of the non-conforming Products. Alcatel's obligation under this limited warranty is subject to compliance with Alcatel's then-current Return Material Authorization ("RMA") procedures. All replaced Products will become the property of Alcatel. Exchange Products not returned to Alcatel will be invoiced at full Product list prices. Replacement Products may be new, reconditioned or contain refurbished materials. In connection with any warranty services hereunder, Alcatel may in its sole discretion modify the Product at no cost to you to improve its reliability or performance.

#### **Warranty Claim Procedures**

Should a Product fail to conform to the limited warranty during the applicable warranty period as described above, Alcatel must be notified during the applicable warranty period in order to have any obligation under the limited warranty.

The End Customer or their designated reseller must obtain a Return Material Authorization number (RMA number) from Alcatel for the non-conforming Product and the non-conforming Product must be returned to Alcatel according to the then-current RMA procedures. The End Customer or their designated reseller is responsible to ensure that the shipments are insured, with the transportation charges prepaid and that the RMA number is clearly marked on the outside of the package. Alcatel will not accept collect shipments or those returned without an RMA number clearly visible on the outside of the package.

#### **Exclusions and Restrictions**

Alcatel shall not be responsible for any software, firmware, information or memory data contained in, stored on or integrated with any Product returned to Alcatel pursuant to any warranty or repair.

Upon return of repaired or replaced Products by Alcatel, the warranty with respect to such Products will continue for the remaining unexpired warranty or sixty (60) days, whichever is longer. Alcatel may provide out-of-warranty repair for the Products at its then-prevailing repair rates.

The limited warranty for the Product does not apply if, in the judgment of Alcatel, the Product fails due to damage from shipment, handling, storage, accident, abuse or misuse, or it has been used or maintained in a manner not conforming to Product manual instructions, has been modified in any way, or has had any Serial Number removed or defaced. Repair by anyone other than Alcatel or an approved agent will void this warranty.

EXCEPT FOR ANY EXPRESS LIMITED WARRANTIES FROM ALCATEL SET FORTH ABOVE, THE PRODUCT IS PROVIDED "AS IS", AND ALCATEL AND ITS SUPPLIERS MAKE NO WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO PRODUCT OR ANY PART THEREOF, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. ALCATEL'S SUPPLIERS MAKE NO DIRECT WARRANTY OF ANY KIND TO END CUSTOMER FOR THE LICENSED MATERIALS. NEITHER ALCATEL NOR ANY OF ITS SUPPLIERS WARRANT THAT THE LICENSED MATERIALS OR ANY PART THEREOF WILL MEET END CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, OR ERROR-FREE, OR THAT ANY ERRORS IN THE PRODUCT WILL BE CORRECTED. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO END CUSTOMER. THIS LIMITED WARRANTY GIVES END CUSTOMER SPECIFIC LEGAL RIGHTS. END CUSTOMER MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ALCATEL OR ITS SUPPLIERS BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES (OR DIRECT DAMAGES IN THE CASE OF ALCATEL'S SUPPLIERS) ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE ARISING OUT OF OR RELATED TO THE PRODUCT OR ANY USE OR INABILITY TO USE THE PRODUCT, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF ALCATEL AND/OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. ALCATEL NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

# **Software License Agreement**

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE SOFTWARE AND ASSOCIATED DOCUMENTATION THAT IS PROVIDED WITH THIS AGREEMENT ("SOFTWARE," "DOCUMENTATION," AND COLLECTIVELY, "LICENSED MATERIALS").

BY USING ANY LICENSED MATERIALS, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND YOU WILL BE CONSENTING TO BE BOUND BY THEM. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, DO NOT USE THE LICENSED MATERIALS AND RETURN THE LICENSED MATERIALS AND ANY EQUIPMENT PROVIDED BY ALCATEL IN CONNECTION THEREWITH ("EQUIPMENT") UNUSED IN THE ORIGINAL SHIPPING CONTAINER TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Software may be provided by Alcatel on a standalone basis ("Standalone Software") or it may be provided embedded in Equipment ("Embedded Software").

#### License.

(a) Subject to the terms and conditions of this Agreement, Alcatel Internetworking, Inc. ("Alcatel"), grants to you ("Licensee") a limited, non-exclusive, non-transferable license, without the right to sublicense: (i) to install and use the Standalone Software, in object code format only, on computer hardware for which all corresponding license fees have been paid; (ii) use one (1) copy of the Embedded Software, in object code format only, solely as embedded in Equipment, each solely in accordance with the Documentation

for Licensee's internal business purposes.

(b) The license set forth above does not include any rights to and Licensee shall not (i) reproduce (except as set forth in Section 1(c)), modify, translate or create any derivative work of all or any portion of the Licensed Materials or Equipment, (ii) sell, rent, lease, loan, provide, distribute or otherwise transfer all or any portion of the Licensed Materials (except as set forth in Section 1(f)), (iii) reverse engineer, reverse assemble or otherwise attempt to gain access to the source code of all or any portion of the Licensed Materials or Equipment, (iv) use the Licensed Materials for third-party training, commercial time-sharing or service bureau use, (v) remove, alter, cover or objuscate any copyright notices, trademark notices or other proprietary rights notices placed or embedded on or in the Licensed Materials or Equipment, (vi) use any component of the Software or Equipment other than solely in conjunction with operation of the Software and as applicable, Equipment, (vii) unbundle any component of the Software or Equipment, (viii) use any component of the Software for the development of or in conjunction with any software application intended for resale that employs any such component, (ix) use the Licensed Materials or Equipment in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or (x) cause or permit any third party to do any of the foregoing.

If Licensee is a European Union resident, Licensee acknowledges that information necessary to achieve interoperability of the Software with other programs is available upon request.

- (c) Licensee may make a single copy of the Standalone Software and Documentation solely for its back-up purposes; provided that any such copy is the exclusive property of Alcatel and its suppliers and includes all copyright and other intellectual property right notices that appear on the original.
- (d) Alcatel may provide updates, corrections, enhancements, modifications or bug fixes for the Licensed Materials ("Updates") to Licensee. Any such Update shall be deemed part of the Licensed Materials and subject to the license and all other terms and conditions hereunder
- (e) Alcatel shall have the right to inspect and audit Licensee's use, deployment, and exploitation of the Licensed Materials for compliance with the terms and conditions of this Agreement.
- (f) Licensee shall have the right to transfer the Embedded Software as embedded in Equipment in connection with a transfer of all of Licensee's right, title and interest in such Equipment to a third party; provided, that, Licensee transfers the Embedded Software and any copies thereof subject to the terms and conditions of this Agreement and such third party agrees in writing to be bound by all the terms and conditions of this Agreement.
- (g) Notwithstanding anything to the contrary herein, certain portions of the Software are licensed under and Licensee's use of such portions are only subject to the GNU General Public License version 2. If Licensee or any third party sends a request in writing to Alcatel at 110 Nortech Parkway, San Jose CA 95134, ATTN: Contracts Administration, Alcatel will provide a complete machine-readable copy of the source code of such portions for a nominal cost to cover Alcatel's cost in physically providing such code.
- 2. Ownership. Alcatel or its suppliers own and shall retain all right, title and interest (including without limitation all intellectual property rights), in and to the Licensed Materials and any Update, whether or not made by Alcatel. Licensee acknowledges that the licenses granted under this Agreement do not provide Licensee with title to or ownership of the Licensee Materials, but only a right of limited use under the terms and conditions of this Agreement. Except as expressly set forth in Section 1, Alcatel reserves all rights and grants Licensee no licenses of any kind hereunder. All information or feedback provided by Licensee to Alcatel with respect to the Software or Equipment shall be Alcatel's property and deemed confidential information of Alcatel.
- 3. Confidentiality. Licensee agrees that the Licensed Materials contain confidential information, including trade secrets, know-how, and information pertaining to the technical structure or performance of the Software, that is the exclusive property of Alcatel as between Licensee and Alcatel. In addition, Alcatel's confidential information includes any confidential or trade secret information related to the Licensed Materials. During the period this Agreement is in effect and at all times thereafter, Licensee shall maintain Alcatel's confidential information in confidence and use the same degree of care, but in no event less than reasonable care, to avoid disclosure of Alcatel's confidential information as it uses with respect to its own confidential and proprietary information of similar type and importance. Licensee agrees to only disclose Alcatel's confidential information to its directors, officers and employees who have a bona fide need to know solely to exercise Licensee's rights under this Agreement and to only use Alcatel's confidential information incidentially in the customary operation of the Software and Equipment. Licensee shall not sell, license, sublicense, publish, display, distribute, disclose or otherwise make available Alcatel's confidential information to any third party nor use such information except as authorized by this Agreement. Licensee agrees to immediately notify Alcatel of the unauthorized disclosure or use of the Licensed Materials and to assist Alcatel in remedying such unauthorized use or disclosure. It is further understood and agreed that any breach of this Section 3 or Section 1(b) is a material breach of this Agreement and any such breach would cause irreparable harm to Alcatel and its suppliers, entitling Alcatel or its suppliers to injunctive relief in addition to all other remedies available at law.
- 4. Limited Warranty & Disclaimer. Any limited warranty for the Licensed Materials and Alcatel's sole and exclusivity liability thereunder is as set forth in Alcatel's standard warranty documentation. In addition, any limited warranty for the Software does not apply to any component of the Software but only to the Software as a whole. EXCEPT FOR ANY EXPRESS LIMITED WARRANTIES FROM ALCATEL IN SUCH DOCUMENTATION, THE LICENSED MATERIALS ARE PROVIDED "AS IS", AND ALCATEL AND ITS SUPPLIERS MAKE NO WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO LICENSED MATERIALS OR ANY PART THEREOF, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, MONINFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. ALCATEL'S SUPPLIERS MAKE NO DIRECT WARRANTY OF ANY KIND TO LICENSEE FOR THE LICENSED MATERIALS. NEITHER ALCATEL NOR ANY OF ITS SUPPLIERS WARRANT THAT THE LICENSED MATERIALS OR ANY PART THEREOF WILL MEET LICENSEE'S REQUIREMENTS OR BE UNINTERRUPTED, OR ERROR-FREE, OR THAT ANY ERRORS IN THE LICENSED MATERIALS WILL BE CORRECTED. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.
- 5. Term and Termination. This Agreement is effective until terminated. License may terminate this Agreement at any time by destroying all copies of the Software. This Agreement and all licenses granted hereunder will terminate immediately without notice from Alcatel if Licensee fails to comply with any provision of this Agreement. Upon any termination, Licensee must destroy all copies of the Licensed Materials. Sections 1(b), 2, 3, 4(b), 5, 6, 7, 8, 9 and 10 shall survive any termination of this Agreement.
- 6. Export. The Software is specifically subject to U.S. Export Administration Regulations. Licensee agrees to strictly comply with all export, re-export and import restrictions and regulations of the Department of Commerce or other agency or authority of the United States or other applicable countries, and not to transfer, or authorize the transfer of, directly or indirectly, the Software or any direct product thereof to a prohibited country or otherwise in violation of any such restrictions or regulations. Licensee's failure to comply with this Section is a material breach of this Agreement. Licensee acknowledges that Licensee is not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria or a party listed in the U.S. Table of Denial Orders or U.S. Treasury Department List of Specially Designated Nationals.
- 7. Government Restricted Rights. As defined in FAR section 2.101, DFAR section 252.227-7014(a)(1) and DFAR section

- 252.227-7014(a)(5) or otherwise, the Software provided in connection with this Agreement are "commercial items," "commercial computer software" and/or "commercial computer software documentation." Consistent with DFAR section 227.7202, FAR section 12.212 and other sections, any use, modification, reproduction, release, performance, display, disclosure or distribution thereof by or for the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions shall be deemed "technical data-commercial items" pursuant to DFAR section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR section 227.7015(b).
- 8. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ALCATEL OR ITS SUPPLIERS BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES (OR DIRECT DAMAGES IN THE CASE OF ALCATEL'S SUPPLIERS) ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE ARISING OUT OF OR UNDER THIS AGREEMENT OR ANY USE OR INABILITY TO USE THE LICENSED MATERIALS OR EQUIPMENT, OR FOR BREACH OF THIS AGREEMENT. ALCATEL'S TOTAL LIABILITY ARISING OUT OF OR UNDER THIS AGREEMENT, OR USE OR INABILITY TO USE THE LICENSED MATERIALS OR EQUIPMENT, OR FOR BREACH OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID FOR THE SOFTWARE (FOR THE STANDALONE SOFTWARE) AND THE PRICE PAID FOR THE EQUIPMENT (FOR THE EMBEDDED SOFTWARE AND EQUIPMENT). THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF ALCATEL AND/OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.
- 9. Third Party Beneficiaries. Alcatel's suppliers are intended third party beneficiaries of this Agreement. The terms and conditions herein are made expressly for the benefit of and are enforceable by Alcatel's suppliers; provided, however, that Alcatel's suppliers are not in any contractual relationship with Licensee. Alcatel's suppliers include without limitation: (a) Hifn, Inc., a Delaware corporation with principal offices at 750 University Avenue, Los Gatos, California; and (b) Wind River Systems, Inc. and its suppliers.
- 10. General. This Agreement is governed and interpreted in accordance with the laws of the State of California, U.S.A. without reference to conflicts of laws principles and excluding the United Nations Convention on Contracts for the Sale of Goods. The parties consent to the exclusive jurisdiction of, and venue in, Santa Clara County, California, U.S.A. Licensee shall not transfer, assign or delegate this Agreement or any rights or obligations hereunder, whether voluntarily, by operation of law or otherwise, without the prior written consent of Alcatel (except as expressly set forth in Section 1(f)). Subject to the foregoing, the terms and conditions of this Agreement shall be binding upon and inure to the benefit of the parties to it and their respective heirs, successors, assigns and legal representatives. This Agreement constitutes the entire agreement between Alcatel and Licensee with respect to the subject matter hereof, and merges all prior negotiations and drafts of the parties with regard thereto. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, by Alcatel shall be effective unless in writing. If any of the provisions of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable under any applicable statute or rule of law, such provision shall, to that extent, be deemed omitted.

#### **SSH Source Code Statement**

C 1995 - 2004 SAFENET, Inc. This software is protected by international copyright laws. All rights reserved. SafeNet is a registered trademark of SAFENET, Inc., in the United States and in certain other jurisdictions. SAFENET and the SAFENET logo are trademarks of SAFENET, Inc., and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved

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

Components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

- o Markus Friedl
- o Theo de Raadt
- o Niels Provos
- o Dug Song
- o Aaron Campbell
- o Damien Miller
- o Kevin Steves
- o Daniel Kouril
- o Per Allansson

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR 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

#### **OpenSSL Project License Statements**

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

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.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

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

#### **Trademarks and Service Marks**

Alcatel® and the Alcatel logo are registered trademarks of Alcatel. Xylan®, OmniSwitch®, OmniStack®, and Alcatel OmniVista® are trademarks of Alcatel Internetworking, Inc. All other trademarks, service marks, and product names used in this document are the property of their respective owners.

Copyright © 2004 by Airespace, Inc. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Airespace, Inc.

This OmniAccess product contains components which may be covered by one or more of the following U.S. patents: U.S. Patent No. 6,339,830 U.S. Patent No. 6,070,243.

# **Contacting Alcatel Technical Support**

An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at eservice.ind.alcatel.com, call us at 1-800-995-2696, or email us at support@ind.alcatel.com.

Alcatel, 26801 West Agoura Road, Calabasas, CA 91301

Telephone: (818) 880-3500

• FAX: (818) 880-3505

info@ind.alcatel.com

US Customer Support—(800) 995-2696

International Customer Support—(818) 878-450

Internet—http://eservice.ind.alcatel.com

#### **RMA Procedures**

Contact Alcatel Technical Support for a Return Material Authorization (RMA) for your OmniAccess AP(s). Please have the following available when making a call:

- Company and Contact information
- Equipment model number(s)
- Alcatel Wireless Operating System software revision level (ALCATEL\_2\_0\_x\_x)
- ACS Software revision level (2.0.x.x)
- Symptom(s)
- Network configuration

You can find Alcatel Technical Support information at <a href="http://www.alcatel.com/">http://www.alcatel.com/</a>.

# **FCC Statements for OmniAccess APs**

This section includes the following FCC statements for the OmniAccess AP:

- Class A Statement
- RF Radiation Hazard Warning
- Non-Modification Statement
- Deployment Statement

#### **Class A Statement**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

# **RF Radiation Hazard Warning**

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location such that the antenna of the device will be greater than 20 cm (8 in.) from all persons. Using higher gain antennas and types of antennas not covered under the FCC certification of this product is not allowed.

Installers of the radio and end users of the Alcatel OmniAccess Wireless Enterprise Platform must adhere to the installation instructions provided in this manual.

# **Non-Modification Statement**

Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Unauthorized antennas, modifications, or attachments could damage the badge and could violate FCC regulations and void the user's authority to operate the equipment.



**Note:** Refer to the <u>Alcatel OmniAccess Wireless System Release Notes</u> for 802.11a external antenna information. Contact Alcatel Internetworking, Inc. for a list of FCC-approved 802.11a and 802.11b/g external antennas.

# **Deployment Statement**

This product is certified for indoor deployment only. Do not install or use this product outdoors.

# FCC Statements for Alcatel OmniAccess Switches and Appliances

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

To ensure compliance with EMC standards applied to the 4012 and 4024 Alcatel OmniAccess Wireless Switches, shielded twisted pair (STP) 10/100Base-T cabling must be used.

# **Safety Considerations**

- The OAW-GSX and OAW-GSX2 Network Adapter Modules and OAW-4102 OmniAccess Wireless Appliances contain Class 1 Lasers (Laser Klasse 1) according to EN 60825-1+A1+A2.
- Model 4012 and 4024 PoE Alcatel OmniAccess Wireless Switches are only intended for installation in Environment A (same-building deployment) as defined in IEEE 802.3af. All interconnected equipment must be contained within the same building including the interconnected equipment's associated LAN connections.
- MAKE SURE that plenum-mounted OmniAccess APs and OmniAccess 1200R APs are powered using Power Over Ethernet (POE) to comply with safety regulations.

# **Table of Contents**

# Welcome to the Alcatel OmniAccess Wireless Product Guide!

# Legal Information

Limited Product Warranty ii

Products ii

Limited Warranty ii

Exclusive Remedy ii

Warranty Claim Procedures ii

Exclusions and Restrictions iii

Software License Agreement iii

SSH Source Code Statement vi

OpenSSL Project License Statements vi

Trademarks and Service Marks vi

**Contacting Alcatel Technical Support** 

RMA Procedures vii

#### FCC Statements for OmniAccess APs

Class A Statement viii

RF Radiation Hazard Warning viii

Non-Modification Statement viii

Deployment Statement viii

FCC Statements for Alcatel OmniAccess Switches and Appliances

Safety Considerations

**Table of Contents** 

# **OVERVIEWS**

#### About the Alcatel OmniAccess Wireless System

About the Alcatel Wireless Operating System 3

Single-Alcatel OmniAccess Switch or Appliance Deployments 3

Multiple-Alcatel OmniAccess Switch and Appliance Deployments 5

About Alcatel Wireless Operating System Security 6

About Alcatel Wired Security 7

Layer 2 and Layer 3 Operation 8

Operational Requirements 8

Configuration Requirements 8

About OmniVista AirView Software 8

About the Master Alcatel OmniAccess Switch or Appliance 9

About the Primary Alcatel OmniAccess Switch or Appliance 10

**About Client Roaming 10** 

Same-Alcatel OmniAccess Switch or Appliance (Layer 2) Roaming 10

Inter-Alcatel OmniAccess Switch and Appliance (Layer 2) Roaming 11

Inter-Subnet (Layer 3) Roaming 11

Special Case: Voice Over IP Telephone Roaming 11

About External DHCP Servers 11

Per-WLAN Assignment 12

Per-Interface Assignment 12

Security Considerations 12

About Alcatel Mobility Groups 12

**About Alcatel Wired Connections 14** 

Between Alcatel OmniAccess Wireless Switches and APs 14

Between Alcatel OmniAccess Switches and Appliances and Other Network Devices 15

About Alcatel WLANs 16

About Access Control Lists 16

About Identity Networking 16

About Port Mirroring 17

About File Transfers 18

About Power Over Ethernet 18

## About Alcatel OmniAccess Switches and Appliances

4012 and 4024 OmniAccess Wireless Switch Models 20

4102 OmniAccess Wireless Appliance Model 20

Alcatel OmniAccess Switch and Appliance Features 21

Alcatel OmniAccess Switch and Appliance Model Numbers 23

OmniAccess Wireless Switch Direct-Connect Mode 23

Alcatel OmniAccess Switches and Appliances in Appliance Mode 24

OmniAccess Wireless Switch Hybrid Mode 25

About Distribution System Ports 25

About the Management Interface 26

About the AP-Manager Interface 27

About Operator-Defined Interfaces 28

About the Virtual Interface 28

About the Service Port 28

About the Service-Port Interface 29

About the Startup Wizard 29

About Alcatel OmniAccess Switch and Appliance Memory 30

Alcatel OmniAccess Switch and Appliance Failover Protection 30

Network Connection to the Alcatel OmniAccess Switch or Appliance 31

Model 4012 and 4024 Alcatel OmniAccess Wireless Switches 32

Model 4102 OmniAccess Wireless Appliances 33

Enhanced Security Module 33

# About Alcatel OmniAccess Wireless Access Points

About Alcatel OmniAccess Remote Edge Access Points 36

About OmniAccess AP Models 38

About OmniAccess AP External and Internal Antennas 38

External Antenna Connectors 39

Antenna Sectorization 39

802.11a Internal Antenna Patterns 39

802.11b/g Internal Antenna Patterns 41

About OmniAccess AP LEDs 43

About OmniAccess AP Connectors 44

About OmniAccess AP Power Requirements 45

About OmniAccess AP External Power Supply 46

About OmniAccess AP Mounting Options 46

About OmniAccess AP Physical Security 46

About OmniAccess AP Monitor Mode 47

About Third-Party Access Points

**About Roque Access Points** 

Rogue AP Location, Tagging and Containment 49

About the OmniVista Air Control System Software

About the ACS Software Java Admin Client 51

About the ACS Software Browser Client 51

About the ACS Floor Plan Editor 51

About ACS Alcatel OmniAccess Switch and Appliance Autodiscovery 52 About the Alcatel Web Browser Interface About the Command Line Interface

#### SOLUTIONS

Alcatel Wireless Operating System Security

Overview 56

Layer 1 Solutions 56

Layer 2 Solutions 56

Layer 3 Solutions 57

Single Point of Configuration Policy Manager Solutions 57

Rogue Access Point Solutions 57

Rogue Access Point Challenges 57

Tagging and Containing Rogue Access Points 57

Integrated Security Solutions 58

Simple, Cost-Effective Solutions 58

Converting an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 Mode

Using the Alcatel OmniAccess Switch or Appliance Web Browser 59

Using the ACS Software Browser Client Interface 61

Converting an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 Mode

Using the Alcatel OmniAccess Switch or Appliance Web Browser 64

Using the ACS Software Browser Client Interface 64

Configuring a Firewall for an ACS Software Server

Configuring the System for SpectraLink NetLink Telephones

Using the Command Line Interface 67

Using the Web Browser Interface 67

Using the OmniVista Air Control System Software 68

Using Management over Wireless

Using the Command Line Interface 70

Using the Web Browser Interface 70

Configuring a WLAN for a DHCP Server

Using the Command Line Interface 71

Using the Web Browser Interface 71

Customizing the Web Auth Login Screen

Default Web Auth Operation 72

Customizing Web Auth Operation 74

Clearing and Restoring the Alcatel Logo 74

Changing the Web Title 74

Changing the Web Message 75

Changing the Logo 75

Creating a Custom URL Redirect 76

Verifying your Web Auth Changes 77

Sample Customized Web Auth Login Page 77

Configuring Identity Networking for Alcatel Wireless Operating System 2.0

**RADIUS Attributes 79** 

# **TASKS**

Using the Alcatel OmniAccess Wireless System CLI

Logging Into the CLI 84

Using a Local Serial Connection 84

Using a Remote Ethernet Connection 85

Logging Out of the CLI 86

CLI Tree Structure 87

Navigating the CLI 87

Viewing Network Status 88

# Configuring the Alcatel OmniAccess Switch or Appliance

Collecting Alcatel OmniAccess Switch or Appliance Parameters 89

Configuring System Parameters 90

Time and Date 90

Country 90

Supported 802.11a and 802.11b/g Protocols 91

Users and Passwords 92

#### Configuring Alcatel OmniAccess Switch and Appliance Interfaces 92

Verifying and Changing the Management Interface 93

Creating and Assigning the AP-Manager Interface 93

Creating, Assigning and Deleting Operator-Defined Interfaces 94

Verifying and Changing the Virtual Interface 95

Enabling Web and Secure Web Modes 95

Configuring Spanning Tree Protocol 96

# Creating Access Control Lists 97

# Configuring WLANs 97

WLANs 97

VLANs 99

Layer 2 Security 99

Layer 3 Security 101

Local Netuser 104

Quality of Service 104

Activating WLANs 104

Configuring Mobility Groups 105

Configuring RADIUS 105

Configuring SNMP 105

#### Configuring Other Ports and Parameters 106

Service Port 106

OmniVista AirView Software 106

Serial (CLI Console) Port 107

802.3x Flow Control 107

System Logging 107

Transferring Files To and From an Alcatel OmniAccess Switch or Appliance 107

Updating the Alcatel Wireless Operating System Software 108

Using the Startup Wizard 109

Adding SSL to the Web Browser Interface 110

Locally-Generated Certificate 111

Externally-Generated Certificate 111

Adding SSL to the 802.11 Interface 113

Locally-Generated Certificate 113

Externally-Generated Certificate 114

Saving Configurations 116

Clearing Configurations 116

Erasing the Alcatel OmniAccess Switch or Appliance Configuration 117

Resetting the Alcatel OmniAccess Switch or Appliance 117

#### Using the OmniVista Air Control System Software

Starting and Stopping ACS Software 119

Starting an ACS Software Server as an Application 119

Starting the ACS Software Server as a Service 120

Stopping the ACS Software Server Application 121

Stopping the ACS Software Service 121

Checking the ACS Software Service Status 122

Starting an ACS Software Browser Client 123

Starting an ACS Software Java Admin Client 124

Stopping an ACS Software Browser Client 125

Stopping an ACS Software Java Admin Client 125

Configuring the ACS Software Browser Client 126

Adding Devices to the ACS Software Database 126

Manually Adding an Alcatel OmniAccess Switch or Appliance to ACS 127

Adding a Campus Map to the ACS Database 129

Adding a Building to a Campus 132

Adding a Standalone Building to the ACS Database 136

Adding an Outdoor Area to a Campus 138

Adding Floor Plans to a Campus Building 141

Adding Floor Plans to a Standalone Building 145

Adding APs to Floor Plan and Outdoor Area Maps 149

Troubleshooting with ACS Software 155

Detecting and Locating Rogue Access Points 155

Acknowledging Roque APs 159

Locating Clients 159

Finding Coverage Holes 160

Pinging a Network Device Using ACS 161

Viewing System Status 161

Managing ACS Software and Database 162

Installing ACS Software Server and ACS Software Client 162

Installing ACS Software Client 162

Updating ACS Software Server and ACS Software Client 162

Updating ACS Software Java Admin Client 164

Reinitializing the ACS Software Database 164

Administering ACS Users and Passwords 165

# Using the Alcatel Web Browser Interface

Adding OmniAccess APs to an Alcatel OmniAccess Switch or Appliance 168

Adding CA Certificates to an Alcatel OmniAccess Switch or Appliance 168

Adding ID Certificates to an Alcatel OmniAccess Switch or Appliance 169

#### Troubleshooting

Using Error Messages 171

Using Reason and Status Codes in the Trap Log 174

Client Reason Codes 174

Client Status Codes 175

# **REFERENCES**

Glossary

Alcatel OmniAccess Wireless System Supported Regulatory Domains

# Alcatel OmniAccess Wireless System CLI Reference

? command

Help Command

Viewing Configurations

show 802.11a 203

show 802.11b 204

show acl 205

SHOW ADVANCED 802.11A COMMANDS 205

show advanced 802.11a channel 205

show advanced 802.11a group 206

show advanced 802.11a logging 206

show advanced 802.11a monitor 206

show advanced 802.11a txpower 207

show advanced 802.11a profile 207

show advanced 802.11a summary 208

SHOW ADVANCED 802.11B COMMANDS 208

show advanced 802.11b channel 209

show advanced 802.11b group 209

show advanced 802.11b logging 209

show advanced 802.11b monitor 210

show advanced 802.11b txpower 210

show advanced 802.11b profile 211

show advanced 802.11b summary 211

show advanced timers 212

show ap auto-rf 212

show ap config 214

show ap stats 217

show ap summary 218

show arp switch 218

SHOW AP COMMANDS 219

show blacklist 219

SHOW CERTIFICATE COMMANDS 219

show certificate compatibility 219

show certificate summary 220

SHOW CLIENT COMMANDS 220

show client ap 220

show client detail 220

show client summary 221

show client username 222

show country 222

show cpu 223

show custom-web 223

show debug 223

show eventlog 224

show interface 224

show inventory 225

show load-balancing 225

show loginsession 225

show macfilter 226

show mgmtuser 226

SHOW MIRROR COMMANDS 226

show mirror ap 227

show mirror foreignap 227

show mirror mac 227

show mirror port 228

show mobility summary 228

show msglog 228

show netuser 229

show network 229

show qos queue\_length all 230

show port 230

**SHOW RADIUS COMMANDS 231** 

show radius acct statistics 231

show radius auth statistics 232

show radius summary 232

SHOW ROGUE AP COMMANDS 233

show rogue ap detailed 233

show rogue ap summary 233

SHOW ROGUE CLIENT COMMANDS 234

show rogue client detailed 234

show rogue client summary 234

show route summary 235

show serial 235

show sessions 235

show snmpcommunity 236

show snmptrap 236

show snmpv3user 236

show snmpversion 237

show spanningtree port 237

show spanningtree switch 238

SHOW STATS COMMANDS 238

show stats port 238

show stats switch 240

show switchconfig 241

show sysinfo 241

show syslog 242

show time 242

show trapflags 242

show traplog 243

show watchlist 244

show wlan 244

show wlan summary 245

show wps-peers summary 246

#### **Setting Configurations**

CONFIG 802.11A COMMANDS 248

config 802.11a antMode 248

config 802.11a beaconperiod 249

config 802.11a channel 249

config 802.11a disable 250

config 802.11a dtim 250

config 802.11a enable 251

config 802.11a rate 252

config 802.11a txPower 252

CONFIG 802.11B COMMANDS 253

config 802.11b 11gSupport 254

config 802.11b antenna 254

config 802.11b beaconperiod 255

config 802.11b channel 255

config 802.11b disable 256

config 802.11b diversity 256 confia 802.11b dtim 257 config 802.11b enable 258 config 802.11b rate 258 config 802.11b txPower 259 config acl 259 CONFIG ADVANCED 802.11A COMMANDS 260 config advanced 802.11a channel foreign 261 config advanced 802.11a channel load 261 config advanced 802.11a channel noise 261 config advanced 802.11a channel update 262 config advanced 802.11a factory 262 config advanced 802.11a group-mode 262 config advanced 802.11a logging channel 263 config advanced 802.11a logging coverage 263 config advanced 802.11a logging foreign 263 config advanced 802.11a logging load 264 config advanced 802.11a logging noise 264 config advanced 802.11a logging performance 264 config advanced 802.11a logging power 264 config advanced 802.11a monitor coverage 265 config advanced 802.11a monitor load 265 config advanced 802.11a monitor noise 265 config advanced 802.11a monitor signal 266 config advanced 802.11a power-update 266 config advanced 802.11a profile clients 266 config advanced 802.11a profile coverage 267 config advanced 802.11a profile customize 267 config advanced 802.11a profile exception 268 config advanced 802.11a profile foreign 268 config advanced 802.11a profile level 268 config advanced 802.11a profile noise 269 config advanced 802.11a profile throughput 269 config advanced 802.11a profile utilization 270 CONFIG ADVANCED 802.11B COMMANDS 270 config advanced 802.11b channel foreign 271 config advanced 802.11b channel load 271 config advanced 802.11b channel noise 272 config advanced 802.11b channel update 272 config advanced 802.11b factory 272 config advanced 802.11b group-mode 273 config advanced 802.11b logging channel 273 config advanced 802.11b logging coverage 273 config advanced 802.11b logging foreign 274 config advanced 802.11b logging load 274 config advanced 802.11b logging noise 274 config advanced 802.11b logging performance 274 config advanced 802.11b logging power 275 config advanced 802.11b monitor coverage 275 config advanced 802.11b monitor load 275 config advanced 802.11b monitor noise 276

config advanced 802.11b monitor signal 276

config advanced 802.11b power-update 276

config advanced 802.11b profile clients 277

config advanced 802.11b profile coverage 277

config advanced 802.11b profile customize 277

config advanced 802.11b profile exception 278

config advanced 802.11b profile foreign 278

config advanced 802.11b profile level 279

config advanced 802.11b profile noise 279

config advanced 802.11b profile throughput 279

config advanced 802.11b profile utilization 280

CONFIG ADVANCED TIMERS COMMANDS 280

config advanced timers auth-timeout 280

config advanced timers rogue-ap 281

**CONFIG AP COMMANDS 281** 

config ap add 281

config ap delete 282

config ap disable 282

config ap enable 282

config ap location 283

config ap name 283

config ap port 283

config ap primary-base 284

config ap reset 284

config ap stats-timer 284

config blacklist 285

config certificate 285

config client deauthenticate 285

config country 286

config custom-web 286

**CONFIG INTERFACE COMMANDS 286** 

config interface acl 287

config interface address 287

config interface create 287

config interface delete 288

config interface dhcp 288

config interface hostname 288

config interface port 288

config interface vlan 289

config load-balancing 289

config loginsession close 289

**CONFIG MACFILTER COMMANDS 290** 

config macfilter add 290

config macfilter delete 290

config macfilter mac-delimiter 291

config macfilter wlan-id 291

**CONFIG MGMTUSER COMMANDS 291** 

config mgmtuser add 291

config mgmtuser delete 292

config mgmtuser password 292

**CONFIG MIRROR COMMANDS 292** 

config mirror ap 293

config mirror foreignap 293

config mirror mac 293

config mirror port 294

CONFIG MOBILITY GROUP COMMANDS 294

config mobility group discovery 294

config mobility group member 295

**CONFIG NETUSER COMMANDS 295** 

config netuser add 295

config netuser delete 295

config netuser password 296

config netuser wlan-id 296

CONFIG NETWORK COMMANDS 296

config network arptimeout 297

config network bcast-ssid 297

config network dsport 297

config network master-base 298

config network mgmt-via-wireless 298

config network params 299

config network rf-mobility-domain 299

config network secureweb 299

config network secweb-passwd 300

config network ssh 300

config network telnet 300

config network usertimeout 301

config network vlan 301

config network webmode 301

CONFIG PORT COMMANDS 302

config port adminmode 302

config port autoneg 302

config port linktrap 303

config port physicalmode 303

config port power 304

config prompt 304

config gos queu length 304

**CONFIG RADIUS ACCT COMMANDS 305** 

config radius acct add 305

config radius acct delete 305

config radius acct disable 306

config radius acct enable 306

**CONFIG RADIUS AUTH COMMANDS 306** 

config radius auth add 306

config radius auth delete 307

config radius auth disable 307

config radius auth enable 307

config rogue ap 308

confia roque client 308

**CONFIG ROUTE COMMANDS 309** 

config route add 309

config route delete 309

**CONFIG SERIAL COMMANDS 309** 

config serial baudrate 309

config serial timeout 310

**CONFIG SESSIONS COMMANDS 310** 

config sessions maxsessions 310

config sessions timeout 311

**CONFIG SNMP COMMUNITY COMMANDS 311** 

config snmp community accessmode 311

config snmp community create 311

config snmp community delete 312

config snmp community ipaddr 312

config snmp community mode 313

config snmp syscontact 313

config snmp syslocation 313

**CONFIG SNMP TRAPRECEIVER COMMANDS 313** 

config snmp trapreceiver create 314

config snmp trapreceiver delete 314

config snmp trapreceiver mode 314

CONFIG SNMP V3USER COMMANDS 315

config snmp v3user create 315

config snmp v3user delete 315

config snmp version 316

CONFIG SPANNINGTREE PORT COMMANDS 316

config spanningtree port mode 316

config spanningtree port pathcost 317

config spanningtree port priority 317

**CONFIG SPANNINGTREE SWITCH COMMANDS 317** 

config spanningtree switch bridgepriority 318

config spanningtree switch forwarddelay 318

config spanningtree switch hellotime 318

config spanningtree switch maxage 319 config spanningtree switch mode 319

CONFIG SWITCHCONFIG COMMANDS 320

config switchconfig flowcontrol 320

config switchconfig mode 320

config syslog 320

config sysname 321

config time 321

**CONFIG TRAPFLAGS COMMANDS 321** 

config trapflags aaa 322

config trapflags ap 322

config trapflags authentication 322

config trapflags client 323

config trapflags configsave 323

config trapflags ipsec 323

config trapflags linkmode 323

config trapflags multiusers 324

config trapflags roqueap 324

config trapflags rrm-params 324

config trapflags rrm-profile 325

config trapflags stpmode 325

**CONFIG WATCHLIST COMMANDS 325** 

config watchlist add 325

config watchlist delete 326

config watchlist enable/disable 326

config wlan blacklist 326

**CONFIG WLAN COMMANDS 327** 

config wlan create 327

config wlan delete 327

config wlan dhcp\_server 327

config wlan disable 328

config wlan enable 328

config wlan mac-filtering 328

config wlan gos 329

config wlan radio 329

CONFIG WLAN SECURITY COMMANDS 330

config wlan security 802.1X 330

config wlan security 802.1X encryption 331

config wlan security cranite 331

config wlan security ipsec 331

config wlan security ipsec authentication 332

config wlan security ipsec encryption 332

config wlan security ipsec ike authentication 333

config wlan security ipsec ike dh-group 333

config wlan security ipsec ike lifetime 334

config wlan security ipsec ike phase1 334

config wlan security passthru 334

config wlan security static-wep-key 335

config wlan security static-wep-key encryption 335

config wlan security web 336

config wlan security web passthru 336

config wlan security wpa 336

config wlan security wpa encryption 337

config wlan timeout 337

config wlan vlan 338

**CONFIG WPS COMMANDS 338** 

config wps contain-adhoc 338

config wps dot11 339

config wps deny-invalid-ap 339

config wps encryption 340

config wps invalid-ssid 340

config wps misconfigured-ap 340

config wps missing-ap 341

config wps preamble 341

config wps radio 342

config wps rldp 342

CONFIG WPS-PEERS COMMANDS 342

config wps-peers group member 343

config wps-peers secure-mode 343

Saving Configurations

save config 344

Clearing Configurations, Logfiles, and Other Actions

clear ap-config 345

clear arp 345 clear config 346 clear stats port 346 clear stats switch 346 clear redirect-url 347 clear transfer 347 clear traplog 347 clear webimage 348 clear webmessage 348 clear webtitle 348 Uploading and Downloading Files and Configurations transfer download certpassword 350 transfer download datatype 350 transfer download filename 351 transfer download mode 351 transfer download path 352 transfer download serverip 352 transfer download start 352 transfer download tftpPktTimeout 353 transfer download tftpMaxRetries 353 transfer upload datatype 353 transfer upload filename 354 transfer upload mode 354 transfer upload path 354 transfer upload serverip 355 transfer upload start 355 Troubleshooting debug aaa 357 debug airewave-director 358 debug arp 358 debug bcast 359 debug crypto 359 debug dhcp 360 debug disable-all 360 debug 80211-events 360 debug 80211-frames 361 debug dot1x 361 debug l2age 361 debug lwapp 362 debug mac addr 362 debug mac disable 362 debug ntp 363 debug pem 363 debug pm 363

Alcatel OmniAccess Wireless System Web Browser Online Help Using the Web Browser Interface Menu Bar 2

debug poe 364 debug transfer 366 Selector Area 3

Main Data Page 3

Administrative Tools 3

Button Area 3

Applying Parameters 4

Refreshing the Screen 4

Troubleshooting 4

# Monitor Menu Bar Selection

Summary 5

Switch Statistics 7

Ports Statistics 8

Ports > Statistics 9

Rogue APs 14

Rogue AP Detail 15

802.11a OmniAccess Radios 17

Radio > Statistics 17

802.11b OmniAccess Radios 21

Clients 21

Clients > Detail 22

**RADIUS Servers 25** 

RADIUS Servers > Authentication Stats 26

RADIUS Servers > Accounting Stats 28

#### WLANs Menu Bar Selection

WLANs 30

WLANs > New 30

WLANs > Edit 31

# Switch Menu Bar Selection

General 35

Inventory 36

Interfaces 37

Interfaces > New 38

Interfaces > Edit 38

Network Routes 40

Network Routes > New 40

Static Mobility Group Members 41

Mobility Group Member > New 41

Mobility Group Member > Edit All 41

Mobility Statistics 42

Switch Spanning Tree Configuration 44

Ports 46

Ports > Configure 47

Port > Configure 48

Master Switch Configuration 51

# Wireless Menu Bar Selection

OmniAccess APs 52

OmniAccess APs > Details 53

802.11a OmniAccess Radios 55

802.11a OmniAccess Radios > Configure 55

802.11 AP Interfaces > Performance Profile 57

802.11a AP Interfaces > Details 58

802.11b OmniAccess Radios 63

802.11b/g OmniAccess Radios > Configure 63

802.11b/g AP Interfaces > Details 65

Third-Party APs 70

Third-Party APs > New 70

Third-Party APs > Edit 71

802.11a Global Parameters 71

802.11a Global Parameters > Auto RF 72

802.11b/g Global Parameters 75

802.11b/g Global Parameters > Auto RF 75

Country 78

Timers 79

## Security Menu Bar Selection

**RADIUS Authentication Servers 80** 

RADIUS Authentication Servers > New 81

RADIUS Authentication Servers > Edit 81

**RADIUS Accounting Servers 82** 

RADIUS Accounting Servers > New 82

RADIUS Accounting Servers > Edit 83

Local Net Users 83

Local Net Users > New 83

Local Net Users > Edit 84

MAC Filtering 84

MAC Filters > New 84

MAC Filters > Edit 85

Disabled Clients 85

Disabled Client > New 85

Disabled Client > Edit 86

Access Control Lists 86

Access Control Lists > New 86

Access Control Lists > Edit 86

Access Control Lists > Rules > Edit 88

CA Certification 90

ID Certificate 90

ID Certificate > New 90

Web Authentication Certificate 91

Rogue Policy 92

# Management Menu Bar Selection

Summary 93

SNMP System Summary 94

SNMP V3 Users 95

SNMP V3 Users > New 95

SNMP v1/v2c Community 96

SNMP v1/v2c Community > New 96

SNMP v1/v2c Community > Edit 97

SNMP Trap Receiver 98

SNMP Trap Receiver > New 99

SNMP Trap Receiver > Edit 99

SNMP Trap Controls 99

Trap Logs 102

HTTP Configuration 104

Telnet-SSH Configuration 105

Serial Port Configuration 105

Local Management Users 106

Local Management Users > New 106

CLI Sessions 107

Syslog Configuration 107

Mgmt Via Wireless 107

Message Logs 108

System Resource Information 108

Switch Crash 108

AP Crash 108

AP Crash Information 109

#### Commands Menu Bar Selection

Download File to Switch 110

Upload File from Switch 110

System Reboot 111

System Reboot > Save? 111

System Reboot > Confirm 111

Reset to Factory Default 112

Set Time 112

# Using the Configuration Wizard

Collect the Initial Configuration Settings 113

Connect Your Web Browser to the Alcatel OmniAccess Switch or Appliance 114

Configuration Wizard System Information 114

Service Interface Configuration 114

Management Interface Configuration 115

Miscellaneous Configuration 115

Virtual Interface Configuration 115

WLAN Policy Configuration 116

**RADIUS Server Configuration 116** 

802.11 Configuration 117

Configuration Wizard Completed 117

# OmniVista Air Control System Online Help

Logging into ACS

Using the ACS Interface

Tabs/Menu Bar 3

Sidebar Area 4

Alarm Monitor 4

Command Buttons 5

Main Data Page 5

Administrative Tools 5

Applying Parameters 5

Refreshing the Screen 6

Map Icons 6

# Viewing System Maps, Devices, Templates and Reports

Monitor Predicted Coverage (RSSI) 10

Monitor Channels on Floor Map 11

Monitor Tx Power Levels on Floor Map 11

Monitor Coverage Holes on Floor Map 12

```
Monitor Users on Floor Map 12
Monitor Clients From Floor Map 12
MONITOR/Alarms Menu Bar Selection 13
Monitor Alarms 13
Monitor Rogue AP Alarms 14
Monitor Alarms > Rogue AP < MACaddress > Detecting APs 15
Monitor Rogue Alarm > Events 15
Monitor Alarm > Events > Rogue AP <MACaddress> 16
MONITOR/Events Menu Bar Selection 17
Monitor Events 17
Monitor Alarm > Events > <device name> <MACaddress> 17
Monitor Link Test Results 18
MONITOR/Network Menu Bar Selection 18
Monitor Network Summary 18
   Coverage Areas 19
   Most Recent Critical Rogue APs 19
   Top 5 APs 19
   Top 5 Coverage Holes 20
   Clients 20
   Left Sidebar 20
MONITOR/Maps Menu Bar Selection 20
Monitor Maps 21
Monitor Maps > Campus 21
Monitor Maps > Campus > Building 22
Monitor Maps > Campus > Building > Floor 23
Monitor Maps > Building 24
Monitor Maps > Building > Floor 25
Monitor Maps > Campus > <outdoor area> 27
Monitor Alarms > Rogue AP < MACaddress > 27
Monitor Alarms > Rogue AP < MACaddress > 2 29
MONITOR/Switches Menu Bar Selection 29
Monitor Switches > Search Results 29
Monitor Switches > < IPaddress > Summary 29
Monitor Switches > <IPaddress> > Ports > n 31
Monitor Switches > < IPaddress > Spanning Tree Protocol 35
Monitor Switches > <IPaddress> > CLI Sessions 37
Monitor Switches > < IPaddress> > WLANs 37
Monitor Switches > < IPaddress > Ports 38
Monitor Switches > <IPaddress> > RADIUS Authentication Servers 38
Monitor Switches > < IPaddress > > RADIUS Accounting Servers 40
Monitor < IPaddress > Local Authentication 41
Monitor Switches > < IPaddress > Mobility Stats 42
Monitor Switches > <IPaddress> > 802.11a Parameters 43
Monitor Switches > <IPaddress> > 802.11a RRM Groups 46
Monitor Switches > <IPaddress> > Switch 802.11b/g Parameters 47
Monitor Switches > <IPaddress> > 802.11b/g RRM Groups 49
Monitor < IPaddress > Interface 50
Monitor < IPaddress > Network Route 50
Monitor < IPaddress > Mobility Group < name > > Group Members 51
Monitor WLAN 51
Monitor < IPaddress > WLANs > < WLAN ID > 52
```

Monitor Client <cli>ent name> 53

Monitor Disabled Clients 56

Monitor Access Control List 57

Monitor Access Control List Template 57

Monitor < IPaddress > Access Control List > < listname > 57

Monitor < IPaddress > Certificate 58

Monitor < IPaddress > > Trap Receivers 59

MONITOR/Access Points Menu Bar Selection 59

Monitor Access Points > Search Results 59

Monitor Access Points > <name> 61

Monitor Access Points > <name> > <Radio Type> 62

On Demand Statistics 63

Operational Parameters 64

802.11 MAC Counters 68

Monitor RADIUS Authentication Server 70

Monitor Local Authentication 70

Monitor Local Authentication > Template <name> 71

MONITOR/Clients Menu Bar Selection 71

Monitor Clients Summary 71

Monitor Watch Lists 73

Monitor Watch Lists > < list name > 73

Monitor 802.11a Parameters 74

Monitor 802.11a RRM Thresholds 75

Monitor 802.11b/g Parameters 75

Monitor 802.11b/g RRM Thresholds Template 76

Monitor 802.11b/g RRM Intervals Template 77

Monitor Historically Known Rogue AP 77

Monitor TFTP Server 77

Monitor Trap Receiver 78

Monitor Trap Controls 78

Monitor Telnet SSH Template 79

Monitor Syslog Configuration 79

Monitor Access Points > Load 80

Monitor Access Points > Dynamic Power Control 80

Monitor Access Points > Noise 81

Monitor Access Points > Interference 81

Monitor Access Points > Coverage (RSSI) 81

Monitor Access Points > Coverage (SNR) 81

Monitor Access Points > Up Time 81

Monitor < IPaddress > Audit Reports 81

Monitor < IPaddress > Audit Report 82

Adding Maps, Devices and Templates

Configure Maps > New Campus 85

Configure Campus > New Building 85

Configure Campus > New Outdoor Area 86

Configure Maps > New Building 87

Configure Maps > Properties 87

Configure Building > New Floor 87

Configure Building > New Floor 2 88

Configure <building name> Edit Floor <floor name> 89

CONFIGURE/Switches Menu Bar Selection 89

Configure All Switches 89

Configure Add Switch 90

Configure < IPaddress > Add Interface 91

Configure < IPaddress > Add Network Route 92

Configure < IPaddress > Mobility Group < name > 92

Configure < IPaddress > Mobility Group Member 92

Configure < IPaddress> > WLAN Template > Add From Template 93

Configure WLAN Template 96

Configure WLAN > New Template 97

Configure < IPaddress> > Local Auth. > Add from Template 100

Configure Access Control List > New Template 101

Configure Access Control List > Add Template Rule <name> 101

Configure Access Control > Add Template <name> 102

Configure < IPaddress > Access Control List > < listname > 103

Configure < IPaddress> > Access Control List > Add from Template 104

Configure < IPaddress > Certificate Details 104

Configure < IPaddress > > Web Auth Certificate 105

Configure < IPaddress > Download Web Auth Certificate to Switch 105

Configure < IPaddress> > Rogue Policy Setup 106

Configure < IPaddress > OmniAccess AP 106

Configure < IPaddress > Connected Third Party AP 107

Configure < IPaddress > Connected Third Party AP > Add New 107

Configure < IPaddress > > Trap Receiver > Add From Template 108

CONFIGURE/Access Points Menu Bar Selection 108

Configure All Access Points 108

Configure < IPaddress> > OmniAccess AP > < name> > 802.11x > Perf. Profile 109

Configure Add Access Points 110

Configure Position Access Points on Floor <floor name> 110

Configure Access Points > OmniAccess AP > <name> > 802.11a 111

Configure Access Points > OmniAccess AP > <name> > 802.11b 112

Config <IPaddr> > OmniAccess AP > <name> > 802.11a > WLANs Overridden 114

Configure Remove Access Points 114

Configure Add Foreign AP 115

Configure Disabled Clients 115

Configure Black List Client > <MACaddress> 116

Configure Clients > Add to Watch List > <MAC address> 116

Configure Watch Lists > New Watch List 116

Configure Watch Lists > Edit > <name> 117

Configure Watch List > <watch list name> > Apply to Switches 117

Configure Watch List > <watch list name> > Remove From Switches 117

Configure Historically Known Rogue AP > Add Rogue AP 118

Configure TFTP Server > Add TFTP Server 118

Configure Software Version > Add 118

CONFIGURE/Templates Menu Bar Selection 119

Configure RADIUS Authentication Server > New Template 119

Configure < IPaddress> > RADIUS Auth. Server > Add From Template 119

Configure RADIUS Authentication Server 120

Configure < IPaddress> > RADIUS Authentication Server 120

Configure RADIUS Accounting Server > New Template 121

Configure RADIUS Accounting Server 121

Configure <IPaddress> > RADIUS Accounting Server > Add From Template 122

Configure Local Authentication > New Template 123

Configure Disabled Clients > New Template 123

Configure < IPaddress > Disabled Clients > Add From Template 123

Configure 802.11a Parameters > New Template 124

Configure 802.11a RRM Thresholds > New Template 125

Configure 802.11a RRM Intervals > New Template 126

Configure 802.11b/g Parameters > Add Template <name> 126

Configure 802.11b/g RRM Thresholds > New Template 127

Configure 802.11b/g Thresholds > New Template 128

Configure 802.11b/g RRM Intervals > New Template 129

Configure Trap Receiver > New Template 129

Configure Trap Controls > New Template 130

Configure Telnet SSH Configuration > New Template 132

Configure Syslog Configuration > New Template 133

## Editing Templates, Maps and Devices

Configure Historically Known Rogue AP > Rogue AP < MACaddress > 135

Configure WLAN Template > Template <name> 135

Configure RADIUS Authentication Server > Template <name> 139

Configure RADIUS Accounting Server > Template <name> 140

Configure <IPaddress> > RADIUS Accounting Server 141

Configure Disabled Clients > Template <MACaddress> 141

Configure Template > <template name> > Apply to Switches 142

Configure 802.11a Parameters > Template <name> 142

Configure 802.11a RRM Thresholds > Template <name> 143

Configure 802.11a RRM Intervals > Template <name> 144

Configure 802.11b/g Parameters > Template <name> 144

Configure 802.11b/g RRM Thresholds > Template <name> 146

Configure 802.11b/g RRM Intervals > Template <name> 147

Configure Trap Receiver > Template <name> 147

Configure Trap Controls > Template <name> 147

Configure Telnet SSH Configuration > Template <name> 150

Configure Syslog Configuration > <template name> 151

Configure Maps > Edit Campus <name> 151

Configure Campus > Edit Outdoor Area <name> 152

Configure <campus name> > Edit Building <building name> 152

Configure Maps > Edit Building > <name> 153

Configure Access Point > OmniAccess AP > <name> 153

Configure < IPaddress > Connected Third Party AP > New 155

Configure < IPaddress > Switch General 156

Configure < IPaddress > Networking Setups 159

Configure < IPaddress > Interface 160

Configure < IPaddress > Network Route 161

Configure < IPaddress > Switch STP Properties 161

Configure Local Authentication 162

Configure Disabled Clients > Template <template name> 163

Configure < IPaddress > Disabled Clients 163

Configure Access Control List > Template <name> 163

Configure < IPaddress > CA Certification 164

Configure < IPaddress> > Switch 802.11 165

Configure < IPaddress> > 802.11a Parameters 166

Configure < IPaddress> > 802.11a RRM Thresholds 167

```
Configure < IPaddress> > 802.11a RRM Intervals 168
Configure < IPaddress > > 802.11a Grouping Control 169
Configure < IPaddress > > 802.11b/g Parameters 169
Configure <IPaddress> > 802.11b/g RRM Thresholds 171
Configure < IPaddress> > 802.11b/g RRM Intervals 172
Configure < IPaddress> > 802.11b/g RRM Grouping Control 172
Configure <IPaddress> > Ports 173
Configure < IPaddress > Ports > < port# > 174
Configure < IPaddress > Ports > < # > 174
Configure < IPaddress> > Trap Receiver 175
Configure < IPaddress > Trap Controls 175
Configure < IPaddress> > Telnet SSH Configuration 178
Configure < IPaddress > Syslog Configuration 178
Configure < IPaddress > > WEB Admin 178
Configure < IPaddress > Download Web Admin Certificate 179
Configure TFTP Server > TFTP Server < name > 180
```

**Operating Devices** 

Configure < IPaddress > Switch Commands 181

Restore to Factory Default Command 182

<IPaddress> > Refresh Config 182

<IPaddress> > Restore Config 183

<IPaddress> > Set Time 183

Upload File Command 183

**Download Configuration Command 184** 

Download Software to Switch 184

Download Software 185

# Alcatel OmniAccess Wireless Access Point Deployment Guide

#### **Deployment Overview**

# Step 1: Determining Deployment Requirements

Assumptions 3

Protocol Requirements 3

Coverage Area Requirements 4

Building Type 4

Building Homogeneity 5

Average Client Throughput 5

Voice over IP Requirements 8

# Step 2: Determining Deployment Strategy

Professional Site Survey 9

RF Prediction with Optional Site Survey 10

Basic Guidelines with Optional Site Survey 10

# Sample Basic Guidelines Process

Step A: Determine Radius and Z Factor 11

Step B. Determine How Many APs are Needed 13

Step C. Optional Minimal Site Survey 14

Step D. Place Access Points 14

# Step 3: Optional Minimal Site Survey

Collecting Tools and Materials 16

Selecting OmniAccess AP Locations 16

Enabling Site Survey Mode 16

Preparing Optional OmniAccess AP Tripod Test Assemblies 19

Positioning an OmniAccess AP at Each Planned Location 21 Verifying RF Coverage Using the Alcatel Site Survey Tool 21

# Step 4. OmniAccess AP Placement Guidelines

Collecting Maps or Building Floor Plans 22

Noting Any Deployment Constraints 22

Access Point Placement Guidelines 22

OmniAccess AP Placement 23

Step 5: Where to Go from Here

# Internal-Antenna OmniAccess AP Quick Installation Guide

#### ATTENTION!

Overview

Step 1: Collecting Required Tools and Supplies

Step 2: Configuring the OmniAccess AP Before Installation

Preparing a Version 2.0 OmniAccess AP 5

Configuration Setup 5

Does My AP Qualify for this Procedure? 5

Configuration Steps for an OmniAccess AP 5

Step 3: Preparing Mounting Locations

Step 4: Mounting the OmniAccess APs

Ceiling Mount Base 10

Ceiling-Mount Clips 11

Projection Wall Mount 13

Flush Wall Mount 15

Step 5: Returning MAC Information

# **Planning Notes**

About Cables 18

About External Antennas 18

**About Mounting Options 18** 

About Physical Security 19

FCC Statements for OmniAccess APs 19

Class A Statement 19

RF Radiation Hazard Warning 19

Non-Modification Statement 19

Deployment Statement 19

# External-Antenna OmniAccess AP Quick Installation Guide

# ATTENTION!

Overview

Step 1: Collecting Required Tools and Supplies

Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation

Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R 5

Configuration Setup 5

Does My AP Qualify for this Procedure? 5

Configuration Steps for an OmniAccess AP or OmniAccess AP 1200R 5

Alternate Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R 7

Configuration Setup 8

Does My AP Qualify for this Procedure? 8

Configuration Steps for an OmniAccess AP or OmniAccess AP 1200R 8

Step 3: Preparing Mounting Locations

Step 4: Mounting the OmniAccess APs

Ceiling Mount Base 13

Ceiling-Mount Clips 15

**Projection Wall Mount 16** 

Flush Wall Mount 18

# Step 5: Returning MAC Information

# Planning Notes

About Cables 22

About External Antennas 22

**About Mounting Options 23** 

About Physical Security 24

#### FCC Statements for OmniAccess APs 24

Class A Statement 24

RF Radiation Hazard Warning 24

Non-Modification Statement 24

Deployment Statement 24

# Alcatel OmniAccess Switch and Appliance Quick Installation Guide

FCC Statements for Alcatel OmniAccess Switches and Appliances 1

#### Overview

## Step 1: Collecting Required Tools and Information

Hardware Installation 6

CLI Console 6

Local TFTP Server 6

Initial System Configuration Information 6

Step 2: Determining a Location

Step 3: Installing the Chassis

Step 4: Connecting and Using the CLI Console

Step 5: Performing Power On Self Test

Step 6: Using the Startup Wizard

Step 7: Logging In

Step 8: Connecting the Network (Distribution System)

Step 9: Connecting the Service Port Interfaces

Step 10: Connecting Access Points

Step 11: Where to Go from Here

# Enhanced Security Module Quick Installation Guide

Collecting Required Tools and Supplies

Installing the Enhanced Security Module

Removing the Enhanced Security Module

# 1000Base-SX Network Adapter Module Quick Installation Guide

Collecting Required Tools and Supplies

Installing the 1000Base-SX Network Adapter Module

Removing the 1000Base-SX Network Adapter Module

# 1000Base-T Network Adapter Module Quick Installation Guide

Collecting Required Tools and Supplies

Installing the 1000Base-T Network Adapter Module

# Removing the 1000Base-T Network Adapter Module

# ACS Quick Installation Guide

Overview

Step 1: Verifying the Workstation Configuration

Step 2: Installing Client and Server Software

Step 3: Starting and Stopping the ACS Software Server

Starting the ACS Software Server as an Application 6

Starting the ACS Software Server as a Service 6

Stopping the ACS Software Server Application 7

Stopping the ACS Software Service 7

Step 4: Starting and Stopping an ACS Software Client

Starting an ACS Software Browser Client 9

Starting an ACS Software Java Admin Client 10

Stopping an ACS Software Browser Client 11

Stopping an ACS Software Java Admin Client 11

Step 5: Where to Go From Here

# ACS Floor Plan Editor Quick Installation Guide

Installing the ACS Floor Plan Editor

Starting the ACS Floor Plan Editor

Using the ACS Floor Plan Editor

Shutting Down the ACS Floor Plan Editor

# Alcatel Site Survey Tool User Guide

## BEFORE YOU BEGIN

Site Survey Goals 2

Supported Network Standards 2

Survey Safety 2

Operating Environment 3

User Training 3

Abbreviations and Definitions 3

# Getting Started

System Overview 4

System Requirements 4

Installing the Site Survey Tool 5

Supported Adapters 5

**Untested Adapters 6** 

Updating the WLAN Adapter Driver 6

**Technical Support 8** 

# Alcatel Client

**Using Alcatel Client 9** 

Working with Configuration Profiles 9

Changing Adapter Settings 10

# Site Survey Tool User Interface

Overview 11

Site Survey Tool User Interface 11

Projects and Surveys 12

Using Map Images 12

Using the Browser View 13

Exporting Map Image to a File 15

Exporting Survey Data to a File 15

Printing a Map Image 15

# Recording Data with the Site Survey Tool

Starting to Work with the Site Survey Tool 16

Recording a Site Survey with Map 17

Recording a Site Survey without a Map 18

Signals Tab 19

Record Tab 19

Survey Properties 19

Marking Exact Access Point Locations 19

Access Point Properties 20

# Analysis Features

Performing Analysis 21

Signal Strength (RSSI) 21

Signal to Noise Ratio (SNR) 23

Interference 24

Strongest Access Point 25

Access Point Count 25

Signals at Channel 26

Access Point Placement Tip 26

Access Point Location 27

Transmission Speed 28

# The Basics of Site Survey

Background of Site Survey 30

When Site Survey is Needed 30

Defining WLAN Requirements 30

## Site Survey Guidelines

General Wireless LAN Setup Steps 32

Visual Site Inspection 32

Performing the Survey 33

Locating Access Points 34

Verifying Network Coverage 34

Network Quality and Channel Planning 35

Improving the Network Based on Survey Results 35

Finishing the Network Design and Documenting Results 36

Implementing Location Aware Networks 36

# Upgrading a License

Purchasing a License 37

Upgrading the License 37

Troubleshooting

# Alcatel OmniAccess Wireless System Release Notes 2.0.113.3

Alcatel OmniAccess Wireless Enterprise Platform Components

Requirements for Alcatel OmniAccess Wireless System Components

New Features Available in Release 2.0

Features Not Available in this Release

Features Improved in this Release

**Technical Notes** 

Open Issues in Alcatel Wireless Operating System Software Interoperability Tables

## ACS Software Release Notes 2.0.67.0

Alcatel OmniAccess Wireless Enterprise Platform Components Requirements for OmniVista Air Control System New Features Improvements in this Release Technical Notes for the OmniVista Air Control System Technical Notes for the Alcatel Site Survey Tool Technical Notes for the ACS Floor Plan Editor Open Issues in the OmniVista Air Control System Software

# **OVERVIEWS**

Refer to the following for information about the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System) and other high-level subjects:

- About the Alcatel OmniAccess Wireless System
  - Alcatel Wireless Operating System
  - Single-Alcatel OmniAccess Switch or Appliance Deployments
  - Multiple-Alcatel OmniAccess Switch and Appliance Deployments
  - Alcatel Wireless Operating System Security
  - Alcatel Wired Security
  - Layer 2 and Layer 3 Operation
  - OmniVista AirView Software
  - Master Alcatel OmniAccess Switch or Appliance
  - Primary Alcatel OmniAccess Switch or Appliance
  - Client Roaming
  - External DHCP Servers
  - Alcatel Mobility Group
  - Alcatel Wired Connections
  - Alcatel WLANs
  - <u>Identity Networking</u>
  - Port Mirroring
  - Transferring Files
  - Power Over Ethernet
- Alcatel OmniAccess Switches and Appliances
- Alcatel OmniAccess Wireless Access Points
- <u>Third-Party Access Points</u>
- Roque Access Points
- OmniVista Air Control System Software
  - ACS Software Java Admin Client
  - ACS Software Browser Client
  - ACS Floor Plan Editor
  - ACS Alcatel OmniAccess Switch and Appliance Autodiscovery
- Alcatel Web Browser Interface
- Command Line Interface

# **About the Alcatel OmniAccess Wireless System**

The Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System) is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Alcatel OmniAccess Wireless System simplifies deploying and managing large scale wireless LANs and enables a unique best-in-class security infrastructure. The Alcatel Wireless Operating System manages all subscriber, communications, and system administration functions, performs <code>OmniVista AirView Software</code> functions, manages system-wide mobility policies using the Alcatel Wireless Operating System Security solution, and coordinates all security functions using the <code>Alcatel Wireless Operating System Security</code> framework.

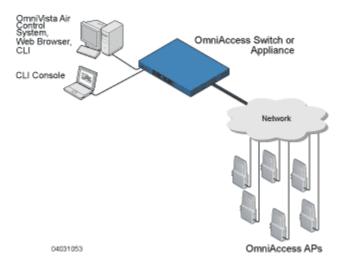
The Alcatel OmniAccess Wireless System consists of Alcatel OmniAccess Wireless Switches and Appliances (<u>Alcatel OmniAccess Switches and Appliances</u>) and their associated OmniAccess APs (<u>Alcatel OmniAccess Wireless Access Points</u>) controlled by the Alcatel Wireless Operating System, all managed by any or all of the Alcatel Wireless Operating System user interfaces.

- The OmniVista Air Control System Software (ACS Software Server) interface is used to
  configure and monitor one or more Alcatel OmniAccess Switches and Appliances and associated
  APs, and has tools to facilitate large-system monitoring and control. The <u>OmniVista Air Control</u>
  System Software runs on Windows 2000 workstations.
- A full-featured CLI (command line interface) can be used to configure and monitor individual Alcatel OmniAccess Switches and Appliances. Refer to the <u>Command Line Interface</u> section.
- A full-featured Web Browser (HTTP) interface hosted by Alcatel OmniAccess Switches and Appliances running on any workstation with a supported Web browser can be used to configure and monitor individual Alcatel OmniAccess Switches and Appliances. See the <u>Alcatel Web Browser Interface</u> section.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Alcatel solution also allows service providers to incorporate their existing Cisco 1200, Cisco 350 and ORINOCO 2000 Access Points (*Third-Party Access Points*) into an expanding Alcatel network.

The following figure shows the Alcatel OmniAccess Wireless System components, which can be simultaneously deployed across multiple floors and buildings.

Figure - Alcatel OmniAccess Wireless System Components in Appliance Mode



Refer to the following for more information:

- <u>Alcatel Wireless Operating System</u>
- Single-Alcatel OmniAccess Switch or Appliance Deployments
- <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u>
- Alcatel Wireless Operating System Security
- Alcatel Wired Security
- Layer 2 and Layer 3 Operation
- OmniVista AirView Software
  - Master Alcatel OmniAccess Switch or Appliance
  - Primary Alcatel OmniAccess Switch or Appliance
  - Client Roaming
  - External DHCP Servers
  - Alcatel Mobility Group
  - Alcatel Wired Connections
  - Alcatel WLANs
  - Port Mirroring
  - <u>Transferring Files</u>
  - Power Over Ethernet
- Alcatel OmniAccess Switches and Appliances
- Alcatel OmniAccess Wireless Access Points
- Third-Party Access Points
- Rogue Access Points
- OmniVista Air Control System Software
  - ACS Software Java Admin Client
  - ACS Software Browser Client
  - ACS Floor Plan Editor
  - ACS Alcatel OmniAccess Switch and Appliance Autodiscovery
- Alcatel Web Browser Interface
- Command Line Interface

## **About the Alcatel Wireless Operating System**

The Alcatel Wireless Operating System is software that controls Alcatel OmniAccess Wireless Switches and Alcatel OmniAccess Wireless Access Points. It includes <u>Alcatel Wireless Operating System Security</u> and <u>OmniVista AirView Software</u> functions.

## **Single-Alcatel OmniAccess Switch or Appliance Deployments**

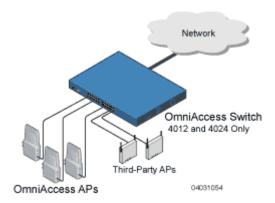
As described in <u>About the Alcatel OmniAccess Wireless System</u>, a standalone Alcatel OmniAccess Wireless Switch or Appliance can support Alcatel OmniAccess Wireless Access Points (OmniAccess APs) and third-party APs across multiple floors and buildings simultaneously, and supports the following features:

- Autodetecting and autoconfiguring OmniAccess APs as they are added to the network, as described in *OmniVista AirView Software*.
- Full control of Alcatel OmniAccess Wireless Access Points.
- Control of associated <u>Third-Party Access Points</u> through the native third-party AP interface, and real-time control of system-wide WLAN Web, 802.1X, and IPSec security policies.
- Full control of up to 16 OmniAccess AP and one third-party AP WLAN (SSID) policies, as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>.

The following figures show typical single OmniAccess Wireless Switch deployed in <u>Direct-Connect Mode</u> and <u>Appliance Mode</u>.

- In Direct-Connect Mode, OmniAccess APs and third-party APs connect directly to the Model 4012 or 4024 OmniAccess Wireless Switch front panel, with or without the OmniAccess Wireless Switch providing *Power Over Ethernet* to the APs.
- Note: Alcatel OmniAccess Wireless Switches can connect through multiple physical ports to multiple subnets in the Network. This can be helpful, for instance, when Alcatel OmniAccess Wireless System operators want to confine multiple VLANs to separate subnets.

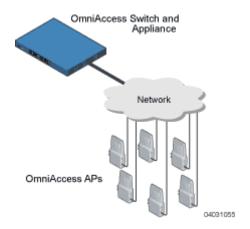
Figure - Typical Single 4012 or 4024 OmniAccess Wireless Switch Deployed in Direct-Connect Mode



- In Appliance Mode, OmniAccess APs connect to the Model 4012 or 4024 Alcatel OmniAccess Wireless Switches or 4102 OmniAccess Wireless Appliances through the network. The network equipment may or may not provide <u>Power Over Ethernet</u> to the OmniAccess APs.
- Note: Alcatel OmniAccess Wireless Switches and Appliances can connect through the Management Interface to multiple subnets in the Network. This can be helpful, for instance, when Alcatel OmniAccess Wireless System operators want to confine multiple VLANs to separate subnets using <a href="#Operator-Defined Interfaces">Operator-Defined Interfaces</a>.

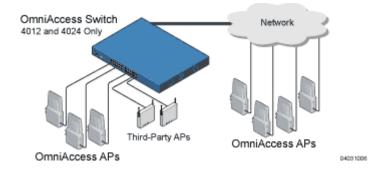
Note that the 4102 OmniAccess Wireless Appliance uses two redundant GigE connections to bypass single network failures. At any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

Figure - Typical Alcatel OmniAccess Wireless Switches and Appliances Deployed in Appliance Mode



- In Hybrid Mode, the APs simultaneously connect to the Model 4012 or 4024 OmniAccess Wireless Switch in Direct-Connect and Appliance Mode, with or without the OmniAccess Wireless Switch or the network equipment providing <a href="Power Over Ethernet">Power Over Ethernet</a> to the OmniAccess APs.
- Note: Alcatel OmniAccess Wireless Switches can connect through the Management Interface to multiple subnets in the Network. This can be helpful, for instance, when Alcatel OmniAccess Wireless System operators want to confine multiple VLANs to separate subnets using <a href="#Operator-Defined Interfaces">Operator-Defined Interfaces</a>.

Figure - Typical 4012 or 4024 Single OmniAccess Wireless Switch Deployed in Hybrid Mode



# Multiple-Alcatel OmniAccess Switch and Appliance Deployments

Each OmniAccess Wireless Switch can support OmniAccess APs and third-party APs across multiple floors and buildings simultaneously. Similarly, each OmniAccess Wireless Appliance can support OmniAccess APs across multiple floors and buildings simultaneously. However, full functionality of the Alcatel OmniAccess Wireless System is realized when it includes multiple Alcatel OmniAccess Switches and Appliances. That is, a multiple-Alcatel OmniAccess Switch and Appliance system has the following additional features over a single-Alcatel OmniAccess Switch or Appliance deployment:

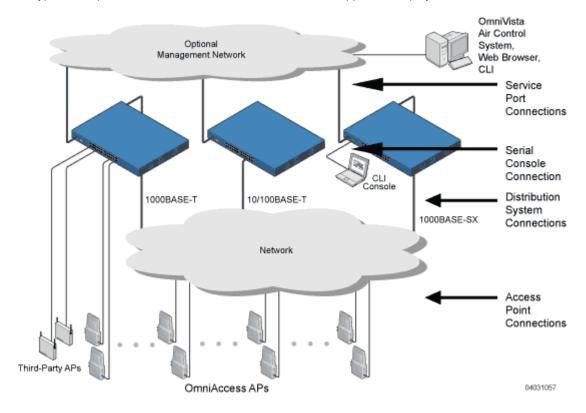
Autodetecting and autoconfiguring Alcatel OmniAccess Switch or Appliance RF parameters as the Alcatel OmniAccess Switches and Appliances are added to the network, as described in *OmniVista AirView Software*.

- <u>Same-Alcatel OmniAccess Switch or Appliance (Layer 2) Roaming</u> and <u>Inter-Subnet (Layer 3)</u> Roaming.
- Automatic OmniAccess AP failover to any redundant Alcatel OmniAccess Switch or Appliance with unused ports (refer to <u>Alcatel OmniAccess Switch and Appliance Failover Protection</u>).

The following figure shows a typical multiple-Alcatel OmniAccess Switch and Appliance deployment, with the Alcatel OmniAccess Switch or Appliance in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u> and <u>Hybrid Mode</u>. The figure also shows an optional dedicated Service Network, and the three physical connection types between the network and the Alcatel OmniAccess Switch or Appliance, as further described in <u>Network Connection to an Alcatel OmniAccess Switch or Appliance</u>.

Note: Alcatel OmniAccess Wireless Switches and Appliances can connect through the Management Interface to multiple subnets in the Network. This can be helpful, for instance, when Alcatel OmniAccess Wireless System operators want to confine multiple VLANs to separate subnets using <a href="#Operator-Defined Interfaces">Operator-Defined Interfaces</a>.

Figure - Typical Multiple-Alcatel OmniAccess Wireless Switch and Appliance Deployment



## **About Alcatel Wireless Operating System Security**

Alcatel Wireless Operating System Security bundles Layer 1, Layer 2 and Layer 3 security components into a simple, system-wide policy manager that creates independent security policies for each of up to 16 Alcatel WLANs and one third-party WLAN. (Refer to <u>Alcatel WLANs</u>.)

One of the barriers that made enterprises avoid deploying 802.11 networks was the inherent weakness of 802.11 WEP (Wired Equivalent Privacy) encryption. Because WEP is so insecure, enterprises have been looking for more secure solutions for business-critical traffic.

The 802.11 WEP weakness problem can be overcome using robust industry-standard security solutions, such as:

- 802.1X dynamic keys with EAP (extended authorization protocol), or
- WPA (Wi-Fi protected access) dynamic keys. The Alcatel WPA implementation includes:
  - TKIP + Michael (temporal key integrity protocol + message integrity code checksum) dynamic keys, or
  - WEP (Wired Equivalent Privacy) keys.

The WEP problem can be further solved using industry-standard Layer 3 security solutions, such as:

- Terminated and pass-through VPNs (virtual private networks), and
- Terminated and pass-through IPSec (IP security) protocols. The terminated Alcatel IPSec implementation includes:
  - IKE (internet key exchange),
  - DH (Diffie-Hellman) groups, and
  - Three optional levels of encryption: DES (ANSI X.3.92 data encryption standard), 3DES (ANSI X9.52-1998 data encryption standard), or AES/CBC (advanced encryption standard/cipher block chaining).

The Alcatel IPSec implementation also includes industry-standard authentication using:

- MD5 (message digest algorithm), or
- SHA-1 (secure hash algorithm-1).
- The Alcatel OmniAccess Wireless System supports local and RADIUS MAC Address (media access control) filtering.
- The Alcatel OmniAccess Wireless System supports local and RADIUS user/password authentication.
- The Alcatel OmniAccess Wireless System also uses manual and automated Disabling to block access to network services. In manual Disabling, the operator blocks access using client MAC addresses. In automated Disabling, which is always active, the Alcatel Wireless Operating System software automatically blocks access to network services for an operator-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This can be used to deter brute-force login attacks.

These and other <u>Alcatel Wireless Operating System Security</u> features use industry-standard authorization and authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic.

For information about Alcatel wired security, refer to Alcatel Wired Security.

## **About Alcatel Wired Security**

Many traditional Access Point vendors concentrate on security for the Wireless interface similar to that described in the <u>Alcatel Wireless Operating System Security</u> section. However, for secure Alcatel Omni-Access Switch and Appliance Service Interfaces (<u>OmniVista Air Control System Software</u>, <u>Alcatel Web Browser Interface</u>, and <u>Command Line Interface</u>), Alcatel OmniAccess Switch and Appliance to AP, and inter-Alcatel OmniAccess Switch and Appliance communications during device servicing and <u>Client Roaming</u>, the Alcatel Wireless Operating System includes built-in security.

Each OmniAccess Wireless Switch, OmniAccess Wireless Appliance, and OmniAccess AP is manufactured with a unique, signed X.509 certificate. This certificate is used to authenticate IPSec tunnels between devices. These IPSec tunnels ensure secure communications for mobility and device servicing.

Alcatel OmniAccess Switches and Appliances and OmniAccess APs also use the signed certificates to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any OmniAccess Wireless Switch, OmniAccess Wireless Appliance or OmniAccess AP.

For information about Alcatel wireless security, refer to Alcatel Wireless Operating System Security.

# **Layer 2 and Layer 3 Operation**

The LWAPP communications between Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs can be conducted at ISO Data Link Layer 2 or Network Layer 3, whether the connections are made in *Direct-Connect Mode*, *Appliance Mode*, or *Hybrid Mode*.

## **Operational Requirements**

The requirement for Layer 2 LWAPP communications is that the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs must be connected directly to each other or connected through Layer 2 devices on the same subnet. This is the default operational mode for the Alcatel OmniAccess Wireless System. Note that when the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, OmniAccess APs, and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) are on different subnets, these devices must be operated in Layer 3 mode.

The requirement for Layer 3 LWAPP communications is that the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, OmniAccess APs, and OmniAccess 1200R APs can be connected directly to each other, connected through Layer 2 devices on the same subnet, or connected through Layer 3 devices across subnets.

Note that all Alcatel OmniAccess Switches and Appliances in an <u>Alcatel Mobility Group</u> must use the same LWAPP Layer 2 or Layer 3 mode, or you will defeat the Mobility software algorithm.

#### **Configuration Requirements**

When you are operating the Alcatel OmniAccess Wireless System in Layer 2 mode, you must configure a <u>Management Interface</u> to control your Layer 2 communications.

When you are operating the Alcatel OmniAccess Wireless System in Layer 3 mode, you must configure a <u>Management Interface</u> to control your Layer 2 communications, and an <u>AP-Manager Interface</u> to control OmniAccess AP- and OmniAccess AP 1200R-to-Alcatel OmniAccess Switch or Appliance Layer 3 communications.

#### **About OmniVista AirView Software**

Alcatel Internetworking, Inc. is the only company to offer the powerful, comprehensive, and dynamic OmniVista AirView Software solution to the 802.11 market. The OmniVista AirView Software allows Alcatel OmniAccess Switches and Appliances to continually monitor their associated OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) for the following information:

- Traffic Load -- How much total bandwidth is used for transmitting and receiving traffic. This
  allows WLAN managers to track network growth and plan network growth ahead of client
  demand
- Interference -- How much traffic is coming from other 802.11 sources.
- Noise -- How much non-802.11 noise is interfering with the currently-assigned channel.
- Coverage -- Received Signal Strength (RSSI) and Signal to Noise Ratio (SNR) for all clients.
- Nearby APs.

Using the collected information, the OmniVista AirView Software can periodically reconfigure the 802.11 RF network within operator-defined limits for best efficiency. To do this, OmniVista AirView Software:

- Dynamically reassigns channels to increase capacity and performance, both within the same Alcatel OmniAccess Switch or Appliance and across multiple Alcatel OmniAccess Switches and Appliances.
- Adjusts the transmit power to balance coverage and capacity, both within the same Alcatel OmniAccess Switch or Appliance and across multiple Alcatel OmniAccess Switches and Appliances.
- Allows the operator to assign nearby OmniAccess APs and OmniAccess 1200R APs into groups to streamline OmniVista AirView Software algorithm processing.
- As new clients associate, they are load balanced across grouped OmniAccess APs reporting to each Alcatel OmniAccess Switch or Appliance. This is particularly important when many clients converge in one spot (such as a conference room or auditorium), because OmniVista AirView Software can automatically force some subscribers to associate with nearby APs, allowing higher throughput for all clients.
- Automatically detect and configure new OmniAccess APs and OmniAccess 1200R APs as they
  are added to the network. The OmniVista AirView Software automatically adjusts nearby
  OmniAccess APs and OmniAccess 1200R APs to accommodate the increased coverage and
  capacity.
- Automatically detect and configure new Alcatel OmniAccess Switches and Appliances as they
  are added to the network. The OmniVista AirView Software automatically distributes associated
  OmniAccess APs and OmniAccess 1200R APs to maximize coverage and capacity.
- Detect and report coverage holes, where clients consistently connect to an OmniAccess AP or OmniAccess AP 1200R at a very low signal strength.
- Automatically define Alcatel OmniAccess Switch and Appliance Groups within operator-defined Mobility Groups.

The OmniVista AirView Software solution thus allows the operator to avoid the costs of laborious historical data interpretation and individual Alcatel OmniAccess Wireless Access Point or OmniAccess AP 1200R reconfiguration. The power control features of OmniVista AirView Software ensure client satisfaction, and the coverage hole detection feature can alert the operator to the need for an additional (or relocated) OmniAccess AP or OmniAccess AP 1200R.

Note that the OmniVista AirView Software uses separate monitoring and control for each of the deployed networks: 802.11a and 802.11b/802.11g. Also note that the OmniVista AirView Software is automatically enabled, but can be customized or disabled for individual OmniAccess APs.

Finally, for operators requiring easy manual configuration, the OmniVista AirView Software can recommend the best OmniAccess Radio settings, and then assign them on operator command.

The OmniVista AirView Software controls produce a network that has optimal capacity, performance, and reliability. The OmniVista AirView Software functions also free the operator from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. Finally, the OmniVista AirView Software controls ensure that clients enjoy a seamless, trouble-free connection through the Alcatel 802.11 network.

## **About the Master Alcatel OmniAccess Switch or Appliance**

When you are adding OmniAccess APs to a <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u> network configured in <u>Appliance Mode</u>, it is convenient to have all OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) associate with one Master Alcatel OmniAccess Wireless Switch or Appliance on the same subnet. That way, the operator does not have to log into multiple Alcatel OmniAccess Switches and Appliances to find out which Alcatel OmniAccess Switch or Appliance newly-added OmniAccess APs or OmniAccess 1200R APs associated with.

One Alcatel OmniAccess Switch or Appliance in each subnet can be assigned as the Master Alcatel OmniAccess Switch or Appliance while adding OmniAccess APs and OmniAccess 1200R APs. As long as a Master Alcatel OmniAccess Switch or Appliance is active on the same subnet, all new OmniAccess APs and OmniAccess 1200R APs without a *Primary Alcatel OmniAccess Switch or Appliance* assigned automatically attempt to associate with the Master Alcatel OmniAccess Switch or Appliance. This process is described in *Alcatel OmniAccess Switch and Appliance Failover Protection*.

The operator can monitor the Master Alcatel OmniAccess Switch or Appliance using the <u>Alcatel Web Browser Interface</u> or the <u>OmniVista Air Control System Software</u> GUI, and watch as OmniAccess APs and OmniAccess 1200R APs associate with the Master Alcatel OmniAccess Switch or Appliance. The operator can then verify OmniAccess AP and OmniAccess AP 1200R configuration and assign a <u>Primary Alcatel OmniAccess Switch or Appliance</u> to the OmniAccess AP or OmniAccess AP 1200R, and reboot the OmniAccess AP or OmniAccess AP 1200R so it reassociates with its Primary Alcatel OmniAccess Switch or Appliance.



**Note:** OmniAccess APs and OmniAccess 1200R APs without a *Primary Alcatel OmniAccess Switch or Appliance* assigned always search for a Master Alcatel OmniAccess Switch or Appliance first upon reboot. After adding OmniAccess APs and OmniAccess 1200R APs through the Master Alcatel OmniAccess Switch or Appliance, assign a Primary Alcatel OmniAccess Switch or Appliance to each OmniAccess AP and OmniAccess AP 1200R. Alcatel recommends that you disable the Master Alcatel OmniAccess Switch or Appliance setting on all Alcatel OmniAccess Switches and Appliances after initial configuration.

# **About the Primary Alcatel OmniAccess Switch or Appliance**

In <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u> networks, OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) can associate with any Alcatel OmniAccess Wireless Switch or Appliance in <u>Appliance Mode</u> on the same subnet. To ensure that each OmniAccess AP and OmniAccess AP 1200R associates with a particular Alcatel OmniAccess Switch or Appliance, the operator can assign a Primary Alcatel OmniAccess Switch or Appliance to the OmniAccess AP or OmniAccess AP 1200R.

When an OmniAccess AP or OmniAccess AP 1200R is added to a network, it looks for its Primary Alcatel OmniAccess Switch or Appliance first, then a <u>Master Alcatel OmniAccess Switch or Appliance</u>, then the least-loaded Alcatel OmniAccess Switch or Appliance with available AP ports. Refer to <u>Alcatel OmniAccess Switch and Appliance Failover Protection</u> for more information.

## **About Client Roaming**

The Alcatel OmniAccess Wireless System supports seamless client roaming across OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) managed by the same Alcatel OmniAccess Wireless Switch or Appliance, between Alcatel OmniAccess Switches and Appliances in the same <u>Alcatel Mobility Group</u> on the same subnet, and across Alcatel OmniAccess Switches and Appliances in the same Mobility Group on different subnets. The following chapters describe the three modes of roaming supported by the Alcatel OmniAccess Wireless System.

#### Same-Alcatel OmniAccess Switch or Appliance (Layer 2) Roaming

Each Alcatel OmniAccess Switch and Appliance supports same-Alcatel OmniAccess Switch or Appliance client roaming across OmniAccess APs, OmniAccess 1200R APs, and third-party APs managed by the same Alcatel OmniAccess Switch or Appliance, whether in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u> or <u>Hybrid Mode</u>. This roaming is transparent to the client, as the session is sustained and the client continues using the same DHCP-assigned or client-assigned IP Address. Same-Alcatel OmniAccess Switch or Appliance roaming is supported in <u>Single-Alcatel OmniAccess Switch or Appliance Deployments</u> and <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u>.

## Inter-Alcatel OmniAccess Switch and Appliance (Layer 2) Roaming

Similarly, in <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u>, the Alcatel OmniAccess Wireless System supports client roaming across OmniAccess APs, OmniAccess 1200R APs, and third-party APs managed by Alcatel OmniAccess Switches and Appliances in the same mobility group and on the same subnet. This roaming is also transparent to the client, as the session is sustained and a tunnel between Alcatel OmniAccess Switches and Appliances allows the client to continue using the same DHCP- or client-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP Address or a 169.254.\*.\* client auto-IP Address, or when the operator-set session timeout is exceeded.

Note that the OmniAccess 1200R APs at a remote location must be on the same subnet to support roaming.

#### Inter-Subnet (Layer 3) Roaming

Similarly, in *Multiple-Alcatel OmniAccess Switch and Appliance Deployments*, the Alcatel OmniAccess Wireless System supports client roaming across OmniAccess APs, OmniAccess 1200R APs, and third-party APs managed by Alcatel OmniAccess Switches and Appliances in the same mobility group on different subnets. This roaming is transparent to the client, because the session is sustained and a tunnel between the Alcatel OmniAccess Switches and Appliances allows the client to continue using the same DHCP-assigned or client-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP Address or a 169.254.\*.\* client auto-IP Address, or when the operator-set session timeout is exceeded.

Note that the OmniAccess 1200R APs at a remote location must be on the same subnet to support roaming.

## **Special Case: Voice Over IP Telephone Roaming**

802.11 VoIP telephones actively seek out associations with the strongest RF signal to ensure best Quality of Service (QoS) and maximum throughput. The minimum VoIP telephone requirement of 20 millisecond or shorter latency time for the roaming handover is easily met by the Alcatel Omni-Access Wireless System, which has an average handover latency of nine or fewer milliseconds.

This short latency period is controlled by Alcatel OmniAccess Switches and Appliances, rather than allowing independent APs to negotiate roaming handovers.

The Alcatel OmniAccess Wireless System supports 802.11 VoIP telephone roaming across OmniAccess APs, OmniAccess 1200R APs, and third-party APs managed by Alcatel OmniAccess Switches and Appliances on different subnets, as long as the Alcatel OmniAccess Switches and Appliances are in the same mobility group. This roaming is transparent to the VoIP telephone, because the session is sustained and a tunnel between Alcatel OmniAccess Switches and Appliances allows the VoIP telephone to continue using the same DHCP-assigned IP Address as long as the session remains active. Note that the tunnel is torn down and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP Address or a 169.254.\*.\* VoIP telephone auto-IP Address, or when the operator-set session timeout is exceeded.

#### **About External DHCP Servers**

The Alcatel Wireless Operating System is designed to appear as a DHCP Relay to the network and as a DHCP Server to clients with industry-standard external DHCP Servers that support DHCP Relay. This means that each Alcatel OmniAccess Wireless Switch or Appliance appears as a DHCP Relay agent to the DHCP Server. This also means that the Alcatel OmniAccess Switch or Appliance appears as a DHCP Server at the virtual IP Address to wireless clients.

Because the Alcatel OmniAccess Switch or Appliance captures the client IP Address obtained from a DHCP Server, it maintains the same IP Address for that client during same-Alcatel OmniAccess Switch or Appliance, inter-Alcatel OmniAccess Switch and Appliance, and inter-subnet *Client Roaming*.

#### **Per-WLAN Assignment**

All <u>Alcatel WLANs</u> can be configured to use the same or different DHCP Servers, or no DHCP Server. This allows operators considerable flexibility in configuring their Wireless LANs, as further described in the <u>Alcatel WLANs</u> section.

Note that Alcatel WLANs that support <u>Management over Wireless</u> must allow the management (device servicing) clients to obtain an IP Address from a DHCP Server.

#### **Per-Interface Assignment**

- The Layer 2 <u>Management Interface</u> can be configured for a primary and secondary DHCP server.
- The Layer 3 <u>AP-Manager Interface</u> can be configured for a primary and secondary DHCP server.
- Each of the <u>Operator-Defined Interfaces</u> can be configured for a primary and secondary DHCP server.
- The Virtual Interface does not use DHCP servers.
- The <u>Service-Port Interface</u> an be configured to enable or disable DHCP servers.

#### **Security Considerations**

For enhanced security, it is recommended that operators require all clients to obtain their IP Addresses from a DHCP server. To enforce this requirement, all <u>Alcatel WLANs</u> can be configured with a 'DHCP Required' setting and a valid DHCP Server IP Address, which disallows client static IP Addresses. If a client associating with a WLAN with 'DHCP Required' set does not obtain its IP Address from the designated DHCP Server, it is not allowed access to any network services.

Note that if 'DHCP Required' is selected, clients must obtain an IP address via DHCP. Any client with a static IP address will not be allowed on the network. The Alcatel OmniAccess Switch or Appliance monitors DHCP traffic since it acts as a DHCP proxy for the clients.

If slightly less security is tolerable, operators can create <u>Alcatel WLANs</u> with 'DHCP Required' disabled and a valid DHCP Server IP Address. Clients then have the option of using a static IP Address or obtaining an IP Address from the designated DHCP Server.

Operators are also allowed to create separate <u>Alcatel WLANs</u> with 'DHCP Required' disabled and a DHCP Server IP Address of 0.0.0.0. These WLANs drop all DHCP requests and force clients to use a static IP Address. Note that these WLANs do not support <u>Management over Wireless</u>.

## **About Alcatel Mobility Groups**

Alcatel OmniAccess Wireless System operators can define Mobility Groups to allow client roaming across groups of Alcatel OmniAccess Wireless Switches and Appliances. Because the Alcatel OmniAccess Switches and Appliances in <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u> can detect each other across the network and over the air, it is important that each enterprise, institution, and wireless internet service provider isolate their Alcatel OmniAccess Switches and Appliances. The Alcatel Wireless Operating System makes it easy for operators to create this isolation by allowing them to assign a Mobility Group Name to their Alcatel OmniAccess Switches and Appliances. This assignment can be made using the <u>Alcatel Web Browser Interface</u>, the <u>OmniVista Air Control System Software</u>, or the <u>Command Line Interface</u>.

Note that all the Alcatel OmniAccess Switches and Appliances in a Mobility Group must use the same LWAPP <u>Layer 2 and Layer 3 Operation</u>, or you will defeat the Mobility software algorithm.

The following figure shows the results of creating Mobility Group Names for two groups of Alcatel Omni-Access Switches and Appliances. The Alcatel OmniAccess Switches and Appliances in the ABC Mobility Group recognize and communicate with each other through their <u>Alcatel OmniAccess Wireless Access Points</u> and <u>Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)</u> and through their shared subnets, but the ABC Mobility Group tags the XYZ OmniAccess APs and OmniAccess 1200R APs as <u>Rogue Access Points</u>. Likewise, the Alcatel OmniAccess Switches and Appliances in the XYZ Mobility Group do not recognize or communicate with the Alcatel OmniAccess Switches and Appliances in the ABC Mobility Group. This feature ensures Mobility Group isolation across the network.

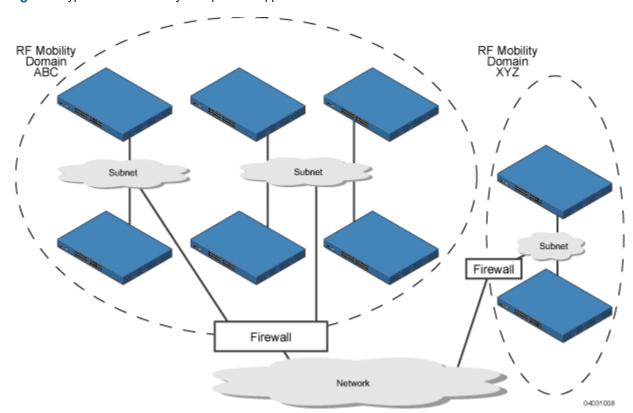


Figure - Typical Alcatel Mobility Group Name Application

Note: Alcatel recommends that you assign one set of VLANs for WLANs and a different set of VLANs for mobility groups to ensure that Alcatel OmniAccess Switches and Appliances properly route VLAN traffic.

The Alcatel Mobility Group feature can also be used to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different Mobility Group names to different Alcatel OmniAccess Switches and Appliances within the same wireless network.

If enabled, OmniVista AirView Software operation is constrained within each Alcatel Mobility Group.

Note: Because the Alcatel OmniAccess Switches and Appliances talk to each other when they are in the same mobility group, Alcatel recommends that operators do not add physically-separated Alcatel OmniAccess Switches and Appliances to the same static mobility group to avoid unnecessary traffic on the network.

## **About Alcatel Wired Connections**

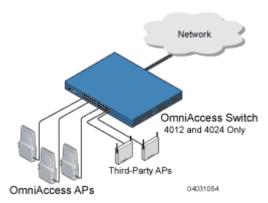
The Alcatel OmniAccess Wireless System components communicate with each other using industry-standard Ethernet cables and connectors. The following sections contain details of the Alcatel wired connections.

#### **Between Alcatel OmniAccess Wireless Switches and APs**

When operated in <u>Direct-Connect Mode</u>, the 4012 and 4024 <u>Alcatel OmniAccess Switches and Appliances</u> uses standard 802.3 CAT-5 (Category 5) or higher twisted-pair Ethernet cables to connect to <u>Alcatel OmniAccess Wireless Access Points</u>, <u>Alcatel OmniAccess Remote Edge Access Points (Omni-Access 1200R APs)</u>, and <u>Third-Party Access Points</u>. The CAT-5 cable is rated to carry 100 Mbps (recommended for 802.11a, 802.11a/b, 802.11a/g or 802.11a/b/g installations) or 10 Mbps (only recommended for low-bandwidth applications and 802.11b-only installations).

The 4012 and 4024 Alcatel OmniAccess Wireless Switches connect to the network using one or more copper 10/100Base-T cables and/or copper or fiber-optic GigE cables.

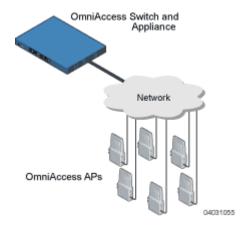
Note that the 4102 OmniAccess Wireless Appliances operate only in <u>Appliance Mode</u>, and do not connect directly to any Access Points.



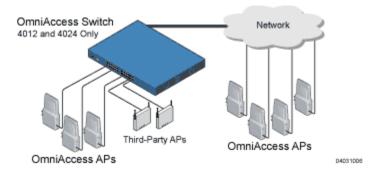
When the Alcatel OmniAccess Wireless Switch or Appliance is operated in <u>Appliance Mode</u>, the OmniAccess APs communicate with the Alcatel OmniAccess Switch or Appliance through the network. The 4012 and 4024 Alcatel OmniAccess Wireless Switches connect to the network using one or more copper 10/100Base-T cables and/or copper or fiber-optic GigE cables.

The 4102 OmniAccess Wireless Appliance connects to the network using two fiber-optic GigE cables: two redundant GigE connections to bypass single network failures. At any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

Note that the 4102 OmniAccess Wireless Appliances only operate in <u>Appliance Mode</u>, and do not connect directly to any Access Points.



When the 4012 and 4024 Alcatel OmniAccess Wireless Switches are operated in <u>Hybrid Mode</u>, some OmniAccess APs and third-party APs use the CAT-5 cable to connect to the OmniAccess Wireless Switch in <u>Direct-Connect Mode</u> and some connect in <u>Appliance Mode</u>. The OmniAccess Wireless Switch connects to the network using one or more copper 10/100Base-T cables and/or copper or fiber-optic GigE cables.



Standard CAT-5 cable supports a 100 m (328 ft.) run between the OmniAccess APs and the OmniAccess Wireless Switch. This allows a single OmniAccess Wireless Switch to serve OmniAccess APs in multiple buildings and/or floors in a single building.

The standard CAT-5 cable can also be used to conduct power for the OmniAccess APs from a network device equipped with <u>Power Over Ethernet</u> (PoE) capability. This power distribution plan can be used to reduce the cost of individual AP power supplies and related cabling.

#### Between Alcatel OmniAccess Switches and Appliances and Other Network Devices

The 4012 and 4024 Alcatel OmniAccess Wireless Switches communicate with other Alcatel OmniAccess Wireless Switches and Appliances or network devices through one or more standard CAT-5 cables connected to any front-panel port, which supports up to 100 Mbps, and/or through standard rear-panel Gigabit Ethernet (or GigE) cables, which supports up to 1 Gbps (1,000 Mbps).

The 4102 OmniAccess Wireless Appliance connects to the network using two front-panel fiber-optic GigE cables: two redundant GigE connections to bypass single network failures. At any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

#### **About Alcatel WLANs**

The Alcatel OmniAccess Wireless System can control up to 16 Wireless LANs for <u>Alcatel OmniAccess Wireless Access Points</u> and/or <u>Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)</u>, plus one WLAN for <u>Third-Party Access Points</u>. Each WLAN has a separate WLAN ID (1 through 17), a separate WLAN SSID (WLAN Name), and can be assigned unique security policies. A separate WLAN 17 can be created for <u>Third-Party Access Points</u> connected to a Model 4012 or 4024 OmniAccess Wireless Switch front panel in <u>Direct-Connect Mode</u>.

The OmniAccess APs and OmniAccess 1200R APs broadcast all active Alcatel WLAN SSIDs and enforce the policies defined for each WLAN, while only the operator-managed third-party APs broadcast the third-party AP SSID and enforce the operator-defined policies as described in *Third-Party Access Points*.

Note that many enterprises use different WLANs to separate traffic for different sections or departments.



**Note:** Alcatel recommends that you assign one set of VLANs for WLANs and a different set of VLANs for mobility groups to ensure that Alcatel OmniAccess Switches and Appliances properly route VLAN traffic.

If <u>Management over Wireless</u> is enabled across an Alcatel OmniAccess Wireless System, the Alcatel OmniAccess Wireless System operator can manage the System across the enabled WLAN using CLI and Telnet (<u>Command Line Interface</u>), http/https (<u>Alcatel Web Browser Interface</u>), and SNMP (<u>OmniVista Air Control System Software</u>).

To configure the Alcatel WLANs, refer to Configuring WLANs.

#### **About Access Control Lists**

The Alcatel Wireless Operating System allows you to define up to 64 Access Control Lists (ACLs), similar to standard firewall Access Control Lists. Each ACL can have up to 64 Rules (filters).

Operators can use ACLs to control client access to multiple VPN servers within a given WLAN. If all the clients on a WLAN must access a single VPN server, use the IPSec/VPN Gateway Passthrough setting in <a href="IPSec Passthrough">IPSec Passthrough</a>, <a href="WLANS">WLANS</a> > <a href="Edit">Edit</a> or <a href="Configure <a href="Configure <a href="IPAddress">Configure <a href="IPAddress">IPAddress</a> > <a href="WLAN Template">WLAN Template</a> > <a href="Add From Template">Add From Template</a> section.

After they are defined, the ACLs can be applied to the <u>Management Interface</u>, the <u>AP-Manager Interface</u>, or any of the <u>Operator-Defined Interfaces</u>.

Refer to <u>Access Control Lists > New</u> in the <u>Alcatel OmniAccess Wireless System Web Browser Online Help</u> or <u>Creating Access Control Lists</u> in the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> sections for instructions on how to configure the Access Control Lists.

## **About Identity Networking**

The Alcatel OmniAccess Wireless Switch and Appliance can have the following parameters applied to all clients associating with a particular WLAN: QoS, global or Interface-specific DHCP server, Layer 2 and Layer 3 Security Policies, and default Interface (which includes physical port, VLAN and ACL assignments).

However, the Alcatel OmniAccess Switch or Appliance can also have individual clients (MAC addresses) override the preset WLAN parameters by using MAC Filtering or by Allowing AAA Override parameters. This configuration can be used, for example, to have all company clients log into the corporate WLAN, and then have clients connect using different QoS, DHCP server, Layer 2 and Layer 3 Security Policies, and Interface (which includes physical port, VLAN and ACL assignments) settings on a per-MAC Address basis.

When Alcatel OmniAccess Wireless System operators configure MAC Filtering for a client, they can assign a different VLAN to the MAC Address, which can be used to have AWOS automatically reroute the client to the <u>Management Interface</u> or any of the <u>Operator-Defined Interfaces</u>, each of which have

their own VLAN, ACL, DHCP server, and physical port assignments. This MAC Filtering can be used as a coarse version of AAA Override, and normally takes precedence over any AAA (RADIUS or other) Override.

However, when <u>Allow AAA Override</u> is enabled, the RADIUS (or other AAA) server can alternatively be configured to return QoS and ACL on a per-MAC Address basis. <u>Allow AAA Override</u> gives the AAA Override precedence over the MAC Filtering parameters set in the Alcatel OmniAccess Switch or Appliance; if there are no AAA Overrides available for a given MAC Address, the AWOS uses the MAC Filtering parameters already in the Alcatel OmniAccess Switch or Appliance. This AAA (RADIUS or other) Override can be used as a finer version of AAA Override, but only takes precedence over MAC Filtering when <u>Allow AAA Override</u> is enabled.

Note that in all cases, the Override parameters (Operator-Defined Interface and QoS, for example) must already be defined in the Alcatel OmniAccess Switch or Appliance configuration.

In all cases, the AWOS will use QoS and ACL provided by the AAA server or MAC Filtering regardless of the Layer 2 and/or Layer 3 authentication used.

Also note that the AWOS will only move clients from the default Alcatel WLAN VLAN to a different VLAN when configured for MAC filtering, 802.1X, and/or WPA Layer 2 authentication.

To configure the Alcatel WLANs, refer to Configuring WLANs.

## **About Port Mirroring**

For troubleshooting, the Alcatel OmniAccess Wireless System operator can Mirror a transmit and receive data stream through a 4012 or 4024 OmniAccess Wireless Switch client, OmniAccess AP, and/or third-party AP data stream to another physical port on a 4012 or 4024 OmniAccess Wireless Switch.

Step 1. Set up a Mirror Port on the OmniAccess Wireless Switch.

- In the Command Line Interface (CLI), use the <u>config mirror port</u> command and enable Mirror Mode for the physical front-panel port.
- In the Web Browser Interface, navigate to the <u>Port > Configure</u> page and enable Mirror Mode for the physical front-panel port.
- In the ACS interface, navigate to the <u>Monitor Switches > <IPaddress> > Ports > n</u> page and enable Mirror Mode for the physical front-panel port.

All data to and from mirrored clients, OmniAccess APs, and/or Third-Party APs will now appear on this port.

**Step 2.** Once you have set up a front-panel Mirror Port, configure one or more clients, OmniAccess APs, and/or Third-Party APs to mirror data to the selected Mirror Port.

- Mirror a client by enabling Mirror Mode:
  - In the Command Line Interface (CLI), use the <u>config mirror mac</u> command and enable Mirror Mode for the client.
  - In the Web Browser Interface, navigate to the <u>Clients > Detail</u> page and enable Mirror Mode for the client.
  - In the ACS interface, navigate to the <u>Configure Access Point > OmniAccess AP > <name > and enable Mirror Mode for the client.</u>
- Mirror an OmniAccess AP by enabling Mirror Mode:
  - In the CLI, navigate to the <u>config mirror ap</u> command and enable Mirror Mode for the OmniAccess AP.
  - In the Web Browser Interface, use the <u>OmniAccess APs > Details</u> page and enable Mirror Mode for the OmniAccess AP.

- In the ACS interface, navigate to the <u>Configure <IPaddress> > OmniAccess AP</u> and enable Mirror Mode for the OmniAccess AP.
- Mirror any Third-Party AP (up to 100 simultaneous clients) by enabling Mirror Mode:
  - In the CLI, use the <u>config mirror foreignap</u> command and enable Mirror Mode for the Third-Party AP port on the OmniAccess Wireless Switch.
  - In the Web Browser Interface, navigate to the <u>Third-Party APs > Edit</u> page and enable Mirror Mode for the Third-Party AP port on the OmniAccess Wireless Switch.
  - In the ACS interface, navigate to the <u>Configure <IPaddress> > Connected Third Party AP</u> and enable Mirror Mode for the Third-Party AP port on the OmniAccess Wireless Switch.
- Note: If the Third-Party AP has more than 100 simultaneous clients, you will have to enable Mirror Mode individually for the remaining clients.

#### **About File Transfers**

The Alcatel OmniAccess Wireless System operator can upload and download Alcatel Wireless Operating System code, configuration, and certificate files to and from an Alcatel OmniAccess Wireless Switch or Appliance using CLI commands, Alcatel Web Browser Interface commands, or OmniVista Air Control System Software (ACS Software) commands.

- To use CLI commands, refer to <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u>.
- To use the Web Browser Interface, go to <u>Using the Alcatel Web Browser Interface</u>.
- To use ACS Software Server commands, continue with <u>Using the OmniVista Air Control System</u> Software.

#### **About Power Over Ethernet**

Alcatel OmniAccess Wireless Switches and OmniAccess APs support 802.3af-compatible Power over Ethernet (PoE), which can reduce the cost of discrete power supplies, additional wiring, conduits, outlets, and installer time. PoE also frees installers from having to mount <u>Alcatel OmniAccess Wireless Access Points</u>, <u>Alcatel OmniAccess Remote Edge Access Points</u> (OmniAccess 1200R APs) or other powered equipment near AC outlets, providing greater flexibility in positioning OmniAccess APs and OmniAccess 1200R APs for maximum coverage.

When you are using PoE, the installer runs a single CAT-5 cable from each OmniAccess AP or OmniAccess AP 1200R to the PoE-equipped Alcatel OmniAccess Switches or Appliances or other network elements, to a PoE power hub, or to a Alcatel Single-Line PoE Injector, described in *OmniAccess AP Models*. When the PoE equipment determines that the OmniAccess AP or OmniAccess AP 1200R is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the OmniAccess AP or OmniAccess AP 1200R.

The PoE cable length is limited by the 100Base-T or 10Base-T specification to 100 m or 200 m, respectively.

- Note: OmniAccess APs and OmniAccess 1200R APs can receive power from the OmniAccess Wireless Switch or any other network device conforming to the IEEE 802.3af standard.
- Note: Each OmniAccess AP and OmniAccess AP 1200R can alternatively receive power from an OmniAccess AP External Power Supply.

The OmniAccess Wireless Switch can be ordered with or without PoE, as required. It can be ordered with internal PoE, an external third-party PoE hub, or an Alcatel Single-Line PoE Injector. Contact Alcatel for recommended external PoE equipment.

# **About Alcatel OmniAccess Switches and Appliances**

The Alcatel OmniAccess Wireless Switch and Appliance are enterprise-class high-performance wireless switching platforms that support 802.11a and 802.11b/802.11g protocols. They operate under control of the Alcatel Wireless Operating System, and include the OmniAccess Wireless Switched Architecture, which results in an Alcatel OmniAccess Wireless System that can automatically adjust to real-time changes in the 802.11 RF environment. The Alcatel OmniAccess Switches and Appliances are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security. Also see:

- 4012 and 4024 OmniAccess Wireless Switch Models
- 4102 OmniAccess Wireless Appliance Model
- Alcatel OmniAccess Switch and Appliance Features
- Alcatel OmniAccess Switch and Appliance Model Numbers
- Direct-Connect Mode
- Appliance Mode
- Hybrid Mode
- Distribution System Ports
- Management Interface
- AP-Manager Interface
- Operator-Defined Interfaces
- Virtual Interface
- Service Port
- Service-Port Interface
- Startup Wizard
- Alcatel OmniAccess Switch and Appliance Memory
- Alcatel OmniAccess Switch and Appliance Failover Protection
- Network Connection to an Alcatel OmniAccess Switch or Appliance
- Enhanced Security Module
- Alcatel Wired Connections
- Alcatel OmniAccess Wireless Access Points
- Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)
- Alcatel WLANs
- Identity Networking
- Port Mirroring
- Configuring the Alcatel OmniAccess Switch or Appliance
- <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u>
- Updating the Alcatel Wireless Operating System Software
- <u>Clearing Configurations</u>
- Resetting the Alcatel OmniAccess Switch or Appliance

Alcatel OmniAccess Switch and Appliance Quick Installation Guide

#### 4012 and 4024 OmniAccess Wireless Switch Models

<u>About the Alcatel OmniAccess Wireless System</u> gives a comprehensive overview of the Alcatel OmniAccess Wireless System and the place of the Alcatel OmniAccess Wireless Switches and Appliances in that system. The following figure shows the 4024 OmniAccess Wireless Switch. The 4012 OmniAccess Wireless Switch is similar to the 4024, but has 12 front-panel RJ-45 jacks instead of 24.

Figure - 4024 OmniAccess Wireless Switch



The 4012 and 4024 Alcatel OmniAccess Wireless Switches are one-unit high 802.11 Wireless Switches that communicate directly (*Direct-Connect Mode*), indirectly (*Appliance Mode*), or both (*Hybrid Mode*) with up to 24 (Model 4024) or 12 (Model 4012) associated *Alcatel OmniAccess Wireless Access Points*, *Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)* and/or *Third-Party Access Points*. The 4012 and 4024 Alcatel OmniAccess Wireless Switches can be factory- or field-equipped with an Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks, and with one 1000Base-T (copper) or a single- or dual-1000Base-SX (fiber-optic) Network Adaptor Module to allow the OmniAccess Wireless Switch to communicate with the network at GigE (Gigabit Ethernet) speeds.

The two redundant GigE connections on the dual-1000Base-SX (fiber-optic) Network Adaptor Module allow the OmniAccess Wireless Switch to bypass single network failures. At any given time one of the dual-1000Base-SX (fiber-optic) Network Adaptor Module GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

# 4102 OmniAccess Wireless Appliance Model

The following figure shows the 4102 OmniAccess Wireless Appliance, which has two redundant front-panel SX/LC jacks.

Figure - 4102 OmniAccess Wireless Appliance



The 4102 OmniAccess Wireless Appliances are one-unit high 802.11 Wireless Appliances that communicate indirectly through the network (<u>Appliance Mode</u>) with up to 36 associated <u>Alcatel OmniAccess</u> <u>Wireless Access Points</u> and/or <u>Alcatel OmniAccess Remote Edge Access Points</u> (<u>OmniAccess 1200R APs</u>). The 4102 OmniAccess Wireless Appliances can be factory-ordered with an Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks, and with two (4102)

1000Base-SX network connectors to allow the OmniAccess Wireless Appliance to communicate with the network at GigE (Gigabit Ethernet) speeds.

The two redundant GigE connections on the 4102 allow the OmniAccess Wireless Appliance to bypass single network failures. At any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

## **Alcatel OmniAccess Switch and Appliance Features**

Because Alcatel OmniAccess Wireless Switches and Appliances perform most of the processes normally performed by SOHO Access Points, it can reduce the amount of inter-AP traffic on the wired backbone network when used in *Direct-Connect Mode*. When operated in *Appliance Mode*, Alcatel OmniAccess Switches and Appliances connect to the associated OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) through the network. When deployed in *Hybrid Mode*, Alcatel OmniAccess Wireless Switches simultaneously communicate with their associated APs through their front-panel ports as well as through the network.

Note that the 4102 OmniAccess Wireless Appliances are designed to operate exclusively in <u>Appliance Mode</u>. As such, they are limited to controlling <u>Alcatel OmniAccess Wireless Access Points</u> and <u>Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)</u>.

After each Alcatel OmniAccess Switch or Appliance is installed and configured, the Alcatel Wireless Operating System *OmniVista AirView Software* is activated, and the Alcatel Wireless Operating System manages and controls associated OmniAccess APs, OmniAccess 1200R APs and/or third-party APs (*Direct-Connect Mode* only), with information about their relative positions, IP Addresses, and MAC addresses. This information allows all Alcatel OmniAccess Switches and Appliances within each *Alcatel Mobility Group* to constantly monitor and dynamically adjust the RF environment, maximizing performance, minimizing interference, and distributing the client load.

When operated in <u>Direct-Connect Mode</u>, the 4012 or 4024 Alcatel OmniAccess Wireless Switches communicate directly with OmniAccess APs, OmniAccess 1200R APs and third-party APs via 10/100Base-T Ethernet cables.

When operated in <u>Appliance Mode</u>, the 4012 and 4024 Alcatel OmniAccess Wireless Switches communicate with OmniAccess APs and OmniAccess 1200R APs via 10/100Base-T Ethernet or 1000Base-T or 1000Base-SX cables through the network. Note that the optional dual-1000Base-SX module uses two redundant GigE connections to bypass single network failures. At any given time one of the dual-1000Base-SX module GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

When operated in <u>Appliance Mode</u>, the 4102 OmniAccess Wireless Appliances communicate with Omni-Access APs and OmniAccess 1200R APs via 1000Base-SX cables through the network. Note that the 4102 OmniAccess Wireless Appliance uses two redundant GigE connections to bypass single network failures. At any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

The 4012 or 4024 Alcatel OmniAccess Wireless Switches communicate with network via one or more front-panel 10/100Base-T Ethernet ports and/or 1000Base-T or 1000Base-SX Network ports. The 4102 OmniAccess Wireless Appliances communicate with network via two (4102) 1000Base-SX Network Ports: the 4102 OmniAccess Wireless Appliance uses two redundant GigE connections to bypass single network failures.

Regardless of operating mode, the network operator can control the Alcatel OmniAccess Switches and Appliances with the following Alcatel Wireless Operating System device servicing interfaces:

 With optional <u>OmniVista Air Control System Software</u> (ACS Software Server) inband or out-of-band via a front-panel 10/100Base-T Service port (Service Interface), or via the network (Management Interface).

- With the built-in <u>Command Line Interface</u> via a serial RS232-C Console Port (direct connection), or via the network (Telnet connection).
- With the built-in <u>Alcatel Web Browser Interface</u> via a dedicated 10/100Base-T Service port (recommended), or via the network, using either http or https (http + SSL).

Refer to the following for more information about the Alcatel OmniAccess Switches and Appliances:

- 4012 and 4024 OmniAccess Wireless Switch Models
- 4102 OmniAccess Wireless Appliance Model
- Alcatel OmniAccess Switch and Appliance Model Numbers
- <u>Direct-Connect Mode</u>
- Appliance Mode
- Hybrid Mode
- Distribution System Ports
- Management Interface
- <u>AP-Manager Interface</u>
- <u>Operator-Defined Interfaces</u>
- <u>Virtual Interface</u>
- Service Port
- Service-Port Interface
- Startup Wizard
- Alcatel OmniAccess Switch and Appliance Memory
- <u>Alcatel OmniAccess Switch and Appliance Failover Protection</u>
- Network Connection to an Alcatel OmniAccess Switch or Appliance
- <u>Enhanced Security Module</u>
- Alcatel Wired Connections
- <u>Alcatel OmniAccess Wireless Access Points</u>
- Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)
- Alcatel Wired Connections
- Alcatel WLANs
- <u>Port Mirroring</u>
- Configuring the Alcatel OmniAccess Switch or Appliance
- <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u>
- <u>Updating the Alcatel Wireless Operating System Software</u>
- <u>Clearing Configurations</u>
- Resetting the Alcatel OmniAccess Switch or Appliance
- Alcatel OmniAccess Switch and Appliance Quick Installation Guide

## **Alcatel OmniAccess Switch and Appliance Model Numbers**

The Alcatel OmniAccess Wireless Switch and Appliance models are as follows:

- OAW-4012 12-Port OmniAccess Wireless Switch with an optional 1000Base-T or 1000Base-SX/LC Network Adapter, used in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u>, and <u>Hybrid Mode</u>.
- OAW-4024 24-Port OmniAccess Wireless Switch with an optional 1000Base-T or 1000Base-SX/LC Network Adapter, used in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u>, and <u>Hybrid Mode</u>.
- OAW-4012-DWP Twelve-Port OmniAccess Wireless Switch with built-in PoE Hub and an optional 1000Base-T or 1000Base-SX/LC Network Adapter, used in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u>, and <u>Hybrid Mode</u>.
- OAW-4024-DWP 24-Port OmniAccess Wireless Switch with built-in PoE Hub and an optional 1000Base-T or 1000Base-SX/LC Network Adapter, used in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u>, and <u>Hybrid Mode</u>.
- (UNUSED COMPONENT) 36-Port OmniAccess Wireless Appliance with one 1000Base-SX/LC Network Adapter, used only in *Appliance Mode*.
- OAW-4102 36-Port OmniAccess Wireless Appliance with one 1000Base-SX/LC Network Adapter, used only in <u>Appliance Mode</u>. The 4102 OmniAccess Wireless Appliance uses two redundant GigE connections to bypass single network failures. That is, at any given time one of the 4102 OmniAccess Wireless Appliance GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

Note that all Alcatel OmniAccess Switch and Appliance models come from the factory with 19-inch EIA equipment rack flush-mount ears and tabletop mounting feet.

The following upgrade modules are also available:

- OAW-ESM Enhanced Security Module: Supports VPN, IPSec and other processor-intensive security options. This is a factory-orderable and field-installable option for all Alcatel OmniAccess Switches and Appliances.
- OAW-GT 1000Base-T Network Adapter Module: Supports 1000Base-T connections to the network. This is a factory-orderable and field-installable option for 4012 and 4024 Alcatel OmniAccess Wireless Switches.
- OAW-GSX Single-1000Base-SX Network Adapter Module: Supports 1000Base-SX connections to the network. This is a factory-orderable and field-installable option for 4012 and 4024 Alcatel OmniAccess Wireless Switches.
- OAW-GSX2 Dual-1000Base-SX Network Adapter Module: Supports two 1000Base-SX connections to the network. This is a factory-orderable and field-installable option for 4012 and 4024 Alcatel OmniAccess Wireless Switches. The dual-1000Base-SX module uses two redundant GigE connections to bypass single network failures. At any given time one of the dual-1000Base-SX module GigE connections is active and the other is passive. Upon a network failure, the active connection becomes passive, and the passive connection becomes active.

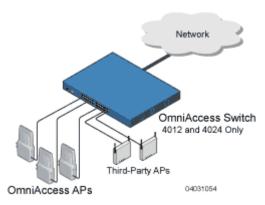
#### **OmniAccess Wireless Switch Direct-Connect Mode**

The 4012 and 4024 Alcatel OmniAccess Wireless Switches can be operated in Direct-Connect Mode, in *Appliance Mode*, or in *Hybrid Mode*, either in ISO Data Link Layer 2 or Network Layer 3 (*Layer 2 and Layer 3 Operation*). In Direct-Connect Mode, the Alcatel OmniAccess Wireless Switches are directly connected to up to 24 (Model 4024) or up to 12 (Model 4012) OmniAccess APs and/or third-party APs

over CAT-5 or higher Ethernet cabling. The benefit of this mode is that the Alcatel OmniAccess Wireless Switches can provide *Power Over Ethernet*.

The following figure shows an OmniAccess Wireless Switch in the Direct-Connect Mode, and the rest of the section describes the 4012 and 4024 OmniAccess Wireless Switch connections to the network.

Figure - OmniAccess Wireless Switch Direct-Connect Mode



The OmniAccess Wireless Switch filters packets and forwards them between LAN segments. When the OmniAccess Wireless Switch is operated in Direct-Connect Mode, it transmits data between all connected OmniAccess APs and third-party APs, which results in fewer packets being placed on the backbone network.

The 4012 and 4024 Alcatel OmniAccess Wireless Switches communicate with the backbone network via a 1000Base-T or 1000Base-SX Network Port, or via any front-panel 10/100Base-T Ethernet port as described in the <u>Network Connection to an Alcatel OmniAccess Switch or Appliance</u> section.

The Alcatel OmniAccess Wireless Switch or Appliance uses industry-standard SNMP protocol to communicate with the <u>OmniVista Air Control System Software</u>, and communicates with Alcatel Wireless Operating System device servicing interfaces as follows:

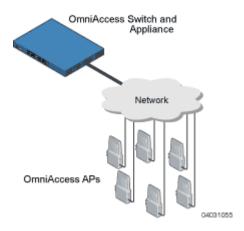
- With an optional ACS Software Server or other Alcatel Wireless Operating System Service Interface, either directly connected or through an out-of-band Alcatel Wireless Operating System Service Network, or via a dedicated 10/100Base-T <u>Service Port</u>.
- With an optional VT-100 CLI console via a serial RS232-C Console Port.
- Note: Alcatel recommends that you not use the network for your Alcatel Wireless Operating System device service, because a service outage on your network means that you have no dedicated path to the OmniAccess Wireless Switch.

The OmniAccess Wireless Switch can be equipped with built-in <u>Power Over Ethernet</u> circuitry, an external PoE hub, or an Alcatel Single Inline Power over Ethernet Injector which allows associated OmniAccess APs, Alcatel OmniAccess Remote Edge Access Points, and/or third-party APs to receive power over the CAT-5 Ethernet cabling.

## Alcatel OmniAccess Switches and Appliances in Appliance Mode

All 4012 and 4024 Alcatel OmniAccess Wireless Switches and 4102 OmniAccess Wireless Appliances can be operated in Appliance Mode. (The 4012 and 4024 Alcatel OmniAccess Wireless Switches can also be operated in *Direct-Connect Mode* or *Hybrid Mode*.) In Appliance Mode, the Alcatel OmniAccess Switch or Appliance communicates indirectly with up to 36 (Model 4102), up to 24 (Model 4024) or up to 12 (Model 4012) associated OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points through the network. The following figure shows an Alcatel OmniAccess Switch or Appliance in Appliance Mode.

Figure - Alcatel OmniAccess Wireless Switch or Appliance Deployed in Appliance Mode

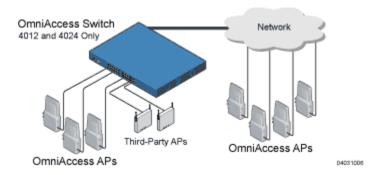


The Alcatel OmniAccess Switch or Appliance communicates with the network using one of the interfaces described in the *Network Connection to an Alcatel OmniAccess Switch or Appliance* section.

# **OmniAccess Wireless Switch Hybrid Mode**

The 4012 and 4024 Alcatel OmniAccess Wireless Switches can be operated in Hybrid Mode, <u>Appliance Mode</u> or <u>Direct-Connect Mode</u>. In Hybrid Mode, the OmniAccess Wireless Switch communicates directly and indirectly with up to 24 (Model 4024) or up to 12 (Model 4012) associated OmniAccess APs, Alcatel OmniAccess Remote Edge Access Points, and/or third-party APs over Ethernet cabling, and with associated OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points through the network. The following figure shows an OmniAccess Wireless Switch in Hybrid Mode.

Figure - OmniAccess Wireless Switch Deployed in Hybrid Mode



The OmniAccess Wireless Switch communicates with the network using one of the interfaces described in the <u>Network Connection to an Alcatel OmniAccess Switch or Appliance</u> section.

## **About Distribution System Ports**

A Distribution System (DS) port is a physical port (see <u>Alcatel Wired Connections</u>) through which the Alcatel OmniAccess Switch or Appliance talks to the network and other Access Points. DS Ports are where packets are exchanged between the Alcatel OmniAccess Wireless System WLANs and the rest of the network. The DS Ports can also be used to communicate with OmniAccess APs in Appliance Mode or Hybrid Mode.

- The 4102 OmniAccess Wireless Appliance supports a single Distribution System port because it has two redundant 1000Base-SX physical ports that must connect to the same subnet.
- The OmniAccess Wireless Switch can have as many Distribution System ports as it has 10/100/1000Base-T/-SX physical ports, except when the Switch is equipped with a dual-port 1000Base-SX Network Adapter Module. When the Switch is equipped with a dual-port 1000Base-SX Network Adapter Module, the Network Adapter Module's two redundant physical ports must connect to the same subnet.
- **Note:** The Distribution System Port cannot be assigned to the dedicated Alcatel OmniAccess Switch or Appliance front-panel <u>Service Port</u>.

As described in <u>Layer 2 and Layer 3 Operation</u>, when the LWAPP communications are set to Layer 2 (same subnet) operation, the Distribution System must have one <u>Management Interface</u> to control all inter-Alcatel OmniAccess Switch and Appliance and all Alcatel OmniAccess Switch and Appliance-to-AP communications, regardless of the number of physical Distribution System ports.

Also as described in <u>Layer 2 and Layer 3 Operation</u>, when the LWAPP communications are set to Layer 3 (different subnet) operation, the Distribution System must have one <u>Management Interface</u> to control all inter-Alcatel OmniAccess Switch and Appliance communications, and must have one <u>AP-Manager Interface</u> to control all Alcatel OmniAccess Switch and Appliance-to-AP communications, regardless of the number of physical Distribution System ports.

Each physical Distribution System port can also have between one and 64 <u>Operator-Defined Interfaces</u> assigned to it. Each Operator-Defined Interface is individually configured, and allows VLAN communications to exist on the Distribution System port(s).

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

# **About the Management Interface**

The logical Management Interface controls Layer 2 communications between Alcatel OmniAccess Wireless Switches and Appliances, OmniAccess APs, Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs), and *Third-Party Access Points*.

The Management Interface is assigned to one physical port (<u>Alcatel Wired Connections</u>), through which it communicates with other network devices and other access points. However, the Management Interface can also communicate through all other physical ports except the front-panel <u>Service Port</u> as follows:

- Sends messages through the Layer 2 network to autodiscover and communicate with other Alcatel OmniAccess Switches and Appliances through all physical ports except the front-panel <u>Service Port</u>.
- Listens across the Layer 2 network for OmniAccess AP LWAPP polling messages to autodiscover, associate with, and communicate with as many OmniAccess APs as it can.
- Note: Should an OmniAccess Wireless Appliance or OmniAccess Wireless Switch in Appliance Mode fail, its dropped OmniAccess APs poll the network for another Alcatel OmniAccess Switch or Appliance. When an online Alcatel OmniAccess Switch or Appliance has any remaining AP ports, the Management Interface listens to the network for OmniAccess AP polling messages to autodiscover, associate with, and communicate with as many OmniAccess APs as it can. Refer to the Alcatel OmniAccess Switch and Appliance Failover Protection section for more information.
- Note: The Management Interface cannot be assigned to the dedicated Alcatel OmniAccess Switch or Appliance front-panel <u>Service Port</u>.

The Management Interface uses the burned-in Alcatel OmniAccess Switch or Appliance Distribution System MAC address, and must be configured for the following:

- VLAN assignment.
- Fixed IP Address, IP netmask, and default gateway.
- Physical port assignment.
- Primary and Secondary DHCP Servers.
- Access Control List, if required.

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

## **About the AP-Manager Interface**

The logical AP-Manager Interface controls Layer 3 communications between Alcatel OmniAccess Wireless Switches and Appliances, OmniAccess APs, and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs).

Note: The AP-Manager Interface does not control communications with <u>Third-Party Access Points</u>, because the third-party APs must be connected directly to the 4012 or 4024 Omni-Access Wireless Switch front-panel ports (Layer 2 operation).

The AP-Manager Interface is assigned to one physical port (<u>Alcatel Wired Connections</u>), and can be on the same subnet and physical port as the <u>Management Interface</u>. The AP-Manager Interface can communicate through any physical port except the front-panel <u>Service Port</u> as follows:

- Sends Layer 3 messages through the network to autodiscover and communicate with other Alcatel OmniAccess Switches and Appliances.
- Listens across the network for Layer 3 OmniAccess AP and OmniAccess AP 1200R LWAPP polling messages to autodiscover, associate with, and communicate with as many OmniAccess APs and OmniAccess 1200R APs as it can.
- Note: Should an OmniAccess Wireless Appliance or OmniAccess Wireless Switch in Appliance Mode fail, its dropped OmniAccess APs and OmniAccess 1200R APs poll the network for another Alcatel OmniAccess Switch or Appliance. When an online Alcatel OmniAccess Switch or Appliance has any remaining AP ports, the AP-Manager Interface listens to the network for OmniAccess AP and OmniAccess AP 1200R polling messages to autodiscover, associate with, and communicate with as many OmniAccess APs and OmniAccess 1200R APs as it can. Refer to the Alcatel OmniAccess Switch and Appliance Failover Protection section for more information.
- Note: The AP-Manager Interface cannot be assigned to the dedicated Alcatel OmniAccess Switch or Appliance front-panel *Service Port*.

The AP-Manager Interface must be configured for the following:

- VLAN assignment.
- Fixed IP Address (must be different than the Management Interface IP address, but must be on the same subnet as the Management Interface), IP netmask, and default gateway.
- Physical port assignment.
- Primary and Secondary DHCP Servers.
- Access Control List, if required.

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

## **About Operator-Defined Interfaces**

Each Alcatel OmniAccess Switch and Appliance can support up to 64 Operator-Defined Interfaces. Each Operator-Defined Interface controls VLAN and other communications between Alcatel OmniAccess Wireless Switches and Appliances and all other network devices connected to an individual physical port. Between one and 64 Operator-Defined Interfaces can be assigned to <u>Alcatel WLANs</u>, physical <u>Distribution System Ports</u>, the Layer 2 <u>Management Interface</u>, and the Layer 3 <u>AP-Manager Interface</u>.



**Note:** Operator-Defined Interfaces cannot be assigned to the dedicated Alcatel OmniAccess Switch or Appliance front-panel *Service Port*.



**CAUTION:** Operator-Defined Interface names cannot have spaces in them. If an Operator-Defined Interface name contains a space, you may not be able to edit its configuration using the *Command Line Interface*.

Each Operator-Defined Interface must be configured for the following:

- VLAN number.
- Fixed IP Address, IP netmask, and default gateway.
- Physical port assignment.
- Primary and Secondary DHCP Servers.
- Access Control List, if required.

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

#### **About the Virtual Interface**

The Virtual Interface controls Layer 3 Security and Mobility manager communications for Alcatel Omni-Access Wireless Switches and Appliances. It maintains the DNS Gateway hostname used by Layer 3 Security and Mobility managers to verify the source of certificates when Layer 3 Web Auth is enabled.

The Virtual Interface must be configured for the following:

- Any fictitious, unassigned, unused Gateway IP Address.
- DNS Gateway Host Name.

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

#### **About the Service Port**

The physical Service port on the Alcatel OmniAccess Wireless Switch or Appliance front panel is a 10/100Base-T Ethernet port dedicated to Alcatel Wireless Operating System device service, and was formerly known as the Management port. The Service Port is controlled by the <u>Service-Port Interface</u>.

The Service Port is configured with an IP Address, subnet mask, and IP assignment protocol different from the <u>Management Interface</u>. This allows the operator to manage the Alcatel OmniAccess Switch or Appliance directly or through a dedicated Alcatel Wireless Operating System service network, such as 10.1.2.x, which can ensure Alcatel Wireless Operating System device service access during network downtime.

Alcatel created the Service port to remove the Alcatel OmniAccess Wireless System device service from the network data stream to improve security and to provide a faster service connection.

Note that you cannot assign a Gateway to the Service port, so the port is not routable, unlike the other front-panel 10/100Base-T ports. However, you can set up dedicated routes to network management devices.

Also note that the Service Port is not auto-sensing, unlike the other front-panel 10/100Base-T ports: you must use the correct straight-through or crossover Ethernet cable to communicate with the Service Port.

Refer to the <u>Configuring Other Ports and Parameters</u> for information on how to configure the Service Port.

#### **About the Service-Port Interface**

The Service-Port Interface controls communications through the dedicated Alcatel OmniAccess Switch or Appliance front-panel *Service Port*.

**Note:** The Service-Port Interface can only be assigned to the dedicated Alcatel OmniAccess Switch or Appliance front-panel <u>Service Port</u>.

The Service-Port Interface uses the burned-in Alcatel OmniAccess Switch or Appliance Service Port MAC address, and must be configured for the following:

- Whether or not DHCP Protocol is activated.
- IP Address and IP netmask.

Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> section for configuration instructions.

## **About the Startup Wizard**

When an Alcatel OmniAccess Wireless Switch or Appliance is powered up with a new factory Alcatel Wireless Operating System software load or after being reset to factory defaults, the bootup script runs the Startup Wizard, which prompts the installer for initial configuration. The Startup Wizard:

- Ensures that the Alcatel OmniAccess Switch or Appliance has a System Name, up to 32 characters.
- Adds an Administrative User Name and Password, each up to 24 characters.
- Ensures that the Alcatel OmniAccess Switch or Appliance can communicate with the CLI, ACS Software, or Web Browser Alcatel Wireless Operating System device service interfaces (either directly or indirectly) through the <u>Service Port</u> by accepting a valid IP configuration protocol (none or DHCP), and if 'none', IP Address and netmask. If you do not want to use the Service port, enter 0.0.0.0 for the IP Address and netmask; this disables the Service Port.
- Note: Alcatel recommends that you not use the network for your Alcatel Wireless Operating System management, because a service outage on your network means that you have no dedicated path to the OmniAccess Wireless Switch.
- Ensures that the Alcatel OmniAccess Switch or Appliance can communicate with the network (802.11 Distribution System) through the <u>Management Interface</u> by collecting a valid static IP Address, netmask, default router IP address, VLAN identifier, and physical port assignment.
- Prompts for the IP address of the DHCP server used to supply IP addresses to clients, the Alcatel OmniAccess Switch or Appliance Management Interface, and optionally to the Service Port Interface.
- Asks for the LWAPP Transport Mode, described in <u>Layer 2 and Layer 3 Operation</u>.
- Collects the Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Allows you to enter the <u>Alcatel Mobility Group</u> (RF Group) Name.
- Collects the WLAN 1 802.11 SSID, or Network Name.

- Asks you to define whether or not clients can use static IP addresses. Yes = more convenient, but lower security (session can be hijacked), clients can supply their own IP Address, better for devices that cannot use DHCP. No = less convenient, higher security, clients must DHCP for an IP Address, works well for Windows XP devices.
- If you want to configure a RADIUS server from the Startup Wizard, the RADIUS server IP address, communication port, and Secret.
- Collects the Country Code. (Refer to <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> and <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u>.
- Enables and/or disables the 802.11a, 802.11b and 802.11g OmniAccess AP networks.
- Enables or disables <u>OmniVista AirView Software</u>.

To use the Startup Wizard, refer to *Using the Startup Wizard*.

## **About Alcatel OmniAccess Switch and Appliance Memory**

The Alcatel OmniAccess Wireless Switches and Appliances contain two kinds of memory: volatile RAM, which holds the current, active Alcatel OmniAccess Switch or Appliance configuration, and NVRAM (non-volatile RAM), which holds the reboot configuration. When you are configuring the Alcatel Wireless Operating System in an Alcatel OmniAccess Switch or Appliance, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the Alcatel OmniAccess Switch or Appliance reboots in the current configuration.

Knowing which memory you are modifying is important when you are:

- Using the <u>Startup Wizard</u>
- Clearing Configurations
- Saving Configurations
- Resetting the Alcatel OmniAccess Switch or Appliance
- Logging Out of the CLI

## **Alcatel OmniAccess Switch and Appliance Failover Protection**

Each Alcatel OmniAccess Wireless Switch and Appliance with front-panel 10/100Base-T ports can normally associate with as many OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) as it has physical ports. Thus, a 12-port 4012 OmniAccess Wireless Switch can associate with 12 OmniAccess APs and OmniAccess 1200R APs, and a 24-port 4024 OmniAccess Wireless Switch can associate with 24 OmniAccess APs and OmniAccess 1200R APs.

However, when an Alcatel OmniAccess Switch or Appliance in Appliance Mode fails, each 4012 and 4024 OmniAccess Wireless Switch can associate with twice as many OmniAccess APs and OmniAccess 1200R APs as it has physical ports. Thus, a 12-port 4012 OmniAccess Wireless Switch can associate with 24 OmniAccess APs and OmniAccess 1200R APs, and a 24-port 4024 OmniAccess Wireless Switch can associate with 48 OmniAccess APs and OmniAccess 1200R APs.



**CAUTION:** This excess OmniAccess AP and OmniAccess AP 1200R load will cause your Alcatel OmniAccess Switches and Appliances to slow down, generate log messages, and provide lower data throughput for the associated clients.

Model 4102 OmniAccess Wireless Appliances can associate with up to 36 OmniAccess APs and Omni-Access 1200R APs in Appliance Mode, and have no front-panel 10/100Base-T ports. Note that the 4102 OmniAccess Wireless Appliances can only associate with 36 (not 72) OmniAccess APs and OmniAccess 1200R APs.

**Note:** During installation, Alcatel recommends that you connect all OmniAccess APs and OmniAccess 1200R APs to a configured Alcatel OmniAccess Switch or Appliance, and configure each OmniAccess AP and OmniAccess AP 1200R for final operation. This step configures each OmniAccess AP and OmniAccess AP 1200R for *Primary Alcatel OmniAccess Switch or Appliance*, and allows it to store the configured *Alcatel Mobility Group* information.

During failover recovery, the configured OmniAccess APs and OmniAccess 1200R APs will obtain an IP address from the local DHCP server (only in Layer 3 Operation), attempt to contact their Primary Alcatel OmniAccess Switch or Appliance, and then attempt to contact the IP addresses of the other Alcatel OmniAccess Switches and Appliances in the Mobility group. This will prevent the OmniAccess APs and OmniAccess 1200R APs from spending time sending out blind polling messages, resulting in a faster recovery period.

In a multiple-Alcatel OmniAccess Switch and Appliance system (refer to <u>Multiple-Alcatel OmniAccess Switch and Appliance Deployments</u>), this means that if one Alcatel OmniAccess Switch or Appliance fails, its dropped OmniAccess APs and OmniAccess 1200R APs reboot and do the following under direction of the <u>OmniVista AirView Software</u>:

- Obtain an IP address from a local DHCP server (one on the local subnet).
- If the OmniAccess AP or OmniAccess AP 1200R has a <u>Primary Alcatel OmniAccess Switch or Appliance</u> assigned, it attempts to associate with that Alcatel OmniAccess Switch or Appliance.
- If the OmniAccess AP or OmniAccess AP 1200R has no Primary Alcatel OmniAccess Switch or Appliance assigned or if its Primary Alcatel OmniAccess Switch or Appliance is unavailable, it attempts to associate with a <u>Master Alcatel OmniAccess Switch or Appliance</u> on the same subnet.
- If the OmniAccess AP or OmniAccess AP 1200R finds no Master Alcatel OmniAccess Switch or Appliance on the same subnet, it attempts to contact stored Mobility Group members by IP address.
- Should none of the Mobility Group members be available, and if the OmniAccess AP or OmniAccess AP 1200R has no Primary Alcatel OmniAccess Switch or Appliance assigned and there is no Master Alcatel OmniAccess Switch or Appliance active, it attempts to associate with the least-loaded Alcatel OmniAccess Switch or Appliance on the same subnet to respond to its discovery messages with unused ports.

This means that when sufficient Alcatel OmniAccess Switches and Appliances are deployed in <u>Appliance Mode</u>, should one Alcatel OmniAccess Switch or Appliance fail, active OmniAccess AP client sessions are momentarily dropped while the dropped OmniAccess AP associates with an unused port on another Alcatel OmniAccess Switch or Appliance, allowing the client device to immediately reassociate and reauthenticate.

Because the OmniAccess APs and/or third-party APs plug into the front of the OmniAccess Wireless Switch when it is deployed in *Direct-Connect Mode*, Alcatel OmniAccess Switch and Appliance Failover Protection is not supported for OmniAccess APs or OmniAccess 1200R APs in Direct-Connect Mode.

## **Network Connection to the Alcatel OmniAccess Switch or Appliance**

The 4012 and 4024 OmniAccess Wireless Switch can be operated in <u>Hybrid Mode</u>, <u>Appliance Mode</u> or <u>Direct-Connect Mode</u>. The 4102 OmniAccess Wireless Appliance can be operated in <u>Appliance Mode</u>. Regardless of operating mode, the Alcatel OmniAccess Switches and Appliances use the network as an 802.11 Distribution System.

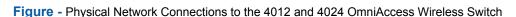
Regardless of the Ethernet port type or speed, each Alcatel OmniAccess Switch and Appliance monitors and communicates with its related Alcatel OmniAccess Switches and Appliances across the network.

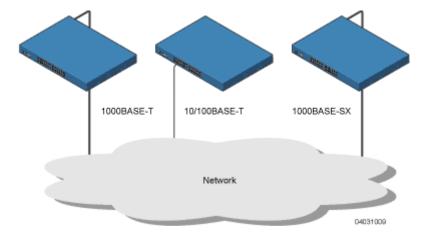
#### Model 4012 and 4024 Alcatel OmniAccess Wireless Switches

The 4012 and 4024 OmniAccess Wireless Switch can communicate with the network through one or more physical interfaces. The three physical interface types are:

- A GigE 1000Base-SX fiber-optic cable with an LC connector can plug into the optional Single-Port (OAW-GSX) Network Adapter Module, or two GigE 1000Base-SX fiber-optic cables with LC connectors can plug into the optional Dual-Port (OAW-GSX2) Network Adapter Module on the rear of the OmniAccess Wireless Switch.
- Alternatively, a GigE 1000Base-T copper cable can plug into the optional RJ-45 (OAW-GT)
   Network Adapter Module connector on the rear of the OmniAccess Wireless Switch.
- Alternatively, an Ethernet 10/100Base-T cable can plug into any of RJ-45 10/100Base-T connectors on the front of the OmniAccess Wireless Switch.
- Note: The 4012 and 4024 Alcatel OmniAccess Wireless Switches can have multiple physical connections to different subnets to allow the OmniAccess Wireless Switch to control OmniAccess APs on the different subnets. The <a href="Management Interface">Management Interface</a> that allows Alcatel OmniAccess Switches and Appliances to communicate with each other can only be assigned to one subnet.

This means that an Alcatel OmniAccess Wireless System with all Alcatel OmniAccess Switches and Appliances on the same subnet can be operated in Layer 2 mode, and that an Alcatel OmniAccess Wireless System with Alcatel OmniAccess Switches and Appliances on the different subnets must be operated in Layer 3 mode, and that the Alcatel OmniAccess Switches and Appliances on different subnets must communicate with each other through a router.





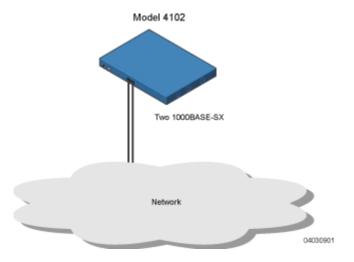
As described in <u>Layer 2 and Layer 3 Operation</u>, when the Alcatel OmniAccess Wireless System operates in Layer 2 mode, a <u>Management Interface</u> is automatically created and then assigned to one physical port, and an <u>AP-Manager Interface</u> Interface is not required. However, when the Alcatel OmniAccess Wireless System operates in Layer 3 mode, a Management Interface is created and then assigned to one physical port, and an AP-Manager Interface must be created to allow the Alcatel OmniAccess Switch or Appliance to support communications between Alcatel OmniAccess Switches and Appliances and OmniAccess APs; the AP-Manager Interface can be on the same subnet as the Management Interface, and can be assigned to the same physical port as the Management Interface.

#### Model 4102 OmniAccess Wireless Appliances

The 4102 OmniAccess Wireless Appliances can communicate with the network through two (4102) physical ports, and the logical <u>Management Interface</u> can be assigned to the two physical ports. The physical port description follows:

• Two GigE 1000Base-SX fiber-optic cables can plug into the LC connectors on the front of the 4102 OmniAccess Wireless Appliance, and they must be connected to the same subnet. Note that the two GigE ports are redundant--the first port that becomes active is the master, and the second port becomes the backup port. If the first connection fails, the standby connection becomes the master, and the failed connection becomes the backup port.

Figure - Physical Network Connections to the 4102 OmniAccess Wireless Appliance

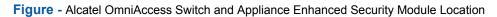


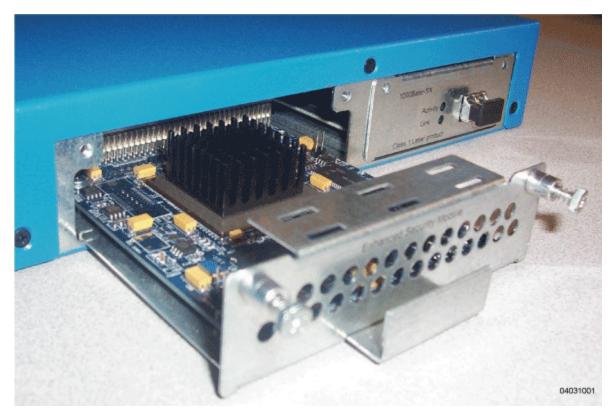
# **Enhanced Security Module**

All Alcatel OmniAccess Wireless Switches and Appliances can be equipped with an optional Enhanced Security Module (OAW-ESM), which slides into the rear panel of the Alcatel OmniAccess Switch or Appliance. The Enhanced Security Module adds significant hardware encryption acceleration to the Alcatel OmniAccess Wireless Switch or Appliance, which enables the following through the <u>Management Interface</u>:

- Sustain up to 1 Gbps throughput with Layer 2 and Layer 3 encryption enabled.
- Provide a built-in VPN server for mission-critical traffic.
- Support high-speed, processor-intensive encryption, such as IPSec and 3DES.

The following figure shows the Enhanced Security Module sliding into the rear of a 4012 or 4024 Omni-Access Wireless Switch. The Enhanced Security Module can also be installed into the rear panel of a 4102 Omni-Access Wireless Appliance, but the 1000Base-T card is not an option on the 4102 Omni-Access Wireless Appliance.





## **About Alcatel OmniAccess Wireless Access Points**

The OmniAccess AP is a part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System). When associated with an <u>Alcatel OmniAccess Switches and Appliances</u> as described below, the OmniAccess AP provides advanced 802.11a and/or 802.11b/g Access Point functions in a single aesthetically pleasing plenum-rated enclosure. The following figure shows the two types of Alcatel OmniAccess Wireless Access Point: without and with connectors for external antennas.

Note that Alcatel also offers an 802.11a/b/g Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs), which are OmniAccess APs designed for remote deployment, OmniVista AirView Software control via a WAN link, and which includes connectors for external antennas.

Figure - Alcatel OmniAccess Wireless Access Points

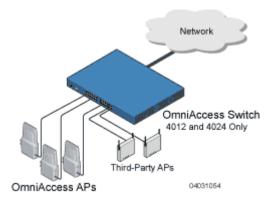


A. External-Antenna Model B. Internal-Antenna Model

Note that the OmniAccess AP is manufactured in a neutral color so it blends into most environments (but can be painted), contains pairs of high-gain internal antennas for unidirectional (180-degree) or omnidirectional (360-degree) coverage (*OmniAccess AP External and Internal Antennas*), and is plenum-rated for installations in hanging ceiling spaces.

In the Alcatel OmniAccess Wireless System, most of the processing responsibility is removed from traditional SOHO (small office, home office) APs and resides in the Alcatel OmniAccess Wireless Switches and Appliances. The following figure shows <u>Alcatel OmniAccess Wireless Access Points</u> and <u>Third-Party Access Points</u> connected to the 4012 or 4024 OmniAccess Wireless Switch front panel in <u>Direct-Connect Mode</u>.

Figure - 4012 and 4024 OmniAccess Wireless Switch and Access Points



Refer to the following for more information on OmniAccess APs:

- Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs)
- OmniAccess AP Models
- OmniAccess AP External and Internal Antennas
- OmniAccess AP LEDs
- OmniAccess AP Connectors
- OmniAccess AP Power Requirements
- OmniAccess AP External Power Supply
- OmniAccess AP Mounting Options
- OmniAccess AP Physical Security
- <u>Monitor Mode</u>
- Alcatel OmniAccess Wireless Access Point Deployment Guide

#### **About Alcatel OmniAccess Remote Edge Access Points**

The only exception to the general rule of <u>Alcatel OmniAccess Wireless Access Points</u> being continuously controlled by Alcatel OmniAccess Switches or Appliances is the Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R). The OmniAccess AP 1200R is intended to be located at a remote site, initially configured by an Alcatel OmniAccess Switch or Appliance, and normally controlled by an Alcatel OmniAccess Switch or Appliance.

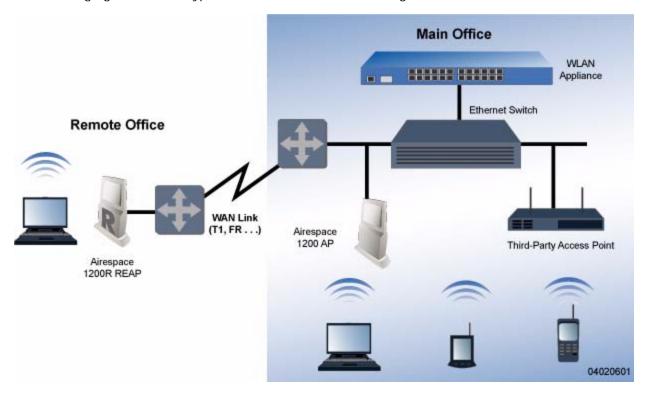
However, because the OmniAccess AP 1200R bridges the client data (compared with other OmniAccess APs, which pass all client data through their respective Alcatel OmniAccess Switch or Appliance), if the WAN link breaks between the OmniAccess AP 1200R and its Alcatel OmniAccess Switch or Appliance, the OmniAccess AP 1200R continues transmitting WLAN 1 client data through other OmniAccess 1200R APs on its local subnet. However, it cannot take advantage of features accessed from the Alcatel OmniAccess Switch or Appliance, such as establishing new VLANs, until communication is reestablished.

The OmniAccess AP 1200R includes the traditional SOHO (small office, home office) AP processing power, and thus can continue operating if the WAN link to its associated Alcatel OmniAccess Switch or Appliance fails. Because it is configured by its associated Alcatel OmniAccess Switch or Appliance, it has the same WLAN configuration as the rest of the Alcatel OmniAccess Wireless System (refer to <u>Alcatel WLANs</u>). As long as it remains connected to its Alcatel OmniAccess Switch or Appliance, it varies its

transmit power and channel selection under control of the *OmniVista AirView Software*, and performs the same Rogue AP location as any other OmniAccess AP.

Note that the OmniAccess AP 1200R can support multiple WLANs while it is connected to its Alcatel OmniAccess Switch or Appliance. However, when it loses connection to its Alcatel OmniAccess Switch or Appliance, it supports only one WLAN on its local subnet.

The following figure shows a typical OmniAccess AP 1200R configuration:



Note that the OmniAccess AP 1200R must have a DHCP server available on its local subnet, so it can obtain an IP address upon reboot. Also note that the OmniAccess 1200R APs at each remote location must be on the same subnet to allow client roaming.

Refer to the following for more information on OmniAccess APs:

- <u>Alcatel OmniAccess Wireless Access Points</u>
- OmniAccess AP Models
- OmniAccess AP External and Internal Antennas
- OmniAccess AP LEDs
- OmniAccess AP Connectors
- OmniAccess AP Power Requirements
- OmniAccess AP External Power Supply
- OmniAccess AP Mounting Options
- OmniAccess AP Physical Security
- <u>Monitor Mode</u>
- Alcatel OmniAccess Wireless Access Point Deployment Guide

Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide

#### About OmniAccess AP Models

The OmniAccess AP includes one 802.11b/802.11g radio (OAW-1200BGE), or one 802.11a and one 802.11b/g radio (OAW-1200ABGE and OAW-1200ABGR). The OmniAccess AP is available in the following configurations:

- OAW-1200BGE OmniAccess AP with one 802.11b/g radio and four high-gain internal antennas, one 5 GHz external antenna adapter, and two 2.4 GHz external antenna adapters.
- OAW-1200BG OmniAccess AP with one 802.11b/g radio, four high-gain internal antennas, and no external antenna adapters.
- <u>OAW-1200ABGE</u> OmniAccess AP with one 802.11a and one 802.11b/g radio and four high-gain internal antennas, one 5 GHz external antenna adapter, and two 2.4 GHz external antenna adapters.
- <u>OAW-1200ABG</u> OmniAccess AP with one 802.11a and one 802.11b/g radio, four high-gain internal antennas, and no external antenna adapters.
- <u>OAW-1200ABGR</u> Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R) with one 802.11a and one 802.11b/g radio and four high-gain internal antennas, one 5 GHz external antenna adapter, and two 2.4 GHz external antenna adapters.

The OmniAccess AP is shipped with a color-coordinated ceiling mount base and hanging-ceiling rail clips. You can also order projection- and flush-mount sheet metal wall mounting bracket kits. The base, clips, and optional brackets allow quick mounting to ceiling or wall.

The OmniAccess AP can be powered by <u>Power Over Ethernet</u> or by an <u>OmniAccess AP External Power Supply</u>. The external power supply model is:

 <u>OAW-AP-PWR</u> - Optional External 110-220 VAC-to-48 VDC Power Supply for any OmniAccess AP.

The Single Inline PoE injector model is:

 <u>OAW-IPWR</u> - Optional Single 802.3af Inline Power over Ethernet Injector for any OmniAccess AP, powered by 90-250 VAC.

The projection and flush sheet metal wall mount bracket model is:

• <u>OAW-WAL-BKT</u> - Optional sheet metal wall-mount bracket kit for any OmniAccess AP. Includes one projection-mount and one flush-mount bracket per kit.

#### About OmniAccess AP External and Internal Antennas

Note: OmniAccess APs and OmniAccess 1200R APs must use the factory-supplied internal or external antennas to avoid violating FCC requirements and voiding the user's authority to operate the equipment. Refer to <u>FCC Statements for OmniAccess APs</u> for detailed information.

The 1200 OmniAccess AP and OmniAccess AP 1200R enclosure contains one 802.11a and/or one 802.11b/g radio and four (two 802.11a and two 802.11b/g) high-gain antennas, which can be independently enabled or disabled to produce a 360-degree omnidirectional coverage area.

Note that the wireless LAN operator can disable either one of each pair of the OmniAccess AP internal antennas to produce a 180-degree sectorized coverage area. This feature can be useful, for instance, for outside-wall mounting locations where coverage is only desired inside the building, and in a back-to-back arrangement that can allow twice as many clients in a given area.

The following sections contain more information about OmniAccess AP internal and external antennas:

• External Antenna Connectors

- Antenna Sectorization
- 802.11a Internal Antenna Patterns
- 802.11b/g Internal Antenna Patterns

#### **External Antenna Connectors**

The OAW-1200BGE, OAW-1200ABGE and OAW-1200ABGR OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points have male reverse-polarity TNC jacks for installations requiring factory-supplied external directional or high-gain antennas. The external antenna option can create more flexibility in OmniAccess AP and OmniAccess AP 1200R antenna placement.



**Note:** The OAW-1200BG, and OAW-1200ABG OmniAccess APs are designed to be used exclusively with the internal high-gain antennas, and have no jacks for external antennas.

Note that the 802.11b/g 2.4 GHz Left external antenna connector is associated with the internal Side A antenna, and that the 2.4 GHz Right external antenna connector is associated with the internal Side B antenna. When you have 802.11b/g diversity enabled, the Left external or Side A internal antennas are diverse from the Right external or Side B internal antennas.

Also note that the 802.11a 5 GHz Left external antenna connector is separate from the internal antennas, and adds diversity to the 802.11a transmit and receive path. Note that no external 802.11a antennas are certified in FCC-regulated areas, but external 802.11a antennas may be certified for use in other regulatory domains.

#### **Antenna Sectorization**

Note that the Alcatel OmniAccess Wireless System supports Antenna Sectorization, which can be used to increase the number of clients and/or client throughput in a given air space. Installers can mount two OmniAccess APs and/or OmniAccess 1200R APs back-to-back, and the Alcatel OmniAccess Wireless System operator can disable the second antenna in both OmniAccess APs or OmniAccess 1200R APs to create a 360-degree coverage area with two sectors.

Installers can also mount OmniAccess APs and/or OmniAccess 1200R APs on the periphery of a building and disable the Side B internal antennas. This configuration can be used to supply service to the building interior without extending coverage to the parking lot, at the cost of eliminating the internal antenna diversity function.

#### **802.11a Internal Antenna Patterns**

The OAW-1200ABG, OAW-1200ABGE and OAW-1200ABGR OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points contain one 802.11a radio, which drives two fully-enclosed high-gain antennas that provide a large 360-degree coverage area. The two internal antennas are used at the same time to provide a 360-degree (Omnidirectional) coverage area, or either antenna can be disabled to provide a 180-degree (Sectorized) coverage area.

When equipped with an optional factory-supplied external antenna, the OAW-1200ABG, OAW-1200ABGE and OAW-1200ABGR 802.11a OmniAccess Radio supports receive and transmit diversity between the internal antennas and the external antenna. The diversity function provided by OmniAccess Radios can result in lower multipath fading, fewer packet retransmissions, and higher client throughput.



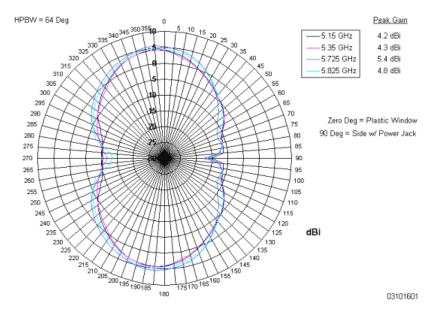
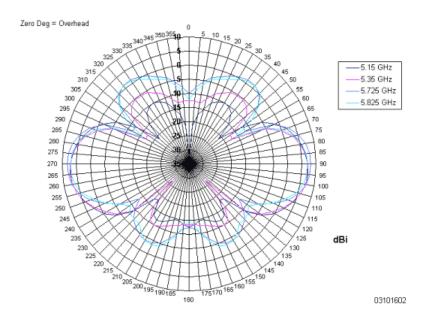


Figure - 1200 OmniAccess AP 802.11a OMNI (Dual Internal) Elevation Antenna Gain Pattern



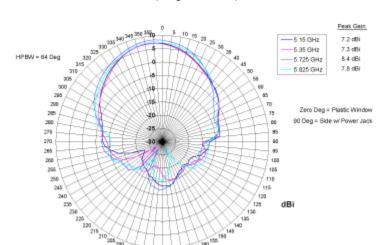
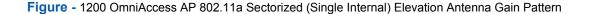
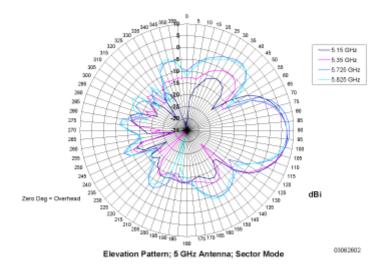


Figure - 1200 OmniAccess AP 802.11a Sectorized (Single Internal) Azimuth Antenna Gain Pattern



Azimuth Pattern; 5 GHz Antenna; Sector Mode



#### 802.11b/g Internal Antenna Patterns

The OAW-1200BG, OAW-1200BGE, OAW-1200ABG, OAW-1200ABGE and OAW-1200ABGR OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points contain one 802.11b/g radio which drives two fully-enclosed high-gain antennas which can provide a large 360-degree coverage area. The two internal antennas can be used at the same time to provide a 360-degree (Omnidirectional) coverage area, or either antenna can be disabled to provide a 180-degree (Sectorized) coverage area.

The OAW-1200BG, OAW-1200BGE, OAW-1200ABG, OAW-1200ABGE and OAW-1200ABGR 802.11b/g OmniAccess Radios support receive and transmit diversity between the internal antennas and/or optional factory-supplied external antennas.

Figure - 1200 OmniAccess AP 802.11b/g OMNI (Dual Internal) Azimuth Antenna Gain Pattern

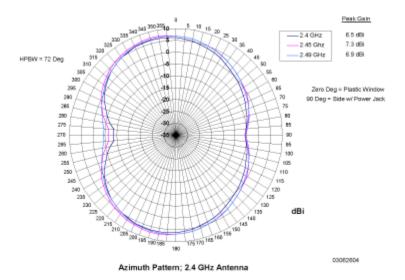
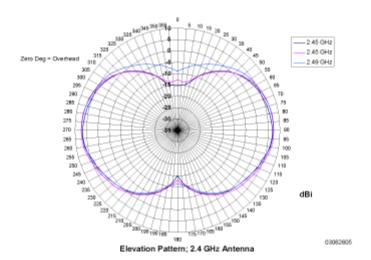


Figure - 1200 OmniAccess AP 802.11b/g OMNI (Dual Internal) Elevation Antenna Gain Pattern



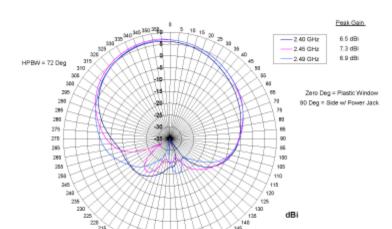


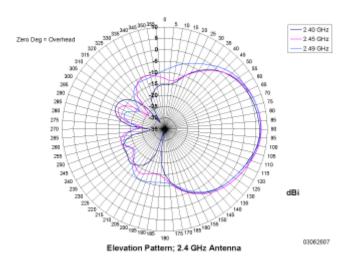
Figure - 1200 OmniAccess AP 802.11b/g Sectorized (Single Internal) Azimuth Antenna Gain Pattern

Figure - 1200 OmniAccess AP 802.11b/g Sectorized (Single Internal) Elevation Antenna Gain Pattern

190

Azimuth Pattern; 2.4 GHz Antenna

03062906



## **About OmniAccess AP LEDs**

Each OmniAccess AP is equipped with four LEDs across the top of the case. They can be viewed from nearly any angle. The LEDs indicate power and fault status, 2.4 GHz (802.11b/g) OmniAccess Radio activity, and 5 GHz (802.11a) OmniAccess Radio activity.

This LED display allows the wireless LAN manager to quickly monitor the OmniAccess AP status. For more detailed troubleshooting instructions, refer to the *Troubleshooting* section.

## **About OmniAccess AP Connectors**

The OAW-1200BGE, OAW-1200ABGE and OAW-1200ABGR OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points have the following external connectors:

- One RJ-45 Ethernet jack, used for connecting the OmniAccess AP or OmniAccess AP 1200R to the 4012 or 4024 OmniAccess Wireless Switch or to the network.
- One 48 VDC power input jack, used to plug in an optional factory-supplied external power adapter.
- Three male reverse-polarity TNC antenna jacks, used to plug optional external antennas into the OmniAccess AP or OmniAccess AP 1200R: two for an 802.11b/g radio, and one for an 802.11a radio.
- Note: The OAW-1200BG and OAW-1200ABG OmniAccess APs are designed to be used exclusively with the internal high-gain antennas, and have no jacks for external antennas.

Figure - OmniAccess AP and OmniAccess AP 1200R External Antenna Connectors



A. 2.4 GHz/802.11b Left External Antenna, Power, and Ethernet



B. 5 GHz/802.11a and 2.4 GHz/802.11b Right External Antennas

The OmniAccess AP or OmniAccess AP 1200R communicates with an Alcatel OmniAccess Wireless Switch or Appliance using standard CAT-5 (Category 5) or higher 10/100 Mbps twisted pair cable with

RJ-45 connectors. Plug the CAT-5 cable into the RJ-45 jack on the side of the OmniAccess AP or OmniAccess AP 1200R.

Note that the OmniAccess AP or OmniAccess AP 1200R can receive power over the CAT-5 cable from the OmniAccess Wireless Switch or network equipment. Refer to <u>Power Over Ethernet</u> for more information about this option.

The OmniAccess AP or OmniAccess AP 1200R can be powered from an optional factory-supplied external AC-to-48 VDC power adapter. If you are powering the OmniAccess AP or OmniAccess AP 1200R using an external adapter, plug the adapter into the 48 VDC power jack on the side of the OmniAccess AP or OmniAccess AP 1200R.

The OmniAccess AP or OmniAccess AP 1200R includes two 802.11a and two 802.11b/g high-gain internal antennas, which provide omnidirectional coverage. However, some OmniAccess AP models and the OmniAccess AP 1200R can also use optional factory-supplied external high-gain and/or directional antennas, as described in *OmniAccess AP External and Internal Antennas*. When you are using external antennas, plug them into the male reverse-polarity TNC jacks on the side of the OAW-1200BGE, OAW-1200ABGE OmniAccess APs and OAW-1200ABGR OmniAccess AP 1200R as described in the *Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide*.



**Note:** The OmniAccess APs and OmniAccess 1200R APs must use the factory-supplied internal or external antennas to avoid violating FCC regulations and voiding the user's authority to operate the equipment, as described in <u>FCC Statements for OmniAccess APs</u>.

## **About OmniAccess AP Power Requirements**

Each OmniAccess AP or and Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R) requires a 48 VDC nominal (between 38 and 57 VDC) power source capable of providing 7 Watts. The polarity of the DC source does not matter because the OmniAccess AP can use either a +48 VDC or a -48 VDC nominal source.

OmniAccess APs can receive power from an *OmniAccess AP External Power Supply* (which draws power from a 110-220 VAC convenience outlet) plugged into the side of the OmniAccess AP case, or from *Power Over Ethernet*.

Figure - Typical OmniAccess AP External Power Supply



For more information about the OmniAccess AP specifications and capacities, refer to <u>Specifications</u>, available in the Alcatel Marketing Literature.

## **About OmniAccess AP External Power Supply**

The OmniAccess AP or OmniAccess AP 1200R can receive power from an external 110-220 VAC-to-48 VDC power supply or from *Power Over Ethernet* equipment.

The external power supply (OAW-AP-PWR) plugs into a secure 110 through 220 VAC convenience outlet. The converter produces the required 48 VDC output (*OmniAccess AP Power Requirements*) for the OmniAccess AP. The converter output feeds into the side of the OmniAccess AP through a 48 VDC jack (*OmniAccess AP Connectors*).

## **About OmniAccess AP Mounting Options**

Refer to the <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> for the OmniAccess AP mounting options.

## **About OmniAccess AP Physical Security**

The side of the OmniAccess AP housing includes a slot for a Kensington MicroSaver Security Cable. You can use any MicroSaver Security Cable to ensure that your OmniAccess AP stays where you mounted it!

Refer to the <u>Kensington</u> website for more information about their security products, or to the <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> for installation instructions.

## **About OmniAccess AP Monitor Mode**

The OmniAccess APs, Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs), Alcatel OmniAccess Wireless Switches, and OmniAccess Wireless Appliances are capable of performing rogue detection and containment while providing regular service.

However, if the administrator would prefer to dedicate specific OmniAccess APs to rogue detection and containment, or if a network that provides only Wireless Protection Service (WPS) functions is desired, the Monitor mode should be enabled for individual OmniAccess APs and OmniAccess 1200R APs.

The Monitor function is set for all 802.11 OmniAccess Radios on a per-OmniAccess AP basis in the OmniAccess APs > Details section in the Alcatel OmniAccess Wireless System Web Browser Online Help.

# **About Third-Party Access Points**

The Alcatel OmniAccess Wireless System can control power and/or channel parameters for existing Cisco 1200, Cisco 350 and ORiNOCO 2000 Access Points using the third-party AP user interface from within the *OmniVista Air Control System Software* application. In addition, the Alcatel OmniAccess Wireless System can be used to enforce real-time control of system-wide 802.1X security policies for third-party AP WLANs as described in *Alcatel Wireless Operating System Security*.

- ACS supports VxWorks versions of Cisco Aironet 1200 and Aironet 350 APs. Apart from status
  monitoring, it allows configuring the channel and power level. The user is also allowed to
  navigate from ACS GUI to AP web pages to make more involved configuration changes. The
  MIB supported is the "ieee802dot11 MIB".
- ACS also supports ORiNOCO 2000 APs for status monitoring and for configuring parameters such as the Channel Select Mode, Channel Number, and Distance Between APs. The supported MIB is "orinocco MIB". ACS allows navigating to the AP web pages for more involved configuration changes.
- Note: Third-party APs must be connected directly to the front panel of 4012 and 4024 Alcatel OmniAccess Wireless Switches for the Alcatel Wireless Operating System to control them using the third-party AP WLAN 17. Because the 4102 OmniAccess Wireless Appliances do not have front-panel AP ports, WLAN 17 is not supported on the 4102 OmniAccess Wireless Appliances.

## **About Rogue Access Points**

Because they are inexpensive and readily available, employees are plugging unauthorized rogue access points (rogue APs) into existing LANs and building ad hoc wireless networks without IT department knowledge or consent.

These rogues can be a serious breach of network security, because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogues, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users and war chalkers frequently publish unsecure access point locations, increasing the odds of having the enterprise security breached.

Rather than using a person with a scanner to manually detect rogue APs, the Alcatel OmniAccess Wireless System automatically collects information on rogue access points detected by its managed Alcatel OmniAccess Wireless Access Points and Third-Party Access Points, by MAC and IP Address, and allows the system operator to locate, tag and monitor them as described in the Detecting and Locating Rogue Access Points section. The Alcatel Wireless Operating System can also be used to discourage rogue AP clients by sending them deauthenticate and disassociate messages from one to four Omni-Access APs. Finally, the Alcatel Wireless Operating System can be used to automatically discourage all clients attempting to authenticate with all rogue APs on the enterprise subnet. Because this real-time detection is automated, it saves labor costs used for detecting and monitoring rogue APs while vastly improving LAN security.

Note that the peer-to-peer, or ad-hoc, clients can also be considered rogue APs.

See also Roque AP Location, Tagging and Containment.

## **Rogue AP Location, Tagging and Containment**

This built-in detection, tagging, monitoring and containment capability allows system administrators to take required actions:

- Locate roque APs as described in <u>Detecting and Locating Roque Access Points</u>.
- Receive new rogue notifications, eliminating hallway scans.
- Monitor unknown rogues until they are eliminated or acknowledged.
- Determine the closest authorized <u>Alcatel OmniAccess Wireless Access Points</u> and <u>Third-Party Access Points</u>, making directed scans faster and more effective.
- Contain rogue APs by sending their clients deauthenticate and disassociate messages from one
  to four OmniAccess APs. This containment can be done for individual rogue APs by MAC
  address, or can be mandated for all rogue APs connected to the enterprise subnet.
- Tag rogue APs:
  - Acknowledge rogue APs when they are outside of the LAN and do not compromise the LAN or WLAN security.
  - Accept rogue APs when they do not compromise the LAN or WLAN security.
  - Tag rogue APs as unknown until they are eliminated or acknowledged.
  - Tag rogue APs as contained and discourage clients from associating with the rogue AP, by having between one and four OmniAccess APs transmit deauthenticate and disassociate messages to all rogue AP clients. This function contains all active channels on the same rogue AP.

To facilitate automated rogue detection in a crowded RF space, OmniAccess APs can be configured to operate in <u>Monitor Mode</u>, allowing monitoring without creating unnecessary interference.

## **About the OmniVista Air Control System Software**

The OmniVista Air Control System Software (ACS Software Server) is an Alcatel Wireless Operating System management tool that extends the capabilities of the <u>Alcatel Web Browser Interface</u> and the <u>Command Line Interface</u> from an individual Alcatel OmniAccess Wireless Switch or Appliance to a network of Alcatel OmniAccess Switches and Appliances.

The ACS Software Server includes the same configuration, performance monitoring, security, fault management, and accounting options used at the Alcatel OmniAccess Switch and Appliance level, but adds a graphical view of multiple Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances and managed Access Points.

ACS Software Server simplifies configuring and monitoring Alcatel OmniAccess Switches and Appliances while decreasing data entry errors with the <u>ACS Alcatel OmniAccess Switch and Appliance Autodiscovery</u> algorithm. The ACS Software Server also uses industry-standard SNMP protocol to communicate with the Alcatel OmniAccess Switches and Appliances.

The ACS Software Server can be run as a normal Windows application, or can be installed as a service, which runs continuously and resumes running after a reboot.

Note that the operator can access the ACS Software Server through the <u>ACS Software Java Admin Client</u>, which allows the ACS Software Server administrator to administer user accounts and schedule periodic maintenance tasks, and the <u>ACS Software Browser Client</u>, which allows ACS Software Server operators to control all other permitted ACS Software functions.

The ACS Software also includes the <u>ACS Floor Plan Editor</u>, which allows you to vectorize bitmapped campus, floor plan, and outdoor area maps, add and change wall types, and import the resulting .FPE wall format maps into the ACS Software database. The .FPE files allow the ACS RF Prediction Tool to make much better RF predictions based on OmniAccess AP signal strength, and accurate wall and window RF attenuation.

The value added by ACS Software includes graphical views of the following:

- Auto-discovery of <u>Alcatel OmniAccess Wireless Access Points</u> as they associate with Alcatel OmniAccess Switches and Appliances, and manual association of <u>Third-Party Access Points</u> with Alcatel OmniAccess Switches and Appliances.
- Auto-discovery of <u>Roque Access Points</u>.
- Map-based organization of Access Point areas, helpful when the enterprise spans more than one geographical area. (Refer to *Configuring the ACS Software Browser Client*.)
- User-supplied Campus, Building and Floor graphics, which show the following:
  - Locations and status of managed Access Points. (Refer to <u>Adding Devices to the ACS Software Database</u>.)
  - Approximate locations of rogue APs, based on signal strength received by nearest managed OmniAccess APs. (Refer to <u>Detecting and Locating Rogue Access Points</u>.)
  - Coverage hole alarm information for APs is based on received signal strength from clients. This information appears in a tabular rather than map format. (Refer to <u>Finding</u> <u>Coverage Holes</u>.)
  - RF coverage maps.
  - Locations of rogue APs and clients.
- System-wide control:
  - Network, OmniAccess Wireless Switch, OmniAccess Wireless Appliance and managed AP configuration is streamlined using customer-defined templates.
  - Network, OmniAccess Wireless Switch, OmniAccess Wireless Appliance and managed AP status and alarm monitoring.

- Automated monitoring: rogue APs, coverage holes, security violations, Alcatel OmniAccess Switches and Appliances, and OmniAccess APs.
- Full event logs available for rogue APs, coverage holes, security violations, Alcatel OmniAccess Switches and Appliances, and OmniAccess APs.
- ACS Software Server allows navigating to a third-party AP native Web interface for configuration and monitoring. Refer to <u>Third-Party Access Points</u> for supported third-party AP models.
- Automatic channel and power level assignment by <u>OmniVista AirView Software</u>.
- User-defined automatic Alcatel OmniAccess Switches and Appliances status audits, missed trap polling, configuration backups, and policy cleanups.

#### **About the ACS Software Java Admin Client**

The ACS Software Java Admin Client interface allows the ACS Software Server administrator to create, modify and delete user accounts, change passwords, assign permissions, and schedule periodic maintenance tasks through a Java window. These administrative tasks are usually reserved to the ACS Software Server administrator.

As part of user administration, the ACS Software Server administrator creates new usernames passwords and assigns them to predefined permissions groups. This task is described in <u>Managing ACS Software and Database</u>.

#### About the ACS Software Browser Client

The ACS Software Browser Client interface allows the ACS Software Server operator to create and configure Alcatel OmniAccess Wireless System coverage area layouts, configure system operating parameters, monitor real-time Alcatel OmniAccess Wireless System operation, and perform trouble-shooting tasks using a standard HTTP or HTTPS Web Browser window.

Alcatel Internetworking, Inc. recommends the Internet Explorer 6.0 or later Web Browser for full access to the ACS functionality, although Netscape Navigator and other Web Browsers are also supported with a slightly altered look-and-feel.



**Note:** The HTTPS (SSL over HTTP) interface is enabled by default, and the HTTP interface can be manually activated in the <u>Command Line Interface</u>, <u>Alcatel Web Browser Interface</u> and <u>ACS Software Browser Client</u>.

The ACS Software Server administrator can create ACS Software Browser Client operator user names and passwords, and can assign the individual operator accounts to various permission levels, from read-only to full read-write control using the *ACS Software Java Admin Client*.

ACS Software Browser Client operators perform their tasks as described in <u>Using the OmniVista Air</u> <u>Control System Software</u>.

## **About the ACS Floor Plan Editor**

The ACS Floor Plan Editor converts architectural, mechanical and technical drawings, graphics, maps and other types of line artwork from raster bitmaps to wall (vector) formats. Operators can use scanners to digitize paper drawings into supported file formats for import into ACS. The ACS Floor Plan Editor automatically recognizes and represents the data in a wall format which can then be imported into your ACS (*OmniVista Air Control System Software*) program.

Because of its ability to create smooth straight, angled, and semi-angled outlines, the ACS Floor Plan Editor is used to convert floor plan maps, define the wall characteristics, and import the resulting .FPE wall format maps into the ACS database. The .FPE files allow the ACS RF Prediction Tool to make much

better RF predictions based on OmniAccess AP signal strength, and accurate wall, window and cubicle RF attenuation.

Otherwise, you may want to save raster images in .BMP, .TIFF, .JPEG, or .PNG raster formats. Note that you can also edit existing .FPE map files.

The output wall files can be saved in .FPE (Alcatel wall format) for importing directly into the ACS database. The output wall files can also be saved in the following formats, but ACS does not recognize these file types: .DXF (AutoCAD), .AI (Adobe Illustrator), .EMF (enhanced metafile), .WMF (Windows metafile), and .TXT (ASCII XY).

Note that there are no restrictions on the input or output image size.

- Note: The quality of ACS Floor Plan Editor recognition is higher for higher resolution data. Use 400 to 600 dots per inch (dpi) scans whenever possible.
- Note: Alcatel strongly recommends that you create images with the long axis horizontal (land-scape format) to ensure the best viewing in ACS.

### **About ACS Alcatel OmniAccess Switch and Appliance Autodiscovery**

Manually adding Alcatel OmniAccess Switch and Appliance data to a management database can be time consuming, and is susceptible to data entry errors. The <u>OmniVista Air Control System Software</u> (ACS Software Server) includes a built-in Alcatel OmniAccess Wireless Switch and Appliance configuration upload function that speeds up database creation while eliminating errors.

Alcatel OmniAccess Switch and Appliance Autodiscovery is limited to the <u>Alcatel Mobility Group</u> subnets defined by the Alcatel OmniAccess Wireless System operator.

<u>ACS Alcatel OmniAccess Switch and Appliance Autodiscovery</u> allows operators to search for a single Alcatel OmniAccess Switch or Appliance by IP Address. The Autodiscovery function finds the Alcatel OmniAccess Switch or Appliance on the network with the specified IP Address, and automatically enters the discovered Alcatel OmniAccess Switch and Appliance information into the ACS Software Server database.

As <u>Alcatel OmniAccess Wireless Access Points</u> or <u>Alcatel OmniAccess Remote Edge Access Points</u> (<u>OmniAccess 1200R APs</u>) associate with an Alcatel OmniAccess Switch or Appliance, the Alcatel OmniAccess Switch or Appliance immediately transmits the OmniAccess AP or OmniAccess AP 1200R information to the <u>OmniVista Air Control System Software</u>, which automatically adds the OmniAccess AP or OmniAccess AP 1200R to the ACS Software Server database.

Once the OmniAccess AP or OmniAccess AP 1200R information is in the ACS Software Server database, operators can add the OmniAccess AP or OmniAccess AP 1200R to the appropriate spot on an ACS Software Server map using <u>Adding APs to Floor Plan and Open Area Maps</u>, so the topological map of the air space remains current.

## **About the Alcatel Web Browser Interface**

The Alcatel Web Browser Interface is built into each Alcatel OmniAccess Switch and Appliance. The Web Browser Interface allows up to five users to simultaneously browse into the built-in Alcatel OmniAccess Wireless Switch or Appliance http/https (http + SSL) Web server, configure parameters, and monitor operational status for the Alcatel OmniAccess Switch or Appliance and its associated Access Points.

Note: Alcatel strongly recommends that you enable the https: and disable the http: interfaces to ensure more robust security for your Alcatel OmniAccess Wireless System.

Because the Alcatel Web Browser Interface works with one Alcatel OmniAccess Switch or Appliance at a time, the Alcatel Web Browser Interface is especially useful when you wish to configure or monitor a single Alcatel OmniAccess Switch or Appliance.

Note: Some popup window filters can be configured to block the Alcatel Web Browser Online Help windows. If your system cannot display the Online Help windows, disable or reconfigure your browser popup filter software.

Refer to <u>Using the Alcatel Web Browser Interface</u> for more information on the Alcatel Web Browser Interface.

## **About the Command Line Interface**

The Alcatel OmniAccess Wireless System Command Line Interface (CLI) is built into the Alcatel OmniAccess Wireless Switches and Appliances, and is one of the Alcatel Wireless Operating System user interfaces described in *About the Alcatel OmniAccess Wireless System*. The CLI allows operators to use a VT-100 emulator to locally or remotely configure, monitor and control individual Alcatel OmniAccess Switches and Appliances, and to access extensive debugging capabilities.

Because the CLI works with one Alcatel OmniAccess Switch or Appliance at a time, the Command Line Interface is especially useful when you wish to configure or monitor a single Alcatel OmniAccess Switch or Appliance.

The Alcatel OmniAccess Switch or Appliance and its associated OmniAccess APs can be configured and monitored using the Command Line Interface (CLI), which consists of a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulators to simultaneously configure and monitor all aspects of the Alcatel OmniAccess Switch or Appliance and associated OmniAccess APs.

Refer to <u>Using the Alcatel OmniAccess Wireless System CLI</u> and the <u>Alcatel OmniAccess Wireless System CLI Reference</u> for more information.

## **SOLUTIONS**

- Alcatel Wireless Operating System Security
- Converting an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 Mode
- Converting an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 Mode
- <u>Configuring a Firewall for an ACS Software Server</u>
- Configuring the System for SpectraLink NetLink Telephones
- Management over Wireless
- <u>Configuring a WLAN for a DHCP Server</u>
- <u>Customizing the Web Auth Login Screen</u>
- <u>Configuring Identity Networking for Alcatel Wireless Operating System 2.0</u>

# **Alcatel Wireless Operating System Security**

Alcatel Wireless Operating System Security includes the following sections:

- Overview
- Layer 1 Solutions
- Layer 2 Solutions
- Layer 3 Solutions
- <u>Single Point of Configuration Policy Manager Solutions</u>
- Roque Access Point Solutions
- Integrated Security Solutions
- Simple, Cost-Effective Solutions

#### Overview

The industry-leading Alcatel Wireless Operating System Security solution bundles potentially complicated Layer 1, Layer 2 and Layer 3 802.11 Access Point security components into a simple policy manager that customizes system-wide security policies on a per-WLAN basis (*Alcatel Wireless Operating System Security*). Unlike SOHO (small office, home office) 802.11 products, the Alcatel Wireless Operating System Security solution included in the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System) provides simpler, unified, and systematic security management tools.

One of the biggest hurdles to WLAN deployment in the enterprise is the WEP (Wired Equivalent Privacy) encryption, which has proven to be a weak standalone encryption method. A newer problem is the availability of low-cost APs, which can be connected to the enterprise network and used to mount 'man-in-the-middle' and denial-of-service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the new 802.11 benefits. Finally, the 802.11 security configuration and management cost has been daunting for resource-bound IT departments.

## **Layer 1 Solutions**

The Alcatel Wireless Operating System Security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically disabled (blocked from access) until the operator-set timer expires.

#### **Layer 2 Solutions**

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions, such as: 802.1X dynamic keys with EAP (extended authorization protocol), or WPA (Wi-Fi protected access) dynamic keys. The Alcatel WPA implementation includes AES (advanced encryption standard), TKIP + Michael (temporal key integrity protocol + message integrity code checksum) dynamic keys, or WEP (Wired Equivalent Privacy) static keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between Alcatel OmniAccess Switches and Appliances and OmniAccess APs are secured by passing data through IPSec tunnels.

## **Layer 3 Solutions**

The WEP problem can be further solved using industry-standard Layer 3 security solutions, such as VPNs (virtual private networks) and IPSec (IP security) protocols. The Alcatel IPSec implementation includes IKE (internet key exchange), DH (Diffie-Hellman) groups, and three optional levels of encryption: DES (ANSI X.3.92 data encryption standard), 3DES (ANSI X9.52-1998 data encryption standard), or AES/CBC (advanced encryption standard/cipher block chaining). Disabling is also used to automatically block Layer 3 access after an operator-set number of failed authentication attempts.

The Alcatel IPSec implementation also includes industry-standard authentication using: MD5 (message digest algorithm), or SHA-1 (secure hash algorithm-1).

The Alcatel OmniAccess Wireless System supports local and RADIUS MAC (media access control) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses.

Finally, the Alcatel OmniAccess Wireless System supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

## **Single Point of Configuration Policy Manager Solutions**

When the Alcatel OmniAccess Wireless System is equipped with OmniVista Air Control System Software, you can configure system-wide security policies on a per-WLAN basis. SOHO Access Points force you to individually configure security policies on each AP, or use a third-party appliance to configure security policies across multiple APs.

Because the Alcatel OmniAccess Wireless System security policies can be applied across the whole system from the OmniVista Air Control System Software, errors can be eliminated and the overall effort is greatly reduced.

## **Rogue Access Point Solutions**

#### **Rogue Access Point Challenges**

Rogue Access Points can disrupt WLAN operations by hijacking legitimate clients and using plaintext or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as passwords and username. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular NIC to transmit and instructing all others to wait, which results in legitimate clients being unable to access the WLAN resources. WLAN service providers thus have a strong interest in banning rogue access points from the air space.

The Alcatel Wireless Operating System Security solution uses the <u>OmniVista AirView Software</u> function to continuously monitor all nearby OmniAccess APs, and automatically discover rogue access points, and locate them as described in <u>Detecting and Locating Rogue Access Points</u>.

## **Tagging and Containing Rogue Access Points**

When the Alcatel OmniAccess Wireless System is monitored using <u>OmniVista Air Control System Software</u>, the ACS Software Server generates the flags as rogue access point traps, and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the OmniAccess APs closest to each rogue access point, allowing Known or Acknowledged rogues (no further action), marking them as Alert rogues (watch for and notify when active), or marking them as Contained rogues (have between one and four OmniAccess APs Discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

When the Alcatel OmniAccess Wireless System is monitored using an <u>Alcatel Web Browser Interface</u> or an <u>Command Line Interface</u>, the interface displays the known rogue access points by MAC address. The

operator then has the option of marking them as Known or Acknowledged rogues (no further action), marking them as Alert rogues (watch for and notify when active), or marking them as Contained rogues (have between one and four OmniAccess APs Discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

## **Integrated Security Solutions**

- Alcatel Wireless Operating System Security is built around a robust 802.1X AAA (authorization, authentication and accounting) engine, which allows operators to rapidly configure and enforce a variety of security policies across the Alcatel OmniAccess Wireless System.
- The <u>Alcatel OmniAccess Switches and Appliances</u> and <u>Alcatel OmniAccess Wireless Access Points</u> are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Alcatel Wireless Operating System Security policies are assigned to individual WLANs, and
   Alcatel OmniAccess Wireless Access Points simultaneously broadcast all (up to 16) configured
   WLANs. This can eliminate the need for additional APs, which can increase interference and
   degrade system throughput.
- The <u>Alcatel OmniAccess Switches and Appliances</u> securely terminates IPSec VPN clients, which
  can reduce the load on centralized VPN concentrators.
- Alcatel Wireless Operating System Security uses the <u>OmniVista AirView Software</u> function to
  continually monitor the air space for interference and security breaches, and notify the operator
  when they are detected.
- Alcatel Wireless Operating System Security works with industry-standard aaa (authorization, authentication and accounting) servers, making system integration simple and easy.
- The Alcatel Wireless Operating System Security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the Alcatel OmniAccess Switch and Appliance can be equipped with an Enhanced Security Module that provides extra hardware required for the most demanding security configurations.

## Simple, Cost-Effective Solutions

Because the Alcatel OmniVista AirView Software function is enabled from the factory, the IT department does not need to create a detailed rollout plan to continually monitor APs, or to individually update APs, resulting in very low input required from the IT department or Wireless LAN manager. This means less money spent deploying, configuring, updating, and monitoring the Alcatel OmniAccess Wireless System.

# **Converting an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 Mode**

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 Mode, use one of the following procedures:

- Using the Alcatel OmniAccess Switch or Appliance Web Browser
- <u>Using the ACS Software Browser Client Interface</u>

#### Using the Alcatel OmniAccess Switch or Appliance Web Browser

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 LWAPP Transport Mode using the Alcatel OmniAccess Switch or Appliance Web Browser Interface, complete the following steps:



**CAUTION:** This procedure will cause your OmniAccess APs to go offline until the Alcatel OmniAccess Switch or Appliance reboots and the associated OmniAccess APs reassociate with the Alcatel OmniAccess Switch or Appliance.

- Note: Layer 3 Mode requires that all subnets that the Alcatel OmniAccess Switches or Appliances are connected to include at least one DHCP server. When you have completed this procedure, the Alcatel OmniAccess Switch or Appliance stores its IP address in its associated OmniAccess APs. When each OmniAccess AP is powered up, it obtains an IP address from the local DHCP server, and connects to its Primary Alcatel OmniAccess Switch or Appliance IP address.
- Note: Layer 3 Mode requires that all subnets that contain Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances and OmniAccess APs are routable to each other.
  - To use the Alcatel OmniAccess Wireless System in Layer 3 mode, you must create an AP Manager Interface, which manages communications between each Alcatel OmniAccess Switch or Appliance and its associated OmniAccess APs. This AP Manager Interface will require a fixed IP address, which must be different from the Management Interface IP address, but which can be on the same subnet as the Management Interface.
- 2. MAKE SURE that all the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs are on the same subnet: that they are only connected through Layer 2 devices. If possible, connect the OmniAccess APs directly (or through Layer 2 devices) to the front-panel 10/100Base-T ports on any 4012 or 4024 OmniAccess Wireless Switch.



**CAUTION:** This step is very important! You must configure the Alcatel OmniAccess Switches or Appliances and associated OmniAccess APs to operate in Layer 3 mode BEFORE completing the conversion.

- 3. Verify that the OmniAccess APs are assigned to the desired Alcatel OmniAccess Switch or Appliance. If you do not complete this step, the OmniAccess APs will fail to associate with the Alcatel OmniAccess Switch or Appliance after completing the conversion.
  - A. Select WIRELESS/OmniAccess APs to navigate to the OmniAccess APs page, and click Detail to have the Web Browser interface display the OmniAccess APs > Details page.
  - B. On the OmniAccess APs > Details page for each OmniAccess AP, verify that the **Primary Switch Name** is correct. If you change the Primary Switch Name, click **Apply** to save the change to the OmniAccess AP.
- 4. Select **WIRELESS/OmniAccess APs** to navigate to the **OmniAccess APs** page, and MAKE SURE that all the OmniAccess APs are listed before you continue with the next step.

If you do not complete this step, the OmniAccess APs may fail to associate with the Alcatel OmniAccess Switch or Appliance after completing the conversion.

- 5. Change the LWAPP Transport Mode from Layer 2 to Layer 3:
  - A. Select **SWITCH/General** to navigate to the General page, and change Layer 2 LWAPP Transport Mode to **Layer 3**.
  - B. Click **Apply** to send the changes to the Alcatel OmniAccess Switch or Appliance and the associated OmniAccess APs. Click **OK** to continue.
- Select COMMANDS/Reboot to navigate to the System Reboot page, and click Reboot to display the Reboot System > Save? page.
- In the Reboot System > Save? page, click Save and Reboot to have the Alcatel Wireless Operating System save the new configuration to and reboot the Alcatel OmniAccess Switch or Appliance.
  - The Alcatel OmniAccess Switch or Appliance reboots.
- 8. Select **SWITCH/Interfaces** to navigate to the **Interfaces** page, and verify that Alcatel Wireless Operating System has automatically added the **ap-manager** interface.
- 9. Configure the ap-manager interface. In the Interfaces page, click the ap-manager Interface Edit button to have the Web Browser display the Interfaces > Edit page. In the Interfaces > Edit page:
  - Optionally add a VLAN Identifier.
  - Enter the ap-manager IP Address and Netmask obtained in Step 1.
  - Add a Gateway IP address.
  - Enter the **physical port number** for the Distribution System connection to the Alcatel OmniAccess Switch or Appliance.
  - Enter a Primary DHCP Server IP address.
  - Enter a **Secondary DHCP Server IP address**. (This can be the same as the Primary DHCP Server IP address if you do not have a second DHCP server on this subnet.)
  - Optionally select an **ACL** (Access Control List) from the pulldown menu.
  - Click **Apply** to add the edited AP Manager Interface definition to the list of interfaces.
- 10. From the **Interfaces** page, verify that the **management** interface is properly configured with a different IP Address than the **ap-manager** interface.
- 11. Save the new configuration and restart your Alcatel OmniAccess Wireless System:
  - A. Select **COMMANDS/Reboot** to navigate to the **System Reboot** page, and select **Reboot**.
  - B. On the Reboot System > Save page, click **Save and Reboot** to save the changes to and reboot the Alcatel OmniAccess Switch or Appliance.
  - C. Click **OK** to confirm the save and reboot.
- 12. After the Alcatel OmniAccess Switch or Appliance has rebooted, select **SWITCH/General** to navigate to the **General** page, and verify that the LWAPP Transport Mode is set to **Layer 3**.
- 13. Power down each OmniAccess AP to save the Layer 3 configuration to nonvolatile memory.
- 14. Connect each OmniAccess AP to its final location in the network. Each OmniAccess AP connects to its Primary Alcatel OmniAccess Switch or Appliance, downloads a copy of the latest Alcatel Wireless Operating System code, and starts reporting its status to the Alcatel OmniAccess Switch or Appliance. Note that this can take a few minutes for each OmniAccess AP.

You have completed the LWAPP Transport Mode conversion from Layer 2 to Layer 3. The **ap-manager** interface now controls all communications between Alcatel OmniAccess Switches or Appliances and OmniAccess APs on different subnets. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### **Using the ACS Software Browser Client Interface**

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 2 to Layer 3 LWAPP Transport Mode using the ACS Software Browser Client Interface, complete the following steps:



**CAUTION:** This procedure will cause your OmniAccess APs to go offline until the Alcatel OmniAccess Switch or Appliance reboots and the associated OmniAccess APs reassociate with the Alcatel OmniAccess Switch or Appliance.

- Note: Layer 3 Mode requires that all subnets that the Alcatel OmniAccess Switches and Appliances and are connected to include at least one DHCP server. When you have completed this procedure, the Alcatel OmniAccess Switch or Appliance stores its IP address in its associated OmniAccess APs. When each OmniAccess AP is powered up, it obtains an IP address from the local DHCP server, and connects to its Primary Alcatel OmniAccess Switch or Appliance IP address.
- Note: Layer 3 Mode requires that all subnets that contain Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances and OmniAccess APs are routable to each other.
  - To use the Alcatel OmniAccess Wireless System in Layer 3 mode, you will need to create an AP Manager Interface, which manages communications between each Alcatel OmniAccess Switch or Appliance and its associated OmniAccess APs. This AP Manager Interface will require a fixed IP address, which must be different from, but which must be on the same subnet as the Management Interface.
  - 2. MAKE SURE that all the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs are on the same subnet: that they are only connected through Layer 2 devices. If possible, connect the OmniAccess APs directly (or through Layer 2 devices) to the front-panel 10/100Base-T ports on the 4012 or 4024 OmniAccess Wireless Switch.



**CAUTION:** This step is very important! You must configure the Alcatel OmniAccess Switches or Appliances and associated OmniAccess APs to operate in Layer 3 mode BEFORE completing the conversion.

- 3. Select **CONFIGURE/Access Points** to navigate to the **All Access Points** page, and verify that the **Primary Switch Name** is correct for all OmniAccess APs. If you change the Primary Switch Name, click **Apply** to save the change to each OmniAccess AP.
- 4. Select **CONFIG/Access Points** to navigate to the **All Access Points** page, and MAKE SURE that the OmniAccess APs are associated with the Alcatel OmniAccess Switch or Appliance before you continue with the next step.
  - If you do not complete this step, the OmniAccess APs may fail to associate with the Alcatel OmniAccess Switch or Appliance after completing the conversion.
- 5. Change the LWAPP Transport Mode from Layer 2 to Layer 3:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page, and select the Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> Switch General** page.
  - B. From the <IP address> > Switch General page, select **System/Networking** to display the **<IP address> > Networking Setups** page.
  - C. On the <IP address> > Networking Setups page, change Layer 2 LWAPP Transport Mode to Layer 3 and click Save.

- D. ACS displays a Please reboot the system for the LWAPP Mode change to take effect message; click **OK**.
- 6. Create a new AP Manager Interface:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page, and select the desired Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> > Switch General** page.
  - B. In the <IP address> > Switch General page, select **System/Interfaces** to have ACS display the **<IP address> > Interface** page.
  - C. In the <IP address> > Interface page, select **System/Interfaces** and then click **GO** to have ACS display a second **<IP address> > Interface** page.
    - Add an Interface Name ap manager.
    - Enter the AP Manager IP Address obtained in Step 1.
    - Optionally add a VLAN ID.
    - Add a **Gateway IP address**.
    - Enter the **physical port number** for the Distribution System connection to the Alcatel OmniAccess Switch or Appliance.
    - Enter a Primary DHCP Server IP address.
    - Enter a **Secondary DHCP Server IP address**. (This can be the same as the Primary DHCP Server IP address if you do not have a second DHCP server on this subnet.)
    - Optionally select an **ACL** (Access Control List) from the pulldown menu.
    - Click **Save** to add the AP Manager Interface to the list of interfaces.
  - D. Use the browser **Back** button (ALT-Left Arrow) to return to the first **<IP address> Interface** page, and verify that ACS has added the **ap manager** Interface Name to the list of Interfaces.
- 7. From the first **<IP address> > Switch General** page, verify that the **management** interface is properly configured with a different IP Address than the **ap manager** interface.
- 8. Save the new configuration and restart your Alcatel OmniAccess Wireless Switch or Appliance:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page.
  - B. Select the Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> > Switch General** page.
  - C. From the <IP address> > Switch General page, select **System/Commands** to display the **<IP address> > Switch Commands** page.
  - D. On the <IP address> > Switch Commands page, under Administrative Commands, select **Save Config to Flash** and click **GO** to save the changed configuration to the Alcatel OmniAccess Switch or Appliance.
  - E. On the <IP address> > Switch Commands page, under Administrative Commands, select **Reboot** and click **GO** to reboot the Alcatel OmniAccess Switch or Appliance. Then click **OK** to confirm the save and reboot.
- 9. After the Alcatel OmniAccess Switch or Appliance has rebooted, verify that the LWAPP Transport Mode is now Layer 3:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page, and select the desired Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> > Switch General** page.
  - 3. From the <IP address> > Switch General page, select **System/Networking** to display the **<IP address> > Networking Setups** page.

- C. On the <IP address> > Networking Setups page, verify that the Current LWAPP Transport Mode is **Layer 3**.
- 10. Select CONFIGURE/Access Points to navigate to the All Access Points page, and MAKE SURE that the OmniAccess APs are associated with the Alcatel OmniAccess Switch or Appliance before you continue with the next step. If you do not complete this step, the OmniAccess APs may fail to associate with the desired Alcatel OmniAccess Switch or Appliance after completing the conversion.
- 11. Power down each OmniAccess AP to save the Layer 3 configuration to nonvolatile memory.
- 12. Connect each OmniAccess AP to its final location in the network. Each OmniAccess AP connects to its Primary Alcatel OmniAccess Switch or Appliance, downloads a copy of the latest Alcatel Wireless Operating System code, and starts reporting its status to the Alcatel OmniAccess Switch or Appliance. Note that this can take a few minutes for each OmniAccess AP.

You have completed the LWAPP Transport Mode conversion from Layer 2 to Layer 3. The **ap-manager** interface now controls all communications between Alcatel OmniAccess Switches or Appliances and OmniAccess APs on different subnets. Continue with the *Alcatel OmniAccess Wireless Product Guide*.

# **Converting an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 Mode**

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 Mode, perform one of the following tasks:

- Using the Alcatel OmniAccess Switch or Appliance Web Browser
- <u>Using the ACS Software Browser Client Interface</u>

#### Using the Alcatel OmniAccess Switch or Appliance Web Browser

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 LWAPP Transport Mode using the Alcatel OmniAccess Switch or Appliance Web Browser Interface, complete the following steps:



**CAUTION:** This procedure will cause your OmniAccess APs to go offline until the Alcatel OmniAccess Switch or Appliance reboots and the associated OmniAccess APs reassociate with the Alcatel OmniAccess Switch or Appliance.

1. MAKE SURE that all the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs are on the same subnet: that they are only connected through Layer 2 devices.



**CAUTION:** This step is very important! If you change the Alcatel OmniAccess Wireless System From Layer 3 to Layer 2 while the Alcatel OmniAccess Switches or Appliances and OmniAccess APs are on different subnets, they will be UNABLE TO COMMUNICATE with each other after the conversion to Layer 2 mode.

- Select SWITCH/General to navigate to the General page, and change Layer 3 LWAPP Transport Mode to Layer 2. Then click Apply to send the changes to the Alcatel OmniAccess Switch or Appliance. Click OK to continue.
- Select COMMANDS/Reboot to navigate to the System Reboot page, and select Reboot. On the Reboot System > Save page, click Save and Reboot to save the changes to and to reboot the Alcatel OmniAccess Switch or Appliance. Then click OK to confirm the save and reboot.
- After the Alcatel OmniAccess Switch or Appliance has rebooted, select SWITCH/General to navigate to the General page, and verify that the current LWAPP Transport Mode is set to Layer 2.
- 5. Also select **SWITCH/Interfaces** to navigate to the Interfaces page, and verify that the **ap-manager** interface is removed from the list of Interface Names.

You have completed the LWAPP Transport Mode conversion from Layer 3 to Layer 2. The Alcatel Wireless Operating System software will now control all communications between Alcatel OmniAccess Switches or Appliances and OmniAccess APs on the same subnet. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## **Using the ACS Software Browser Client Interface**

When you wish to convert an Alcatel OmniAccess Wireless System from Layer 3 to Layer 2 LWAPP Transport Mode using the ACS Software Browser Client Interface, complete the following steps:



**CAUTION:** This procedure will cause your OmniAccess APs to go offline until the Alcatel OmniAccess Switch or Appliance reboots and the associated OmniAccess APs reassociate with the Alcatel OmniAccess Switch or Appliance.

MAKE SURE that all the Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, and OmniAccess APs are on the same subnet: that they are only connected through Layer 2 devices.



**CAUTION:** This step is very important! If you change the Alcatel OmniAccess Wireless System From Layer 3 to Layer 2 while the Alcatel OmniAccess Switches or Appliances and OmniAccess APs are on different subnets, they will be UNABLE TO COMMUNICATE with each other after the conversion to Layer 2 mode.

- 2. Change the LWAPP Transport Mode from Layer 3 to Layer 2:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page, and select the Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> Switch General** page.
  - B. On the <IP address> > Switch General page, select **System/Networking** to display the <**IP address> > Networking Setups** page.
  - C. On the <IP address> > Networking Setups page, change Layer 3 LWAPP Transport Mode to Layer 2 and click Save.
  - D. ACS may display a Please reboot the system for the LWAPP Mode change to take effect message; if so, click **OK**.
- 3. Restart your Alcatel OmniAccess Wireless System:
  - A. On the <IP address> > Networking Setups page, select **System/Commands** to display the **<IP address> > Switch Commands** page.
  - B. On the <IP address> > Switch Commands page, under Administrative Commands, select **Save Config to Flash** and click **GO** to save the changed configuration to the Alcatel OmniAccess Switch or Appliance. Click **OK** to continue.
  - C. On the <IP address> > Switch Commands page, under Administrative Commands, select **Reboot** and click **GO** to reboot the Alcatel OmniAccess Switch or Appliance. Then click **OK** to confirm the save and reboot.
- 4. After the Alcatel OmniAccess Switch or Appliance has rebooted, verify that the LWAPP Transport Mode is now Layer 2:
  - A. Select **CONFIGURE/Switches** to navigate to the **All Switches** page, and select the Alcatel OmniAccess Switch or Appliance by IP address to have ACS display the **<IP address> Switch General** page.
  - B. On the <IP address> > Switch General page, select **System/Networking** to display the **<IP address> > Networking Setups** page.
  - C. On the <IP address> > Networking Setups page, verify that the LWAPP Transport Mode is set to Layer 2.

You have completed the LWAPP Transport Mode conversion from Layer 3 to Layer 2. The Alcatel Wireless Operating System software will now control all communications between Alcatel OmniAccess Switches or Appliances and OmniAccess APs on the same subnet. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# Configuring a Firewall for an ACS Software Server

When an ACS Software Server and an ACS Software Browser Client are on different sides of a firewall, they cannot communicate unless the following ports on the firewall are opened to two-way traffic:

- 80 (TCP)
- 1299 (TCP)
- 4000 (TCP)
- 5009 (TCP)
- 5010 (TCP)
- 6789 (RMI)

Open these ports to configure your firewall to allow communications between an ACS Software Server and an ACS Software Browser Client. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# Configuring the System for SpectraLink NetLink Telephones

SpectraLink NetLink Telephones require an extra Alcatel Wireless Operating System configuration step to optimize integration with Alcatel Wireless Operating System. That configuration step is to enable long preambles in the Alcatel Wireless Operating System using the:

- Using the Command Line Interface
- <u>Using the Web Browser Interface</u>
- Using the OmniVista Air Control System Software

#### **Using the Command Line Interface**

Use this procedure to optimize the Alcatel Wireless Operating System to communicate with SpectraLink NetLink Telephones using a long preamble.

- Log into the Command Line Interface as described in <u>Logging Into the CLI</u>.
- Use the **show 802.11b** command to view the following parameter:

```
Short Preamble mandatory..... Enabled
```

which shows the Alcatel Wireless Operating System default, Short Preamble Enabled; if this is the case, continue with this procedure.

If this parameter indicates Short Preamble Disabled, this Alcatel OmniAccess Wireless Switch or Appliance is already optimized for SpectraLink NetLink Telephones; if desired, continue with the *Alcatel OmniAccess Wireless Product Guide*.

- Disable the 802.11b/g network using the config 802.11b disable network command.
- Enable long preambles using the config 802.11b preamble long command.
- Enable the 802.11b/g network using the config 802.11b enable network command.
- Reboot the Alcatel OmniAccess Switch or Appliance using the reset system command.

Answer  $\mathbf{y}$  to the The system has unsaved changes. Would you like to save them now? (y/n) prompt.

- The Alcatel OmniAccess Switch or Appliance reboots.
- Verify that the Alcatel OmniAccess Switch or Appliance is properly configured by logging back into the CLI and using the show 802.11b command to view the following parameters:

```
802.11b Network..... Enabled
Short Preamble mandatory.... Disabled
```

which shows that the 802.11b/g Network is Enabled and the Short Preamble is Disabled (Long Preamble is Enabled).

 This Alcatel OmniAccess Switch or Appliance is now optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### **Using the Web Browser Interface**

Use this procedure to optimize the Alcatel Wireless Operating System to communicate with SpectraLink NetLink Telephones using a long preamble.

- Log into the Web Browser Interface as described in <u>Using the Alcatel Web Browser Interface</u>.
- Use Wireless / Global RF / 802.11b/g Network to view the 802.11b/g Global Parameters page.
- When the Short Preamble Enabled box is checked, the Alcatel Wireless Operating System is set to the default, Short Preamble Enabled; if this is the case, continue with this procedure.

If this parameter indicates that Short Preamble is Disabled (box is unchecked), this Alcatel OmniAccess Wireless Switch or Appliance is already optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

- Enable long preambles by unchecking the Short Preamble Enabled box.
- Click the Apply button to update the Alcatel OmniAccess Switch or Appliance.
- Note: If you do not already have a CLI session active, Alcatel strongly recommends that you start a CLI session to reboot the Alcatel OmniAccess Switch or Appliance with Save and watch the reboot process. Another reason to use the CLI is that the Web Browser loses its connection to the Alcatel OmniAccess Switch or Appliance when it reboots.
  - If you decide to reboot the Alcatel OmniAccess Switch or Appliance using the CLI, continue with the Reboot and Verify steps found in the <u>Using the Command Line Interface</u> section. Otherwise, continue with this section.
  - Reboot the Alcatel OmniAccess Switch or Appliance using Commands / Reboot / Reboot.
    - Click **OK** in response to the Configuration will be saved and switch will be rebooted. Click ok to confirm. prompt.
  - The Alcatel OmniAccess Switch or Appliance reboots.
  - Verify that the Alcatel OmniAccess Switch or Appliance is properly configured by logging back into the Web Browser Interface and using the Wireless / Global RF / 802.11b/g Network command to view the 802.11b/g Global Parameters page.
  - When the Short Preamble Enabled box is unchecked, this Alcatel OmniAccess Switch or Appliance is optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### **Using the OmniVista Air Control System Software**

Use this procedure to optimize the Alcatel Wireless Operating System to communicate with SpectraLink NetLink Telephones using a long preamble.

- Log into the OmniVista Air Control System Software (ACS Software Browser Client) as described in Starting an ACS Software Browser Client.
- Navigate to the Configuration / Configure Switches / <Alcatel OmniAccess Switch or Appliance IP Address> / 802.11b/g / 802.11b/g Params page.
- When **Short Preamble** is Enabled, the Alcatel Wireless Operating System is set to the default, Short Preamble Enabled: if this is the case, continue with this procedure.
  - If this parameter shows Short Preamble Disabled, this Alcatel OmniAccess Switch or Appliance is already optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- Enable long preambles by setting Short Preamble to Disabled.
- Click the Apply button to update the Alcatel OmniAccess Switch or Appliance.
- Save the Alcatel OmniAccess Switch or Appliance configuration using the Switch Config/Save Config command.
- Reboot the Alcatel OmniAccess Switch or Appliance using Switch Commands/Reboot.
  - Click **OK** in response to the Please save configuration by clicking 'Save Config' under 'Switch Config' menu. Do you want to continue Rebooting anyway? **prompt**.
- The Alcatel OmniAccess Switch or Appliance reboots. This will take some time, during which ACS loses its connection to the Alcatel OmniAccess Switch or Appliance.

- Note: You can use a CLI session to view the Alcatel OmniAccess Switch or Appliance reboot process. When you can log into the Alcatel OmniAccess Switch or Appliance CLI, continue with this procedure.
  - Verify that the Alcatel OmniAccess Switch or Appliance is properly configured by displaying the ACS Software Client and navigating to the Monitor / Troubleshoot / Switch Status / <Alcatel OmniAccess Switch or Appliance IP Address> / 802.11b/g / Stats page.
  - On the Stats page, verify that **Short Preamble Implemented** is set to No, which indicates that this Alcatel OmniAccess Switch or Appliance is optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# **Using Management over Wireless**

The Alcatel Management over Wireless feature allows Alcatel OmniAccess Wireless System operators to monitor and configure their local Alcatel OmniAccess Wireless Switch or Appliance using a wireless client. This feature is supported for all management tasks except uploads to and downloads from (transfers to and from) the Alcatel OmniAccess Wireless Switch or Appliance.

Before you can use the Management over Wireless feature, you must properly configure the Alcatel OmniAccess Wireless Switch or Appliance using either of the following two sections:

#### **Using the Command Line Interface**

- In the CLI, use the show network command to verify whether the Mgmt Via Wireless Interface is Enabled or Disabled. If Mgmt Via Wireless Interface is Disabled, continue with Step 2. Otherwise, continue with Step 3.
- 2. To Enable Management over Wireless, use the following command:
  - >config network mgmt-via-wireless enable
  - to enable Management over Wireless for the WLAN.
- 3. Use a wireless client to associate with an OmniAccess AP connected to the Alcatel OmniAccess Wireless Switch or Appliance you wish to manage.
- 4. Use the telnet < Alcatel OmniAccess Wireless Switch or Appliance Network or DS Port IP Address> command and log into the CLI to verify that you can manage the WLAN using a wireless client.

## **Using the Web Browser Interface**

- In the Alcatel Web Browser Interface, use the Management/Mgmt Via Wireless links to navigate to the Management Via Wireless page.
- 2. In the **Management Via Wireless** page, verify that the **Enable Switch Management to be accessible from Wireless Clients** selection box is checked. If the selection box is not checked, continue with Step 2. Otherwise, continue with Step 3.
- In the Management Via Wireless page, check the Enable Switch Management to be accessible from Wireless Clients selection box to select Management over Wireless for the WLAN.
- 4. Click **Apply** to enable Management over Wireless for the WLAN.
- 5. Use a wireless client web browser to connect to the Alcatel OmniAccess Wireless Switch or Appliance Management Port or DS Port IP Address, and log into the Alcatel OmniAccess Switch or Appliance Web Browser Interface to verify that you can manage the WLAN using a wireless client.

# Configuring a WLAN for a DHCP Server

### **Using the Command Line Interface**

- 1. In the CLI, use the **show wlan** command to verify whether you have a valid DHCP server assigned to the WLAN. If you have no DHCP server assigned to the WLAN, continue with Step 2. Otherwise, continue with Step 4.
- 2. If necessary, use the following commands:
  - >config wlan disable <WLAN id>
  - >config wlan dhcp\_server <WLAN id> <DHCP IP Address>
  - >config wlan enable <WLAN id>

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), and <DHCP IP Address> = DHCP server IP Address.

- 3. Use the **show wlan** command to verify that you have a DHCP server assigned to the WLAN.
- 4. Use the ping <DHCP IP Address> command to verify that the WLAN can communicate with the DHCP server.

#### **Using the Web Browser Interface**

- 1. In the Alcatel Web Browser Interface, navigate to the **WLANs** page.
- Locate the WLAN which you wish to configure for Management over Wireless, and click the associated Edit link to display the WLANs > Edit page.
- 3. Under **General Policies**, check the **DHCP Relay/DHCP Server IP Addr** to verify whether you have a valid DHCP server assigned to the WLAN. If you have no DHCP server assigned to the WLAN, continue with Step 4. Otherwise, continue with Step 9.
- 4. Under General Policies, deselect the Admin Status Enabled box.
- 5. Click **Apply** to disable the WLAN.
- In the DHCP Relay/DHCP Server IP Addr box, enter a valid DHCP server IP Address for this WLAN
- 7. Under General Policies, select the Admin Status Enabled box.
- 8. Click **Apply** to assign the DHCP server to the WLAN and to enable the WLAN. You are returned to the **WLANs** page.
- In the upper-right corner of the WLANs page, click Ping and enter the DHCP server IP Address to verify that the WLAN can communicate with the DHCP server.

# **Customizing the Web Auth Login Screen**

When an Alcatel system operator uses Web Authorization (Web Auth) to authenticate clients, the operator must define User Names and Passwords for each client, and then the clients must enter a valid User Name and Password when prompted. Because the Alcatel OmniAccess Wireless System operator may want to customize the Web Auth Login screen, the following two sections describe the default operation and how to customize the Web Auth Login screen.

- <u>Default Web Auth Operation</u>
- Customizing Web Auth Operation
- Sample Customized Web Auth Login Page

# **Default Web Auth Operation**

When the network operator uses Web Authorization (Web Auth) to authorize clients, the first time clients attempt to access a URL they may receive a Security Alert from their web browser similar to the following:

Figure - Typical Security Alert



After answering Yes to the **Do you want to Proceed?** prompt or if there is no Security Alert, Alcatel Wireless Operating System redirects the client to a Login screen that the client must use to log in using an authorized user name and password. The following figure shows a typical default Alcatel Login Screen:

Figure - Default Alcatel Login Screen



The client must respond with a User Name and Password predefined using the <u>Local Net Users > New</u> Web Browser page, or using the <u>config netuser add</u> Command Line Interface (CLI) command.

Note that the Default Alcatel Login Screen contains Alcatel-specific text and a logo in four customizable areas:

- The Alcatel logo in the upper-right corner can be deleted and restored.
- The Web Title "Welcome to the Alcatel wireless network".
- The Web Message "Alcatel is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work."
- A blank area on the right side of the screen for a user-supplied Logo or other graphic.

The Alcatel logo, Web Title, Web Message, and Logo can be customized for each Alcatel OmniAccess Wireless System as described in the <u>Customizing Web Auth Operation</u> section.

When the client has entered a valid User Name and Password, Alcatel Wireless Operating System typically displays some version of the following Login Successful page, and then redirects the authenticated client to the originally-requested URL.

Figure - Default Login Successful Screen



Note that the Default Login Successful Screen contains a pointer to the operator-defined Virtual Gateway Address URL, redirect https://1.1.1.1/logout.html. This redirect is defined by the Virtual Gateway IP Address parameter (1.1.1.1) entered while <u>Using the Startup Wizard</u>, as the Virtual Gateway Address in the <u>Interfaces</u> Web Browser page, or using the <u>config interface create</u> Command Line Interface (CLI) command.

Also note that the Alcatel OmniAccess Wireless System operator may want to redirect the authenticated client to a different URL. This is described in the <u>Customizing Web Auth Operation</u> section.

# **Customizing Web Auth Operation**

You can customize Web Auth operation <u>Using the Alcatel OmniAccess Wireless System CLI</u> commands as follows:

- <u>Clearing and Restoring the Alcatel Logo</u>
- Changing the Web Title
- Changing the Web Message
- Changing the Logo
- Creating a Custom URL Redirect
- <u>Verifying your Web Auth Changes</u>
- Sample Customized Web Auth Login Page

# **Clearing and Restoring the Alcatel Logo**

You can delete or restore the Alcatel logo shown in the  $\underline{\textit{Default Web Auth Operation}}$  section using the config custom-web weblogo command:

>config custom-web weblogo <disable/enable>

Refer to the <u>Sample Customized Web Auth Login Page</u> for an example.

# **Changing the Web Title**

You can change the Web Title shown in the <u>Default Web Auth Operation</u> section using the config custom-web webtitle command:

### >config custom-web webtitle '<string>'

To change the Web Title again, enter the config custom-web webtitle command again with a new <string> in single quotes. Refer to the <u>Sample Customized Web Auth Login Page</u> for an example.

To change the Web Title back to the Alcatel default "Welcome to the Alcatel wireless network", use the clear webtitle command:

>clear webtitle

# **Changing the Web Message**

You can change the Web Message shown in the <u>Default Web Auth Operation</u> section using the config custom-web webmessage command:

>config custom-web webmessage `<string>'

To change the Web Message again, enter the config custom-web webtitle command again with a new <string> in single quotes. Refer to the <u>Sample Customized Web Auth Login Page</u> for an example.

To change the Web Message back to the Alcatel default "Alcatel is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.", use the clear webmessage command:

>clear webmessage

# **Changing the Logo**

You can add or change a Logo or other graphic in the right side of the Web Auth Login screen as described in the <u>Default Web Auth Operation</u> section using the following instructions.

- <u>Preparing the TFTP Server</u>
- Copying the Logo or Graphic to the TFTP Server
- <u>Downloading the Logo or Graphic</u>

#### **Preparing the TFTP Server**

- Make sure you have a TFTP server available for the Logo or Graphic image download.
  - If you are downloading through the Service port, the TFTP server MUST be on the same subnet as the Service port, because the Service port is not routable.
  - If you are downloading through the DS (Distribution System) network port, the TFTP server can be on the same or a different subnet, because the DS port is routable.
- In the CLI, use the ping <IP Address> command to ensure the Alcatel OmniAccess Switch or Appliance can contact the TFTP server.
- Note: The TFTP server cannot run on the same computer as the <u>OmniVista Air Control System Software</u>, because the ACS Software and the TFTP server use the same communication port.

# Copying the Logo or Graphic to the TFTP Server

- Create a Logo or Graphic image in .JPG, .GIF, or .PNG format with a maximum size of 30 kilobits (recommended size = 180 W x 360 H pixels).
- Make sure the Logo or Graphic image filename contains no spaces.
- Copy the desired Logo or Graphic image file to the default directory on your TFTP server.

# **Downloading the Logo or Graphic**

• In the CLI, use the transfer download start command, and answer 'n' to the prompt to view the current download settings:

#### >transfer download start

To change the download settings, use the following:

```
>transfer download mode tftp
>transfer download datatype image
>transfer download serverip <TFTP server IP address>
>transfer download filename <filename.gif|filename.jpg|filename.png>
>transfer download path <absolute TFTP server path to the update file>
```

- Note: Some TFTP servers require only a forward slash "/" as the <TFTP server path>, and the TFTP server automatically determines the path to the correct directory.
  - In the CLI, use the transfer download start command to view the updated settings, and answer 'y' to the prompt to confirm the current download settings and start the Alcatel Wireless Operating System code download:

#### >transfer download start

To change the Logo or Graphic image again, repeat these commands again using a new filename. Refer to the <u>Sample Customized Web Auth Login Page</u> for an example.

To remove the Logo or Graphic image from the Web Browser Login screen, use the clear webimage command:

```
>clear webimage
```

# **Creating a Custom URL Redirect**

To have Alcatel Wireless Operating System redirect all clients to a specific URL (including http:// or https://) after Web Authentication, use the config custom-web redirect url command:

```
>config custom-web redirecturl <URL>
```

To change the Web Message again, enter the config custom-web redirect-url command again with a new <URL>.

For example, if you want to redirect all clients to www.AcompanyBC.com, use the following command:

```
>config custom-web redirecturl https://www.AcompanyBC.com/
```

To change the redirect back to the originally-requested URL, use the clear redirect-url command:

### >clear redirecturl

# **Verifying your Web Auth Changes**

Use the show custom-web command to verify your Web Auth operation changes:

#### **Default State**

#### >show custom-web

Alcatel Logo	Enabled
CustomLogo	Disabled
Custom Title	Disabled
Custom Message	Disabled
Custom Redirect URL	Disabled
External Web Authentication Mode	Disabled
External Web Authentication URL	Disabled

# **Typical Modified State**

#### >show custom-web

Alcatel Logo	Disabled	
CustomLogo	00_logo.gif	
Custom Title	Welcome to the AcompanyBC Wireless LAN!	
Custom Message	Contact the System Administrator for a	
Username and Password.		
Custom Redirect URL	rect URLhttp://www.AcompanyBC.com	
External Web Authentication Mode	Disabled	
External Web Authentication URL	Disabled	

# Sample Customized Web Auth Login Page

Here is a sample of a customized Web Auth Login page, and the commands used to create it:

```
>config custom-web weblogo disable
```

```
>config custom-web webtitle 'Welcome to the AcompanyBC Wireless LAN!'
```

>config custom-web webmessage 'Contact the System Administrator for a Username and Password.'

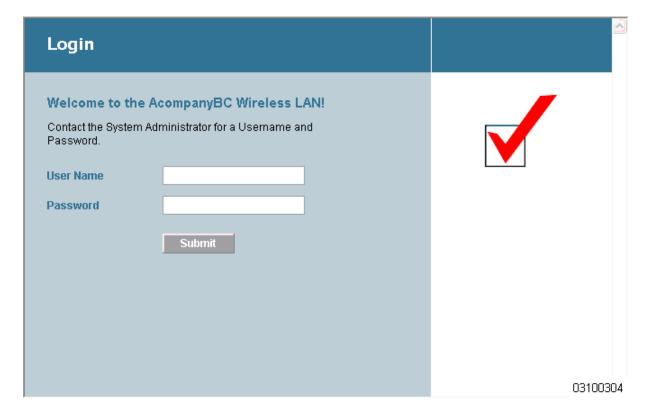
#### >transfer download start

Custom Title...... Welcome to the AcompanyBC Wireless LAN!

Custom Message	ontact the System Administrator for a
Custom Redirect URL h	ttp://www.AcompanyBC.com
Alcatel Logo	Enabled
CustomLogo	00_logo.gif
Custom Title	Welcome to the AcompanyBC Wireless LAN!
Custom Message	Contact the System Administrator for a
Username and Password.	
Custom Redirect URL	http://www.AcompanyBC.com
External Web Authentication Mode	Disabled
External Web Authentication URL	Disabled

When a client attempts to connect to a URL, the following customized Web Auth screen appears:

Figure - Sample Customized Login Screen



After a successful Web Authorization, the client is redirected to the http://www.AcompanyBC.com URL.

# **Configuring Identity Networking for Alcatel Wireless Operating System 2.0**

This document explains the Identity Networking feature of Alcatel Wireless Operating System 2.0, how it is configured and the expected behavior for various security policies.

In previous Alcatel Wireless Operating System releases, each WLAN had a static policy that would be applied to all mobile clients associated with the SSID. Although very powerful, this method has limitations since it requires clients to associate with different SSIDs to inherit different QoS and security policies.

The 2.0 version of the Alcatel Wireless Operating System includes a feature, Identity Networking, that allows the network to advertise a single SSID, yet allow for specific users to inherit different QoS or security policies, based on their user profiles. The specific policies that may be overridden include:

- Quality of Service. When present in a RADIUS Access Accept, the *QoS-Level* value overrides the QoS value specified in the WLAN profile.
- ACL. When the ACL attribute is present in the RADIUS Access Accept, the system applies the
   <u>ACL-Name</u> to the client station after authentication occurs. This overrides any ACLs that are
   assigned to the interface.
- VLAN. When a VLAN <u>Interface-Name</u> or <u>VLAN-Tag</u> is present in a RADIUS Access Accept, the system places the client on a specific interface.
  - **Note:** This feature is ONLY available with MAC Filtering, 802.1X and WPA. This feature WILL NOT WORK with Web Auth or IPSec.
- Tunnel Attributes. **Note:** When any of the other RADIUS attributes in this section are returned, the *Tunnel Attributes* must also be returned.

In order for this feature to be enabled, on a per WLAN basis, the Enable AAA Override configuration flag must be enabled.

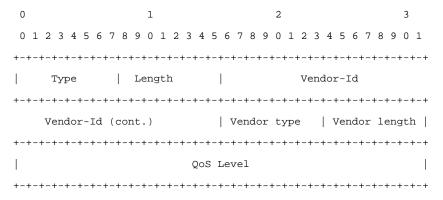
The Airespace Operating System's local MAC Filter database has been extended to include the interface name, allowing local MAC filters to specify which interface the client should be assigned to. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

The following sections explain the RADIUS attributes.

#### **RADIUS Attributes**

#### QoS-Level

This attribute indicates the Quality of Service level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. A summary of the QoS-Level Attribute format is shown below. The fields are transmitted from left to right.

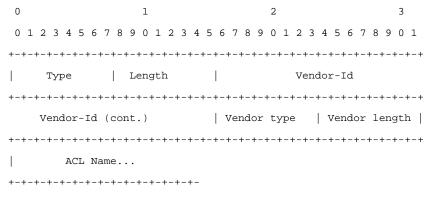


Type - 26 for Vendor-Specific

- Length 10
- Vendor-Id 6139
- Vendor type 2
- Vendor length 4
- Value Three octets:
  - 0 Bronze
  - 1 Silver
  - 2 Gold

#### **ACL-Name**

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The fields are transmitted from left to right.



- Type 26 for Vendor-Specific
- Length >7
- Vendor-Id 6139
- Vendor type 6
- Vendor length >0
- Value A string that includes the name of the ACL to use for the client

# Interface-Name

This attribute indicates the VLAN Interface a client is to be associated to.

A summary of the Interface-Name Attribute format is shown below. The fields are transmitted from left to right.

+-+-+-+-+-+-+-+-+-+-+-+-+-

- Type 26 for Vendor-Specific
- Length >7
- Vendor-Id 6139
- Vendor type 5
- Vendor length >0
- Value A string that includes the name of the interface the client is to be assigned to.

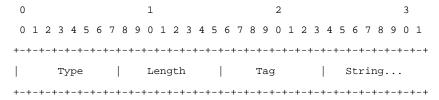
NOTE: This Attribute only works when MAC Filtering is enabled, or if 802.1X or WPA is used as the security policy.

### **VLAN-Tag**

This attribute indicates the group ID for a particular tunneled session, and is also known as the Tunnel-Private-Group-ID attribute.

This attribute MAY be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and SHOULD be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It SHOULD be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The fields are transmitted from left to right.



- Type 81 for Tunnel-Private-Group-ID.
- Length >= 3
- Tag The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag field is greater than 0x00 and less than or equal to 0x1F, it SHOULD be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag field is greater than 0x1F, it SHOULD be interpreted as the first byte of the following String field.
- String This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

#### **Tunnel Attributes**

Note: When any of the other RADIUS attributes in this section are returned, the Tunnel Attributes must also be returned.

Reference [RFC2868] defines RADIUS tunnel attributes used for authentication and authorization, and [RFC2867] defines tunnel attributes used for accounting. Where the IEEE 802.1X Authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular Virtual LAN (VLAN), defined in [IEEE8021Q], based on the result of the authentication. This can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X Authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the Access- Request.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that the VLANID is 12-bits, taking a value between 1 and 4094, inclusive. Since the Tunnel-Private-Group-ID is of type String as defined in [RFC2868], for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag field. As noted in [RFC2868], section 3.1:

- The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it MUST be zero (0x00).
- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag field of greater than 0x1F is interpreted as the first octet of the following field.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X Authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag field SHOULD be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F SHOULD be chosen.

# **TASKS**

You can perform the following tasks using the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System):

- The <u>Alcatel OmniAccess Wireless Access Point Deployment Guide</u> helps you determine the number of Alcatel OmniAccess Wireless Access Points a site needs, where to place the Alcatel OmniAccess Wireless Access Points, and to perform a minimal site survey, if necessary.
- The <u>External-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> provides steps for installing OmniAccess APs with internal antennas and connectors for external antennas
- The <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> provides steps for installing OmniAccess APs with internal antennas and no connectors for external antennas.
- The <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u> guides you through installing Alcatel OmniAccess Wireless Switches and Appliances.
- The <u>ACS Quick Installation Guide</u> gives details on how to install OmniVista Air Control System Software (ACS Software).
- <u>Using the Alcatel OmniAccess Wireless System CLI</u> describes how to access and use the Alcatel OmniAccess Wireless System Command Line Interface.
- <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> details how to use the CLI to configure an Alcatel OmniAccess Wireless Switch or Appliance.
- <u>Using the Alcatel Web Browser Interface</u> helps operators access and use the Alcatel Web Browser Interface.
- <u>Using the OmniVista Air Control System Software</u> describes how to access and use the OmniVista Air Control System Software.
- <u>Updating the Alcatel Wireless Operating System Software</u> provides operators with instructions on how to update the Alcatel OmniAccess Switch or Appliance (and associated OmniAccess AP) Alcatel Wireless Operating System software.
- <u>Updating ACS Software Server and ACS Software Client</u> describes how to update OmniVista Air Control System Software Server and Client loads on ACS Software workstations.
- <u>Updating ACS Software Java Admin Client</u> helps you to update OmniVista Air Control System Software Client loads on ACS Software workstations.
- Adding SSL to the Web Browser Interface provides instructions on how to add SSL certificates
  and keys to the Alcatel OmniAccess Switch and Appliance Web Browser Interface to create an
  https: interface.
- <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u> describes uploading and downloading files from an Alcatel OmniAccess Switch or Appliance.
- <u>Viewing Network Status</u> helps you monitor the Alcatel OmniAccess Wireless System network status.
- <u>Troubleshooting</u> contains steps you can use to troubleshoot the Alcatel OmniAccess Wireless System.

# **Using the Alcatel OmniAccess Wireless System CLI**

The <u>Command Line Interface</u> allows operators to configure any Alcatel OmniAccess Wireless Switch or Appliance and its associated OmniAccess APs using the Command Line Interface. Refer to the following sections or refer to the <u>Alcatel OmniAccess Wireless System CLI Reference</u> for more information:

- <u>Logging Into the CLI</u>
  - Using a Local Serial Connection
  - <u>Using a Remote Ethernet Connection</u>
- Logaina Out of the CLI
- Navigating the CLI
- Using the Startup Wizard
- Saving Configurations
- Erasing the Alcatel OmniAccess Switch or Appliance Configuration
- Resetting the Alcatel OmniAccess Switch or Appliance

# Logging Into the CLI

You may access the Alcatel OmniAccess Wireless Switch or Appliance CLI using either of two methods:

- A direct ASCII serial connection to the Alcatel OmniAccess Switch or Appliance Console Port.
- A remote console session over Ethernet through the pre-configured Service or <u>Management Interface</u> port (configured using the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>).

The following sections contain information on how to use the Command Line Interface. This document assumes the Alcatel OmniAccess Switch or Appliance has been initialized as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>.

Before you log into the Command Line Interface, you must setup your connectivity and environment variables based on the type of connection you are using. Refer to the appropriate section for your connection:

- Using a Local Serial Connection
- Using a Remote Ethernet Connection

# **Using a Local Serial Connection**

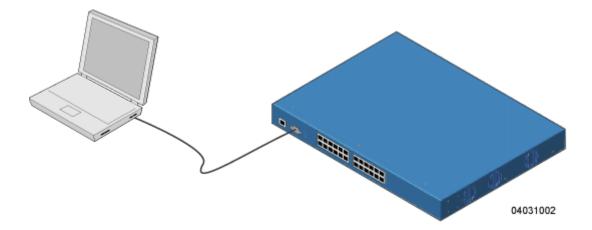
**Note:** You can use the local serial connection at any time, whether or not the Alcatel Omni-Access Switch or Appliance has been configured as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>.

#### You will need:

- A computer running a terminal emulation program and a DB-9 serial port
- DB-9 male to female null-modem serial cable

Use this procedure to configure a serial connection to your Alcatel OmniAccess Switch or Appliance:

1. Connect your computer to the Alcatel OmniAccess Switch or Appliance using the DB-9 null-modem serial cable as shown in the following figure.



- 2. Verify that your terminal emulation (HyperTerminal, ProComm, minicom, tip, or other) interface is configured with the following parameters:
  - 9600 baud
  - 8 data bits
  - 1 stop bit
  - no parity
  - no hardware flow control
- 3. In your terminal emulation program, open a session with the Alcatel OmniAccess Switch or Appliance.
- 4. Press **<RETURN>**. The CLI returns a login prompt.
- 5. Enter a valid login and password to enter the CLI. (The default login and password are admin and admin, respectively.)

User:

Password:

Note that the login and password functions are case sensitive.

6. The CLI displays the root level system prompt:

```
(system prompt)>
```

The CLI allows a default of five users to be logged in at a time, but this number can be set from zero to five users.

The system prompt can be any alphanumeric string, up to 31 characters command. Because this is a user-defined variable, it is omitted from the rest of this documentation.

The CLI automatically logs you out without saving any changes after a short period of inactivity. This automatic logout can be set from 0 (never log out), or form 1 to 160 minutes.

You are now logged into the CLI.

# **Using a Remote Ethernet Connection**

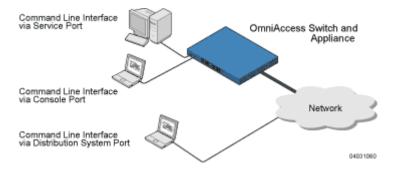
You will need:

- A computer with access to the Alcatel OmniAccess Switch or Appliance over the Ethernet network
- The IP Address of the Alcatel OmniAccess Switch or Appliance

You may use either a terminal emulation program or a DOS shell for the Telnet session.

Note: By default, Telnet sessions are not allowed. You will need to enable Telnet sessions using your serial connection and CLI, or via the Web interface.

Your computer may connect to the Alcatel OmniAccess Switch or Appliance through the network using one of a variety of paths as shown in the following illustration.



- 1. Verify that your terminal emulation or DOS shell interface is configured with the following parameters:
  - Ethernet address
  - Port 23
- 2. In your terminal emulation interface, use the Alcatel OmniAccess Switch or Appliance IP Address to Telnet to the Alcatel OmniAccess Switch or Appliance Command Line Interface. The CLI returns a login prompt.
- 3. Enter a valid login and password to enter the CLI. (The default login and password are admin and admin, respectively.)

User:

Password:

Note that the login and password functions are case sensitive. The CLI allows a default of five users to be logged in at a time, but this number can be set from zero to five users.

4. The CLI displays the root level system prompt:

```
(system prompt)>
```

The CLI allows a default of five users to be logged in at a time, but this number can be set from zero to five users.

The system prompt can be any alphanumeric string, up to 31 characters, and can be changed. Because this is a user-defined variable, it is omitted from the rest of this documentation.

The CLI automatically logs you out without saving any changes after a short period of inactivity. This automatic logout can be set from 0 (never log out), or from 1 to 160 minutes.

You are now logged into the CLI.

# **Logging Out of the CLI**

• When you are done using the Command Line Interface, navigate to the root level and enter logout. You will be prompted to save any changes you have made to the volatile RAM.

**Note:** If you have recently cleared the volatile RAM configurations using <u>Clearing Configurations</u> and you save the configuration from the volatile RAM to the NVRAM, you will have to reconfigure the Alcatel OmniAccess Wireless Switch or Appliance after reboot using the <u>Startup Wizard</u>.

# **CLI Tree Structure**

The Command Line Interface tree structure is organized around five levels:

```
Root Level 2
Level 3
Level 4
Level 5
```

Following are some examples of CLI commands and their position in the tree structure.

```
help
clear
    config
show
    802.11a
config
    advanced
        802.11a
            profile
                noise
                level
save
    config
transfer
    download
        start
```

To view the latest CLI tree structure, log onto the CLI and use the Navigating the CLI commands.

# **Navigating the CLI**

- You start at the root level.
- At the root level, type 'help' to see systemwide navigation commands.
- At all levels, type '?' to view the commands available from the current location.
- At all levels, type a command followed by '?' or '?' to view the parameters available for the command.
- Type any command name to move up to that level.
- Type 'exit' to go down a level.

- Enter <CTRL-Z> to return to the root level.
- From the root level, you can enter the whole command name. For instance, you can enter:

```
>config prompt "Ent1"
```

to change the system prompt to Ent1 >.

- To save your changes from active working RAM to non-volatile RAM (NVRAM) so they are retained upon reboot, use the save config command at the CLI root level.
- To reset the Alcatel OmniAccess Switch or Appliance without logging out, use the reset system
  command at the root level of the CLI tree structure.
- When you are done using the CLI console, navigate to the root level and enter logout. You will be prompted to save any changes you have made from the active working RAM to the non-volatile RAM (NVRAM).

# **Viewing Network Status**

Use the following <u>Command Line Interface</u> commands to view the status of the network controlled by an <u>Alcatel OmniAccess Switches and Appliances</u>.

 Use the show client commands to display client information for each OmniAccess AP 802.11a and 802.11b/g RF coverage area, to display detailed information for a client connected through a particular OmniAccess AP, and display a summary of clients connected through the Alcatel OmniAccess Wireless System:

```
>show client ap [802.11a/802.11b] <OmniAccess AP>
>show client detail <MAC addr>
>show client summary
```

If you need to, use the **config client deauthenticate** command to deauthenticate an individual <MAC address>.

- Use the show rogue-ap summary and show rogue-ap detail commands to discover rogue
   APs on the subnet. If necessary, use the config rogue-ap acknowledged, config rogue-ap
   alert, and config rogue-ap known commands to mark the rogue APs in the Alcatel
   OmniAccess Wireless System database.
- In general, use the show commands to view the Alcatel OmniAccess Wireless System status.
- To test a link to a MAC address, use the linktest command at the CLI root level. Note that linktest does not work for IPSec links.
- To ping an IP Address, use the ping command at the CLI root level.

Continue with <u>Using the Alcatel OmniAccess Wireless System CLI</u>.

# **Configuring the Alcatel OmniAccess Switch or Appliance**

This section assumes that the Alcatel OmniAccess Wireless Switch or Appliance is already installed, initially configured, and connected as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>.

Continue with the following sections to configure an Alcatel OmniAccess Switch or Appliance using the Command Line Interface (CLI):

- <u>Logging Into the CLI</u>
- Navigating the CLI
- Collecting Alcatel OmniAccess Switch or Appliance Parameters
- Configuring System Parameters
- Configuring Alcatel OmniAccess Switch and Appliance Interfaces
- Configuring WLANs
- Configuring Mobility Groups
- <u>Configuring RADIUS</u>
- Configuring SNMP
- Configuring Other Ports and Parameters
- Transferring Files To and From an Alcatel OmniAccess Switch or Appliance
- Updating the Alcatel Wireless Operating System Software
- Using the Startup Wizard
- Adding SSL to the Web Browser Interface
- Clearing Configurations
- <u>Saving Configurations</u>
- Resetting the Alcatel OmniAccess Switch or Appliance
- <u>Erasing the Alcatel OmniAccess Switch or Appliance Configuration</u>
- Logging Out of the CLI

Continue with *Using the Alcatel OmniAccess Wireless System CLI*.

# **Collecting Alcatel OmniAccess Switch or Appliance Parameters**

Collect the high-level Alcatel OmniAccess Wireless Switch or Appliance parameters:

### **System Parameters**

- Supported protocols: 802.11a and/or 802.11b/g.
- New usernames and passwords (optional).

#### **Network (Distribution System) Parameters**

- Distribution System (network) port static IP Address, netmask, and optional default gateway IP Address from the network planner.
- Service port static IP Address and netmask from the network planner (optional).
- Distribution System physical port (1000Base-T, 1000Base-SX, or 10/100Base-T).
- Distribution System port VLAN assignment (optional).

- Distribution System port Web and Secure Web mode settings, enabled or disabled.
- Distribution System port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age.

#### **WLAN Parameters**

 WLAN Configuration: VLAN assignments, Layer 2 Security settings, Layer 3 Security settings, QoS assignments.

#### **Mobility Parameters**

- Mobility Settings: Mobility Group Name (optional).

#### **RADIUS Parameters**

RADIUS Settings.

#### **SNMP Parameters**

SNMP Settings.

#### **Other Parameters**

- Other Port and Parameter Settings: Service port, Alcatel OmniVista AirView Software, third-party APs, Serial/CLI Console port, 802.3x Flow Control, and System Logging.

# **Other Actions**

- Assemble all files that may need uploading or downloading to the Alcatel OmniAccess Switch or Appliance, including the latest AWOS code.

Continue with Configuring System Parameters.

# **Configuring System Parameters**

The Alcatel OmniAccess Wireless Switch or Appliance requires a few basic system parameters to communicate with other network devices. Perform the following to set these parameters:

#### **Time and Date**

- Use the show time command to view the Alcatel OmniAccess Switch or Appliance time and date.
- If necessary, set the Alcatel OmniAccess Switch or Appliance time and date by entering:

```
>config time MM/DD/YY HH:MM:SS
```

• Use the **show time** command to verify that the Alcatel OmniAccess Switch or Appliance has stored your input. Continue with the next parameter.

# **Country**

The Alcatel OmniAccess Switch or Appliance has been designed to be used in countries with different 802.11 regulatory domains.

- Use the **show country** command to view the Alcatel OmniAccess Switch or Appliance country regulatory domain.
- If necessary, set the Alcatel OmniAccess Switch or Appliance regulatory domain by entering:

```
>config country <domain>
```

Where <domain> =

- US (United States of America), which allows 802.11b and 802.11g operation and 802.11a Low, Medium, and High bands.
- USL (US Low), which allows 802.11b and 802.11g operation and 802.11a Low and Medium bands. (Used for legacy 802.11a interface cards that do not support 802.11a High band.)
- AU (Australia), which allows 802.11a and 802.11b/g.
- AT (Austria), which allows 802.11a and 802.11b/g.
- BE (Belgium), which allows 802.11a and 802.11b/g.
- CA (Canada), which allows 802.11b/g.
- DK (Denmark), which allows 802.11a and 802.11b/g.
- FI (Finland), which allows 802.11a and 802.11b/g.
- FR (France), which allows 802.11a and 802.11b/g.
- DE (Germany), which allows 802.11a and 802.11b/g.
- GR (Greece), which allows 802.11b/g.
- IE (Ireland), which allows 802.11a and 802.11b/g.
- IN (India), which allows 802.11a and 802.11b.
- IT (Italy), which allows 802.11a and 802.11b/g.
- JP (Japan), which allows 802.11a and 802.11b/g.
- KR (Republic of Korea), which allows 802.11a and 802.11b/g.
- LU (Luxembourg), which allows 802.11a and 802.11b/g.
- NL (Netherlands), which allows 802.11a and 802.11b/g.
- PT (Portugal), which allows 802.11a and 802.11b/g.
- ES (Spain), which allows 802.11a and 802.11b/g.
- SE (Sweden), which allows 802.11a and 802.11b/g.
- GB (United Kingdom), which allows 802.11a and 802.11b/g.
- Continue with the next parameter.

### Supported 802.11a and 802.11b/g Protocols

The 802.11a and 802.11b/g protocols can be independently enabled or disabled.

- Use the **show sysinfo** command to view the 802.11a and 802.11b/g enabled/disabled status.
- Make sure these protocols are configured to agree with your wireless network plan and to comply with the Country regulatory domain entered in the previous step using the following commands:

```
>config 802.11a enable network
>config 802.11a disable network
>config 802.11b enable network
>config 802.11b disable network
```

 Use the show sysinfo command to verify that the Alcatel OmniAccess Switch or Appliance has stored your input. Continue with the next parameter.

#### **Users and Passwords**

After you have configured other system parameters, you are urged to change the username and password so unauthorized personnel cannot easily log into the Alcatel OmniAccess Wireless System.

- Use the show mgmtuser command to view the current management user names.
- Use the following commands to add new usernames and add or change passwords:
  - >config mgmtuser add <username> <password> [read-write/read-only]
    >config mgmtuser password <username> <new password>

where <username>, <password> and <new password> = Any ASCII character string, up to 24 characters, case sensitive, with no spaces.

• Use the **show mgmtuser** command to verify that your users have been accepted by the system. Continue with <u>Configuring Alcatel OmniAccess Switch and Appliance Interfaces</u>.

# **Configuring Alcatel OmniAccess Switch and Appliance Interfaces**

As described in the <u>Distribution System Ports</u> section, the OmniAccess Wireless Appliance has two redundant (4102) physical ports, and the OmniAccess Wireless Switch has multiple physical ports. This means that the OmniAccess Wireless Appliance can physically connect to one subnet, and the OmniAccess Wireless Switch can physically connect to multiple subnets.

Each of the physical ports can have multiple Interfaces applied to it:

- The <u>Management Interface</u> controls communications with network equipment for all physical ports in all cases.
  - When the Alcatel OmniAccess Wireless System is operated in Layer 2 Mode (see <u>Layer 2 and Layer 3 Operation</u>), the Management Interface also controls communications between the Alcatel OmniAccess Switch or Appliance and <u>Alcatel OmniAccess Wireless Access Points</u> and <u>Third-Party Access Points</u>.
  - When the Alcatel OmniAccess Wireless System is operated in Layer 3 Mode, the Management Interface no longer controls communications between the Alcatel OmniAccess Switch or Appliance and OmniAccess APs, but continues controlling OmniAccess Wireless Switch Third-Party APs, which can only be directly connected to physical front-panel 10/100Base-T ports.
- When the Alcatel OmniAccess Wireless System is operated in Layer 3 Mode (see <u>Layer 2 and Layer 3 Operation</u>), the <u>AP-Manager Interface</u> controls all communications between the Alcatel OmniAccess Switch or Appliance and <u>Alcatel OmniAccess Wireless Access Points</u>.
- Each physical port can also have between one and 64 <u>Operator-Defined Interfaces</u>, also known as VLAN Interfaces, assigned to it. Each Operator-Defined Interface is individually configured, and allows separate communication streams to exist on any or all of the physical port(s).
- The <u>Virtual Interface</u> controls Layer 3 Security and Mobility manager communications for Alcatel OmniAccess Wireless Switches and Appliances for all physical Ports. It also maintains the DNS Gateway hostname used by Layer 3 Security and Mobility managers to verify the source of certificates when Layer 3 Web Auth is enabled.
- Note that the Alcatel OmniAccess Wireless Switch or Appliance also has a <u>Service-Port Interface</u>, but that Interface can only be applied to the front-panel <u>Service Port</u>.

If you have not already done so, you must decide which physical port(s) you want to use, and then create and assign the following:

- Verifying and Changing the Management Interface
- Creating and Assigning the AP-Manager Interface
- Creating, Assigning and Deleting Operator-Defined Interfaces

Verifying and Changing the Virtual Interface

Continue with the next section to configure the Distribution System IP Address.

# **Verifying and Changing the Management Interface**

Normally, the static <u>Management Interface</u> parameters are defined when the Alcatel OmniAccess Wireless Switch or Appliance is initially configured using the <u>Startup Wizard</u>. However, you may want to verify and/or change its parameters:

- Use the **show interface detailed management** command to view the current Management Interface settings. Note that the Management Interface uses the burned-in MAC address.
- To change any of the parameters, disable all enabled WLANs:
  - >show wlan summary
  - >config wlan disable <1-16, or 17 for Third-Party APs> (repeat for all enabled WLANs)
- And then use the following:
  - >config interface address management <IP addr> <IP netmask> [optional
    gateway]
  - >config interface vlan management <VLAN ID | '0' for untagged>
  - >config interface port management <Physical DS Port Number>
  - >config interface dhcp management <IP addr of Primary DHCP server> <IP addr of optional Secondary DHCP server>
  - >config interface acl management <Access Control List Name> (Note)

using the values collected from the network planner in <u>Collecting Alcatel OmniAccess Switch or Appliance Parameters.</u>

**Note:** If you are applying an Access Control List (ACL) to the Management Interface, you must first configure the ACL using the <u>Creating Access Control Lists</u> section.

Use the **show interface detailed management** command to verify that the Alcatel OmniAccess Switch or Appliance has correctly stored your inputs. Note that this Interface cannot be deleted. Continue with the next section.

# **Creating and Assigning the AP-Manager Interface**

The static <u>AP-Manager Interface</u> only exists when the Alcatel OmniAccess Wireless System is operating in LWAPP Layer 3 Mode (see <u>Layer 2 and Layer 3 Operation</u>).

- Use the show interface summary command to view the current Interfaces.
  - If the Alcatel OmniAccess Wireless System is operating in Layer 2 Mode, the ap-manager interface will not be listed. Either skip this section and continue with <u>Creating, Assigning and Deleting Operator-Defined Interfaces</u>, or go to <u>Converting an Alcatel OmniAccess Wireless</u>
    System from Layer 2 to Layer 3 Mode.
- Use the **show interface detailed ap-manager** command to view the current AP-Manager Interface settings.
- To change any of the parameters, disable all enabled WLANs:
  - >show wlan summary
  - >config wlan disable <1-16, or 17 for Third-Party APs> (repeat for all enabled WLANs)
- And then use the following:

- >config interface address ap-manager <IP addr> <IP netmask> [optional
  gateway]
- >config interface vlan ap-manager <VLAN ID | '0' for untagged>
- >config interface port ap-manager <Physical DS Port Number>
- >config interface dhcp ap-manager <IP addr of Primary DHCP server> <IP addr of optional Secondary DHCP server>
- >config interface acl ap-manager <Access Control List Name> (Note)

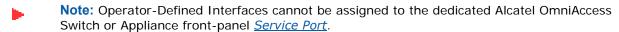
using the values collected from the network planner in <u>Collecting Alcatel OmniAccess Switch or Appliance Parameters</u>.

Note: If you are applying an Access Control List (ACL) to the Management Interface, you must first configure the ACL using the <u>Creating Access Control Lists</u> section.

Use the **show interface detailed ap-manager** command to verify that the Alcatel OmniAccess Switch or Appliance has correctly stored your inputs. Note that this Interface cannot be deleted. Continue with the next section.

# **Creating, Assigning and Deleting Operator-Defined Interfaces**

Each Alcatel OmniAccess Switch and Appliance can support up to 64 dynamic <u>Operator-Defined Interfaces</u>. Each Operator-Defined Interface controls VLAN and other communications between Alcatel OmniAccess Wireless Switches and Appliances and all other network devices. Between one and 64 Operator-Defined Interfaces can be assigned to <u>Alcatel WLANs</u>, physical <u>Distribution System Ports</u>, the Layer 2 <u>Management Interface</u>, and the Layer 3 <u>AP-Manager Interface</u>.





**CAUTION:** Operator-Defined Interface names cannot have spaces in them. If an Operator-Defined Interface name contains a space, you may not be able to edit its configuration using the *Command Line Interface*.

- Use the **show interface summary** command to view the current Operator-Defined Interfaces. They can be identified by the 'dynamic' Interface type.
- To view the details of an Operator-Defined Interface, use the **show interface detailed <operator-defined interface name>** command to view the current Operator-Defined Interface settings.
- To change any of the parameters or add another Operator-Defined Interface, disable all enabled WLANs:
  - >show wlan summary
  - >config wlan disable <1-16, or 17 for Third-Party APs> (repeat for all enabled WLANs)
- And then use the following:
  - >config interface create <operator-defined interface name> <VLAN ID|'0'| for untagged>
  - >config interface address <operator-defined interface name> <IP addr> <IP
    netmask> [optional gateway]
  - >config interface vlan <operator-defined interface name> <VLAN ID|'0' for untagged>
  - >config interface port <operator-defined interface name> <Physical DS Port Number>

>config interface dhcp <operator-defined interface name> <IP addr of Primary DHCP server> <IP addr of optional Secondary DHCP server>

>config interface acl <operator-defined interface name> <Access Control List
Name> (Note)

using the values collected from the network planner in <u>Collecting Alcatel OmniAccess Switch or Appliance Parameters</u>.

Note: If you are applying an Access Control List (ACL) to the Operator-Defined Interface, you must first configure the ACL using the <u>Creating Access Control Lists</u> section.

Use the show interface detailed <operator-defined interface name> and show interface summary commands to verify that the Alcatel OmniAccess Switch or Appliance has correctly stored your inputs.

- To delete an Operator-Defined Interface, use the following command:
  - >config interface delete <operator-defined interface name>

Continue with the next section.

#### **Verifying and Changing the Virtual Interface**

The static <u>Virtual Interface</u> controls Layer 3 Security and Mobility manager communications for Alcatel OmniAccess Wireless Switches and Appliances, and it maintains the DNS Gateway hostname used by Layer 3 Security and Mobility managers to verify the source of certificates when Layer 3 Web Auth is enabled.

- Use the show interface detailed virtual command to view the current AP-Manager Interface settings.
- To change any of the parameters, disable all enabled WLANs:
  - >show wlan summary
  - >config wlan disable <1-16, or 17 for Third-Party APs> (repeat for all enabled WLANs)
- And then use the following:
  - >config interface address virtual <IP addr> where <IP addr> is any fictitious, unassigned, unused Gateway IP Address.
  - >config interface hostname virtual <DNS Host Name>

using the values collected from the network planner in <u>Collecting Alcatel OmniAccess Switch or Appliance Parameters</u>.

Note: If you change any of the Virtual Interface settings, reset the Alcatel OmniAccess Switch or Appliance and save the configuration as described in <u>Resetting the Alcatel OmniAccess</u>

Switch or Appliance.

Use the **show interface detailed virtual** command to verify that the Alcatel OmniAccess Switch or Appliance has correctly stored your inputs. Note that this Interface cannot be deleted. Continue with the next section.

### **Enabling Web and Secure Web Modes**

- Use the following commands to enable (default) or disable the Distribution System port as a Web port and/or a Secure Web port:
  - >config network webmode [enable/disable]
  - >config network secureweb [enable/disable]

Use the **show network** command to verify that your inputs were accepted. Continue with the next parameter.

# **Configuring Spanning Tree Protocol**

Spanning Tree Protocol is initially disabled for the Distribution System (network) ports. You can enable STP on the Alcatel OmniAccess Switch or Appliance for all physical ports using the following commands. If you are not configuring Spanning Tree Protocol at this time, skip this section.

- Use the show spanningtree port and show spanningtree switch commands to view the current STP status.
- Disable STP on the Alcatel OmniAccess Switch or Appliance by entering:

```
>config spanningtree switch mode disable
```

This causes the Alcatel OmniAccess Switch or Appliance to disable support for STP on all ports.

- **Note:** STP must be disabled before the STP parameters can be changed; leave STP disabled until you have finished configuring all associated parameters.
  - Configure the STP port administrative mode on the desired ports using one of the following commands:

```
>config spanningtree port mode 802.1d [<port number>/all] (default)
>config spanningtree port mode fast [<port number>/all]
>config spanningtree port mode off <[<port number>/all]
```

where <port number> = 1 through 13 or 1 through 25, and all = all ports.

Configure STP port path cost on the STP ports using one of the following commands:

```
>config spanningtree port pathcost <1-65535> [<port number>/all] >config spanningtree port mode pathcost auto [<port number>/all] (default)
```

where <1-65535> = Path cost supplied by the network planner, and auto = allow the STP algorithm to automatically assign the path cost (default).

Configure port priority on the STP ports using the following command:

```
>config spanningtree port priority <0-255> <port number> where <0-255> = STP priority for this port (default priority = 128).
```

 If required, configure the Alcatel OmniAccess Switch or Appliance STP bridge priority using the following command:

```
>config spanningtree switch bridgepriority <0-65535>
```

where <0-65535> = STP bridge priority for this Alcatel OmniAccess Switch or Appliance (default priority = 32768).

 If required, configure the Alcatel OmniAccess Switch or Appliance STP forward delay using the following command:

```
>config spanningtree switch forwarddelay <4-30>
```

where <4-30> seconds = STP forward delay for this Alcatel OmniAccess Switch or Appliance (default forward delay = 15 seconds).

• If required, configure the Alcatel OmniAccess Switch or Appliance STP hello time using the following command:

```
>config spanningtree switch hellotime <1-10>
```

where <1-10> seconds = STP hello time for this Alcatel OmniAccess Switch or Appliance (default hello time = 2 seconds).

 If required, configure the Alcatel OmniAccess Switch or Appliance STP maximum age using the following command:

```
>config spanningtree switch maxage <6-40>
```

where <6-40> seconds = STP maximum age for this Alcatel OmniAccess Switch or Appliance (default = 20 seconds).

After all the ports have been configured for the desired STP settings, enter the following:

```
>config spanningtree switch mode enable
```

This procedure allows the Alcatel OmniAccess Switch or Appliance to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

You have configured STP for the Alcatel OmniAccess Switch or Appliance. Verify that your settings are stored in memory using the **show spanningtree port** and **show spanningtree switch** commands. Continue with <u>Configuring WLANs</u>.

# **Creating Access Control Lists**

When you wish to create <u>Access Control Lists</u>, Alcatel Internetworking, Inc. strongly recommends that you use the Alcatel Switch Web Browser Interface. Refer to the <u>Access Control Lists</u> page in the <u>Alcatel OmniAccess Wireless System Web Browser Online Help</u> document.

# **Configuring WLANs**

The Alcatel OmniAccess Wireless Switch and Appliance can control up to 16 Alcatel Wireless LANs plus one third-party AP WLAN as described in <u>Alcatel WLANs</u>. If you are not configuring WLANs at this time, skip this section and continue with <u>Configuring Mobility Groups</u>.

#### **WLANs**

- Use the **show wlan summary** command to display the current WLANs and whether they are enabled or disabled. Note that each Alcatel WLAN is assigned a WLAN ID from 1 to 16, or 17 to assign policies for third-party APs.
- Note: WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="#Appliance Mode">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.
  - If you are creating WLANs, use the following commands:
    - >config wlan create <wlan id> <wlan name>
    - >config wlan create 17 <3rd party wlan name>

where <wlan id> = 1 through 16, <wlan name> = SSID (up to 31 alphanumeric characters), and <wlan id> = 17 and <3rd party wlan name> = SSID for a third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

- Note: When WLAN 1 is created in the <u>Startup Wizard</u>, it is created in enabled mode; disable it until you have finished configuring it. When you create a new WLAN using the config wlan create command, it is created in disabled mode; leave it disabled until you have finished configuring it.
  - If you are modifying enabled WLANs, make sure they are disabled using the **show wlan summary** command. If they are not disabled, use the following to disable them:

>config wlan disable <wlan id>

where <wlan id> = 1 through 16, or 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode). Leave the WLANs in disabled mode until you have finished configuring them.

• If you are deleting WLANs, use the following command:

```
>config wlan delete <wlan id>
```

where <wlan id> = 1 through 16, 17 = third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

#### **DHCP Server**

Each WLAN can be assigned to a DHCP server. Any or all WLANs can be assigned to the same DHCP server, and each WLAN can be assigned to a different DHCP servers. This assignment is mandatory for WLANs that allow *Management over Wireless*, as described in *External DHCP Servers*.

- Use the show wlan command to verify whether you have a DHCP Server assigned to the WLAN.
- If necessary, use the following command:

```
>config wlan dhcp_server <WLAN id> <IP Address>
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), <IP Address> = DHCP Server IP Address,

Use the show wlan command to verify that you have a DHCP Server assigned to the WLAN.

### **MAC Filtering**

Whenever you are going to use MAC filtering for Alcatel OmniAccess Switch or Appliance or RADIUS authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the following commands to configure the MAC Address Filter List:

- Use the show wlan command to verify whether you have MAC filtering enabled or disabled for each WLAN.
- If necessary, use the following command:

```
>config wlan mac-filtering enable <WLAN id>
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

 Use the show wlan command to verify that you have MAC filtering enabled or disabled for each WLAN.

#### Local MAC Filter

Alcatel OmniAccess Switches and Appliances have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

- Use the show macfilter command to verify that you have MAC addresses assigned to WLANs.
- If required, use the following commands to assign local MAC addresses to WLANs, and to configure a WLAN to filter a local client:

```
>config macfilter add <MAC addr> <WLAN id>
```

```
>config macfilter wlan-id <MAC addr> <WLAN id>
```

where <MAC addr> = client MAC address and <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

Use the show macfilter command to verify that you have MAC addresses assigned to WLANs.

#### Disable Timeout

Each WLAN can have a variable timeout for disabled clients (clients who fail to authenticate three times when attempting to associate are automatically blocked, or disabled, from further association attempts). After the disable timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is disabled again.

- Use the show wlan command to check the current WLAN Disable Timeout.
- If necessary, use the following command to change the Disable Timeout:

```
>config wlan blacklist <WLAN id> <timeout>
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), and <timeout> = 1 to 65535 seconds, 0 to disable (blacklist) permanently until the operator manually removes the disabling.

Use the show wlan command to verify the current WLAN Disable Timeout.

#### **VLANs**

- Note: WLANs are created in disabled mode; leave them disabled until you have finished configuring them.
- Note: WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="mailto:Appliance Mode">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.
  - Use the show wlan command to verify VLAN assignment status.
  - To assign a VLAN to a WLAN, use the following command:

>config wlan vlan <wlan id> [<default>/<untagged>/<VLAN ID> <IP Address>
<VLAN Netmask> <VLAN Gateway>]

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), <default> = use the VLAN configured on the network port, <untagged> = use VLAN 0, <VLAN id> = 1 through 4095, <IP Address> = the VLAN IP Address on the Alcatel OmniAccess Switch or Appliance, <VLAN Netmask> = VLAN local IP netmask, and <VLAN Gateway> = VLAN local IP gateway.

• To remove a VLAN assignment from a WLAN, use the following command:

```
>config wlan vlan <WLAN id> untagged
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

 Use the show wlan <wlan id> command to verify that you have correctly assigned a VLAN to the WLAN.

### **Layer 2 Security**

- Note: WLANs are created in disabled mode; leave them disabled until you have finished configuring them.
- Note: WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="https://example.com/Appliance-Mode">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.

# **Dynamic 802.1X Keys and Authorization**

Alcatel OmniAccess Switches and Appliances can control 802.1X dynamic keys using EAP (extended authorization protocol) across OmniAccess APs and third-party (foreign) APs, and supports 802.1X dynamic key settings for the OmniAccess AP WLAN(s).

- Use the **show wlan <wlan id>** command to check the security settings of each WLAN. The default for new WLANs is 802.1X with dynamic keys enabled. If you want to keep a robust Layer 2 policy, leave 802.1X on.
- If you want to change the 802.1X configuration, use the following commands:

```
>config wlan security 802.1X [enable/disable] <wlan id>
```

where <WLAN id> = 1 through 16, 17 = third-party AP WLAN ID (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

• If you want to change the 802.1X encryption for an OmniAccess AP WLAN (not a third-party WLAN), use the following command:

```
>config wlan security 802.1X encryption <wlan id> [40/104/128]
```

where <WLAN id> = 1 through 16, and [40/104/128] = 40/64, 104/128 (default) or 128/152 encryption bits (default = 104/128).

### **WEP Keys**

Alcatel OmniAccess Switches and Appliances can only control WEP keys across OmniAccess APs. Third-party APs control their own WEP keys, so there are no WEP settings for WLAN 17.

- Use the **show wlan <wlan id>** command to check the security settings of each WLAN. The default is 802.1X with dynamic keys enabled.
- If you want to configure the less-robust WEP (Wired Equivalent Privacy) authorization policy, turn 802.1X off:

```
>config wlan security 802.1X disable <wlan id>
```

where <wlan id> = 1 through 16.

• Then configure 40/64, 104/128 or 128/152 bit WEP keys on 802.1X disabled WLANs using the following command:

>config wlan security static-wep-key encryption <wlan id> [40/104/128] [hex/ascii] <key> <key-index>

### where:

- <wlan id> = 1 through 16;
- [hex/ascii] = key character format;
- <key> = Ten hexadecimal digits (any combination of 0-9, a-f, or A-F), or five printable ASCII characters for 40-bit/64-bit WEP keys, 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys, or 32 hexadecimal or 16 ASCII characters for 128-bit/152-bit keys; and
- <key-index> = 1 through 4.
- Note: One unique WEP Key Index can be applied to each WLAN. Because there are only four <key-index> numbers, only four WLANs can be configured for Static WEP Layer 2 encryption. Also note that some legacy clients can only access Key Index 1 through 3 but cannot access Key Index 4.

# **Dynamic WPA Keys and Encryption**

Alcatel OmniAccess Switches and Appliances can only control WPA (Wi-Fi Protected Access) authorization policy across OmniAccess APs. Third-party (foreign) APs control their own authorization policies, so there are no WPA settings for the third-party AP WLAN 17.

- Use the show wlan <wlan id> command to check the security settings of each WLAN. The
  default is 802.1X with dynamic keys enabled.
- If you want to configure the more-robust WPA authorization policy, turn 802.1X off:

```
>config wlan security 802.1% disable <wlan id>
```

where <wlan id> = 1 through 16.

- Then configure authorization and dynamic key exchange on 802.1X disabled WLANs using the following commands:
  - >config wlan security wpa enable <wlan id>
  - >config wlan security wpa encryption aes-ocb <wlan id>
  - >config wlan security wpa encryption tkip <wlan id>
  - >config wlan security wpa encryption wep <wlan id> [40/104/128]

where <wlan id> = 1 through 16, and [40/104/128] = 40/64, 104/128, or 128/156 encryption bits (default = 104).

Use the show wlan command to verify that you have WPA enabled.

# **Layer 3 Security**

- Note: WLANs are created in disabled mode; leave them disabled until you have finished configuring them.
- Note: Using Layer 3 security requires that the Alcatel OmniAccess Switch or Appliance be equipped with an Enhanced Security Module (Crypto Module). The ESM plugs into the rear of the 4012 or 4024 OmniAccess Wireless Switch or is factory-installed in the 4102 OmniAccess Wireless Switch, and provides the extra processing power needed for processor-intensive security algorithms.
- Note: WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="#">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.

#### **IPSec**

IPSec (Internet Protocol Security) supports many Layer 3 security protocols.

- Use the **show wlan** command to show the current IPSec configuration.
- Use the following command to enable IPSec on a WLAN:

```
>config wlan security ipsec [enable/disable] <WLAN id>
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

• Use the **show wlan** command to verify that you have IPSec enabled.

# **IPSec Authentication**

IPSec uses hmac-sha-1 authentication as the default for encrypting WLAN data, but can also use hmac-md5, or no authentication.

- Use the show wlan command to view the current IPSec authentication protocol.
- Use the following command to configure the IPSec IP authentication:

>config wlan security ipsec authentication [hmac-md5/hmac-sha-1/none] <WLAN id>

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

Use the show wlan command to verify that you have correctly set the IPSec authentication.

# **IPSec EncryptionI**

IPSec uses 3DES encryption as the default for encrypting WLAN data, but can also use AES, DES, or no encryption.

- Use the show wlan command to view the current IPSec encryption.
- Use the following command to configure the IPSec encryption:
  - >config wlan security ipsec encryption [3des/aes/des/none] <WLAN id> where aes= AES-CBC, and where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).
- Use the show wlan command to verify that you have correctly set the IPSec encryption.

#### **IKE Authentication**

IPSec IKE (Internet Key Exchange) uses pre-shared key exchanges, x.509 (RSA Signatures) certificates, and XAuth-psk for authentication.

- Use the show wlan command to see if IPSec IKE is enabled.
- Use the following commands to configure IKE authentication on a WLAN with IPSec enabled:
  - >config wlan security ipsec ike authentication certificates <wlan id>
  - >config wlan security ipsec ike authentication xauth-psk <wlan id> <key>
  - >config wlan security ipsec ike authentication pre-shared-key <wlan id> <key>

where <wlan id> = 1 through 16 or 17 (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), certificates = RSA signatures, xauth-psk = XAuth pre-shared key, and <key> = Preshared Key (Eight to 255 ASCII characters, case sensitive).

• Use the show wlan command to verify that you have IPSec IKE enabled.

#### **IKE Diffie-Hellman Group**

IPSec IKE uses Diffie-Hellman groups to block easily-decrypted keys.

- Use the show wlan command to verify whether or not the Alcatel OmniAccess Switch or Appliance has IPSec IKE DH Groups properly set.
- Use the following command to configure the IKE Diffie-Hellman group on a WLAN with IPSec enabled:

```
>config wlan security ipsec ike DH-Group <WLAN id> <group-id>
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode); <group-id> = group-1, group-2 (default), or group-5.

• Use the **show wlan** command to verify that the Alcatel OmniAccess Switch or Appliance has IPSec IKE DH Groups properly set.

### **IKE Phase 1 Aggressive and Main Modes**

IPSec IKE uses the Phase 1 Aggressive (faster) or Main (more secure) mode to set up encryption between clients and the Alcatel OmniAccess Switch or Appliance.

- Use the **show wlan** command to see if the Alcatel OmniAccess Switch or Appliance has IPSec IKE Aggressive mode enabled.
- If necessary, use the following command to configure the IKE Aggressive or Main mode on a WLAN with IPSec enabled:
  - >config wlan security ipsec ike phase1 [aggressive/main] <WLAN id>

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

 Use the show wlan command to verify that you have IPSec IKE Aggressive or Main mode enabled.

#### **IKE Lifetime Timeout**

IPSec IKE uses its timeout to limit the time that an IKE key is active.

- Use the show wlan command to see the current IPSec IKE lifetime timeout.
- Use the following command to configure the IKE lifetime on a WLAN with IPSec enabled:
  - >config wlan security ipsec ike lifetime <WLAN id> <seconds>

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), and <seconds> = 1800 through 345600 seconds (default = 28800 seconds).

Use the show wlan command to verify that you have IPSec IKE timeout properly set.

### **IPSec Passthrough**

IPSec IKE uses IPSec Passthrough to allow IPSec-capable clients to communicate directly with other IPSec equipment. IPSec Passthrough is also known as VPN Passthrough.

- Use the **show wlan** command to see the current IPSec passthrough status.
- Use the following command to configure IKE passthrough for a WLAN:
  - >config wlan security passthru [enable/disable] <WLAN id> [gateway]

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode), and [gateway] = IP Address of IPSec (VPN) passthrough gateway.

Use the show wlan command to verify that you have IPSec passthrough properly set.

#### Web Based Authentication

WLANs can use Web Authentication if IPSec is not enabled on the Alcatel OmniAccess Switch or Appliance. Web Authentication is simple to set up and use, and can be used with SSL to improve the overall security of the wireless LAN.

- Use the **show wlan** command to see the current Web Authentication status.
- Use the following command to configure Web Authentication for a WLAN:
  - >config wlan security web [enable/disable] <WLAN id>

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

Use the show wlan command to verify that you have Web Authentication properly set.

### **Local Netuser**

**Note:** WLANs are created in disabled mode; leave them disabled until you have finished configuring them.

Alcatel OmniAccess Switches and Appliances have built-in network client authentication capability, similar to that provided by a RADIUS authentication server.

- Use the show netuser command to see if the Alcatel OmniAccess Switch or Appliance has network client names assigned to WLANs.
- If required, use the following commands to assign a network client name and password to a particular WLAN, delete a network client, assign a network client password, and assign a network client name to a WLAN without a password:

```
>config netuser add <username> <password> <WLAN id>
```

- >config netuser delete <username>
- >config netuser password <username> <password>
- >config netuser wlan-id <username> <WLAN id>

where <WLAN id> = 1 through 16.

Use the show netuser command to verify that you have net user names assigned to WLANs.

# **Quality of Service**

- Note: WLANs are created in disabled mode; leave them disabled until you have finished configuring them.
- Note: WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="mailto:Appliance Mode">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.

Alcatel OmniAccess Wireless System WLANs support three levels of QoS: Gold/high, Silver/medium and Bronze/low (default). Network administrators can choose to assign the voice traffic WLAN to use Gold QoS, assign the Instant Messaging WLAN to use Bronze QoS, and assign all other traffic between the three QoS levels.

- Use the show wlan command to verify that you have QoS properly set for each WLAN.
- If required, use the following command to configure QoS for each WLAN:

```
>config wlan qos <WLAN id> [bronze/silver/gold]
```

where <WLAN id> = 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode).

Use the show wlan command to verify that you have QoS properly set for each WLAN.

### **Activating WLANs**

After you have completely configured your WLAN settings, activate the WLAN using the config wlan enable command.

Note: Remember that WLAN 17 is only available for third-party APs connected directly to 4012 and 4024 OmniAccess Wireless Switch front-panel connectors. Because the 4102 OmniAccess Wireless Appliances operate exclusively in <a href="mailto:Appliance Mode">Appliance Mode</a>, WLAN 17 cannot be activated for these OmniAccess Wireless Appliances.

Continue with Configuring Mobility Groups.

# **Configuring Mobility Groups**

All Alcatel OmniAccess Wireless Switches and Appliances that can communicate with each other through their Distribution System (network) ports can automatically discover each other and form themselves into groups. Once they are grouped, the Alcatel OmniVista AirView Software function maximizes its inter-Alcatel OmniAccess Switch and Appliance processing efficiency and mobility processing, described in the <u>Client Roaming</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

Alcatel OmniAccess Switch and Appliance group discovery is automatically enabled when two or more members are assigned to the same mobility group name. Note that this feature must be enabled on each Alcatel OmniAccess Switch and Appliance to be included in the discovery process.

- Use the **show mobility summary** command to verify the current Alcatel OmniAccess Switch and Appliance mobility settings.
- To give a Mobility Group a name, use the following command:

```
>config mobility group name <group_name>
```

where <group\_name> = Any ASCII character string, up to 31 characters, case sensitive, with no spaces.

To manually add or delete members to a mobility group, use the following commands:

```
>config mobility group member add <mac-address> <IP addr>
>config mobility group member delete <mac-address> <IP addr>
```

where <mac-address> is the MAC address and where <IP addr> is the IP Address of the group member to be added or deleted.

Use the **show mobility summary** commands to verify that the Alcatel OmniAccess Switch or Appliance mobility is set up correctly. Continue with <u>Configuring RADIUS</u>.

# **Configuring RADIUS**

• When your Alcatel OmniAccess Wireless System is to use an external RADIUS server for accounting and/or authentication, set up the links using the following commands. If you are not configuring RADIUS links at this time, continue with <u>Configuring SNMP</u>.

```
>config radius acct <address>
>config radius acct <port>
>config radius acct <secret>
>config radius acct [disable/enable]
>config radius auth <address>
>config radius auth <port>
>config radius auth <secret>
>config radius auth [disable/enable]
```

where <address> = server name or IP Address, <port> = UDP port number, <secret> = the RADIUS server's secret.

When you have completed these configurations, use the show radius acct statistics, show radius auth statistics and show radius summary commands to verify that the RADIUS links are correctly configured. Continue with <u>Configuring SNMP</u>.

# **Configuring SNMP**

 When your Alcatel OmniAccess Wireless System is to send SNMP protocol to the OmniVista Air Control System Software or any other SNMP manager, configure the SNMP environment using the following commands. If you are not configuring SNMP traps at this time, continue with Configuring Other Ports and Parameters.

```
>config snmp community accessmode <ro/rw> <name>
>config snmp community create <name>
>config snmp community delete <name>
>config snmp community ipaddr <ipaddr> <ipmask> <name>
>config snmp community mode [enable/disable]
>config snmp trapreceiver create <name> <ipaddr>
>config snmp trapreceiver delete <name>
>config snmp trapreceiver ipaddr <old ipaddr> <name> <new ipaddr>
>config snmp trapreceiver mode [enable/disable]
>config snmp syscontact <syscontact name>
>config snmp syslocation <syslocation name>
```

where <ro/rw> = read only/read-write, <name> = SNMP community name, <ipaddr> = SNMP community IP Address, <ipmask> = SNMP community IP mask, <old ipaddr> = old SNMP IP Address, <new ipaddr> = new SNMP IP Address, <syscontact name> = system contact, up to 31 alphanumeric characters, <syslocation name> = system location, up to 31 alphanumeric characters.

When you have completed these configurations, use the **show snmpcommunity** and **show snmptrap** commands to verify that the SNMP traps and communities are correctly configured.

Also use the **show trapflags** command to see the enabled and disabled trapflags. If necessary, use the **config trapflags** commands to enable and disable any or all trapflags.

Continue with Configuring Other Ports and Parameters.

# **Configuring Other Ports and Parameters**

Use the following sections to configure the remaining Alcatel OmniAccess Wireless Switch or Appliance ports and parameters:

- Service Port
- OmniVista AirView Software
- Serial (CLI Console) Port
- 802.3x Flow Control
- System Logging

#### **Service Port**

The Service port on the Alcatel OmniAccess Switch or Appliance front panel can be configured with a separate IP Address, subnet mask, and IP assignment protocol from the Distribution System (network) port. To display and configure the Service port parameters, use the following commands:

```
>show serviceport
>config serviceport params
>config serviceport protocol
```

# **OmniVista AirView Software**

 The Alcatel Wireless Operating System OmniVista AirView Software function automatically recognizes OmniAccess APs as they appear in the air space, and when they are part of the same <u>Alcatel Mobility Group</u>, automatically configures them for optimal operation in their respective frequency bands. Typically, you will not need to manually configure anything after enabling and/or disabling the 802.11a and 802.11b/g networks as described in <u>Configuring System Parameters</u>. However, you may want to fine-tune the network operation using the config 802.11a, config 802.11b, config advanced 802.11a, config advanced 802.11b, config cell, and config load balancing command sets.

# Serial (CLI Console) Port

• The Alcatel OmniAccess Switch or Appliance front-panel serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, use the config serial baudrate and config serial timeout commands to make your changes. Note that if you enter config serial timeout 0, serial sessions never time out.

### 802.3x Flow Control

 802.3x Flow Control is normally disabled on the Alcatel OmniAccess Switch and Appliance. If you would like to change either of these settings, use the config switchconfig flowcontrol command.

# **System Logging**

Alcatel OmniAccess Switches and Appliances are shipped with the syslog function disabled. Use
the show syslog command to view the current syslog status, and if required, use the config
syslog command to send an Alcatel OmniAccess Switch or Appliance log to a remote IP
Address or hostname.

You have configured the basic parameters for an Alcatel OmniAccess Wireless System. Continue with *Using the Alcatel OmniAccess Wireless System CLI*.

# Transferring Files To and From an Alcatel OmniAccess Switch or Appliance

The Alcatel OmniAccess Wireless Switch and Appliance have built-in utilities for uploading and downloading Alcatel Wireless Operating System software, certificate and configuration files. Refer to the following for additional information.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

• Use the CLI **transfer** commands to perform these actions:

```
>transfer download datatype
>transfer download filename
>transfer download mode
>transfer download path
>transfer download serverip
>transfer download start
>transfer upload datatype
>transfer upload filename
>transfer upload mode
>transfer upload serverip
>transfer upload serverip
>transfer upload serverip
>transfer upload start
```

Continue with *Using the Alcatel OmniAccess Wireless System CLI*.

# **Updating the Alcatel Wireless Operating System Software**

When you plan to update the Alcatel OmniAccess Wireless Switch and Appliance (and OmniAccess AP) Alcatel Wireless Operating System software, complete the following.

- Note: You can start the Alcatel Wireless Operating System software update using the <u>Alcatel Web Browser Interface</u>, or <u>Management over Wireless</u>. However, in all three cases, you will lose your connection to the Alcatel OmniAccess Switch or Appliance some time during the update process. For this reason, Alcatel strongly recommends that you use a direct CLI Console Port connection to update the Alcatel Wireless Operating System software.
  - Make sure you have a TFTP server available for the Alcatel Wireless Operating System software download.
    - If you are downloading through the Service port, the TFTP server MUST be on the same subnet as the Service port, because the Service port is not routable.
    - If you are downloading through the DS (Distribution System) network port, the TFTP server can be on the same or a different subnet, because the DS port is routable.
- Note: The TFTP server cannot run on the same computer as the <u>OmniVista Air Control System Software</u>, because the ACS Software and the TFTP server use the same communication port.
- Download the desired Alcatel Wireless Operating System software update file from the Alcatel website to the default directory on your TFTP server.
  - The Alcatel Wireless Operating System code update file is named ALCATEL\_<release\_number>.aes. (For example, ALCATEL\_2\_0\_60\_0.aes.)
- Refer to the <u>Using the Alcatel OmniAccess Wireless System CLI</u> section to connect and use the CLI.
- In the CLI, use the ping <IP Address command to ensure the Alcatel OmniAccess Switch or Appliance can contact the TFTP server.
- In the CLI, use the **transfer download start** command, and answer 'n' to the prompt, to view the current download settings:

To change the download settings, use the following:

```
>transfer download mode tftp
>transfer download datatype code
>transfer download serverip <TFTP server IP address>
>transfer download filename ALCATEL_<release_number>.aes
>transfer download path <absolute TFTP server path to the update file>
```

Note: Some TFTP servers require only a forward slash "/" as the <TFTP server IP address>, and the TFTP server automatically determines the path to the correct directory.

• In the CLI, use the transfer download start command to view the updated settings, and answer 'y' to the prompt to confirm the current download settings and start the Alcatel Wireless Operating System code download:

## >transfer download start

• The Alcatel OmniAccess Switch or Appliance now has the code update in active volatile RAM, but you must save the code update to non-volatile NVRAM and reboot the Alcatel OmniAccess Switch or Appliance:

```
>reset system
```

```
The system has unsaved changes. Would you like to save them now? (y/n) {\bf y}
```

The Alcatel OmniAccess Switch or Appliance completes the bootup process as described in Step 5: Performing Power On Self Test in the Alcatel OmniAccess Switch and Appliance Quick Installation Guide.

Note: If you wish to run a previous version of the Alcatel OmniAccess Switch or Appliance code, follow the instructions in <u>Step 4: Connecting and Using the CLI Console</u> in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u>.

Refer to the <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u> section for other file upload and download instructions.

# **Using the Startup Wizard**

When an Alcatel OmniAccess Wireless Switch or Appliance is powered up with a new factory Alcatel Wireless Operating System software load or after being reset to factory defaults, the bootup script runs the <u>Startup Wizard</u>, which prompts the installer for initial Alcatel OmniAccess Switch or Appliance configuration.

**Note:** To reset the Alcatel OmniAccess Switch or Appliance to factory defaults and rerun the Startup Wizard, refer to *Erasing the Alcatel OmniAccess Switch or Appliance Configuration*.

Use the Startup Wizard to do the following:

- Enter the System (Alcatel OmniAccess Switch or Appliance) Name, up to 32 printable ASCII characters.
- Enter the Administrative User Name and Password, each up to 24 printable ASCII characters. The default Administrative User login and password are admin and admin, respectively.

- Note: The <u>Service-Port Interface</u> and <u>Management Interface</u> must be on different subnets.
  - Enter the <u>Service-Port Interface</u> IP configuration protocol (none, or DHCP). If you do not want to use the Service port or if you want to assign a static IP Address to the Service port, enter none.

If you entered none, enter <u>Service-Port Interface</u> IP Address and netmask on the next two lines. If you do not want to use the Service port, enter 0.0.0.0 for the IP Address and netmask.

- Enter the <u>Management Interface</u> IP Address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier, or '0' for untagged).
- Network Interface (Distribution System) Physical Port number:
  - \* 4012: 1 12 for front panel or 13 for GigE port
  - \* 4024: 1 24 for front panel or 25 for GigE port
  - \* 4102: 1 or 2 for the front panel GigE port
- Enter the IP address of the default DHCP Server that will supply IP Addresses to clients, the Alcatel OmniAccess Switch or Appliance Management Interface, and optionally to the Service Port Interface.
- Enter the LWAPP Transport Mode, LAYER2 or LAYER3 (refer to <u>Layer 2 and Layer 3 Operation</u>).
- Enter the Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Enter the <u>Alcatel Mobility Group</u> (RF Group) Name.
- Enter the WLAN 1 SSID, or Network Name. This is the default SSID that the OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points, or OmniAccess 1200R APs, broadcast when they associate with the Alcatel OmniAccess Switch or Appliance.
- Allow or disallow Static IP Addresses for clients. (Yes = clients can supply their own IP Address. No = clients must request an IP Address from a DHCP server.)
- If you are configuring a RADIUS Server now, enter YES, and the RADIUS Server IP Address, communication port, and Secret. Otherwise, enter NO.
- Enter the Country Code for this installation. Type 'help' to list the supported countries, and refer to <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> and <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u>.
- Independently enable and/or disable the 802.11b, 802.11a, and 802.11g OmniAccess AP networks.
- Enable or disable the *OmniVista AirView Software* (Auto RF).

The Alcatel OmniAccess Switch or Appliance saves your configuration, reboots with your changes, and prompts you to log in or enter 'Recover-Config' to reset the Alcatel OmniAccess Switch or Appliance to factory default configuration and return to the Startup Wizard.

Continue with Using the Alcatel OmniAccess Wireless System CLI.

# Adding SSL to the Web Browser Interface

When you plan to secure the Alcatel OmniAccess Wireless Switch or Appliance HTTP: Web Browser Interface using the https: (HTTP + SSL) protocol, note that the Alcatel Wireless Operating System automatically generates its own local Web Administration SSL certificate and automatically applies it to the Web Browser Interface. Verify whether or not the locally-generated Web Administration certificate is already loaded:

>show certificate summary
Web Administration Certificate..... Locally Generated

```
Web Authentication Certificate...... Locally Generated Certificate compatibility mode:..... off
```

Continue with either of the following two sections:

- Locally-Generated Certificate or an
- Externally-Generated Certificate.

### **Locally-Generated Certificate**

Should you desire to have the Alcatel Wireless Operating System generate a new Web Administration SSL certificate, complete the following:

In the CLI, enter:

```
>config certificate generate webadmin
```

Wait a few seconds, and the Alcatel OmniAccess Switch or Appliance returns:

```
Web Administration certificate has been generated
```

Verify that the Web Administration certificate is properly loaded:

```
>show certificate summary
```

```
Web Administration Certificate.......... Locally Generated Web Authentication Certificate........... Locally Generated Certificate compatibility mode:.......... off
```

Enable Secure Web mode:

```
>config network secureweb enable
```

 Save the SSL certificate, key and secure web password in active working memory to NVRAM (non-volatile RAM) so your changes are retained across reboots:

```
>save config
```

```
Are you sure you want to save? (y/n) \mathbf{y} Configuration Saved!
```

Reboot the Alcatel OmniAccess Switch or Appliance:

```
>reset system
```

```
Are you sure you would like to reset the system? (y/n) \boldsymbol{y} System will now restart!
```

The Alcatel OmniAccess Switch or Appliance completes the bootup process as described in <u>Step 4: Connecting and Using the CLI Console</u> in the <u>Alcatel OmniAccess Switch and Appliance</u> <u>Ouick Installation Guide</u>.

Make sure that operators using the Web Browser Interface know that they may securely log into the Alcatel OmniAccess Switch or Appliance using "https://<Alcatel OmniAccess Switch or Appliance IPaddress>.

Refer to the *Transferring Files To and From an Alcatel OmniAccess Switch or Appliance* section for other file upload and download instructions.

## **Externally-Generated Certificate**

Should you desire to use your own Web Administration SSL certificate, complete the following:

- Make sure you have a TFTP server available for the certificate download:
  - If you are downloading through the Service port, the TFTP server MUST be on the same subnet as the Service port, because the Service port is not routable.

- If you are downloading through the DS (Distribution System) network port, the TFTP server can be on the same or a different subnet, because the DS port is routable.
- Note: The TFTP server cannot run on the same computer as the <u>OmniVista Air Control System Software</u>, because the ACS Software and the TFTP server use the same communication port.
- CAUTION: Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.
- Buy or create your own Web Administration SSL key and certificate. If not already done, use a
  password, <private\_key\_password>, to encrypt the key and certificate in a .PEM encoded file.
  The PEM-encoded file is called a Web Administration Certificate file
  (<webadmincert\_name>.pem).
- Move the <webadmincert\_name>.pem file to the default directory on your TFTP server.
- Refer to the <u>Using the Alcatel OmniAccess Wireless System CLI</u> section to connect and use the CLI.
- In the CLI, use the transfer download start command, and answer 'n' to the prompt, to view the current download settings:

>transfer download start					
Mode	TFTP				
Data Type	Admin Cert				
TFTP Server IP	xxx.xxx.xxx				
TFTP Path	<directory path=""></directory>				
TFTP Filename					
Are you sure you want to start? (y/n) $\boldsymbol{n}$					
Transfer Canceled					

- To change the download settings, use the following:
  - >transfer download mode tftp
  - >transfer download datatype webauthcert
  - >transfer download serverip <TFTP server IP address>
  - >transfer download path <absolute TFTP server path to the update file>
  - >transfer download filename <webadmincert name>.pem
- Note: Some TFTP servers require only a forward slash "/" as the <TFTP server IP address>, and the TFTP server automatically determines the path to the correct directory.
  - Enter the password for the .PEM file, so Alcatel Wireless Operating System can decrypt the Web Administration SSL key and certificate:

```
>transfer download certpassword password>>Setting password to password>
```

• In the CLI, use the transfer download start command to view the updated settings, and answer 'y' to the prompt to confirm the current download settings and start the certificate and key download:

# Mode... TFTP Data Type... Site Cert TFTP Server IP. xxx.xxx.xxx TFTP Path. <directory path> TFTP Filename. <webadmincert\_name>

```
Are you sure you want to start? (y/n) y

TFTP Webadmin cert transfer starting.

Certificate installed.

Please restart the switch (reset system) to use the new certificate.
```

· Verify that the Web Administration certificate is properly loaded:

#### >show certificate summary

```
Web Administration Certificate...... Locally Generated Web Authentication Certificate...... Locally Generated Certificate compatibility mode:..... off
```

Enable Secure Web mode:

#### >config network secureweb enable

 Save the SSL certificate, key and secure web password in active working memory to NVRAM (non-volatile RAM) so your changes are retained across reboots:

#### >save config

```
Are you sure you want to save? (y/n) {\bf y} Configuration Saved!
```

Reboot the Alcatel OmniAccess Switch or Appliance:

#### >reset system

```
Are you sure you would like to reset the system? (y/n) \boldsymbol{y} System will now restart!
```

The Alcatel OmniAccess Switch or Appliance completes the bootup process as described in Step 4: Connecting and Using the CLI Console in the Alcatel OmniAccess Switch and Appliance Quick Installation Guide.

 Make sure that operators using the Web Browser Interface know that they may securely log into the Alcatel OmniAccess Switch or Appliance using "https://<Alcatel OmniAccess Switch or Appliance\_IPaddress>.

Refer to the <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u> section for other file upload and download instructions.

# Adding SSL to the 802.11 Interface

When you plan to use a WebAuth certificate to secure the Alcatel OmniAccess Wireless Switch or Appliance when associating new clients, note that the Alcatel Wireless Operating System automatically generates its own local Web Authentication SSL certificate and automatically applies them to the 802.11 Interface. Verify whether or not the locally-generated Web Authentication certificate is already loaded:

## >show certificate summary

```
Web Administration Certificate........... Locally Generated Web Authentication Certificate............ Locally Generated Certificate compatibility mode:........... off
```

Continue with one of the following two sections to add a <u>Locally-Generated Certificate</u> or an <u>Externally-Generated Certificate</u>.

## **Locally-Generated Certificate**

Should you desire to have the Alcatel Wireless Operating System generate another Web Authentication SSL certificate, complete the following:

In the CLI, enter:

#### >config certificate generate webauth

Wait a few seconds, and the Alcatel OmniAccess Switch or Appliance returns:

```
Web Authentication certificate has been generated
```

Verify that the Web Administration certificate is properly loaded:

```
>show certificate summary
```

```
Web Administration Certificate...... Locally Generated Web Authentication Certificate...... Locally Generated Certificate compatibility mode:..... off
```

 Save the SSL certificate, key and secure web password in active working memory to NVRAM (non-volatile RAM) so your changes are retained across reboots:

```
>save config
```

```
Are you sure you want to save? (y/n) {\bf y} Configuration Saved!
```

Reboot the Alcatel OmniAccess Switch or Appliance:

```
>reset system
```

```
Are you sure you would like to reset the system? (y/n) {\bf y} System will now restart!
```

The Alcatel OmniAccess Switch or Appliance completes the bootup process as described in <u>Step 4: Connecting and Using the CLI Console</u> in the <u>Alcatel OmniAccess Switch and Appliance</u> <u>Quick Installation Guide</u>.

 Make sure that client operators know that they may securely associate with the Alcatel OmniAccess Wireless System.

Refer to the *Transferring Files To and From an Alcatel OmniAccess Switch or Appliance* section for other file upload and download instructions.

## **Externally-Generated Certificate**

Should you desire to use your own WebAuth SSL certificates, complete the following:

- Make sure you have a TFTP server available for the Alcatel Wireless Operating System software download:
  - If you are downloading through the Service port, the TFTP server MUST be on the same subnet as the Service port, because the Service port is not routable.
  - If you are downloading through the DS (Distribution System) network port, the TFTP server can be on the same or a different subnet, because the DS port is routable.
- Note: The TFTP server cannot run on the same computer as the <u>OmniVista Air Control System Software</u>, because the ACS Software and the TFTP server use the same communication port.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

• Buy or create your own WebAuth SSL key and certificate. If not already done, encode the key and certificate, virtual gateway IP Address, and a password, <private\_key\_password>, in a .PEM formatted file. The PEM-encoded file is called a WebAuth Site Certificate file (<webauthcert\_name>.pem).

- Move the <webadmincert\_name>.pem file to the default directory on your TFTP server.
- Refer to the <u>Using the Alcatel OmniAccess Wireless System CLI</u> section to connect and use the CLI.
- In the CLI, use the **transfer download start** command, and answer 'n' to the prompt, to view the current download settings:

#### >transfer download start

- To change the download settings, use the following:
  - >transfer download mode tftp
  - >transfer download datatype webauthcert
  - >transfer download serverip <TFTP server IP address>
  - >transfer download path <absolute TFTP server path to the update file>
  - >transfer download filename <webauthcert\_name>.pem
- Note: Some TFTP servers require only a forward slash "/" as the <TFTP server IP address>, and the TFTP server automatically determines the path to the correct directory.
  - Enter the password included in the .PEM file, so the Alcatel Wireless Operating System can decode the Web Administration SSL key and certificate:

```
>transfer download certpassword password>
>Setting password to password>
```

• In the CLI, use the transfer download start command to view the updated settings, and answer 'y' to the prompt to confirm the current download settings and start the certificate and key download:

## >transfer download start

Verify that the Web Administration certificate is properly loaded:

# >show certificate summary

Web	Administration	Certificate	Locally	Generated
Web	Authentication	Certificate	Locally	Generated
Cert	ificate compati	bility mode:	off	

 Save the SSL certificate, key and secure web password in active working memory to NVRAM (non-volatile RAM) so your changes are retained across reboots:

```
>save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Reboot the Alcatel OmniAccess Switch or Appliance:

```
>reset system  
   Are you sure you would like to reset the system? (y/n) {\bf y}   
   System will now restart!
```

The Alcatel OmniAccess Switch or Appliance completes the bootup process as described in <u>Step 4: Connecting and Using the CLI Console</u> in the <u>Alcatel OmniAccess Switch and Appliance</u> <u>Ouick Installation Guide</u>.

 Make sure that client operators know that they may securely associate with the Alcatel OmniAccess Wireless System.

Refer to the <u>Transferring Files To and From an Alcatel OmniAccess Switch or Appliance</u> section for other file upload and download instructions.

# **Saving Configurations**

As described in <u>Alcatel OmniAccess Switch and Appliance Memory</u>, the Alcatel OmniAccess Wireless Switches and Appliances contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to non-volatile RAM (NVRAM) using one of three commands:

- Use the save config command as detailed below.
- Use the reset system command, described in <u>Resetting the Alcatel OmniAccess Switch or Appliance</u>, which will ask you whether you would like to save configuration changes before the system reboots.
- Use the logout command, described in Logging Out of the CLI, which asks you whether you
  would like to save configuration changes before logging out.

To save the configurations without resetting the Alcatel OmniAccess Switch or Appliance or logging out of the CLI, type:

```
> save config  
 Are you sure you want to save? (y/n)
```

Enter 'y' to save the current configurations from volatile RAM to non-volatile RAM (NVRAM).

You can now continue using the system, log out, or reboot knowing that the Alcatel OmniAccess Switch or Appliance will come up in the same configuration after reboot.

Continue with <u>Using the Alcatel OmniAccess Wireless System CLI</u>.

# **Clearing Configurations**

As described in <u>Alcatel OmniAccess Switch and Appliance Memory</u>, the Alcatel OmniAccess Wireless Switch and Appliance contain two kinds of memory: volatile RAM and NVRAM. To clear the active configuration in the non-volatile RAM, complete the following.

• To clear the Alcatel OmniAccess Switch or Appliance configuration from non-volatile RAM, use the clear config command:

#### >clear config

Are you sure you want to clear the configuration? (y/n)

Enter 'y' to clear the current configurations from non-volatile RAM.

After clearing the Alcatel OmniAccess Switch or Appliance configuration in NVRAM, perform a "Reboot without Save":

```
>reset system
```

```
The system has unsaved changes.
Would you like to save them now? (y/n)
```

Enter "n" to reset the Alcatel OmniAccess Switch or Appliance without saving any outstanding configuration changes from volatile RAM to non-volatile RAM.

When the Alcatel OmniAccess Switch or Appliance reboots, the Alcatel Wireless Operating System displays the Startup Wizard.

Continue with Using the Alcatel OmniAccess Wireless System CLI.

# Erasing the Alcatel OmniAccess Switch or Appliance Configuration

The Wireless LAN operator may wish to move an Alcatel OmniAccess Wireless Switch or Appliance to a different location and reconfigure it.

If the moved Alcatel OmniAccess Switch or Appliance uses the same or nearly the same configuration, use the OmniVista Air Control System Software, Alcatel Web Browser Interface, or Command Line Interface to reconfigure individual Alcatel OmniAccess Switch or Appliance parameters.

If the moved Alcatel OmniAccess Switch or Appliance uses a significantly different configuration, erase the Alcatel OmniAccess Switch or Appliance configuration using the following procedure.

- Enter the reset system command. The reset script prompts you if there are any unsaved changes. Enter 'y' to save changes from active volatile RAM to NVRAM before rebooting the Alcatel OmniAccess Switch or Appliance.
  - The Alcatel OmniAccess Switch or Appliance reboots.
- When you are prompted for a User Name, enter recover-config to restore the factory default configurations.
  - The Alcatel OmniAccess Switch or Appliance reboots and displays the Welcome to the Alcatel Wizard Configuration Tool message.
- Enter the initial configuration of the Alcatel OmniAccess Switch or Appliance as described in Using the Startup Wizard.

Continue with Using the Alcatel OmniAccess Wireless System CLI.

# Resetting the Alcatel OmniAccess Switch or Appliance

After you have installed and configured an Alcatel OmniAccess Switch or Appliance, you can reset the Alcatel OmniAccess Switch or Appliance and view the reboot process on the CLI Console using one of the following two methods:

- Unplug the Alcatel OmniAccess Switch or Appliance from its power source.
- Enter the reset system command. The reset script prompts you if there are any unsaved changes. Enter 'y' to save changes from active volatile RAM to NVRAM (non-volatile RAM) before rebooting the Alcatel OmniAccess Switch or Appliance.

**Note:** If you have already cleared the active volatile RAM as described in <u>Clearing Configurations</u>, entering 'n' in response to this prompt prevents the volatile RAM to NVRAM (non-volatile RAM) from overwriting the cleared configuration in NVRAM. In this case you will be directed to the <u>Startup Wizard</u>.

When the Alcatel OmniAccess Switch or Appliance reboots, the CLI Console displays the following reboot information:

- Initializing the system.
- Verifying the hardware configuration.
- Loading microcode into memory.
- Verifying the Alcatel Wireless Operating System software load.
- Initializing with its stored configurations.
- Displaying the login prompt.

You have seen the boot process on the CLI Console. Either unplug your serial connection, or enter a valid login and password to reenter the CLI.

Continue with <u>Using the Alcatel OmniAccess Wireless System CLI</u>.

# **Using the OmniVista Air Control System Software**

Refer to the following to start, stop, use, and manage ACS Software:

- Starting and Stopping ACS Software
- Configuring the ACS Software Browser Client
- Viewing System Status
- Troubleshooting with ACS Software
- Managing ACS Software and Database

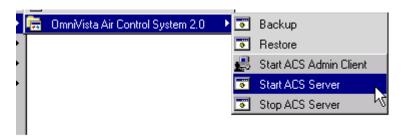
# **Starting and Stopping ACS Software**

- Starting an ACS Software Server as an Application
- Starting the ACS Software Server as a Service
- <u>Stopping the ACS Software Server Application</u>
- Stopping the ACS Software Service
- Checking the ACS Software Service Status
- Starting an ACS Software Browser Client
- Starting an ACS Software Java Admin Client
- Stopping an ACS Software Browser Client
- Stopping an ACS Software Java Admin Client

# Starting an ACS Software Server as an Application

When ACS Software Server has been installed as an application, you can start the ACS Software Server application at any time.

From the Windows **START** button, select the **Programs** menu, and click **OmniVista Air Control System 2.0/Start ACS Server**.



04031151

The start ACS Software Server script opens a **Start ACS Server** DOS window, which displays many Created table and Process: Started messages.

When the **Start ACS Server** window displays Please connect your client to the web server on port 80, the ACS Software Server has started and is ready to host ACS Software Clients.



**CAUTION:** The ACS Software Server may display **Start ACS Server**, **Solid Database**, and **Apache** windows, which you can minimize. DO NOT CLOSE any of these windows, or you can abnormally halt the ACS Software Server. When you plan to shut down the ACS Software Server, refer to <u>Stopping the ACS Software Server Application</u> or <u>Stopping the ACS Software Service</u>.

If desired, continue with **Starting and Stopping ACS Software**.

## Starting the ACS Software Server as a Service

After ACS Software Server has been installed as a service, you can start the ACS Software Server service at any time.

 From the Windows START button, select the Programs menu, and select OmniVista Air Control System 2.0/Start ACS Service.

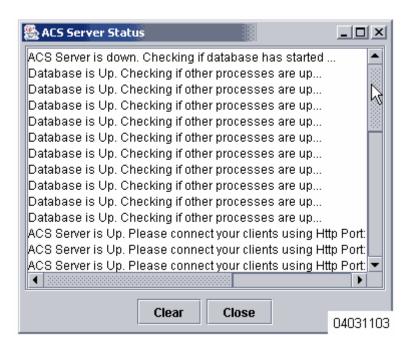


The start ACS Software Server script opens a **Start ACS Service** DOS window, which displays the following messages:

```
The ACS Software2.0 service is starting. . (in the background)
The ACS Software2.0 service was started successfully.

Launching Server Status Window
```

The **Start ACS Service** window displays the **ACS Server Status** window. You can close the **Start ACS Service** DOS window, and view the current ACS Software Service status in the **ACS Server Status** window. When the **Start ACS Service** window displays the ACS Software Server is Up message, the ACS Software service has started and is ready to host ACS Software Clients.



Note that the **ACS Server Status** window is updated about every five seconds. When the **ACS Server Status** window displays the ACS Software Server is Up message, the ACS Software service is ready to host ACS Software Clients.

Note: You can close the ACS Server Status window at any time, if you wish. When you want to view the current ACS Software Server status, from the Windows START button, select the Programs menu, and select OmniVista Air Control System 2.0/Check Server Status to view the ACS Software Server Status window again.

If desired, continue with <u>Starting an ACS Software Browser Client</u>, <u>Starting an ACS Software Java Admin Client</u>, or <u>Using the OmniVista Air Control System Software</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# **Stopping the ACS Software Server Application**

You can stop the ACS Software Server application at any time.

- **Note:** If there are any ACS Software Clients logged in when you stop the ACS Software Server, the ACS Software Client sessions will stop functioning.
  - From the Windows START button, select the **Programs** menu, and select **OmniVista Air** Control System 2.0/Stop ACS Server.

The stop ACS Software Server script opens a **Stop ACS Server** DOS window, which displays the **Shutdown Web NMS Server** window.

- The Stop ACS Server window displays the Press any key to continue prompt.
- Press any key to complete the stop ACS Software Server script.

You have shut down the ACS Software Server application. If desired, continue with the <u>Alcatel Omni-Access Wireless Product Guide</u>.

## **Stopping the ACS Software Service**

You can stop the ACS Software service at any time.

- Note: If there are any ACS Software Clients logged in when you stop the ACS Software Server, the ACS Software Client sessions will stop functioning.
  - From the Windows START button, select the **Programs** menu, and select **OmniVista Air Control System 2.0/Stop ACS Service**.

The stop ACS Software Server script opens a **Stop ACS Service** DOS window and halts the ACS Software service.

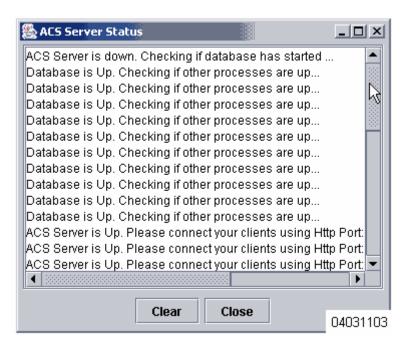
You have shut down the ACS Software service. If desired, continue with the <u>Alcatel OmniAccess</u> Wireless Product Guide.

# **Checking the ACS Software Service Status**

When ACS Software Server is installed as a Service, it runs in the background. That is, it has no windows open, so you cannot directly view its current status. To allow you to check the ACS Software Service status, Alcatel has provided a convenient ACS Software Server Status utility.

 To activate the ACS Software Server Status utility, from the Windows START button, select the Programs menu, and select OmniVista Air Control System Software 2.0/Check Server Status.

The Check Server Status script launches the **Start ACS Service** DOS window, which in turn launches the **ACS Software Server Status** window.



When the ACS Software Service is active, the **ACS Software Server Status** window reports that the ACS Software Server is Up. When the ACS Software Service is inactive, the **ACS Software Server Status** window reports that the ACS Software Server is down. Checking if database has started ...

 You can close the Start ACS Service DOS window and the ACS Software Server Status window at any time.

You have viewed the ACS Software service status. If desired, continue with the <u>Alcatel OmniAccess</u> <u>Wireless Product Guide</u>.

# **Starting an ACS Software Browser Client**

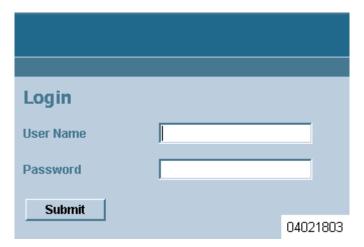
This ACS interface is used by ACS operators as described in <u>ACS Software Browser Client</u>. Starting an ACS Software Browser Client is a simple task.

- Launch an Internet Explorer 6.0 (or other) Web Browser.
- Note: Some documented features may not function properly if you choose to use any Web Browser other than Internet Explorer 6.0.
  - In the Web Browser address field, access the ACS Software Server on port 80 by entering:

http://<localhost|ACS Software Server IP Address>

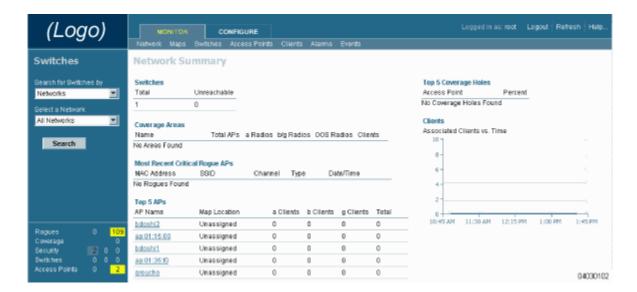
where localhost is used when the ACS Software Server is on the same workstation as the ACS Software Browser Client, and where <acs software Server IP Address> is the IP Address of the ACS Software Server on any workstation.

The ACS Software Server displays the **ACS Login** page.



- In the ACS Login page, enter the following:
  - User Name: Your username (default root).
  - Password: Your password (default public).
- When you have made these entries in the ACS Login page, click Submit.

The ACS Software Browser Client is now active and available for your use, and displays the Network Summary (Network Dashboard), which provides a summary of the Alcatel OmniAccess Wireless System, including reported coverage holes, OmniAccess AP operational data, most recent detected rogue APs, and client distribution over time.



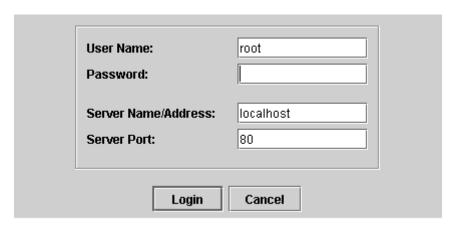
Continue with the <u>Using the OmniVista Air Control System Software</u> or <u>Stopping an ACS Software</u> <u>Browser Client</u> section.

# Starting an ACS Software Java Admin Client

This ACS interface is used by ACS system administrators as described in <u>ACS Software Java Admin</u> <u>Client</u>.

- If not already done, start the ACS Software Server as described in the <u>Starting an ACS Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- From the Windows START button, select the Programs menu, and then select OmniVista Air Control System Software 2.0/Start ACS Admin Client.

The Start ACS Software Admin Client script opens the **OmniVista Air Control System Login Dialog** window.



04031104

- In the OmniVista Air Control System Software Login Dialog window, enter the following:
  - User Name: Superuser username (default Super1).

- Password: Superuser password (default Super1).
- Server Name/Address: localhost, or <hostname> or IP Address if the ACS Software Server is on a remote workstation.
- Port: Leave as 80.
- When you have made these entries, click **Login** to connect your ACS Software Client to the ACS Software Server and have your ACS Software Client display the **OmniVista Air Control System Release 2.0** page.

Continue with the <u>Using the OmniVista Air Control System Software</u> or <u>Stopping an ACS Software Java Admin Client</u> section.

# **Stopping an ACS Software Browser Client**

## **Manually Stopping the Client**

- When you are finished working in the ACS Software Browser Client application, exit the ACS Software Browser Client application page by clicking **Logout** in the upper right corner of the ACS Software Browser Client page. The ACS Software Server displays the **ACS Login** page. Note that you can return to the previous cached screen in the Web Browser. However, if you attempt to access any of the parameters in that screen, you are returned to the **ACS Login** page.
- Alternatively, you can shut down the Web Browser.

The ACS Software Client window shuts down, leaving the ACS Software Server running. If desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## **ACS Software Server Shutdown Stopping the Client**

Occasionally, the system administrator may stop the ACS Software Server while an ACS Software Browser Client is logged in. Should this happen, the Web Browser displays a The page cannot be displayed message.



**Note:** When the ACS Software Browser Client has been stopped by an ACS Software Server shutdown, it does not reassociate with the ACS Software Server when the Server restarts. You must restart the ACS Software Browser Client as described in <u>Starting an ACS Software</u> Browser Client.

If desired, continue with the Alcatel OmniAccess Wireless Product Guide.

# **Stopping an ACS Software Java Admin Client**

### **Manually Stopping the Client**

- When you are finished working in the ACS Software Java Admin Client application, exit the ACS Software Java Admin Client application Z by clicking **Logout.** The ACS Software Server displays the **ACS Login** page.
- Alternatively, you can shut down the Java page.

The ACS Software Java Admin Client window shuts down, leaving the ACS Software Server running. If desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## **ACS Software Server Shutdown Stopping the Client**

Occasionally, the system administrator may stop the ACS Software Server while an ACS Software Java Admin Client is logged in. Should this happen, the Web Browser displays a The page cannot be displayed message.

Note: When the ACS Software Java Admin Client has been stopped by an ACS Software Server shutdown, it does not reassociate with the ACS Software Server when the Server restarts. You must restart the ACS Software Java Admin Client as described in <u>Starting an ACS Software Java Admin Client</u>.

If desired, continue with the Alcatel OmniAccess Wireless Product Guide.

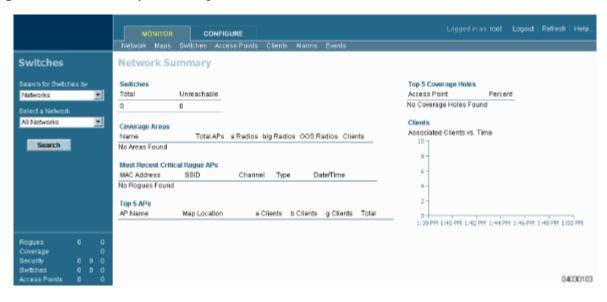
# **Configuring the ACS Software Browser Client**

- Adding Devices to the ACS Software Database
  - Manually Adding an Alcatel OmniAccess Switch or Appliance to ACS
- Adding a Campus Map to the ACS Database
- Adding an Outdoor Area to a Campus
- Adding a Standalone Building to the ACS Database
- Adding Floor Plans to a Standalone Building
- Adding Floor Plans to a Campus Building
- Adding Floor Plans to a Standalone Building
- Adding APs to Floor Plan and Open Area Maps

# **Adding Devices to the ACS Software Database**

When you use ACS Software for the first time, the Network Summary page shows that the Coverage Areas, Most Recent Rogue APs, the Top 5 APs, and the Top 5 Coverage Holes database is empty, as shown in the following figure. The following figure also shows that there are no clients connected to the Alcatel OmniAccess Wireless System at this time.

Figure - Network Summary for Unconfigured ACS Software Database



Note: Alcatel recommends that you manage Alcatel OmniAccess Switches and Appliances via the dedicated front-panel <u>Service Port</u> for improved security. If any Alcatel OmniAccess Switch or Appliance has its Service port disabled, you will have to manage the Alcatel OmniAccess Switch or Appliance through its <u>Management Interface</u>.

There are different ways to add Alcatel OmniAccess Switches and Appliances to the ACS Software database.

• If you have one Alcatel OmniAccess Switch or Appliance, you can manually add it using its <u>Service Port</u> IP Address or its Alcatel OmniAccess Switch or Appliance name. Refer to the <u>Manually Adding an Alcatel OmniAccess Switch or Appliance to ACS</u> section.

# Manually Adding an Alcatel OmniAccess Switch or Appliance to ACS

When you know the IP Address of an Alcatel OmniAccess Wireless Switch or Appliance <u>Service Port</u> or an Alcatel OmniAccess Switch or Appliance name, do the following to add the Alcatel OmniAccess Switch or Appliance to the ACS Software database.

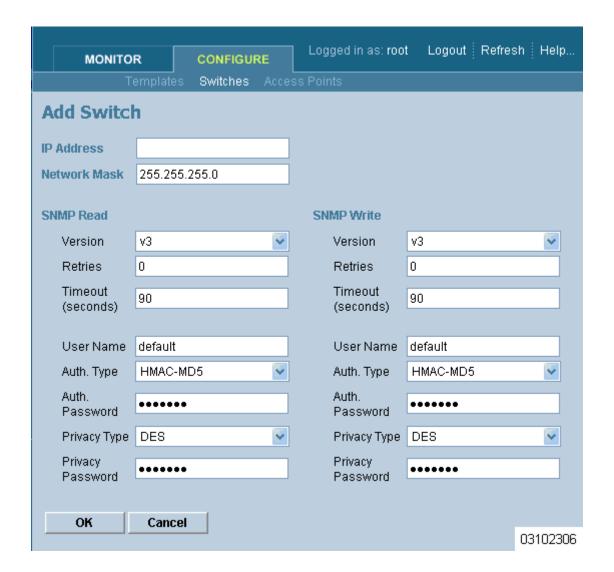
- Select the **Configure** Tab.
- Click Switches to have ACS display the All Switches page.



In the Button Area, select Add Switch.



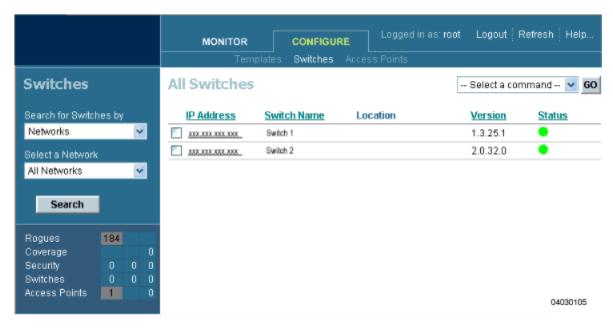
• Click **GO** to have the ACS Software Server display the **Add Switch** page.



- Enter the Alcatel OmniAccess Switch or Appliance IP Address, Network Mask, and required SNMP settings in the **Add Switch** data entry fields.
- Note 1: Alcatel recommends that you manage each Alcatel OmniAccess Switch and Appliance via the dedicated front-panel <u>Service Port</u> for highest security. If any Alcatel OmniAccess Switch or Appliance has its Service ports disabled, you will manage the Alcatel OmniAccess Switch or Appliance through its <u>Management Interface</u>.
- Note 2: Alcatel OmniAccess Switches and Appliances are factory-configured with SNMP Version 2C enabled, which is the most secure and slowest version. After you have logged into the Alcatel OmniAccess Switch or Appliance, you can change the SNMP parameters and re-add the Alcatel OmniAccess Switch or Appliance to the ACS Software database.
  - Click **OK**, and the ACS Software Server displays the **Please wait...** dialog screen while it contacts the Alcatel OmniAccess Switch or Appliance, adds the current Alcatel OmniAccess Switch or Appliance configuration to the ACS Software Server database, and then returns you to the **Add Switch** page.



- Note: If ACS Software does not find an Alcatel OmniAccess Switch or Appliance at the selected IP Address, the **Discovery Status** page displays a No response from device, check SNMP. . . message. Either the <u>Service Port</u> IP Address is set incorrectly (refer to <u>Configuring Other Ports and Parameters</u>), or ACS Software was unable to contact the Alcatel OmniAccess Switch or Appliance (make sure that you can ping the Alcatel OmniAccess Switch or Appliance from the ACS Software Server and retry), or the device has different SNMP settings (verify that the SNMP settings match and retry).
  - You may now add additional Alcatel OmniAccess Switches and Appliances in the Add Switch
    page, or click the Configure Tab to have the ACS Software Server display the All Switches
    page.



You have added Alcatel OmniAccess Switches or Appliances to the ACS Software database. Continue *Using the OmniVista Air Control System Software*.

## Adding a Campus Map to the ACS Database

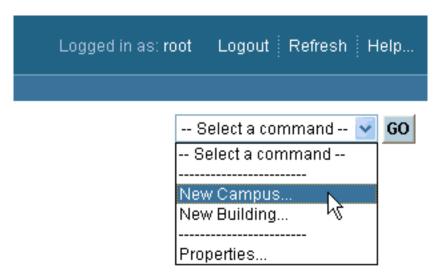
Rather than forcing the ACS Software operator to use only a text-based map to manage the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System), the ACS Software

allows the operator to view the managed System on realistic campus, building, and floor plan maps. This section describes how to add a single campus map to the ACS Software database.

- First, save your maps in .PNG, .JPG, .JPEG, or .GIF format. They can be any size, as ACS automatically resizes the map to fit in its working areas.
- Browse to and import the map(s) from anywhere in your file system.
- Select the Monitor Tab.
- Click Maps to have ACS display the Maps page.

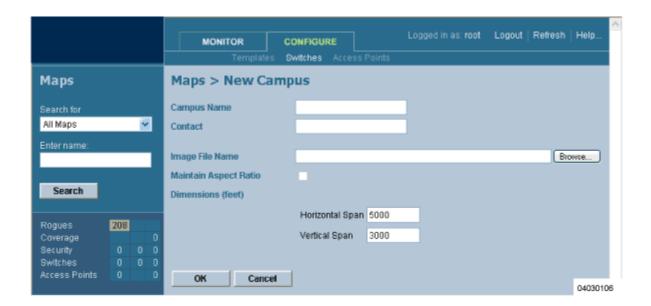


In the Button Area, select New Campus.



03102702

Click GO to have the ACS Software Server display the Maps > New Campus page.

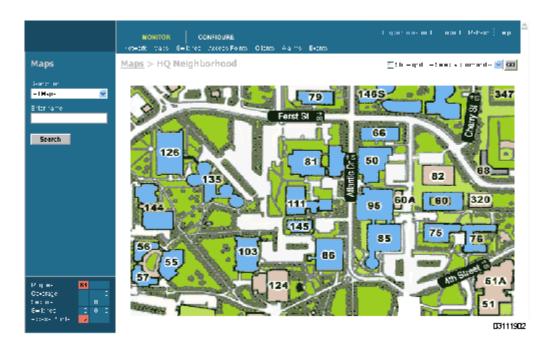


- In the **Maps > New Campus** page, enter the Campus Name and Campus Contact Information, click Browse to search for and select the Campus graphic name, select Maintain Aspect Ratio (if desired), and enter the Horizontal Span and the Vertical Span of the map in feet. (Note that the Campus Horizontal Span and the Vertical Span should be larger than any building or floor plan to be added to the campus.)
- Click **OK** to add the Campus Map to the ACS database. The ACS Software Server displays the Maps page.



The **Maps** page contains a current list of Campus Names, the map type (Campus or Building), and the current Campus Status (Green for OK, Red for Failure, Amber for Alarm).

- You have added a map to the ACS database, which corresponds to a single Campus.
- Ensure that the graphic has been added correctly by clicking the new Campus Name to have the ACS Software Server display the Maps > <Campus Name> page as shown in the following figure.



Repeat this section for any remaining Campuses.

When you have completed this section, continue with <u>Adding an Outdoor Area to a Campus</u> or <u>Adding a Standalone Building to the ACS Database</u>.

## Adding a Building to a Campus

You can add Buildings to the ACS database whether or not you have added maps or Campuses as described in *Adding a Campus Map to the ACS Database*.

To add a Building to the ACS database without associating it with a Campus, continue with <u>Adding a Standalone Building to the ACS Database</u>. To add an Outdoor Area to a Campus in the ACS database, continue with <u>Adding an Outdoor Area to a Campus</u>. Otherwise, add a Building to a Campus in the ACS database by performing the following steps:

- Select the Monitor Tab.
- Click Maps to have ACS display the Maps page.

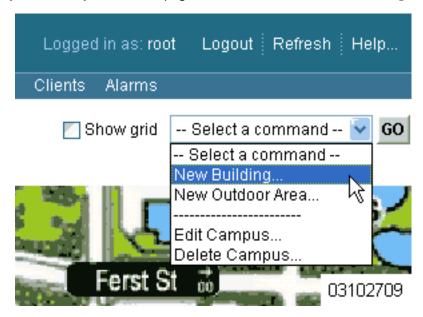


In the Maps Page, select the desired Campus.

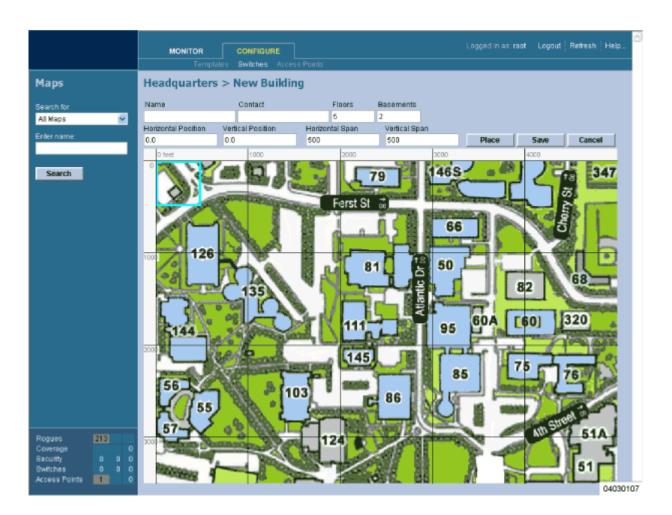


The ACS Software Server displays the **Maps > <Campus Name>** page.

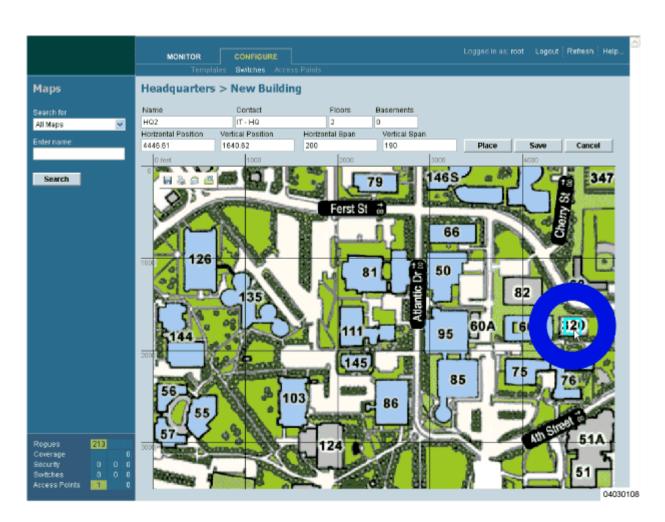
In the Maps > <Campus Name> page Button Area, select New Building.



Click GO to have the ACS Software Server display the <Campus Name> > New Building page.



- In the **<Campus Name> > New Building** page, you can create a virtual Building to organize related Floor Plan maps. To do this:
  - Enter the Building Name.
  - Enter the Building Contact Name.
  - Enter the number of Floors and Basements.
  - Enter an approximate Building Horizontal Span and Vertical Span (width and depth on the map) in feet. Note that these numbers should be larger than or the same as any floors that might be added later.
- Note: Alternatively, you can use **Ctrl-Left-Click** to resize the bounding area in the upper left corner of the Campus map. As you change the size of the bounding area, the Building Horizontal Span and Vertical Span parameters vary to match your changes.
  - Click **Place** to locate the Building on the Campus map. ACS creates a Building rectangle scaled to the size of the Campus map.
  - Left-click on the Building rectangle and drag it to the desired position on the Campus map.



- Click **Save** to save the Building definition and its Campus location in the ACS database. ACS saves the Building name in the Building rectangle on the Campus map. Note that there will be a hyperlink associated with the Building that takes you to the corresponding Map page.



Repeat this section for any remaining Campus Buildings.

When you have completed this section for all Campus Buildings, continue with <u>Adding Floor Plans to a Campus Building</u>.

## Adding a Standalone Building to the ACS Database

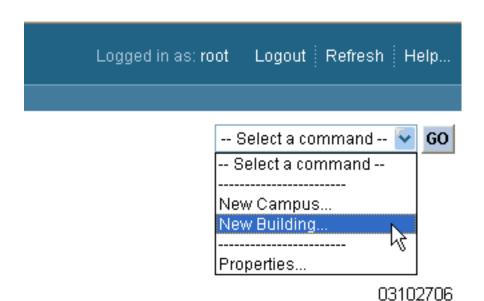
You can add Buildings to the ACS database whether or not you have added maps or Campuses as described in <u>Adding a Campus Map to the ACS Database</u>.

To add a building to a Campus in the ACS database, continue with <u>Adding a Building to a Campus</u>. To add an Outdoor Area to a Campus in the ACS database, continue with <u>Adding an Outdoor Area to a Campus</u>. Otherwise, add a standalone building to a Campus by performing the following steps:

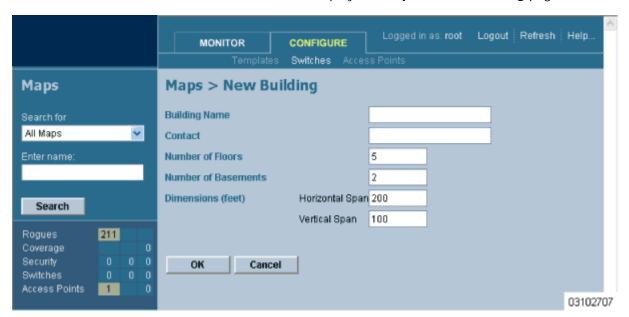
- Select the Monitor Tab.
- Click Maps to have ACS display the Maps page.



In the Button Area, select New Building.



Click GO to have the ACS Software Server display the Maps > New Building page.



- In the Maps > New Building page, you can create a virtual Building to organize related Floor Plan maps. To do this:
  - Enter the Building Name.
  - Enter the Building Contact Name.
  - Enter the number of Floors and Basements.
  - Enter an approximate Building Horizontal Span and Vertical Span (width and depth on the map) in feet. Note that these numbers should be larger than or the same as any floors that might be added later.

- Click **OK** to save the Building definition to the ACS Software database.
- Repeat this section for any remaining Standalone Buildings.

When you have completed this section for all Standalone Buildings, continue with <u>Adding Floor Plans to a Standalone Building</u>.

# Adding an Outdoor Area to a Campus

You can add Outdoor Areas to a Campus in the ACS database whether or not you have added Outdoor Area maps to the ACS database.

To add a building to the ACS database without associating it with a Campus, continue with <u>Adding a Standalone Building to the ACS Database</u>. To add a building to a Campus in the ACS database, continue with <u>Adding a Building to a Campus</u>. Otherwise, add an Outdoor Area to a Campus by performing the following steps:

- If desired, save Outdoor Area maps in .PNG, .JPEG, or .GIF format. Note that you do not need to have a map for the Outdoor Area map(s). The maps can be any size, as ACS automatically resizes the map(s) to fit in its working areas.
- Browse to and import the map(s) from anywhere in your file system.
- Select the Monitor Tab.
- Click Maps to have ACS display the Maps page.

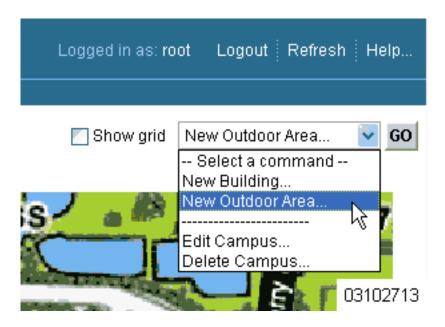


In the Maps Page, select the desired Campus.

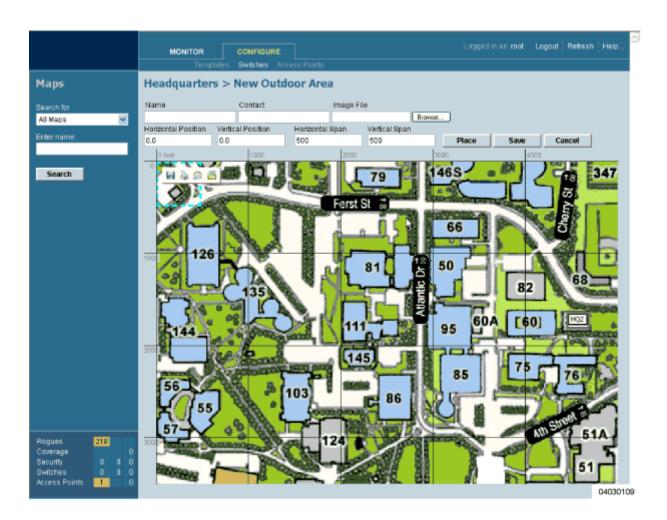


The ACS Software Server displays the **Maps** > **<Campus Name>** page.

In the Maps > <Campus Name> page Button Area, select New Outdoor Area.



 Click GO to have the ACS Software Server display the <Campus Name> > New Outdoor Area page.



- In the <Campus Name> > New Outdoor Area page, you can create a manageable Outdoor Area. To do this:
  - Enter the Outdoor Area Name.
  - Enter the Outdoor Area Contact Name.
  - Enter the Outdoor Area Map filename (optional).
  - Enter an approximate Outdoor Area Horizontal Span and Vertical Span (width and depth on the map) in feet.
- Note: Alternatively, you can use **Ctrl-Left-Click** to resize the bounding area in the upper left corner of the Campus map. As you change the size of the bounding area, the Building Horizontal Span and Vertical Span parameters vary to match your changes.
  - Click Place to locate the Outdoor Area on the Campus map. ACS creates an Outdoor Area rectangle scaled to the size of the Campus map.
  - Left-click on the Outdoor Area rectangle and drag it to the desired position on the Campus map.
  - Click Save to save the Outdoor Area definition and its Campus location in the ACS database. ACS saves the Outdoor Area name in the Outdoor Area rectangle on the

Campus map. Note that there will be a hyperlink associated with the Building Name or Outdoor Area.



Repeat this section for any remaining Outdoor Areas.

When you have completed this section for all Outdoor Areas, continue with <u>Using the OmniVista Air Control System Software</u>.

# **Adding Floor Plans to a Campus Building**

Once you have added a Building to a Campus as described in <u>Adding a Building to a Campus</u>, you can add individual floor plan and basement maps to the Building. Proceed with the following:

- If not already done, save your floor plan map(s) in .FPE, .PNG, .JPG, or .GIF format. They can be any size, as ACS automatically resizes the map(s) to fit in its working areas.
- Note: When you are importing a .FPE floor plan map, you will also need to import a corresponding .PNG, .JPG, or .GIF format floor plan map. Importing the .PNG, .JPG, or .GIF format floor plan map allows ACS to correctly display the floorplan, and importing the .FPE floor plan map allows ACS to properly adjust the RF signal strengths as modified by the walls and other RF obstructions.
  - Browse to and import the map(s) from anywhere in your file system.
  - Select the **Monitor** Tab.
  - Click Maps to have ACS display the Maps page.

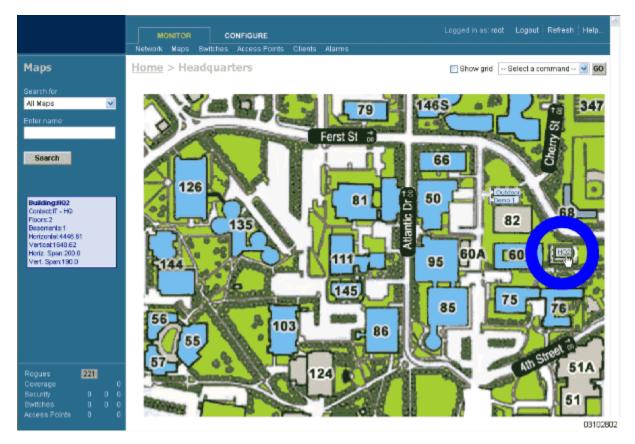


In the Maps Page, select the desired Campus.

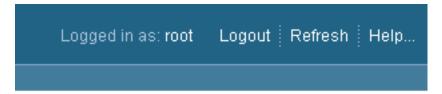


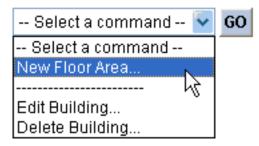
The ACS Software Server displays the **Maps > <Campus Name>** page.

• In the **Maps > <Campus Name>** page Button Area, move the cursor over an existing **Building** rectangle to highlight it. Note that when you highlight the **Building** rectangle, the **Building** description appears in the Sidebar area.



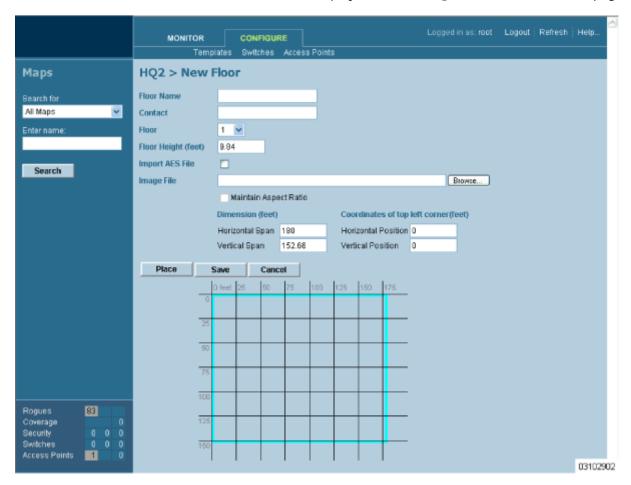
- Left-click on the Building rectangle to have ACS display the Maps > <Campus Name> >
   <Building Name> page.
- In the Button Area, select New Floor Area.



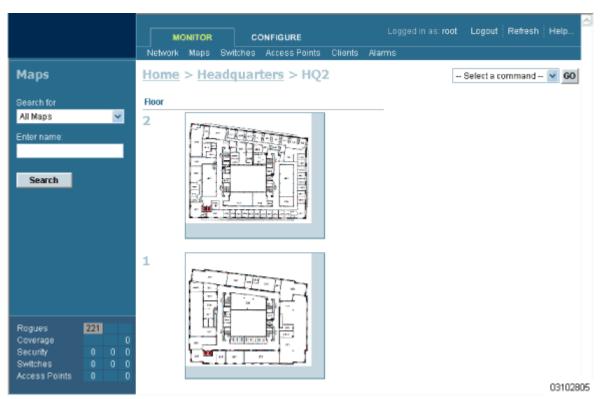


03102803

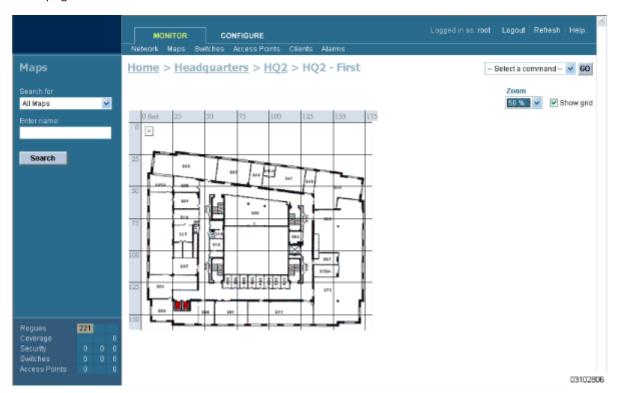
Click GO to have the ACS Software Server display the <Building Name> > New Floor page.



- In the **<Building Name> > New Floor** page, you can add floors to a Building to organize related Floor Plan maps. To do this:
  - Enter the Floor or Basement Name.
  - Enter the Floor or Basement Contact Name.
  - Select the Floor or Basement number.
  - Enter the Floor-to-Floor Height in feet.
  - Also, when you are importing a .FPE floor plan map file from the ACS Floor Plan Editor, click **Browse** to search for and select the desired .FPE Floor or Basement graphic name
  - In all cases, click **Browse** to search for and select the desired Floor or Basement graphic name. Note that when you select the Floor or Basement graphic, ACS displays the graphic in the Building-sized grid.
  - Enter an approximate Floor or Basement Horizontal Span and Vertical Span (width and depth on the map) in feet. Note that these numbers should be smaller than or the same as the Building Horizontal Span and Vertical Span in the ACS database.
  - If necessary, click **Place** to locate the Floor or Basement graphic on the Building grid.
- Note: You can use **Ctrl-Left-Click** to resize the graphic within the Building-sized grid. Leave Maintain Aspect Ratio checked to preserve the original graphic aspect ratio, or uncheck the Maintain Aspect Ratio box to change the graphic aspect ratio. Once again, use **Ctrl-Left-Click** to change the graphic aspect ratio.
  - Click Save to save the Building definition to the ACS database. The ACS Software
     Server displays the floor plan graphic in the Maps > <Campus Name> > <Building
     Name> page.



• In the **Maps** > **<Campus Name**> > **<Building Name**> page, left-click any of the Floor or Basement images to view the floor plan or basement map as shown in the following figure. Note that you can zoom in and out to view the map at different sizes, and can add APs from this page.



Repeat this section for any remaining Floors or Basements.

Continue with <u>Adding Floor Plans to a Standalone Building</u> or <u>Adding APs to Floor Plan and Open Area Maps</u>.

## Adding Floor Plans to a Standalone Building

Once you have added a standalone Building to the ACS database as described in <u>Adding a Standalone</u> <u>Building to the ACS Database</u>, you can add individual floor plan maps to the Building. Proceed with the following:

- If not already done, save your floor plan map(s) in .FPE, .PNG, .JPG, or .GIF format. They can be any size, as ACS automatically resizes the map(s) to fit in its working areas.
- Note: When you are importing a .FPE floor plan map, you will also need to import a corresponding .PNG, .JPG, or .GIF format floor plan map. Importing the .PNG, .JPG, or .GIF format floor plan map allows ACS to correctly display the floorplan, and importing the .FPE floor plan map allows ACS to properly adjust the RF signal strengths as modified by the walls and other RF obstructions.
  - Browse to and import the map(s) from anywhere in your file system.
  - Select the **Monitor** Tab.
- Click Maps to have ACS display the Maps page.

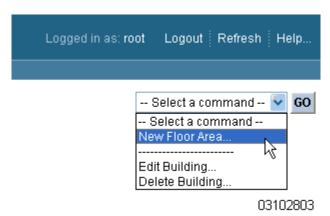


• In the Main Data Page, select the desired **Building**.

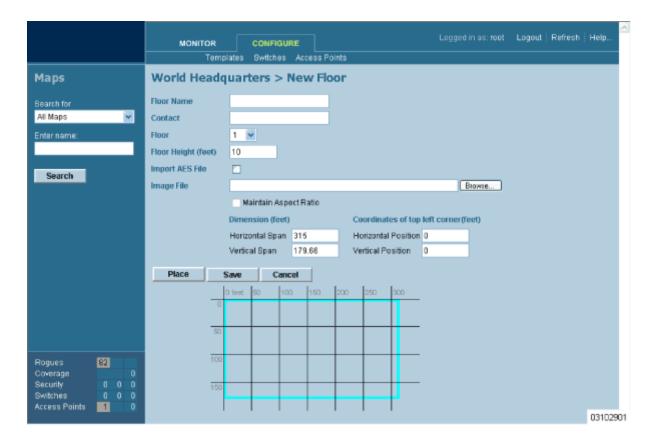


The ACS Software Server displays the **Maps > <Building Name>** page.

• In the Button Area, select **New Floor Area**.



Click GO to have the ACS Software Server display the <Building Name> > New Floor page.



- In the <Building Name> > New Floor page, you can add floors to a Building to organize related Floor Plan maps. To do this:
  - Enter the Floor or Basement Name.
  - Enter the Floor or Basement Contact Name.
  - Select the Floor or Basement number.
  - Enter the Floor-to-Floor Height in feet.
  - If you are importing a .FPE floor plan map file from the ACS Floor Plan Editor, check the Import FPE File box. Otherwise, leave this box unchecked.
    Also, when you are importing a .FPE floor plan map file from the ACS Floor Plan Editor, click **Browse** to search for and select the .FPE desired Floor or Basement graphic name.
  - In all cases, click **Browse** to search for and select the desired Floor or Basement graphic name. Note that when you select the Floor or Basement graphic, ACS displays the graphic in the Building-sized grid.
  - Enter an approximate Floor or Basement Horizontal Span and Vertical Span (width and depth on the map) in feet. Note that these numbers should be smaller than or the same as the Building Horizontal Span and Vertical Span in the ACS database.
  - If necessary, click **Place** to locate the Floor or Basement graphic on the Building grid.

- Note: You can use **Ctrl-Left-Click** to resize the graphic within the Building-sized grid. Leave Maintain Aspect Ratio checked to preserve the original graphic aspect ratio, or uncheck the Maintain Aspect Ratio box to change the graphic aspect ratio. Once again, use **Ctrl-Left-Click** to change the graphic aspect ratio.
  - Click **Save** to save the Building definition to the ACS database. The ACS Software Server displays the floor plan graphic in the **Maps** > **<Building Name>** page.



• In the **Maps > <Building Name>** page, left-click any of the Floor or Basement images to view the floor plan or basement map as shown in the following figure. Note that you can zoom in and out to view the map at different sizes, and can add APs from this page.



Repeat this section for any remaining Floors or Basements.

Continue with <u>Adding Floor Plans to a Campus Building</u> or <u>Adding APs to Floor Plan and Open Area Maps</u>.

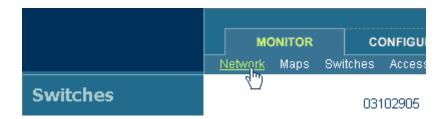
## Adding APs to Floor Plan and Outdoor Area Maps

This procedure assumes that you have added the Floor Plan and/or Outdoor Area maps as described in <u>Adding Floor Plans to a Campus Building</u>, <u>Adding Floor Plans to a Standalone Building</u> and <u>Adding an Outdoor Area to a Campus</u>. This procedure also assumes that you have added Alcatel OmniAccess Switches and Appliances to the ACS database as described in <u>Adding Devices to the ACS Software Database</u> before continuing.

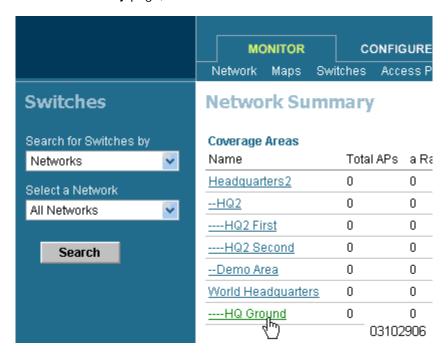
After you have added the .FPE and/or .PNG, .JPG, or .GIF format Floor Plan and Outdoor Area (Coverage Area) maps and Alcatel OmniAccess Switches and Appliances to the ACS database, you can position OmniAccess AP icons on the ACS Software maps to show where they are installed in the Buildings.

Add APs to the Coverage Area maps as follows:

- Select the Monitor Tab.
- Click Network to have ACS display the Network Summary page.



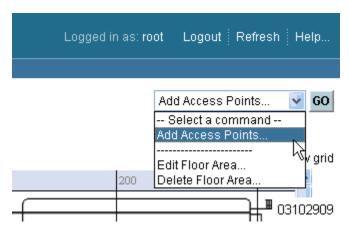
• In the **Network Summary** page, left-click the desired Floor Plan or Outdoor Area map.



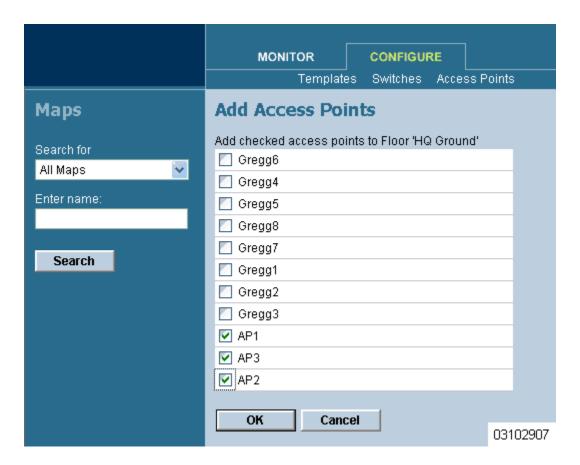
ACS displays the associated Coverage Area Map similar to the following:



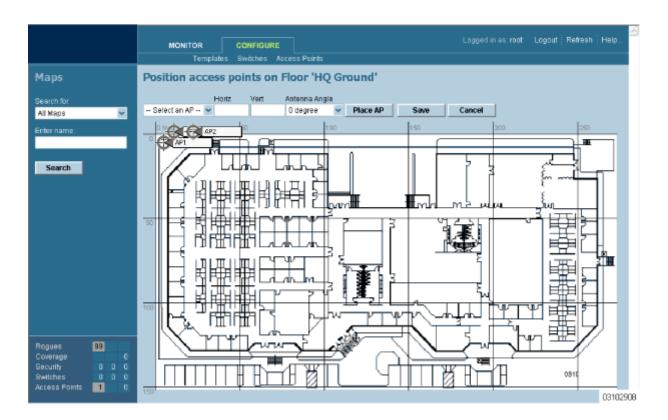
In the Button Area, select Add Access Points.



- Click GO to have the ACS Software Server display the Add Access Points page.
- In the **Add Access Points** page, check the OmniAccess APs to add to the map.



 Click **OK** to have the ACS Software Server add the OmniAccess APs to the map and display the Position Access Points map similar to the following:



Note that the OmniAccess AP icons appear in the upper left area of the map.

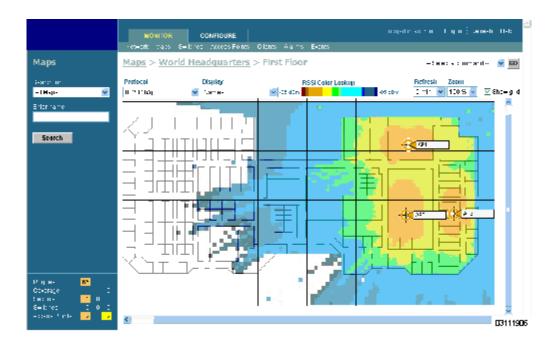
- Left-click and drag the OmniAccess AP icons to indicate their physical locations.
- Highlight each OmniAccess AP icon in turn, and select the Antenna Angle.
- Note 1: The Antenna Angle is relative to the Map "X" axis. Because the origin of the "X" and "Y" axes is at the upper left hand corner of the Map, 0 degrees points Side A of the Omni-Access AP to the right, 90 degrees points Side A down, 180 degrees points Side A to the left, and so on.
- Note 2: In the following example, AP1 and AP3 are set to 90 degrees, and AP2 is set to 0 degrees, so the three OmniAccess APs provide maximum coverage for the inside of the building and not the loading dock.

Also note that the first display is only an approximation of the actual RF signal intensity, because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

• If you have imported a .PNG, .JPG, or .GIF format Coverage Area map, click **Save** to store the OmniAccess AP locations and orientations, and have ACS compute the first-order RF prediction (or "Heat Map") for the Coverage Area.



- If you have imported a .FPE and a .PNG, .JPG, or .GIF format Coverage Area map, click **Save** to store the OmniAccess AP locations and orientations, and have ACS compute the second-order RF prediction (or "Heat Map") for the Coverage Area.
- Note: In the following example, AP1 is set to 0 degrees, and AP2 and AP3 are set to 90 degrees, so the three OmniAccess APs provide maximum coverage for the right wing of the building.
- Note: Also note that in the following example, each OmniAccess AP covers a much smaller area, because of the wall attenuation factored in by the RF Prediction algorithm.



- Note: These two displays are popularly known as a "heat maps", because they shows the relative intensity of the RF signals on the Coverage Area map.
- **Note:** MAKE SURE you have the correct OmniAccess AP in each location on the map with the correct antenna angle. This will become critical later on when you are <u>Finding Coverage Holes</u> and <u>Detecting and Locating Rogue Access Points</u>.
  - Repeat this section to assign OmniAccess APs to the remaining floor plan maps.

You have added OmniAccess APs to floor plan maps. Continue with <u>Using the OmniVista Air Control System Software</u>.

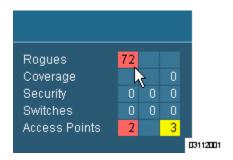
## **Troubleshooting with ACS Software**

- <u>Detecting and Locating Roque Access Points</u>
- Finding Coverage Holes
- <u>Pinging a Network Device Using ACS</u>

## **Detecting and Locating Rogue Access Points**

When the <u>Alcatel OmniAccess Wireless Access Points</u> are powered up and associated with <u>Alcatel OmniAccess Switches and Appliances</u>, the <u>OmniVista Air Control System Software</u> built into the Alcatel Wireless Operating System immediately starts listening for <u>Rogue Access Points</u>. When the Alcatel OmniAccess Switch or Appliance detects a rogue AP, it immediately notifies the ACS Software, which creates a rogue AP alarm.

When the ACS Software receives a rogue AP message from an Alcatel OmniAccess Switch or Appliance, ACS generates an alarm, with an indicator visible in the lower left corner of all ACS Software Browser Client pages. Notice that the following example shows 72 ACS Software Rogue AP alarms.

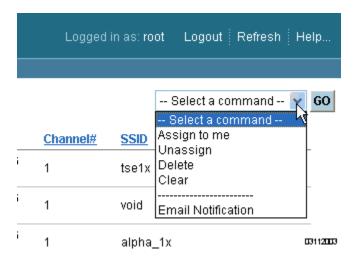


 To see more detail on the Rogue APs, click the Rogues indicator to display the Rogue AP Alarms page.



In the **Rogue AP Alarms** page, you can see the severity of the alarms, the Rogue AP MAC addresses, the rogue types, the owners (ACS operators), the date and time when the rogue APs were first detected, the channel numbers they are broadcasting on, and their SSIDs.

Also in this page, you can highlight one or more entries by checking the desired checkboxes, and then allows you to apply the following commands to all selected rogue AP alarms: **Assign to me**, **Unassign**, **Delete**, **Clear**, or configure **Email Notification** (feature coming in a later release).



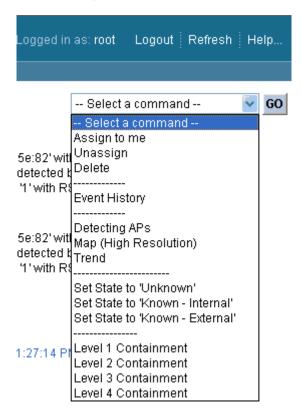
 To see more rogue AP information, click any Rogue MAC Address link to have ACS display the associated Alarms > Rogue AP <MAC address> page.



The **Alarms > Rogue AP <MAC address>** page shows detailed information about the rogue AP alarm, and allows you to modify the rogue AP alarm with the following commands:

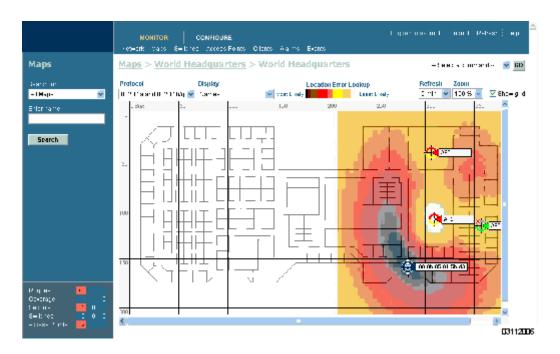
- Assign to me,
- Unassign,
- Delete,
- Show the Event History,
- Display the **Detecting APs** (with Radio Band, Location, SSID, Channel Number, WEP state, short or long preamble, RSSI and SNR),

- Show a high-resolution **Map** with the current calculated location, or a low-resolution **Map** with the rogue AP located at the OmniAccess AP that detects strongest RSSI transmissions.
- Show a **Trend** of recent RSSI signal strength,
- Set the State to **Unknown**, **Known-Internal**, or **Known-External** (as described in *Rogue AP Location, Tagging and Containment*).
- Set up **Level 1** through **Level 4 Containment** (as described in *Rogue AP Location, Tagging and Containment*).



03112005

 In the Alarms > Rogue AP <MAC address> page, select Map to have ACS display the current calculated rogue AP location on the Maps > <building name> > <floor name> page.



Note that the ACS Location (High-Resolution) Software (OV-ACSLOC) compares RSSI signal strength from two or more OmniAccess APs to find the most probable location of the rogue AP, and places a small "skull-and-crossbones" indicator at its most likely location.

Note that the ACS Basic (Low-Resolution) Software (OV-ACS-BASE) function compares RSSI signal strength from the rogue AP, and places a small "skull-and-crossbones" indicator next to the OmniAccess AP receiving the strongest RSSI signal from the rogue AP.

## **Acknowledging Rogue APs**

• To acknowledge known rogue APs, navigate to the **Rogue AP Alarms** page. Right-click the rogue AP (red, unknown) to be acknowledged, and select **Set State to 'Known Internal'** or **Set State to 'Known External'**. In either case, the red rogue AP entry is removed from the **Alarms** Page.

## **Locating Clients**

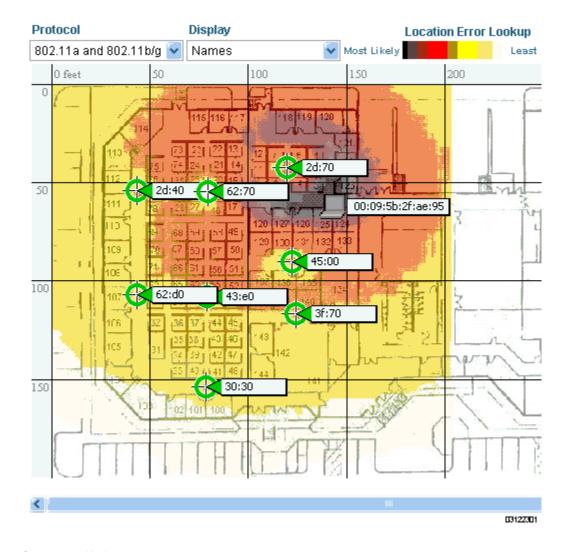
The ACS Software allows system operators to locate clients in the enterprise. Do the following:

- Use Monitor/Clients to navigate to the Clients Summary page.
- From the **Clients Summary** page, in the left sidebar **Search** for **All Clients** to have ACS display the **Clients** page.
- From the **Clients** page, click the **User Name** of the client you want to locate. ACS displays the corresponding **Clients <client name>** page.
- From the **Clients <client name>** page, you have two choices for locating the client:
  - In the pulldown menu, select **Recent Map (high/low resolution)** to locate the client without dissociating it.
  - In the pulldown menu, select **Present Map (high/low resolution)** to dissociate and then locate the client after reassociation. If you make this choice, ACS displays a warning message and asks you to confirm that you want to continue.

Note that the ACS Location (High-Resolution) Software (OV-ACSLOC) compares RSSI signal strength from two or more OmniAccess APs to find the most probable location of the client, and places a small "Laptop" icon at its most likely location.

Note that the ACS Basic (Low-Resolution) Software (OV-ACS-BASE) compares RSSI signal strength from the client, and places a small "Laptop" icon next to the OmniAccess AP receiving the strongest RSSI signal from the client.

Refer to the following illustration for a Heat Map showing client location.



## **Finding Coverage Holes**

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Alcatel Wireless Operating System OmniVista AirView Software identifies these coverage hole areas and reports them to ACS, allowing the IT manager to fill holes based on user demand.

When ACS displays the Top 5 Coverage Holes, click the **Coverage** indicator on the bottom left of the ACS Software Browser Client page (or click MONITOR/Alarms and then search for Alarm Category Coverage) to have ACS display the **Coverage Hole Alarms** page. On the **Coverage Hole Alarms** page, click MONITOR/Maps and then search for **Access Points** by **OmniAccess AP Name** (this search

tool is case-sensitive). ACS displays the **Maps > Search Results** page, which lists the Floor or Outdoor Area where the OmniAccess AP is located. Click the link to display the related **Maps > <building name> > <floor name>** page.

On the **Maps > <building name> > <floor name>** page, look for areas of low signal strength near the OmniAccess AP that reported the coverage hole. Those are the most likely locations of coverage holes. If there do not appear to be any areas of weak signal strength, make sure that the floorplan map is accurate, and if you have used the <u>ACS Floor Plan Editor</u> to create .FPE files, that you have not left out any metal obstructions, such as walls, elevator shafts, stairwells, or bookcases. If so, add them to the .FPE floorplan file and replace the old floorplan with the new floorplan.

## **Pinging a Network Device Using ACS**

- Use CONFIGURE/Switches and click an IP address under the IP Address column, then select System/Commands to access the <IPaddress> > Switch Commands page.
- Select Ping From Switch from the Administrative Commands pulldown and click GO.

Alcatel Wireless Operating System sends a Ping to the selected network element. This is useful for determining if there is connectivity between the Alcatel OmniAccess Switch or Appliance and a particular IP network element. Once you click  $\mathbf{GO}$ , three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it will show No Reply Received from IP xxx.xxx.xxx, otherwise shows Reply received from IP xxx.xxx.xxx.xxx: (send count = 3, receive count = n).

## **Viewing System Status**

Once you have added <u>Alcatel OmniAccess Switches and Appliances</u> and <u>Alcatel OmniAccess Wireless Access Points</u> to the ACS Software database using <u>Configuring the ACS Software Browser Client</u>, you can view the Alcatel OmniAccess Wireless System status as follows:

In the ACS Software Browser Client, click MONITOR/Network to display the <u>Monitor Network Summary</u>. Refer to the following figure and the <u>Monitor Network Summary</u> for more information.

Figure - Typical Network Summary Page



## **Managing ACS Software and Database**

- Installing ACS Software Server and ACS Software Client
- <u>Installing ACS Software Client</u>
- Updating ACS Software Server and ACS Software Client
- <u>Updating ACS Software Java Admin Client</u>
- Reinitializing the ACS Software Database
- Administering ACS Users and Passwords

## **Installing ACS Software Server and ACS Software Client**

Refer to the <u>ACS Quick Installation Guide</u> for instructions on how to install an ACS Software Server and an ACS Software Java Admin Client on the same workstation.

## **Installing ACS Software Client**

Refer to the <u>ACS Quick Installation Guide</u> for instructions on how to install an ACS Software Java Admin Client on a different workstation than the ACS Software Server.

## **Updating ACS Software Server and ACS Software Client**

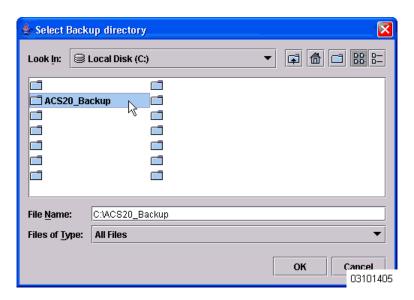
Should you ever need to change the ACS Software Server and ACS Software Client on the same work-station, do the following:

- If possible, stop all ACS Software Clients (<u>Stopping an ACS Software Browser Client</u> and <u>Stopping an ACS Software Java Admin Client</u>) to stabilize the database.
- Stop the ACS Software Server (<u>Stopping the ACS Software Server Application</u> or <u>Stopping the ACS Software Service</u>).

- In the **Select Backup directory** window, manually create a backup directory with no spaces in the name, such as C:\ACS20\_Backup\.
- **Note:** Make sure the directory name does not include any spaces, or the backup script will generate error messages.
  - From the Windows START button, select the Programs menu, and then select OmniVista Air Control System 2.0/Backup.

The backup script opens the **Backup** DOS window and the **Select Backup directory** window.

 In the Select Backup directory window, highlight the backup directory you created above and click OK.



The backup database script creates subdirectories in the C:\ACS20\_Backup\ directory, and backs up the ACS Software database and the floor plan, building, and area maps to the C:\ACS20\_Backup\conf and C:\ACS20\_Backup\mapimages directories.

- When the **Backup Status** window opens and displays the Backup Succeeded. You may restart the ACS Server now. message, click **OK**.
- Uninstall the OmniVista Air Control System Software application using the Control Panel/ Add or Remove Programs application.
- When the **JExpress Uninstaller** window displays Program uninstalled message, click **Finished** to close the **JExpress Uninstaller** window.
- If any part of the **C:\Program Files\ACS20** folder remains on the hard drive, manually delete the folder and all contents.
- Note: If you fail to delete the previous ACS Software installation, you will receive the following error message upon reinstall: ACS Software already installed. Please uninstall the older version before installing this version.
  - Reinstall the ACS Software application as described in <u>Installing ACS Software Server and ACS Software Client</u>.
  - From the Windows START button, select the Programs menu, and then select OmniVista Air Control System 2.0/Restore.

- In the Select Backup directory window, highlight the backup directory you created above and click OK.
- The restore database script restores the ACS Software database and the floor plan, building, and area maps to the new ACS Software installation.
- When the **Restore Status** page opens and displays the Restore Succeeded. You may restart the ACS Software Server now. message, click **OK**.
  - If you receive an error message, scroll down the page to find the error. Normally, the only error that will halt a backup is if an incorrect directory is specified; if this is the case, repeat this procedure with the correct directory to complete the backup.
- Start the ACS Software Server as described in <u>Starting an ACS Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- Start one or more ACS Software Clients as described in <u>Starting an ACS Software Browser Client</u> and <u>Starting an ACS Software Java Admin Client</u>.

### **Updating ACS Software Java Admin Client**

Should you ever need to change the ACS Software Java Admin Client on a separate workstation from the ACS Software Server, do the following:

- Stop the ACS Software Java Admin Client.
- Uninstall the ACS Software Java Admin Client application using the Control Panel Add or Remove Program.
- If necessary, manually delete the C:\Program Files\ACSCLIENT20 folder and all contents.
- Note: If you fail to delete the previous ACS Software Java Admin Client installation, you will receive the following error message upon reinstall: ACS Software already installed. Please uninstall the older version before installing this version.
  - Reinstall the ACS Software Java Admin Client application as described in <u>Installing ACS</u> <u>Software Client</u>.
  - If not already done, start the ACS Software Server as described in <u>Starting an ACS Software</u> Server as an Application or Starting the ACS Software Server as a Service.
  - Start the ACS Software Java Admin Client as described in <u>Starting an ACS Software Java Admin Client</u>.

#### Reinitializing the ACS Software Database

You only have to reinitialize the ACS Software database when the ACS Software Server database becomes corrupted.



**Warning:** If you reinitialize the ACS Software Server database after you have been working in the ACS Software application, you will delete all your saved ACS Software data!

- Navigate to the \ACS20 directory.
- Navigate to the \bin subdirectory.
- In the \bin subdirectory, double-click the reinitDatabase.bat file.
  - The database reinitialize script displays the **startdb.bat** DOS window.
- Select the **startdb.bat** window, and press any key to continue.
  - The startdb.bat script displays the **Reinitialize Web NMS Database** window.
- In response to the Do you want to Reinitialize Web NMS? prompt in the **Reinitialize Web NMS**Database window, select **Yes**.

The **startdb.bat** window displays many "accomplished" messages. When the ACS Software database is reinitialized, the **Reinitialize Web NMS Database** window reappears.

• In response to the Successfully reinitialized the Database prompt in the **Reinitialize Web NMS Database** window, select OK.

The **Reinitialize Web NMS Database** window closes, and the **startdb.bat** window displays a Press any key to continue prompt.

In the startdb.bat window, press any key. The startdb.bat window closes.

You have reinitialized the ACS Software database. Continue with <u>Using the OmniVista Air Control</u> System Software.

## **Administering ACS Users and Passwords**

ACS supports four User Groups:

- To monitor ACS operations, users must be part of the System Monitoring Group.
- To monitor and configure ACS operations, users must be part of the ConfigManagers Group.
- To monitor and configure ACS operations, and perform all system administration tasks except administering ACS users and passwords, users must be part of the **Admin** Group.
- To monitor and configure ACS operations, and perform all system administration tasks including administering ACS users and passwords, users must be part of the **SuperUsers** Group.

This section describes how to add user accounts and assign them to a User Group, change passwords, and delete user accounts using the ACS Software Java Admin Client.

### **Adding User Accounts**

- If not already done, start the ACS Software Server as described in the <u>Starting an ACS Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- If not already done, log into the ACS Software Java Admin Client as described in <u>Starting an ACS Software Java Admin Client</u>.



**Warning:** As soon as you have logged into the ACS Software Client as **Super1**, Alcatel recommends that you create a new superuser assigned to the Super Users Group, and then delete the **Super1** user to prevent undesired access to ACS Super User operations.

- Select User Admin/Security Administration to display the Security Administration page.
- In the **Security Administration** page, click the **Add User** (single person) icon to display the **User Administration** page.
- In the **User Administration** page, add the new user name and password. Click **Next** to display the **User account expiry** and **Password expiry** parameters.
- In this page, accept or change the desired expiration times for the user account and password. Click **Next** to display the **Group based permissions, Direct Assignment,** and **Assign groups for the user** parameters.
- As you are going to assign the new user account to a group which already has permissions assigned, make sure the **Group based permissions** and **Direct Assignment** boxes are checked.
- In the **Assign groups for the user** section, assign the new user account to one of the four User Group names: **System Monitoring**, **ConfigManagers**, **Admin**, or **SuperUsers**.
- Ignore the rest of the fields in this page, and click **Finish** to complete adding the new user account.

- Close the Security Administration page.
- Close the OmniVista Air Control System Release 2.0 page.

The new User Account has been added and can be used immediately. If necessary, refer to the <u>Deleting User Accounts</u> section to delete the default user accounts provided with OmniVista Air Control System Software.

## **Changing Passwords**

- If not already done, start the ACS Software Server as described in the <u>Starting an ACS</u> Software Server as an Application or Starting the ACS Software Server as a Service.
- If not already done, log into the ACS Software Java Admin Client as a user assigned to the SuperUsers Group as described in <u>Adding User Accounts</u>.
- Select User Admin/Security Administration to display the Security Administration page.
- In the Security Administration page, highlight a user account, and select Edit/Change Password to display the Change Password dialog.
- In the Change Password dialog, enter the new password and click Ok to change the password for the selected user account.
- Close the Security Administration page.
- Close the OmniVista Air Control System Release 2.0 page.

The User Account has been changed and can be used immediately.

## **Deleting User Accounts**

- If not already done, start the ACS Software Server as described in the <u>Starting an ACS</u> Software Server as an Application or <u>Starting the ACS Software Server as a Service</u>.
- If not already done, log into the ACS Software Java Admin Client as a user assigned to the **SuperUsers** Group as described in <u>Adding User Accounts</u>.
- Select User Admin/Security Administration to display the Security Administration page.
- In the Security Administration page, highlight the user account to delete, and select Edit/
  Delete to display the Warning! On deleting this user you would no longer be able to log
  on with this user name, are you sure you want to do this? dialog.
- In the **Warning!** dialog, click **Yes** to delete the selected user account.
- Close the Security Administration page.
- Close the OmniVista Air Control System Release 2.0 page.

The deleted User Account can no longer be used.

# **Using the Alcatel Web Browser Interface**

The Alcatel Web Browser Interface is described in *Alcatel Web Browser Interface* section.

Note that you can use either the <u>Service-Port Interface</u> (recommended) or <u>Management Interface</u>, whose IP Address(es) were set using the <u>Startup Wizard</u> or the <u>Configuring System Parameters</u> section. Also note that you can have up to 21 simultaneous Web Browser sessions, but the automatic refresh time for the Monitor/Summary page will be longer if there are more than 10 simultaneous sessions.

Note: Some popup window filters can be configured to block the Alcatel Web Browser Online Help pages. If your system cannot display the Online Help windows, disable or reconfigure your browser popup filter software.

Log into the Alcatel Web Browser Interface by doing the following:

- Start a Web Browser on any workstation connected to the Internet (Alcatel recommends Internet Explorer 6.0 or later for full functionality).
- For an unsecure http connection, enter the Alcatel OmniAccess Wireless Switch or Appliance IP Address (http://<Alcatel OmniAccess Switch or Appliance\_IPaddress>/) in the Web Browser Address field and press <RETURN>.

--OR--

- For a secure https (HTTP + SSL) connection, enter the Alcatel OmniAccess Switch or Appliance IP Address (https://<Alcatel OmniAccess Switch or Appliance\_IPaddress>/) in the Web Browser Address field and press <RETURN>. (This connection was configured using the <u>Adding SSL to the Web Browser Interface</u> procedure.)
- Note: If you receive a "The Document contains no data" error message, the corresponding http Web Mode and/or https Secure Web Mode is disabled. If you receive the error when attempting to use http AND https, use the CLI to log into the Alcatel OmniAccess Switch or Appliance as described in the <u>Using the Alcatel OmniAccess Wireless System CLI</u> section, or use ACS Software to log into the Alcatel OmniAccess Switch or Appliance as described in <u>Using the OmniVista Air Control System Software</u>.
- Note: The first time you access the secure https (http + SSL) Alcatel OmniAccess Switch or Appliance website, you may receive the following Security Alert:



When you see the Security Alert, click Yes.

Once you have logged into the Alcatel Web Browser Interface, use the context-sensitive (F1) online help (included in the <u>Alcatel Wireless Operating System</u> section) to configure and monitor the Alcatel OmniAccess Switch or Appliance.

## Adding OmniAccess APs to an Alcatel OmniAccess Switch or Appliance

There are two scenarios when adding OmniAccess APs to an existing Alcatel OmniAccess Wireless Switch or Appliance using the Web Browser Interface: when adding to an OmniAccess Wireless Switch in <u>Direct-Connect Mode</u>, and when adding to an Alcatel OmniAccess Switch or Appliance in <u>Appliance Mode</u>.

- In Direct-Connect Mode, the OmniAccess APs connect directly to the 4012 or 4024 OmniAccess
  Wireless Switch as described in <u>Alcatel Wired Connections</u>. When an OmniAccess AP powers up
  and searches for an OmniAccess Wireless Switch, the OmniAccess Wireless Switch recognizes it
  and adds it to its list of associated APs.
- In Appliance Mode, the OmniAccess APs connect to the Alcatel OmniAccess Switch or Appliance through the network as described in <u>Alcatel Wired Connections</u>. When an OmniAccess AP powers up, it searches for an Alcatel OmniAccess Switch or Appliance as described in <u>Alcatel OmniAccess Switch and Appliance Failover Protection</u>.

## Adding CA Certificates to an Alcatel OmniAccess Switch or Appliance

Certification Authority public-key certificates are used to authenticate the Web server and encrypt data transmissions between Web server and browser. The CA certificates are issued by a trusted Certification Authority, or CA.

Note: You can obtain a CA Certificate from three sources: Factory-supplied, Operator-generated, and Purchased from a trusted CA. This procedure only applies to adding an Operator-generated or Purchased ID Certificate, as the Factory-supplied Certificate is already stored in the Alcatel OmniAccess Wireless Switch or Appliance NVRAM. You do not need to complete this procedure if you choose to use the Factory-supplied CA Certificate.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

When you obtain certificates (usually in an email from the CA or from your key-generation program), it is a simple matter to add the CA certificate to your Alcatel OmniAccess Switch or Appliance:

- Launch a Web Browser Interface session as described in <u>Using the Alcatel Web Browser</u> <u>Interface</u>.
- Navigate to the <u>CA Certification</u> page in the Web Browser Interface.
- Copy the Certificate (a large block of ASCII characters) from your email or text viewer program, and paste it into the CA Certification box.
- Click Apply.

The CA Certificate is now in the Alcatel OmniAccess Switch or Appliance Volatile RAM. Use 'System Reboot with Save' to save the CA Certificate to NVRAM, so the CA Certificate is preserved across restarts.

## Adding ID Certificates to an Alcatel OmniAccess Switch or Appliance

ID Certificates and Private Keys are used by Web server operators to ensure secure server operation. The ID certificate and key are used to authenticate the server and encrypt data transmissions between server and browser.



**Note:** You can obtain an ID Certificate and Private Key from three sources: Factory-supplied, Operator-generated, and Purchased from a trusted CA. This procedure only applies to adding an Operator-generated or Purchased ID Certificate and Key, as the Factory-supplied Certificate and Key are already stored in the Alcatel OmniAccess Wireless Switch or Appliance NVRAM. You do not need to complete this procedure if you choose to use the Factory-supplied ID Certificate and Key.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

When you obtain ID certificates (usually in an email from the CA or from your key-generation program), it is a simple matter to add the ID certificate and key to your Alcatel OmniAccess Switch or Appliance:

- Launch a Web Browser Interface session as described in <u>Using the Alcatel Web Browser</u> <u>Interface</u>.
- Navigate to the <u>ID Certificate > New</u> page in the Web Browser Interface.
- Type or paste the ID Certificate Name into the Certificate Name box.
- Type a Private Key (Password) into the Certificate Password box.
- Copy the Certificate (a large block of ASCII characters) from your email or text viewer program, and paste it into the ID Certification box.
- Click Apply.

The ID Certificate and Key are now in the Alcatel OmniAccess Switch or Appliance Volatile RAM. Use 'System Reboot with Save' to save the ID Certificate and Key to NVRAM, so the Certificate and Key are preserved across restarts.

# **Troubleshooting**

Use the following sections to troubleshoot your Alcatel OmniAccess Wireless System:

- <u>Using Error Messages</u>
- <u>Using Reason and Status Codes in the Trap Log</u>

## **Using Error Messages**

The Alcatel Wireless Operating System may display any of the error messages described below.

Table - Error Messages and Descriptions

Error Message	Description
STATION_DISASSOCIATE	Client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	Client may have intentionally terminated usage or it could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch or other configuration issues.
STATION_ASSOCIATE_FAIL	Check load on the OmniAccess Radio or signal quality issues.
LRAD_ASSOCIATED	The associated OmniAccess AP is now managed by this Alcatel OmniAccess Wireless Switch or Appliance.
LRAD_DISASSOCIATED	OmniAccess AP may have associated with a different Alcatel OmniAccess Wireless Switch or Appliance or may have become completely unreachable.
LRAD_UP	OmniAccess AP is operational, no action required.
LRAD_DOWN	OmniAccess AP may have a problem or is administratively disabled.
AIRONETAP_UP	Aironet AP is responding to SNMP polls.
AIRONETAP_DOWN	Aironet AP is not responding to SNMP polls, check network connections, OmniAccess AP and its SNMP settings.
ORINOCOAP_UP	ORINOCO AP is responding to SNMP polls.
ORINOCOAP_DOWN	ORINOCO AP is not responding to SNMP polls, check network connections, ORINOCO AP and its SNMP settings.
LRADIF_UP	OmniAccess Radio is UP.
LRADIF_DOWN	OmniAccess Radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	Client density may have exceeded system capacity.

Table - Error Messages and Descriptions (Continued)

Error Message	Description
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceed configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	Possible coverage hole detected - check OmniAccess AP history to see if common problem - add OmniAccess APs if necessary.
LRADIF_LOAD_PROFILE_PASSED	Load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	Detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	Detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	Number of clients receiving poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_ CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue, use maps and trends to investigate.
ROGUE_AP_REMOVED	Detected Rogue has timed out - May have shut down or moved out of coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogues has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	Port may have a problem or is administratively disabled.
LINK_FAILURE	Port may have a problem or is administratively disabled.
AUTHENTICATION_FAILURE	Attempted security breech - please investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.

Table - Error Messages and Descriptions (Continued)

Error Message	Description
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPSec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for attempt to spoof IP Address.
IPSEC_ESP_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	Maximum number of supported OmniAccess Radios exceeded - Check for Alcatel OmniAccess Wireless Switch or Appliance failure in the same Layer 2 network or add another Alcatel OmniAccess Wireless Switch or Appliance.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning and/or other cooling arrangements.
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor ASAP.
TEMPERATURE_SENSOR_CLEAR	Temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check Direct-Connect APs - possible serious failure detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogues has exceeded system threshold.
SWITCH_UP	Alcatel OmniAccess Wireless Switch or Appliance is responding to SNMP polls.
SWITCH_DOWN	Alcatel OmniAccess Wireless Switch or Appliance is not responding to SNMP polls, check Alcatel OmniAccess Wireless Switch or Appliance and SNMP settings.
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the Alcatel OmniAccess Wireless Switch or Appliance.
CONFIG_SAVED	Running configuration has been saved to flash - will be active after reboot.

Table - Error Messages and Descriptions (Continued)

Error Message	Description
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor Alcatel OmniAccess Wireless Switch or Appliance temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for power-supply malfunction.
COLD_START	Alcatel OmniAccess Wireless Switch or Appliance may have been rebooted.
WARM_START	Alcatel OmniAccess Wireless Switch or Appliance may have been rebooted.

## **Using Reason and Status Codes in the Trap Log**

As described in <u>Alcatel OmniAccess Wireless System Web Browser Online Help</u>, the <u>Clients > Detail</u> page lists the Reason and Status Codes you are likely to encounter when reviewing the Trap Logs. For your convenience the Reason and Status Codes and their descriptions are listed in the following sections:

- <u>Client Reason Codes</u>
- Client Status Codes

## **Client Reason Codes**

The Client Reason code may be any of the following:

**Table -** Client Reason Code Descriptions and Meanings

Client Reason Code	Description	Meaning
0	noReasonCode	normal operation
1	unspecifiedReason	client associated but no longer authorized
2	previousAuthNotValid	client associated but not authorized
3	deauthenticationLeaving	the OmniAccess AP went offline, deauthenticating the client
4	disassociationDueToInactivity	client session timeout exceeded
5	disassociationAPBusy	the OmniAccess AP is busy, performing load balancing, for example
6	class2FrameFromNonAuthStation	client attempted to transfer data before it was authenticated
7	class2FrameFromNonAssStation	client attempted to transfer data before it was associated

Table - Client Reason Code Descriptions and Meanings (Continued)

Client Reason Code	Description	Meaning
8	disassociationStaHasLeft	Alcatel Wireless Operating System moved the client to another OmniAccess AP using non-aggressive load balancing
9	staReqAssociationWithoutAuth	client not authorized yet, still attempting to associate with an OmniAccess AP
99	missingReasonCode	client momentarily in an unknown state

## **Client Status Codes**

The Client Status code may be any of the following:

**Table -** Client Status Code Descriptions and Meanings

Client Status Code	Description	Meaning
0	idle	normal operation no rejections of client association requests
1	aaaPending	completing an aaa transaction
2	authenticated	802.11 authentication completed
3	associated	802.11 association completed
4	powersave	client in powersave mode
5	disassociated	802.11 disassociation completed
6	tobedeleted	to be deleted after disassociation
7	probing	client not associated or authorized yet
8	disabled	automatically disabled by Alcatel Wireless Operating System for an operator-defined time

Notes:

# **REFERENCES**

The following references are available:

- <u>Glossary</u>
- Alcatel OmniAccess Wireless System Supported Regulatory Domains
- Alcatel OmniAccess Wireless Access Point Deployment Guide
- Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide
- Alcatel OmniAccess Switch and Appliance Quick Installation Guide
- ACS Quick Installation Guide
- Alcatel OmniAccess Wireless System CLI Reference
- Alcatel OmniAccess Wireless System Web Browser Online Help
- ACS Online Help
- FCC Statements for Alcatel OmniAccess Switches and Appliances
- FCC Statements for OmniAccess APs
- <u>Legal Information</u>

# **Glossary**

#### 10Base-T

An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) with twisted pair cabling and wiring hubs.

#### 100Base-T

An IEEE standard (802.3) for operating 100 Mbps Ethernet networks (LANs) with twisted pair cabling and wiring hubs.

#### 1000Base-SX

An IEEE standard (802.3) for operating 1000 Mbps Ethernet networks (LANs) with fiber optic cables and wiring hubs. Also known as Gigabit Ethernet (GigE). Note that the Alcatel implementation uses small form-factor LC physical connectors for 1000Base-SX connections.

#### 1000Base-T

An IEEE standard (802.3) for operating 1000 Mbps Ethernet networks (LANs) with twisted pair cabling and wiring hubs. Also known as Gigabit Ethernet (GigE).

#### 802.11

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), http://standards.ieee.org. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, to differentiate between the various technology families.

The 802 LAN/MAN Standards Committee (of the IEEE) develops standards for local and metropolitan area networks with the 802.11 section creating standards for wireless local area networks.

802.11 is composed of several standards operating in different radio frequencies. 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11g is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 54 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another proposed standard, 802.11g, is for WLANs operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

## 802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b/g. These additional channels can help avoid radio and microwave interference.

#### 802.11b

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

#### 802.11g

Similar to 802.11b, but this proposed standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology from 802.11b in order to increase bandwidth.

#### 802.11i

A developing IEEE wireless LAN security standard. A subset of the 802.11i standard, WPA, is being deployed at this time.

### 802.1X

An IEEE authentication framework for 802.11 networks. Allows multiple authentication algorithms, including EAP and RADIUS.

#### **Access Point**

A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Some access points can also bridge to each other.

#### ACL

Access Control List. ACLs define what traffic types will be allowed or denied across one or more Interfaces. Each traffic type can be used in multiple ACLs, depending on up to 64 Rules defined for each ACL. If no ACL is applied to an Interface, all traffic types are allowed.

#### Ad-Hoc Mode

A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is one where PCs communicate with each other through an AP. See access point and Infrastructure mode.

#### **AES**

Advanced Encryption Standard. An encryption algorithm selected by the 802.11i task group to provide robust security in wireless networks.

## **Alcatel Wireless Operating System**

Alcatel Wireless Operating System. Software that controls Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances and Alcatel OmniAccess Wireless Access Points. Includes OmniVista AirView Software and Alcatel Wireless Operating System Security functions.

## **Alcatel Wireless Operating System Security**

Part of the Alcatel Wireless Operating System that controls all aspects of Security and roaming for the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System), providing seamless access to business-critical resources.

### **OmniVista AirView Software**

Part of the Alcatel Wireless Operating System that continually monitors associated OmniAccess APs for Traffic Load, Interference, Noise, Coverage, and Nearby APs.

Using the collected information, the OmniVista AirView Software dynamically reassigns channels, adjusts the transmit power to load balance coverage and capacity, allows the operator to group nearby OmniAccess APs, automatically detects and configures new OmniAccess APs, automatically detects and configures new Alcatel OmniAccess Switches and Appliances, and detects and reports coverage holes.

### AP

See Access Point.

#### ΔΡΙ

Application Programming Interface. The interface an application uses to call the operating system and other services. The API is usually defined at the source code level, and provides an interface between the application and the operating system.

# **Applet**

An application or utility program that is designed to do a very specific and limited task.

### **Application Software**

A computer program that is designed to do a general task. For example, word processing, payroll, Internet browsers and graphic design programs would all be considered applications.

#### **Association**

The process used by a client to connect to an Access Point.

#### Authentication

The process used to confirm a client's identity before communication is allowed with other devices connected to the Access Point.

## **Backbone**

The central part of a large network that links two or more subnetworks and is the primary path for data transmission for a large business or corporation. A network can have a wired backbone or a wireless backbone.

#### **Bandwidth**

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of clients, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; Standards 802.11a and 802.11g provide a bandwidth of 54 Mbps. These are the raw capabilities of the network. Many things conspire to reduce these values, including protocol overhead, collisions, and implementation inefficiencies.

### **BIOS**

Basic Input/Output System.

# Bits per Second (bps)

A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second-bps-is often confused with bytes per second-Bps. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps), it is sending data at 1.375 megabytes per second (1.375 Mbps).

# Blacklist

Obsolete reference to the Disable feature.

#### **Bluetooth Wireless**

A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet.

#### Bootloader

An operating system ppcboot module that loads software entities in a defined order to create a functional operating system.

# **Bridge**

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

## **Broadband**

A comparatively fast Internet connection. Services such as ISDN, cable modem, DSL and satellite are all considered broadband as compared to dial-up Internet access. There is no official speed definition of broadband but services of 100 Kbps and above are commonly thought of as broadband.

# **Bus Adapter**

A special adapter card that installs in a PC's PCI or ISA slot and enables the use of PC Card radios in desktop computers. Some companies offer one-piece PCI or ISA Card radios that install directly into an open PC or ISA slot.

#### CA

Certification Authority. A trusted entity or person who issues public-key certificates for data encryption.

#### **Cable Modem**

A kind of converter used to connect a computer to a cable TV service that provides Internet access. Most cable modems have an Ethernet Out cable that attaches to a client's Wi-Fi gateway.

#### Cert

Certificate. Used to authenticate the server and encrypt data transmissions between server and browser. See CA and ID Certificate.

# **Certification Authority**

See CA.

## Cipher

An algorithm used to encrypt data.

## Client

Any computer or handheld device connected to a network that requests services (files, print capability) from another member of the network. Each client is associated with a unique MAC address.

#### **Client Device**

A Client is an wireless LAN end user. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like Access Points and Gateways.

# **Collision Avoidance**

A network node characteristic for detecting traffic before transmitting so it can transmit a signal without risking a collision.

# **CPU**

Central Processing Unit. The microprocessor part of a computer that interprets and executes instructions.

#### **Crossover Cable**

A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one plug to another, the signals cross over.

For instance, in an eight-wire crossover cable, the signal starts on pin one at one end of the cable and ends up on pin eight at the other end. Similarly, the other wires cross over from pin two to pin seven, pin three to pin six, and pin four to pin five.

#### CSMA/CA

CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk" method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios-radios capable of transmission or reception-but not both simultaneously.

Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

#### CSMA/CD

A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

# **DC Power Supply**

A module that converts AC power to DC. Depending on manufacturer and product, these modules can range from typical "wall wart" transformers that plug into a wall socket and provide DC power via a tiny plug to larger, enterprise-level Power Over Ethernet systems that inject DC power into the Ethernet cables connecting access points.

# DES

Data Encryption Standard. A cryptographic algorithm used to protect data transmitted through an unsecured network.

# **DHCP**

A utility that enables a server to dynamically assign IP Addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP Addresses of all the computers on the network. When DHCP is used, it automatically assigns an IP Address to each computing device as it logs onto the network.

#### Dialup

A communication connection via the standard telephone network, or Plain Old Telephone Service (POTS).

#### **Digital Certificate**

An electronic message used to verify a client's identity, and which can be used to encrypt data. Used in asymmetric public/private key encryption, in which public-key encrypted data can only be decrypted with the private key, and vice versa.

#### Disable

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or disabled, from further association attempts for an operator-defined timeout. After the disable timeout, the client is allowed to retry authentication until it associates or fails authentication and is disabled again.

The Alcatel Wireless Operating System also allows operators to permanently Disable clients by MAC address.

Note that this feature was formerly known as Blacklist.

# **Diversity Antenna**

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference.

#### DMZ

Demilitarized Zone. A network layer added between the outside network (least secure) and internal network (most secure) in order to add an extra level of security protection. Many companies choose to locate Wireless Switches, mail servers, Web servers, and remote access servers in the DMZ.

#### DNS

A program that translates URLs to IP Addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP Address on the Internet.

#### **DOS Attacks**

Denial of Service Attacks. A network attack that creates enough congestion to block normal traffic.

#### **DSCP**

Differentiated Services Code Point. A packet header code from 0 - 63 that can be used to define quality of service across the Internet.

#### DSI

Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (Plain Old Telephone Service) telephone wires.

#### **DSSS**

Direct Sequence Spread Spectrum. A carrier modulation technique used for 802.11b transmissions.

#### DTIM

Delivery Traffic Indication Map. A part of the TIM element in 802.11 beacons when a client has frames buffered in the AP for broadcasting or multicasting. The buffered frames are broadcasted or multicasted at each DTIM, when all power-saving clients expecting this data should be awake. See also TIM.

# **Dynamic Encryption Keys**

Regularly-refreshed encryption keys. Used in LEAP and WPA protocols to decrease the ability to decrypt the encoded data.

## EAP

Extensible Authentication Protocol. Used under 802.1X framework as a PPP extension to provide additional authentication options.

#### **EIRP**

Effective Isotropic Radiated Power. The equivalent transmitted signal power relative to a hypothetical isotropic (omnidirectional) radiator, measured in dBi (decibels isotropic).

## Encryption

A method of scrambling data to maintain privacy.

# **Encryption Key**

An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

## **Enterprise**

A term that is often applied to large corporations and businesses. The enterprise market can incorporate office buildings, manufacturing plants, warehouses and R&D facilities, as well as large colleges and universities.

#### **ESSID**

The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) ESSID is also known as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

#### **Ethernet**

International standard networking technology for wired implementations. Basic 10Base-T networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

### **FCS**

Frame Check Sequence. A cyclic redundancy check (CRC) Physical Layer 1 error-detection algorithm.

#### **FIPS**

Federal Information Processing Standard. Refer to FIPS Publication 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) for more information.

# **Firewall**

A system that enforces an access control policy between two or more networks, securing the network(s) and preventing access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

# **FireWire**

A high-speed serial bus system, FireWire is the IEEE 1394 standard for input/output technology that connects multimedia and storage peripherals to a PC. FireWire (Apple), 1394 (Linux) and iLink (Sony) are different names for products that perform the same function. FireWire can provide a bandwidth of about 400 Mbps.

#### .FPE

A filename extension used by the ACS Floor Plan Editor for wall map configuration files. Requires a corresponding .GIF, .JPG, .BMP, or .PNG file when importing into ACS.

### **GARP**

General Attribute Registration Protocol.

### Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

## **GigE**

A Gigabit Ethernet IEEE standard (802.3) for operating 1000 Mbps Ethernet networks (LANs) with fiber optic cables and wiring hubs. See also 1000Base-SX.

#### GUI

Graphical User Interface. A computer user interface based on graphics rather than text; uses a mouse or other input device as well as a keyboard.

#### **GVRP**

GARP VLAN Registration Protocol.

## **HotSpot**

A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as CoolSpots.

#### Hub

A multiport device used to connect PCs to a network via Ethernet cabling or via wireless connections. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

# Ηz

The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535-1605 kHz, the FM broadcast radio frequency band is 88-108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.

## I/O

The term used to describe any operation, program or device that transfers data to or from a computer.

#### **ID Certificate**

A Certificate used by Web server operators to ensure secure server operation. Usually accompanied by a Private Key.

#### IEEE

Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

#### **IEEE 802.11**

A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. See also 802.11, 802.11a, 802.11b, 802.11g and 802.1X. See also WECA.

#### **IKE**

Internet Key Exchange. A protocol used to start, stop and monitor IPSec dynamic tunnels.

# iLink

Sony's term for IEEE1394 technology that provides a bandwidth of about 400 Mbps. Many people also refer to this high-speed communication technology using Apple's original term, FireWire. Future versions of 1394 will greatly increase the bandwidth.

## **Infrastructure Mode**

A client setting providing connectivity to an AP. As compared to Ad-Hoc mode, whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.

## Internet Appliance

A computer that is intended primarily for Internet access, is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, email services, entertainment and personal information management applications. An Internet appliance can be Wi-Fi enabled or it can be connected via a cable to the local network.

#### IΡ

Internet Protocol. A set of rules used to send and receive messages at the Internet address level.

# **IP Address**

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP Address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

## **IP Telephony**

Internet Protocol Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).

#### **IPSec**

IP Security. Protocol used to authenticate and/or encrypt IP data using IPSec and/or IKE secure tunnels. Used to support VPN tunnels across the internet.

# **IPSec Passthrough**

Alcatel Wireless Operating System Security feature that allows IPSec-equipped clients to communicate directly with other IPSec equipment.

# **IPX-SPX**

IPX, short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications.

Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications. Whereas the IPX protocol is similar to IP, SPX is similar to TCP. Together, therefore, IPX-SPX provides connection services similar to TCP/IP.

#### ISA

A type of internal computer bus that allows the addition of card-based components like modems and network adapters. ISA has been replaced by PCI and is not very common anymore.

#### **ISDN**

A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.

#### **ISO Network Model**

A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- Application, Layer 7
- Presentation, Layer 6
- Session, Layer 5
- Transport, Layer 4
- Network, Layer 3
- Data Link, Layer 2
- Physical, Layer 1

The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

#### ISS

A special software application that allows all PCs on a network access to the Internet simultaneously through a single connection and Internet Service Provider (ISP) account.

# **Key Management**

Ensuring that encryption keys are current and synchronized between clients and Access Points. Key management can be performed manually or automatically using 802.1X.

#### LAN

A system of connecting PCs and other devices within close physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

# LEAP

Cisco Wireless EAP. EAP used by Cisco equipment to secure wireless networks with WEP-based devices.

#### LWAPP

The pending IETF (Internet Engineering Task Force) Lightweight Access Point Protocol standard defining communications between Wireless LAN Switches and "Light" Access Points.

#### MAC

Medium Access Control. This is the function of a network controller that determines who gets to transmit when. Each network adapter must be uniquely identified. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

## **Mapping**

Assigning a PC to a shared drive or printer port on a network.

#### MIC

Message Integrity Check. Used to ensure the integrity of a received message.

#### **Mobile Device**

See Client, Client Device.

#### **Mobile Professional**

A salesperson or a "road warrior" who travels frequently and requires the ability to regularly access his or her corporate networks, via the Internet, to post and retrieve files and data and to send and receive email.

# NAT

A network capability that enables a houseful of computers to dynamically share a single incoming IP Address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP Address and creates new IP Address for each client computer on the network.

## **NetBIOS**

Network Basic Input/Output System. An API, or set of network commands, which activates network data transfer operations between IBM PC compatibles.

## **Network Name**

Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

#### NIC

A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

#### **NVRAM**

Non-Volatile Random Access Memory. Any type of memory that does not lose its contents when the main power is removed. (See also Volatile RAM.)

# OFDM

Orthogonal Frequency Division Multiplexing. A multi-carrier modulation technique used for 802.11a and 802.11g transmissions.

# **PC Card**

A removable, credit-card-sized memory or I/O device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

#### PCI

A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

#### **PCMCIA**

Expansion cards now referred to as "PC Cards" were originally called "PCMCIA Cards" because they met the standards created by the Personal Computer Memory Card International Association.

#### **PDA**

Smaller than laptop computers but with many of the same computing and communication capabilities, PDAs range greatly in size, complexity and functionality. PDAs can provide wireless connectivity via embedded Wi-Fi Card radios, slide-in PC Card radios, or Compact Flash Wi-Fi radios.

## **Peer-to-Peer Network**

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

## PEM

Privacy Enhanced Mail. PEM files are created from CSR files by a Certification Authority (CA) using base64 encoding with additional header and footer lines.

## PHY

The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

## Plug and Play

A computer system feature that automatic configures of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

#### POTS

Plain Old Telephone Service. Wired analog telephone service.

#### ppcboot

Alcatel OmniAccess Switch and Appliance Bootloader.

#### PPP

Point-to-Point Protocol.

# **Proxy Server**

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.

#### QoS

Quality of Service. A term that guarantees a specific throughput level. For instance, high QoS can be used to ensure adequate throughput for Voice over WLAN.

#### Range

How far will your wireless network stretch? Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile.

#### **RADIUS**

Remote Authentication Dial-In User Service. An authentication and accounting system used to exclude unauthorized clients.

## **Residential Gateway**

A wireless device that connects multiple PCs, peripherals and the Internet on a home network. Most Wi-Fi residential gateways provide DHCP and NAT as well.

#### RF

Radio Frequency. A frequency within which radio waves may be transmitted.

## **RJ-45**

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

#### Roaming

Moving seamlessly from one AP coverage area to another with no loss in connectivity.

# Router

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

#### RSN

Robust Security Network. An IEEE 802.11i working group strong authentication and encryption standard that uses 802.1X, EAP, AES, TKIP, and MIC.

# **RSSI**

Received Signal Strength Indicator, also known as Signal Strength. A measure of received RF energy, measured in dBm.

### **RTOS**

Real-time operating system. An operating system that features a guaranteed performance per time unit.

### Rx

Receive.

#### Satellite Broadband

A wireless high-speed Internet connection provided by satellites. Some satellite broadband connections are two-way-up and down. Others are one-way, with the satellite providing a high-speed downlink and then using a dial-up telephone connection or other land-based system for the uplink to the Internet.

#### Server

A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

## Site Survey

The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

#### SNR

Signal to Noise Ratio. The ratio of signal intensity to noise intensity, measured in dB.

#### SOHO

A term generally used to describe an office or business with ten or fewer computers and/or employees.

#### SSH

Secure Shell; also known as Secure Socket Shell. SSH data transmissions and passwords to and from Alcatel OmniAccess Wireless Switches and Appliances are encrypted and use digital certificates for authentication from both ends of the connection. SSH is always enabled for Alcatel OmniAccess Switches and Appliances.

When you plan to secure the Alcatel OmniAccess Switch or Appliance Telnet Interface using the SSH protocol, note that the Alcatel Wireless Operating System automatically generates its own local SSH certificate and automatically applies it to the Telnet Interface.

#### **SSID**

A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a name when a mobile device tries to connect to an access point. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to associate with the AP unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

#### SSL

Secure Sockets Layer. Commonly used encryption protocol used by many enterprises to protect the security and integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server to complete a secret key exchange for that session.

When you plan to secure the Alcatel OmniAccess Switch or Appliance HTTP: Web Browser Interface using the https: (HTTP + SSL) protocol, note that the Alcatel Wireless Operating System automatically generates its own local Web Administration SSL certificate and automatically applies it to the Web Browser Interface.

# Static Key

An encryption key that has been entered into both access point and client, used for encrypting data communications. Static WEP keys can be cracked, but AES keys are currently safe for wireless transmissions.

## Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

#### **Subscriber**

A subscriber is the user who accesses network services through an 802.11 client.

#### Switch

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a network traffic policeman: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

#### **TCP**

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP Address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

#### TCP/IP

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the client's computer address on a network. Every computer in a TCP/IP network has its own IP Address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

### **TFTP**

Trivial File Transfer Protocol.

#### TIM

Traffic Indication Map. An element in all 802.11 beacons when a client has frames buffered in the AP. The buffered frames are broadcasted or multicasted at each DTIM, when all power-saving clients expecting this data should be awake. See also DTIM.

#### TKIP

Temporal Key Integrity Protocol. Generates new keys every 10 kb of payload traffic.

# Τx

Transmit.

#### USB

A high-speed bidirectional serial connection between a PC and a peripheral that transmits data at the rate of 12 megabits per second. The new USB 2.0 specification provides a data rate of up to 480 Mbps, compared to standard USB at only 12 Mbps. 1394, FireWire and iLink all provide a bandwidth of up to 400 Mbps.

#### **VLAN**

Virtual LAN. A networking mechanism that makes clients appear as if they are connected to the same network, even if they are physically located on different LAN segments. Alcatel recommends that you assign one set of VLANs for WLANs and a different set of VLANs for mobility groups to ensure that Alcatel OmniAccess Switches and Appliances properly route VLAN traffic.

#### **VoIP**

Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

# **Volatile RAM**

Volatile Random Access Memory. The basic form of computer memory, which can be accessed randomly. In the Alcatel products, the Volatile RAM contains the active settings for current operations. Upon reboot, the Volatile RAM is cleared, and the configurations stored in the NVRAM are copied into the Volatile RAM. (See also NVRAM.)

#### **VPN**

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

#### WAN

A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Telephone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).

## War Chalking

Marking symbols on sidewalks and walls to indicate nearby APs. This allows other 802.11-equipped clients to connect to the Internet using other peoples' APs. This practice was inspired by hobos during the Great Depression who used chalk marks to indicate friendly homes.

### WebAuth

Web Authentication. An application-layer authentication of a user by username and password contained in either a local or RADIUS database.

#### **WECA**

Wireless Ethernet Compatibility Alliance, the former name of the Wi-Fi Alliance.

# WEP

Wired Equivalent Privacy. Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. Alcatel equipment supports the following WEP versions:

40-bit, also called 64-bit encryption.

- 108-bit, also called 128-bit encryption.
- 128-bit, also called 152-bit encryption.

#### Wi-Fi Alliance

An organization of wireless equipment and software providers, formerly known as the Wireless Ethernet Compatibility Alliance (WECA), organized to certify 802.11-based products for interoperability and to promote Wi-Fi as the universal brand name for 802.11-based wireless LAN products.

While all 802.11a/b/g products are called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as 'Wi-Fi Certified'. Currently, all Alcatel OmniAccess Wireless Access Points have 802.11a and 802.11b Wi-Fi certification.

## **WISP**

Wireless Internet Service Provider.

#### **WLAN**

Also referred to as Wireless LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

#### **WPA**

Wi-Fi Protected Access. A subset of the IEEE 802.11i wireless LAN security/encryption standard. Uses TKIP. Currently supported by the Alcatel OmniAccess Wireless Switch and Appliance.

### VG

Virtual Gateway. A virtual (unassigned, reserved) IP address, such as 1.1.1.1, used by Alcatel Layer 3 Security and Mobility managers.

# XAuth

Extended Authentication. A client authentication protocol used with other protocols, such as IKE.

# **Alcatel OmniAccess Wireless System Supported Regulatory Domains**

The Alcatel OmniAccess Wireless System has been approved or is being approved to operate in the following regulatory domains, and fully conforms with current regulatory domain requirements. Note that some of these entries may change over time; consult Alcatel Technical Support for current approvals.

Note that the maximum regulatory Transmit Power Level Limits published here are defined by the Country Code setting, and are regulated on a country by country basis. Also note that the actual maximum transmit power levels may be less than the published regulatory limits.

Country Code/ Country	802.11 Bands	Channels Allowed	Maximum Transmit Power (RadioTx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
AT/ Austria	а	36, 40, 44, 48	60 mW EIRP	In	5.15-5.25	BMV/ FSB-LD047
Adstria	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	130 20047
AU/ Australia	а	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.725-5.825	ACA
	b	1 - 11	200 mW EIRP	Both	2.4-2.4835	
BE/ Belgium	а	36, 40, 44, 48 52, 56, 60, 64	120 mW EIRP 120 mW EIRP	In In	5.15-5.25	BIPT/ Annexe B3 Interface radio HIPERLAN
	b/g	1 - 12 13	100 mW EIRP 100 mW EIRP	In Out	2.4-2.4835	Tadio IIII EREAN
(tbd)/ Brazil	а	(tbd)	1 W EIRP	Both	5.725-5.85	Anatel/ Resolution 305
DIGZII	(tbd	1 - 11	1 W EIRP	Both	2.4-2.4835	Resolution 303
CA/ Canada	а	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	Industry Canada RSS-210
	b/g	1 - 11	1 W+Restricted Antennas	Both	2.4-2.4835	
CH/ Switzer- land and	а	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	OFCOM
Liechten- stein	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
DE/ Germany	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	RegTP/ wlan35
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
DK/ Denmark	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	ITST/ Radio interface speci- fication 00 007
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	

Country Code/ Country	802.11 Bands	Channels Allowed	Maximum Transmit Power (RadioTx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
ES/ Spain	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Ministry of Telecom- munications
	b/g	1 - 11	100 mW EIRP	In	2.412-2.472	
FI/ Finland	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	FICORA/ RLAN Notice
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
FR/ France	а	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	A.R.T./ Decision 01-441
	b/g	1 - 7 8 - 11	100 mW EIRP 100 mW EIRP	Both In	2.4-2.4835 2.4-2.454	
GB/ United Kingdom	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	UKRA/ IR2006
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
GR/ Greece	b/g	1 - 11	100 mW EIRP	In	2.4-2.4835	Ministry of Transport & Communications
HK/ Hong Kong	а	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W+6 dBi=4 W	Both Both Both	5.15-5.25 5.25-5.35 5.725-5.85	OFTA
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
IE/ Ireland	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	COMREG/ ODTR 00/61, ODTR 0062
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
IN/ India	а	(TBD)	(TBD)	(TBD)	(TBD)	(TBD)
maia	b					
IS/ Iceland	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	РТА
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	

Country Code/ Country	802.11 Bands	Channels Allowed	Maximum Transmit Power (RadioTx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
IT/ Italy	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Ministry of Comm
	b/g	1 - 11	100 mW EIRP	In	2.4-2.4835	
JP/ Japan	а	1-3 1-4	100 mW EIRP 100 mW EIRP	Both In	5.03-5.09 5.15-5.25	Telec/ARIB STD-T66
	b	1-14	10 mW/MHz~200mW EIRP	(tbd)	2.4-2.497	
	g	1-13	10 mW/MHz~200mW EIRP	(tbd)	2.4-2.497	
KR/	а	149, 153, 157, 161	150 mW+6 dBi~600 mW	Both	5.725-5.825	RRL/
Republic of Korea	b/g	1-13	150 mW+6 dBi~600 mW	Both	2.4-2.4835	MIC Notice 2003-13
LU/ Luxem- bourg	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	ILR
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
NL/ Nether- lands	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Radiocom Agency
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
NO/ Norway	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	NPT
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
(tbd)/ Philippines	а	(tbd)	(tbd)	(tbd)	5.725-5.875	PDC
i imppines	(tbd)	1-13	100 mW EIRP	(tbd)	2.4-2.4835	
PT/ Portugal	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	NCA
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
SE/ Sweden	а	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	PTS
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	]

Country Code/ Country	802.11 Bands	Channels Allowed	Maximum Transmit Power (RadioTx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
SG/ Singapore	а	36, 40, 44, 48 (tbd)	100 mW EIRP 100 mW EIRP	Both Both	5.15-5.25 5.725-5.85	IDA/ TS SSS Issue 1
	b/g	1 - 11	100 mW EIRP	Both	2.4-2.4835	
TH/ Thailand	а	(tbd)	(tbd)	(tbd)	5.725-5.875	PDT
mananu	b/g	1-13	100 mW EIRP	In	2.4-2.5	
TW/ Taiwan	а	(tbd) 149, 153, 157, 161	50 mW+6 dBi=200 mW 1 W EIRP	In Both	5.25-5.35 5.725-5.825	PDT
	b/g	1-13	1 W EIRP	Both	2.4-2.4835	
US/ United States of America	а	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	FCC Part 15
America	b/g	1 - 11	1 W Conducted Output	Both	2.4-2.4835	
USL/ United States of	а	36, 40, 44, 48 52, 56, 60, 64	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W	In Both	5.15-5.25 5.25-5.35	FCC Part 15
America LOW	b/g	1 - 11	1 W Conducted Output	Both	2.4-2.4835	

# **Alcatel OmniAccess Wireless System CLI Reference**

System Release 2.0

The Alcatel OmniAccess Wireless System Command Line Interface (CLI) allows operators to connect an ASCII console to the Alcatel OmniAccess Switch or Appliance and configure the Alcatel OmniAccess Switch or Appliance and its associated OmniAccess APs using the Command Line Interface. The <u>Using the Alcatel OmniAccess Wireless System CLI</u> section describes most of the high-level CLI tasks, and the following sections provide additional information:

- ? command
- Help Command
- <u>Viewing Configurations</u>
- <u>Setting Configurations</u>
- Saving Configurations
- Clearing Configurations, Logfiles, and Other Functions
- <u>Uploading and Downloading Files and Configurations</u>
- <u>Troubleshooting</u>

# ? command

To display all of the commands in your current level of the command tree, or to display more information about a particular command, use the ? command.

>?

>(command name) ?

When you enter a command information request, put a space between the (command name) and the ? (question mark).

**Example 1** >? (at root level)

Clear Reset the switch or reset configuration to factory

defaults.

**Config** Configure switch options and settings.

Debug Manages system debug options.

Help.

Linktest <MAC addr> Perform a link test to a specified MAC address.

Logout Exit this session. Any unsaved changes are lost.

Ping <ip address> Send ICMP echo packets to a specified IP address.

Reset system Reset options.

Save config Save current switch settings to Non-volatile RAM.

**Show**Display switch options and settings. **Transfer**Transfer a file to or from the switch.

Shows you all the commands and levels available from the root level.

Example 2 >transfer download d?

datatype

shows you that datatype is the only entry at the transfer download level.

Example 3 >transfer download datatype ?

<config/code> Enter datatype: config or code.

shows you the permissible entries for the transfer download datatype

command.

# **Help Command**

To look up keyboard commands, use the help command at the root level.

>help

```
Example
               >help
               HELP:
               Special keys:
               DEL, BS .... delete previous character
               Ctrl-A .... go to beginning of line
               Ctrl-E \dots go to end of line
               Ctrl-F .... go forward one character
               Ctrl-B .... go backward one character
               Ctrl-D .... delete current character
               Ctrl-U, X . delete to beginning of line
               Ctrl-K \dots delete to end of line
               Ctrl-W .... delete previous word
               Ctrl-T .... transpose previous character
               Ctrl-P .... go to previous line in history buffer
               Ctrl-N \dots go to next line in history buffer
               Ctrl-Z .... return to root command prompt
               Tab, <SPACE> command-line completion
               Exit ..... go to next lower command prompt
               ? ..... list choices
```

# **Viewing Configurations**

To view Alcatel OmniAccess Switch or Appliance options and settings, use the show commands.

- show 802.11a
- show 802.11b
- show acl
- show advanced 802.11a
- <u>show advanced 802.11b</u>
- show advanced timers
- show arp switch
- show ap
- show blacklist
- show certificate
- show client
- show country
- show cpu
- <u>show custom-web</u>
- show debug
- show eventlog
- <u>show interface</u>
- show inventory
- <u>show load-balancing</u>
- show loginsession
- show macfilter
- <u>show mgmtuser</u>
- show mirror
- show mobility summary
- show msqloq
- show netuser
- show network
- <u>show gos queue</u> <u>length all</u>
- show port
- show radius
- show roque ap
- <u>show roque client</u>
- show route summary
- <u>show serial</u>

- show sessions
- <u>show snmpcommunity</u>
- show snmptrap
- <u>show snmpv3user</u>
- <u>show snmpversion</u>
- <u>show spanningtree port</u>
- <u>show spanningtree switch</u>
- show stats
- show switchconfig
- show sysinfo
- show syslog
- <u>show time</u>
- show trapflags
- show traplog
- show watchlist
- show wlan
- <u>show wlan summary</u>
- <u>show wps-peers summary</u>

# show 802.11a

To display basic 802.11a options and settings, use the show 802.11a command.

# >show 802.11a

Syntax	show	Display configurations.	
	802.11a	802.11a configurations.	

**Defaults** (none)

Examples >show 802.11a

802.11a Network Enabled					
802.11a Low Band Enabled					
802.11a Mid Band Enabled					
802.11a High Band Enabled					
802.11a Operational Rates					
802.11a 6M Rate Mandatory					
802.11a 9M Rate Supported					
802.11a 12M Rate Mandatory					
802.11a 18M Rate Supported					
802.11a 24M Rate Mandatory					
802.11a 36M RateSupported					
802.11a 48M Rate Supported					
802.11a 54M Rate Supported					
Beacon Interval					
CF Pollable mandatory Disabled					
CF Poll Request mandatory Disabled					
CFP Period 4					

CFP Maximum Duration	100
Default Channel	36
Default Tx Power Level	1
DTIM Period	10
Fragmentation Threshold	2346
Long Retry Limit	4
Maximum Rx Life Time	512
Max Tx MSDU Life Time	512
Medium Occupancy Limit	100
RTS Threshold	2347
Short Retry Limit	7
TI Threshold	-50

#### **Related Commands**

show 802.11b, show advanced 802.11a channel, show advanced 802.11a group, show advanced 802.11a logging, show advanced 802.11a monitor show advanced 802.11a power, show advanced 802.11a profile, show advanced 802.11a summary

# show 802.11b

To display basic 802.11b/g options and settings, use the show 802.11b command.

>show 802.11b

SyntaxshowDisplay configurations.802.11b802.11b/g configurations.

**Defaults** (none)

Examples >show 802.11b

802.11b Network	Enabled
dot11gSupport	Disabled
802.11b Operational Rates	
802.11b 1M Rate	Mandatory
802.11b 2M Rate	Mandatory
802.11b 5.5M Rate	Mandatory
802.11b 11M Rate	Mandatory
Beacon Interval	100
CF Pollable mode	Disabled
CF Poll Request mandatory	
CFP Period	4
CFP Maximum Duration	60
Default Channel	1
Default Tx Power Level	1
DTIM Period	1
ED Threshold	-50
Fragmentation Threshold	2346
Long Retry Limit	4
Maximum Rx Life Time	512
Max Tx MSDU Life Time	512
Medium Occupancy Limit	100
PBCC mandatory	Disabled
RTS Threshold	2347
Short Preamble mandatory	Enabled
Short Retry Limit	7

# **Related Commands**

show 802.11a, show advanced 802.11b channel, show advanced 802.11b group, show advanced 802.11b logging, show advanced 802.11b monitor, show advanced 802.11b txpower, show advanced 802.11b profile, show advanced 802.11b summary

# show acl

To display system Access Control Lists., use the show acl command.

>show acl [summary/detailed]

**Syntax** show acl Command action.

summary Display a summary of the Access Control Lists. detailed Display detailed Access Control List information.

**Defaults** (none)

Examples >acl summary

ACL Name Applied
----Pubs Only Yes
Macnica Yes

**Related Commands** config interface acl

# **SHOW ADVANCED 802.11A COMMANDS**

Use the following show advanced 802.11a commands:

- show advanced 802.11a channel
- show advanced 802.11a group
- show advanced 802.11a logging
- show advanced 802.11a monitor
- show advanced 802.11a txpower
- show advanced 802.11a profile
- show advanced 802.11a summary

# show advanced 802.11a channel

To display the automatic channel assignment configuration and statistics, use the show advanced 802.11a channel command.

#### >show advanced 802.11a channel

**Syntax** show Display configurations.

advanced Advanced parameters.
802.11a 802.11a network.
channel Channel status.

**Defaults** (none)

Examples >show advanced 802.11a channel

Automatic Channel Assignment

Channel Update Contribution..... SN.

Related Commands config 802.11a channel

# show advanced 802.11a group

To display the advanced 802.11a OmniAccess Radio RF grouping, use the show advanced 802.11a group command.

#### >show advanced 802.11a group

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.
	group	RF grouping values.

**Defaults** (none)

Examples >show advanced 802.11a group

Radio RF Grouping

 802.11a Group Mode...
 AUTO

 802.11a Group Update Interval.
 600 seconds

 802.11a Group Leader.
 a5:6b:ac:10:01:6b

 802.11a Group Member.
 a5:6b:ac:10:01:6b

 802.11a Last Run.
 133 seconds ago

**Related Commands** config advanced 802.11a group-mode

# show advanced 802.11a logging

To display advanced 802.11a RF event and performance logging, use the show advanced 802.11a logging command.

#### >show advanced 802.11a logging

Syntax	show	Display configurations.		
	advanced	Advanced narameters		

advanced Advanced parameters. 802.11a 802.11a network.

logging RF event and performance logging.

**Defaults** (none)

Examples > show advanced 802.11a logging

RF Event and Performance Logging

**Related Commands** config advanced 802.11a logging channel, config advanced 802.11a logging

coverage, config advanced 802.11a logging foreign, config advanced 802.11a logging load, config advanced 802.11a logging noise, config advanced 802.11a

logging performance, config advanced 802.11a logging power

# show advanced 802.11a monitor

To display the advanced 802.11a default OmniAccess Radio monitoring, use the show advanced 802.11a monitor command.

>show advanced 802.11a monitor

Syntax show Display configurations.

advanced Advanced parameters. 802.11a 802.11a network.

monitor OmniAccess Radio monitoring values.

**Defaults** (none)

Examples >show advanced 802.11a monitor

Default 802.11a Cell monitoring

 802.11a AP Coverage Interval
 180 seconds

 802.11a AP Load Interval
 60 seconds

 802.11a AP Noise Interval
 180 seconds

 802.11a AP Signal Strength Interval
 60 seconds

Related Commands config advanced 802.11a monitor coverage, config advanced 802.11a monitor

load, config advanced 802.11a monitor noise, config advanced 802.11a monitor

signal

# show advanced 802.11a txpower

To view the advanced 802.11a automatic transmit power assignment, use the show advanced 802.11a txpower command.

#### >show advanced 802.11a txpower

**Syntax** show Display configurations.

advanced Advanced parameters.
802.11a 802.11a network.
txpower Transmit Power.

**Defaults** (none)

Examples >show advanced 802.11a txpower

Automatic Transmit Power Assignment

 Power Assignment Leader
 a5:6b:ac:10:01:6b

 Last Run
 384 seconds ago

**Related Commands** config advanced 802.11a txpower-update, config 802.11a txPower

# show advanced 802.11a profile

To display the advanced 802.11a AP performance profiles, use the show advanced 802.11a profile command.

>show advanced 802.11a profile global

>show advanced 802.11a profile <AP name>

**Syntax** show Display configurations.

advanced Advanced parameters. 802.11a 802.11a network.

profile OmniAccess Radio performance profile.

**Defaults** (none)

# Examples >show advanced 802.11a profile global

Default 802.11a Cell performance profiles

802.11a	Global	Interference threshold	10%
802.11a	Global	noise threshold	-70 dBm
802.11a	Global	RF utilization threshold	80%
802.11a	Global	throughput threshold	1000000 bps
802.11a	Global	clients threshold	12 clients
802.11a	Global	coverage threshold	12 dB
802.11a	Global	coverage exception level	80%
802.11a	Global	client minimum exception lev	3 clients

## >show advanced 802.11a profile AP1

OmniAccess AP performance profile not customized.

This response indicates that the performance profile for this AP is using the global defaults and has not been individually configured.

#### **Related Commands**

config advanced 802.11b profile clients, config advanced 802.11b profile coverage, config advanced 802.11b profile customize, config advanced 802.11b profile exception, config advanced 802.11b profile foreign, config advanced 802.11b profile level, config advanced 802.11b profile noise, config advanced 802.11b profile throughput, config advanced 802.11b profile utilization

# show advanced 802.11a summary

To display the advanced 802.11a AP name, channel, and transmit level summary, use the show advanced 802.11a summary command.

#### >show advanced 802.11a summary

Syntax	show	Display configurations.
	advanced	Advanced parameters.
	802.11a	802.11a network.

summary AP name, channel, and transmit level summary.

**Defaults** (none)

Examples > show advanced 802.11a summary

AP Name	Channel	Power Level
AP1	36*	8
ac:10:02:72:2f:bf	14*	4
ac:10:02:72:2f:c0	6*	7

**Related Commands** show advanced 802.11b summary

# **SHOW ADVANCED 802.11B COMMANDS**

Use the following show advanced 802.11b commands:

- show advanced 802.11b channel
- show advanced 802.11b group
- show advanced 802.11b logging
- show advanced 802.11b monitor
- show advanced 802.11b txpower
- show advanced 802.11b profile

show advanced 802.11b summary

# show advanced 802.11b channel

To display the automatic channel assignment status and statistics, use the show advanced 802.11b channel command.

#### >show advanced 802.11b channel

SyntaxshowDisplay configurations.advancedAdvanced parameters.802.11b802.11b/g network.channelChannel status.

**Defaults** (none)

Examples >show advanced 802.11b channel

Automatic Channel Assignment

Related Commands config 802.11b channel

# show advanced 802.11b group

To display the advanced 802.11b/g OmniAccess Radio RF grouping, use the show advanced 802.11b group command.

## >show advanced 802.11b group

SyntaxshowDisplay configurations.advancedAdvanced parameters.802.11b802.11b/q network.

802.11b 802.11b/g network. group RF grouping values.

**Defaults** (none)

Examples >show advanced 802.11b group

Radio RF Grouping

 802.11b Group Mode.
 AUTO

 802.11b Group Update Interval
 600 seconds

 802.11b Group Leader
 a5:6b:ac:10:01:6b

 802.11b Group Member
 a5:6b:ac:10:01:6b

 802.11b Last Run
 511 seconds ago

**Related Commands** config advanced 802.11b group-mode

# show advanced 802.11b logging

To display advanced 802.11b/g RF event and performance logging, use the show advanced 802.11b logging command.

>show advanced 802.11b logging

**Syntax** show Display configurations.

advanced Advanced parameters.

802.11b 802.11b network.

logging RF event and performance logging.

**Defaults** (none)

Examples >show advanced 802.11b logging

RF Event and Performance Logging

Related Commands config advanced 802.11b logging channel, config advanced 802.11b logging

coverage, config advanced 802.11b logging foreign, config advanced 802.11b logging load, config advanced 802.11b logging noise, config advanced 802.11b

logging performance, config advanced 802.11b logging power

# show advanced 802.11b monitor

To display the advanced 802.11b/g default OmniAccess Radio monitoring, use the show advanced 802.11b monitor command.

>show advanced 802.11b monitor

**Syntax** show Display configurations.

advanced Advanced parameters. 802.11b 802.11b/g network.

monitor OmniAccess Radio monitoring values.

**Defaults** (none)

Examples >show advanced 802.11b monitor

Default 802.11b AP monitoring

Related Commands config advanced 802.11b monitor coverage, config advanced 802.11b monitor

load, config advanced 802.11b monitor noise, config advanced 802.11b

monitor signal

# show advanced 802.11b txpower

To view the advanced 802.11b/g automatic transmit power assignment, use the show advanced 802.11b txpower command.

>show advanced 802.11b txpower

**Syntax** show Display configurations.

advanced Advanced parameters.
802.11b 802.11b/g network.
txpower Transmit power.

**Defaults** (none)

# Examples >show advanced 802.11b txpower

Automatic Transmit Power Assignment

Transmit Power Assignment Mode..... AUTO

 Power Assignment Leader
 a5:6b:ac:10:01:6b

 Last Run
 489 seconds ago

Related Commands config 802.11b txPower

# show advanced 802.11b profile

To display the advanced 802.11b/g OmniAccess Radio performance profiles, use the show advanced 802.11b profile command.

>show advanced 802.11b profile global

>show advanced 802.11b profile <AP name>

**Syntax** show Display configurations.

advanced Advanced parameters.
802.11b 802.11b/g network.
profile AP performance profile.

**Defaults** (none)

# Examples >show advanced 802.11b profile global

Default 802.11b Cell performance profiles

# >show advanced 802.11b profile AP1

OmniAccess AP performance profile not customized

This response indicates that the performance profile for this AP is using the global defaults and has not been individually configured.

#### **Related Commands**

config advanced 802.11b profile clients, config advanced 802.11b profile coverage, config advanced 802.11b profile customize, config advanced 802.11b profile exception, config advanced 802.11b profile foreign, config advanced 802.11b profile level, config advanced 802.11b profile noise, config advanced 802.11b profile throughput, config advanced 802.11b profile utilization

# show advanced 802.11b summary

To display the advanced 802.11b/g OmniAccess AP name, channel, and transmit level summary, use the show advanced 802.11b summary command.

>show advanced 802.11b summary

**Syntax** show Display configurations. advanced Advanced parameters.

802.11b 802.11b/g network.

summary AP name, channel, and transmit level summary.

**Defaults** (none)

Examples >show advanced 802.11b summary

AP name	Channel	Txpower Level
AP1	11*	1
AP2	10*	4
AP3	6*	2

**Related Commands** show advanced 802.11a summary

# show advanced timers

To display the advanced mobility anchor, authentication response, and rogue entry timers, use the show advanced timers command.

#### >show advanced timers

**Syntax** show Display configurations.

advanced Advanced parameters. Advanced system timers.

**Defaults** Shown below in examples.

Examples >show advanced timers

Related Commands config advanced timers auth-timeout, config advanced timers rogue-ap

# show ap auto-rf

To display the auto-rf settings for an OmniAccess AP, use the show ap auto-rf command.

#### >show ap auto-rf <802.11a/802.11b> <AP name>

**Syntax** show Display configurations.

ap auto-rf OmniAccess Radio.

<802.11a/802.11b> 802.11a or 802.11b setting. <AP name> OmniAccess AP name.

**Defaults** (none)

Examples >show ap auto-rf 802.11a AP1

Noise Information

 Noise Profile
 PASSED

 Channel 1
 -96 dBm

 Channel 2
 -96 dBm

 Channel 3
 -93 dBm

 Channel 4
 -92 dBm

 Channel 5
 -96 dBm

Channel 6100 dBm	
Channel 799 dBm	
Channel 896 dBm	
Channel 995 dBm	
Channel 10	
Channel 1197 dBm	
Interference Information	
Interference Profile PASSED	
Channel 172 dBm @ 18 % bus	У
Channel 271 dBm @ 11 % bus	У
Channel 3128 dBm @ 0 % bus	У
Channel 4128 dBm @ 0 % bus	У
Channel 5128 dBm @ 0 % bus	У
Channel 6128 dBm @ 0 % bus	У
Channel 7128 dBm @ 0 % bus	У
Channel 8128 dBm @ 0 % bus	У
Channel 9128 dBm @ 0 % bus	У
Channel 10128 dBm @ 0 % bus	У
Channel 11128 dBm @ 0 % bus	У
Load Information	
Load Profile PASSED	
Receive Utilization	
Transmit Utilization	
Channel Utilization	
Attached Clients 0 clients	
Coverage Information	
Coverage Profile PASSED	
Failed Clients 0 clients	
Client Signal Strengths	
RSSI -100 dbm 0 clients	
RSSI -92 dbm 0 clients	
RSSI -84 dbm 0 clients	
RSSI -76 dbm 0 clients	
RSSI -68 dbm 0 clients	
RSSI -60 dbm 0 clients	
RSSI -52 dbm 0 clients	
Client Signal To Noise Ratios	
SNR 0 dbm 0 clients	
SNR 5 dbm 0 clients	
SNR 10 dbm 0 clients	
SNR 15 dbm 0 clients	
SNR 20 dbm 0 clients	
SNR 25 dbm 0 clients	
SNR 30 dbm 0 clients	
SNR 35 dbm 0 clients	
SNR 40 dbm 0 clients	
SNR 45 dbm 0 clients	
Nearby RADs	
RF Parameter Recommendations	
Channel0	
Power Level0	
RTS/CTS Threshold0	
Fragmentation Threshold0	
Antenna Pattern0	

**Related Commands** 

config 802.11a antenna, config 802.11b antenna, config cell

# show ap config

To display the detailed configuration for an 802.11b/g OmniAccess AP, use the show ap config command.

# >show ap config <802.11a/802.11b/general> <AP name>

>Billow ap	config <002.11a/002.11c	// general/ \Ar hame/	
Syntax	show ap <802.11a/802.11b/ general> <ap name=""></ap>	Display configurations. OmniAccess Radio. 802.11a, 802.11b/g or ge OmniAccess AP name.	neral settings.
Defaults	(none)		
Examples	OmniAccess AP Name Switch Port Number MAC Address OmniAccess AP Location. Primary OmniAccess Wirele Administrative State Operation State Monitor Only Mode S/W Version Boot Version Stats Reporting Period Number Of Slots Rad Model Rad Serial Number Attributes for Slot 0 Radio Type Administrative State Operation State	la AP1  ess Switch.	. AP1 5 00:0b:85:01:18:b0 . default location ADMIN_ENABLED LRAD_STATE_REG Disabled 2.0.113.3 1.1.20.0 0 2 AP-1200 01012203-10057105-01182  RADIO_TYPE_80211a ADMIN_ENABLED SLOT_STATE_UP
	Number Of WLANs  Medium Occupancy Limit CFP Period  CFP MaxDuration  Operation Rate Set 6000 Kilo Bits 9000 Kilo Bits 12000 Kilo Bits 24000 Kilo Bits 36000 Kilo Bits 48000 Kilo Bits 48000 Kilo Bits 54000 Kilo Bits 54000 Kilo Bits  Multi Domain Capability Multi Domain Capability	y Implemented.	2 100 4 60 00:0b:85:01:18:b0  MANDATORY SUPPORTED MANDATORY SUPPORTED MANDATORY SUPPORTED SUPPORTED SUPPORTED SUPPORTED 100 10 TRUE TRUE US

First Chan Num
MAC Operation Parameters  Configuration
Tx Power       5         Tx Power Level 1
Phy OFDM parameters  Configuration
Performance Profile Parameters  Configuration
>show ap config 802.11b AP1           OmniAccess AP Identifier         1           OmniAccess AP Name         AP1           Switch Port Number         5           MAC Address         00:0b:85:01:18:b0           OmniAccess AP Location         default location           Primary OmniAccess Wireless Switch            Administrative State         ADMIN_ENABLED           Operation State         LRAD_STATE_REG           Monitor Only Mode         Disabled           S/W Version         2.0.113.3           Boot Version         1.1.20.0           Stats Reporting Period         0           Number Of Slots         2

Rad Model	
Attributes for Slot 1 Radio Type Administrative State Operation State CellId	ADMIN_ENABLED SLOT_STATE_UP
Station Configuration Configuration Number Of WLANS Medium Occupancy Limit CFP Period CFP MaxDuration BSSID Operation Rate Set 1000 Kilo Bits 2000 Kilo Bits 11000 Kilo Bits Beacon Period DTIM Period Multi Domain Capability Implemented Multi Domain Capability Enabled Country String	2 100 4 60 00:0b:85:01:18:b0  . MANDATORY . MANDATORY . MANDATORY . MANDATORY . MANDATORY . 100 . 1 . TRUE . TRUE
Multi Domain Capability Configuration	1 11
MAC Operation Parameters  Configuration	2347 7 4 2346 512
Tx Power  Num Of Supported Power Levels.  Tx Power Level 1.  Tx Power Level 2.  Tx Power Level 3.  Tx Power Level 4.  Tx Power Level 5.  Tx Power Level 6.  Tx Power Level 7.  Tx Power Level 8.  Tx Power Configuration.  Current Tx Power Level	63 31 15 7 1 0 0 CUSTOMIZED
Phy DSSS parameters Configuration. Current Channel. Current CCA Mode. ED Threshold. Antenna Type.	6 0 -50

Diversity DIVERSITY_ENABLED AntennaMode ANTENNA_OMNI
Performance Profile Parameters  Configuration
Containment Count 0
>show ap config general AP1       1         OmniAccess AP Identifier       1         OmniAccess AP Name       AP1         AP Type       Alcatel         Switch Port Number       5         MAC Address       00:0b:85:01:18:b0         OmniAccess AP Location       Tech Pubs         Primary OmniAccess Wireless Switch       192.168.2.36         Administrative State       ADMIN_ENABLED         Operation State       LRAD_STATE_REG         Monitor Only Mode       Disabled         S/W Version       2.0.113.3         Boot Version       1.1.20.0         Stats Reporting Period       0         Number Of Slots       2         Rad Model       AP-1200         Rad Serial Number       01012203-10057105-01182
config 802.11a antenna, config 802.11b antenna, config cell

# show ap stats

To display the statistics for an 802.11b/g OmniAccess AP, use the show ap stats command.

>show ap stats <802.11a/802.11b> <AP name>

**Syntax** Display configurations. show OmniAccess Radio. ap

<802.11a/802.11b> 802.11a or 802.11b/g statistics.

<AP name> OmniAccess AP name.

**Defaults** (none)

**Examples** >show ap stats 802.11b AP1

> Rad Name..... AP1 Stats Information MulticastTxFrameCnt......0 RetryCount......0 MultipleRetryCount......0

FrameDuplicateCount0
RtsSuccessCount0
RtsFailureCount0
AckFailureCount0
RxFragmentCount0
MulticastRxFrameCnt0
FcsErrorCount0
TxFrameCount0
WepUndecryptableCount0

Related Commands config ap stats-timer

# show ap summary

To display a summary of all APs attached to the Alcatel OmniAccess Switch or Appliance, use the show ap summary command. A list containing each AP name, number of slots, manufacturer, MAC address, location and Alcatel OmniAccess Switch or Appliance port number will be displayed.

#### >show ap summary

**Syntax** show Display configurations.

ap All APs.

summary Summary of all APs.

**Defaults** (none)

Examples >show ap summary

Related Commands show advanced 802.11a summary, show advanced 802.11b summary, show

certificate summary, show client summary, show mobility summary, show

radius summary, show rogue-ap summary, show wlan summary

### show arp switch

To display the Alcatel OmniAccess Switch or Appliance MAC addresses, IP Addresses, and port types, use the show arp switch command.

#### >show arp switch

**Syntax** show Display configurations.

arp MAC addresses, IP Addresses, and port types. switch Alcatel OmniAccess Switch or Appliance parameters.

**Defaults** (none)

Examples >show arp switch

00:C0:A8:87:EA:78	MAC Address	IP Address	Port	VLAN	Type
	00:06:5B:3D:0B:5C	172.16.1.2	-	1	

**Related Commands** debug arp

# **SHOW AP COMMANDS**

Use the following show ap commands:

- show ap auto-rf
- show ap config
- show ap stats
- show ap summary

### show blacklist

To display a summary of all clients manually disabled (blacklisted) from associating with this Alcatel OmniAccess Switch or Appliance, use the show blacklist command. A list containing each manually disabled MAC address is displayed.

b

**Note:** Use the **show blacklist** command to view automatically disabled clients.

#### >show blacklist

**Syntax** show Display configurations.

blacklist Manual disable.

**Defaults** (none)

Examples >show blacklist

MAC Address Description

Related Commands config blacklist add, config blacklist delete, config blacklist description, show

client

### SHOW CERTIFICATE COMMANDS

Use the following show certificate commands:

- <u>show certificate compatibility</u>
- show certificate summary

### show certificate compatibility

To display whether certificates are verified as compatible in the Alcatel OmniAccess Switch or Appliance, use the show certificate compatibility command.

# >show certificate compatibility

**Syntax** show Display configurations.

certificate All certificates.

compatibility Compatibility of certificates.

**Defaults** (none)

Examples >show certificate compatibility

Certificate compatibility mode:..... off

**Related Commands** show certificate summary

# show certificate summary

To display a summary of all certificates active in the Alcatel OmniAccess Switch or Appliance, use the show certificate summary command.

### >show certificate summary

**Syntax** show Display configurations.

certificate All certificates.

summary Synopsis of all certificates.

**Defaults** (none)

Examples >show certificate summary

Web Administration Certificate...... Locally Generated Web Authentication Certificate...... Locally Generated

Certificate compatibility mode:..... off

Related Commands show certificate compatibility

### SHOW CLIENT COMMANDS

Use the following show client commands:

- <u>show client ap</u>
- <u>show client detail</u>
- show client summary
- show client username

### show client ap

To display the clients on an OmniAccess AP, use the show client ap command.

Note: The show client ap command may list the status of automatically disabled clients. Use the show blacklist command to view manually disabled (blacklisted) clients.

### >show client ap <802.11a/802.11b> <AP name>

Syntax show Display configurations.

ap OmniAccess Radio.

<802.11a/802.11b> 802.11a or 802.11b/g clients.

<AP name> OmniAccess AP name.

**Defaults** (none)

Examples >show client ap 802.11b AP1

 MAC Address
 AP ID
 Status
 WLAN Id
 Authenticated

 ----- ----- ----- ----- 

 00:0c:41:0a:33:13
 1
 Associated
 1
 No

Related Commands show client detail, show client summary, show client username, show blacklist

### show client detail

To display detailed information for a client on an OmniAccess AP, use the show client detail command.

Note: The show client ap command may list the status of automatically disabled clients. Use the show blacklist command to view manually disabled (blacklisted) clients.

#### >show client detail <MAC address>

Syntax						
-	ntax show Display configurations. client 802.11a or 802.11b/g c					
	detail	Connectivity informatio				
	<mac address=""></mac>	MAC address of the spe				
	(Wirto dadi ess)	Wite address of the spe	onio onorit.			
Defaults	(none)					
Examples	>show client detail 0	0:0c:41:0a:33:a6				
	Client MAC Address		00:0c:41:0a:33:a6			
	Client Username		N/A			
	AP MAC Address		00:0b:85:01:18:b0			
	Client State		Associated			
	Wireless LAN Id		1			
	IP Address		Unknown			
	Association Id		1			
	Authentication Algorithm	1	Open System			
	Reason Code(					
		0				
		0				
	Mobility State		None			
	Security Policy Complete	d	No			
	Policy Manager State		DHCP_REQD			
	Policy Manager Rule Crea	ted	No			
	NPU Fast Notified		Yes			
	WEP State	Disabled				
	Client Capabilities:					
	CF Pollable		Not implemented			
	CF Poll Request		Not implemented			
	Short Preamble		Implemented			
	PBCC		Not implemented			
	Channel Agility		Not implemented			
	Client Statistics:					
	Number of Bytes Re	ceived	0			
	Number of Bytes Se	nt	0			
	Number of Packets	Received	0			
	Number of Packets	Sent	0			
	Number of Policy E	rrors	0			
	Radio Signal Stren	gth Indicator	Unavailable			
	Signal to Noise Ra	tio	Unavailable			

# Related Commands

show client ap, show client summary, show client username, show blacklist

# show client summary

To display a summary of clients associated with an OmniAccess AP, use the show client summary command.

Note: The show client ap command may list the status of automatically disabled clients. Use the show blacklist command to view manually disabled (blacklisted) clients.

>show client summary

**Syntax** show Display configurations.

client 802.11a or 802.11b/g client.

summary All attached clients.

**Defaults** (none)

Examples >show client summary

**Related Commands** show client ap, show client detail, show client username, show blacklist

### show client username

To display clients by user name, use the show client username command.

>show client username <User Name>

**Syntax** show Display configurations.

username OmniAccess Radio. <User Name> Client User Name.

**Defaults** (none)

Examples >show client username IT\_007

MAC Address AP ID Status WLAN Id Authenticated

00:0c:41:0a:33:13 1 Associated 1 No

**Related Commands** show client ap, show client detail, show client summary

### show country

The Alcatel OmniAccess Switch or Appliance must be configured to comply with the target country's permitted 802.11a and/or 802.11b frequency bands. To display a list of supported countries and their permitted frequency bands, use the show country command. This command also shows you the current country setting for the Alcatel OmniAccess Switch or Appliance.

### >show country

**Syntax** show Display configuration options.

country Supported Countries.

**Defaults** (none)

Examples >show country

Supported Regulatory Domains

 US
 802.11a / 802.11b

 CA
 802.11b

 JP
 802.11a / 802.11b

 KR
 802.11a / 802.11b

 AU
 802.11a / 802.11b

 AT
 802.11a / 802.11b

 BE
 802.11a / 802.11b

 DK
 802.11a / 802.11b

 FI
 802.11a / 802.11b

 FR
 802.11a / 802.11b

 DE
 802.11a / 802.11b

 GR
 802.11b

 IE
 802.11a / 802.11b

IT	802.11a /	802.11b
LU	802.11a /	802.11b
NL	802.11a /	802.11b
PT	802.11a /	802.11b
ES	802.11b	
SE	802.11a /	802.11b
GB	802.11a /	802.11b
USL	802.11a /	802.11b
Configured Country	ed States	

Related Commands show sysinfo

# show cpu

To display current CPU usage information, use the show cpu command.

>show cpu

**Syntax** show cpu Command action.

**Defaults** (none)

Examples >show cpu

Current CPU load: 2.50

**Related Commands** show sysinfo

### show custom-web

To display Web Authentication customization information, use the show custom-web command.

>show custom-web

**Syntax** show custom-web Command action.

**Defaults** (none)

Examples >show custom-web

UnivergeLogo. Enabled
CustomLogo. Disabled
Custom Title. helpdesk
Custom Message. thisistheplace
Custom Redirect URL abc.com

Related Commands config custom-web

### show debug

Use the show debug command, to determine if MAC address debugging is enabled or disabled.

>show debug

**Syntax** show Display configurations.

debug MAC address debugging.

**Defaults** disabled

Examples >show debug

MAC debugging..... disabled

Related Commands debug mac

# show eventlog

Use the show eventlog command, to display the event log.

#### >show eventlog

<b>Syntax</b> show	Display configurations.
--------------------	-------------------------

eventlog System events.

**Defaults** (none)

Examples > show eventlog

	File	Line	TaskID	Code	d	h	m	S
EVENT>	nim.c	154	1234B2DC	00000000	0	0	0	44
EVENT>	bootos.c	447	12346F44	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	121160B4	00000000	0	0	0	44
EVENT>	bootos.c	447	12111D1C	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	121180A4	00000000	0	0	0	44
EVENT>	bootos.c	447	12113C24	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	1210D5CC	00000000	0	0	0	44
EVENT>	bootos.c	445	12109154	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	121176C4	00000000	0	0	0	44
EVENT>	bootos.c	445	12113244	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	121176C4	00000000	0	0	0	43
EVENT>	bootos.c	445	12113244	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	121176C4	00000000	0	0	0	44
EVENT>	bootos.c	445	12113244	AAAAAAA	0	0	0	17
EVENT>	nim.c	154	1210D44C	00000000	0	0	0	42
Would y	you like t	to dis	splay the	next 15	entries	3?	(y/	n)

Related Commands show msglog

### show interface

Use the show interfaces command, to display details of the system interfaces.

### >show interface [summary/detailed] <interface name>

Svntax	show interface	Command action
Sviitax	Show interface	Command action

summary Display a summary of the local interfaces. detailed Display detailed interface information.

interface name Identifies interface name for detailed display

**Defaults** (none)

Examples >show interface summary

Interface Name	Vlan Id	IP Address	Type
	_		
management	2	192.168.2.36	Static
service-port	N/A	172.16.16.199	Static
virtual	N/A	0.0.0.0	Static
vlan_301	301	192.168.2.200	Dynamic

### >show interface detailed management

Interface Name	management
MAC Address	00:0b:85:02:0d:20
IP Address	192.168.2.36

Primary DHCP Server10.1.2.11Secondary DHCP ServerUnconfiguredACLUnconfigured

**Related Commands** config interface

# show inventory

To display a physical inventory of the Alcatel OmniAccess Switch or Appliance, use the show inventory command.

>show inventory

**Syntax** show Display configurations.

inventory Physical Alcatel OmniAccess Switch or Appliance

configuration.

**Defaults** (none)

Examples >show inventory

Switch Description...... OmniAccess Wireless Switch

Machine ModelAS-2402Serial Number102389954Maintenance Level1.1.0.3

Gig Ethernet/Fiber Card...... Absent Crypto Accelerator..... Present

Related Commands show sysinfo

# show load-balancing

To display the status of the load-balancing feature, use the show load-balancing command.

>show load-balancing

**Syntax** show Display configurations.

load-balancing Status load-balancing.

**Defaults** Enabled

Examples > show load-balancing

Aggressive Load Balancing..... Enabled

Related Commands config load-balancing

# show loginsession

To display the existing sessions, use the show loginsession command.

>show loginsession

**Syntax** show Display configurations.

loginsession Current session details.

**Defaults** (none)

Examples >show loginsession

ID User Name Connection From Idle Time Session Time
-----00 admin 172.16.4.84 00:00:00 01:08:18

**Related Commands** config loginsession close

### show macfilter

To display the MAC filter table, use the show macfilter command. The MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers is displayed. The MAC filter table lists the clients that are always allowed to associate with a WLAN.

#### >show macfilter

**Syntax** show Display configurations.

macfilter Filter details.

**Defaults** (none)

Examples >show macfilter

-----

00:0c:41:0a:33:a3 1

Related Commands config macfilter mac-delimiter, config macfilter add, config macfilter delete,

config macfilter description, config macfilter wlan-id

# show mgmtuser

To display the local management user accounts on the Alcatel OmniAccess Switch or Appliance, use the show mgmtuser command.

>show mgmtuser

**Syntax** show Display configurations.

mgmtuser Management users.

**Defaults** (none)

Examples >show mgmtuser

User Name Permissions Description

\_\_\_\_\_\_

admin read-write

**Related Commands** config mgmtuser add, config mgmtuser delete, config mgmtuser password

# **SHOW MIRROR COMMANDS**

Use the following show mirror commands:

- <u>show mirror ap</u>
- show mirror foreignap
- <u>show mirror mac</u>
- show mirror port

# show mirror ap

To view the OmniAccess APs whose transmit and receive data appears on the Mirror Port (see *config mirror port*) for troubleshooting, use the show mirror ap command.

>show mirror ap

**Syntax** show Configure parameters.

mirror Mirror command. ap OmniAccess AP.

**Defaults** (none)

Examples > show mirror ap

AP

AP3

Related Commands config mirror ap, show mirror foreignap, show mirror mac, show mirror port

# show mirror foreignap

To view the third-party APs whose transmit and receive data appears on the Mirror Port (see <u>config</u> <u>mirror port</u>) for troubleshooting, use the show mirror foreignap command.

>show mirror foreignap

**Syntax** show Configure parameters.

mirror Mirror command.

foreignap Third-Party Access Point.

**Defaults** (none)

Examples > show mirror foreignap

Foreign AP Port

**Related Commands** config mirror foreignap, show mirror ap, show mirror mac, show mirror port

# show mirror mac

To view the clients whose transmit and receive data appears on the Mirror Port (see <u>config mirror port</u>) by MAC address, use the show mirror mac command.

>show mirror mac

**Syntax** show Configure parameters.

mirror Mirror command. mac Client MAC address.

**Defaults** (none)

Examples >show mirror mac

Related Commands config mirror mac, show mirror ap, show mirror foreignap, show mirror port

# show mirror port

To view the Mirror Port on the OmniAccess Wireless Switch (used for troubleshooting using a protocol analyzer), use the show mirror port command.

>show mirror port

**Syntax** show Configure parameters.

mirror Mirror command.

port Client, OmniAccess AP, and/or third-party AP data

stream is Mirrored to this port.

**Defaults** (none)

Examples >show mirror port

**Related Commands** config mirror port, show mirror ap, show mirror foreignap, show mirror mac

# show mobility summary

To display the summary information for the Alcatel OmniAccess Switch or Appliance mobility groups, use the show mobility summary command.

>show mobility summary

**Syntax** show Display configurations.

mobility Mobility group. summary Summary details

**Defaults** (none)

Examples > show mobility summary

Mobility Group members configured..... 4

Switches configured in the Mobility Group

MAC Address IP Address 00:0b:85:00:02:50 13.1.1.95 00:0b:85:00:04:80 13.1.1.220 00:0b:85:00:06:00 192.168.2.50 00:0b:85:02:0d:20 192.168.2.36

Related Commands config mobility group discovery, config mobility group member

# show msglog

To display the message logs written to the Alcatel OmniAccess Switch or Appliance database, use the show msglog command. If there are more that 15 entries you are prompted to display the messages shown in the example.

>show msglog

**Syntax** show Display configurations.

msglog Message logs.

**Defaults** (none)

Examples >show msglog

Fri Aug 8 17:25:51 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.

```
Fri Aug 8 17:25:50 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:50 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:49 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:35 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:35 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug
         8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
        8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug
Fri Aug 8 17:25:34 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:33 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:22 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:22 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Fri Aug 8 17:25:21 2003 File: gvr.c : Line: 777 : GVRP: Transmitting msg.
Would you like to display the next 15 entries? (y/n)
```

Related Commands show eventlog

### show netuser

To display local network user accounts, use the show netuser command.

#### >show netuser

**Syntax** show Display configurations.

netuser Network users.

**Defaults** (none)

Examples >show netuser

User Name WLAN Id Description

\_\_\_\_\_\_

krebbis

Related Commands config netuser add, config netuser delete, config netuser password, config

netuser wlan-id

#### show network

To display the network configuration of the Alcatel OmniAccess Switch or Appliance, use the show network command.

#### >show network

**Syntax** show Display configurations.

network Network configuration.

**Defaults** (none)

Examples >show network

 IP Address
 192.168.2.230

 Subnet Mask
 255.255.255.0

 Default Gateway
 192.168.2.1

 Burned In MAC Address
 00:08:85:02:01:00

RF/Mobility Domain Name. default
Web Mode. Enable
Secure Web Mode. Enable
Secure Shell (ssh) Enable
Telnet. Enable
Distribution System Port 1

3/17/04 90-100777-300 Rev 1

User Idle Timeout 300 second	ls
ARP Idle Timeout 300 second	aƙ
OmniAccess AP Default Master Disable	
Management VLAN ID Disable	
Mgmt Via Wireless Interface Disable	
Broadcast Ssid Support Disable	

config network arptimeout, config network bcast-ssid, config network dsport, config network master-base, config network mgmt-via-wireless, config network params, config network rf-mobility-domain, config network secureweb, config network secweb-passwd, config network ssh, config network telnet, config network usertimeout, config network vlan, config network webmode

# show qos queue\_length all

To display quality of service (qos) information (queue length), use the show qos command.

>show qos queue\_length all

**Syntax** show gos Command action

queue\_length all Display all quality of service queue lengths.

**Defaults** (none)

Examples >show qos queue\_length all

**Related Commands** config gos

### show port

To display the Alcatel OmniAccess Switch or Appliance port settings on an individual or global basis, use the show port command.

>show port <port number>

>show port summary

**Syntax** show Display configurations.

port Alcatel OmniAccess Switch or Appliance port.

<port number>/summary Individual port or all ports

**Defaults** (none)

Examples >show port 7

Pr	Туре			-	Physical Status				POE
7	Normal	Disa	Enable	Auto	10 Half	Down	Enable	Enable	Enable
	show now gummany								

### >show port summary

		STP	Admin	Physical	Physical	Link	Link	LACP	
Pr	Type	Stat	Mode	Mode	Status	Status	Trap	Mode	POE
1	Normal	Disa	Enable	Auto	10 Half	Down	Enable	Enable	Enable
2	Normal	Disa	Disable	Auto	10 Half	Down	Enable	Enable	Enable

3	Normal	Disa	Disable	Auto	10	Half	Down	Enable	Disable	Enable
4	Normal	Disa	Disable	Auto	10	Half	Down	Enable	Disable	Enable
5	Normal	Disa	Disable	Auto	10	Half	Down	Enable	Disable	Enable
6	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
7	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
8	Normal	Disa	Disable	Auto	10	Half	Down	Enable	Disable	Enable
9	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
10	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
11	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
12	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
13	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
14	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
15	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Disable	Enable
16	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
17	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
18	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
19	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
20	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
21	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
22	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
23	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable
24	Normal	Disa	Enable	Auto	10	Half	Down	Enable	Enable	Enable

**Syntax** 

config ap port, config network dsport, config mirror port, config port adminmode, config port autoneg, config port linktrap, config port physicalmode, config port power

Display configurations.

RADIUS accounting server.

# **SHOW RADIUS COMMANDS**

Use the following show radius commands:

- <u>show radius acct statistics</u>
- show radius auth statistics
- show radius summary

### show radius acct statistics

To display the RADIUS accounting server statistics for the Alcatel OmniAccess Switch or Appliance, use the show radius acct statistics command.

Statistics

# >show radius acct statistics

radius acct

show

	Statistics	Statistics
Defaults	(none)	
Examples	>show radius acct standard Authentication Servers:	atistics
	Server Index	1
		1.1.1.2
	Msg Round Trip Time	0 (1/100 second)
	First Requests	0
	Retry Requests	0
	Accounting Responses.	0
	Malformed Msgs	0

Bad Authenticator Msgs..... 0

Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

show radius auth statistics, show radius summary

#### show radius auth statistics

To display the RADIUS authentication server statistics for the Alcatel OmniAccess Switch or Appliance, use the show radius auth statistics command.

#### >show radius acct statistics

**Syntax** show Display configurations.

radius acct RADIUS authentication server.

statistics Statistics.

**Defaults** (none)

Examples >show radius auth statistics

Authentication Servers:

 First Requests
 0

 Retry Requests
 0

 Accept Responses
 0

 Reject Responses
 0

 Challenge Responses
 0

 Malformed Msgs
 0

 Bad Authenticator Msgs
 0

 Pending Requests
 0

 Timeout Requests
 0

 Unknowntype Msgs
 0

 Other Drops
 0

**Related Commands** 

show radius acct statistics, show radius summary

# show radius summary

To display the RADIUS authentication and accounting server summary, use the show radius summary command.

#### >show radius summary

**Syntax** show Display configurations.

radius RADIUS authentication server.

summary server summary.

**Defaults** (none)

Examples >show radius summary

Authentication Servers

 Index Server Address
 Port
 State

 1
 10.1.2.10
 1812
 Enabled

Accounting Servers

Index	Server Address	Port	State
1	10.1.2.10	1813	Enabled

**Related Commands** show radius auth statistics, show radius acct statistics

### SHOW ROGUE AP COMMANDS

Use the following rogue ap commands:

- show roque ap detailed
- show rogue ap summary

# show rogue ap detailed

To show details of a rogue access point detected by the Alcatel OmniAccess Switch or Appliance, use the show rogue-ap detailed command.

### >show rogue ap detailed <MAC address>

Syntax	show	Display configurations.
	rogue ap	Rogue access points.
	detailed	Summary information.

<MAC address> AP MAC address.

**Defaults** (none)

examples >show rogue ap detailed 00:40:96:90:d1:6a

```
      Rogue MAC Address
      00:40:96:90:d1:6a

      State
      Alert

      First Time Rogue was Reported
      Sat Aug
      9 15:48:50 2003

      Last Time Rogue was Reported
      Sat Aug
      9 21:16:50 2003
```

Reported By AP 1

 Name
 AP1

 Radio Type
 802.11b

 SSID
 Chichen

 Channel
 6

 RSSI
 -60 dBm

 SNR
 40 dB

**Related Commands** show rogue ap summary

# show rogue ap summary

To display a summary of the rogue access points detected by the Alcatel OmniAccess Switch or Appliance, use the show rogue-ap summary command.

# >show rogue ap summary

Syntax	show	Display configurations.
--------	------	-------------------------

rogue ap Rogue access points. summary Summary information.

**Defaults** (none)

Examples >show rogue ap summary

MAC Address	State	# APs	Last Hear	rd		
00:02:6d:28:37:ab	Alert	1	Sat Aug	9	21:12:50	2003
00:09:6b:54:23:90	Alert	1	Sat Aug	9	21:12:50	2003
00:0b:65:00:80:40	Alert	1	Sat Aug	9	21:10:50	2003

**Related Commands** show rogue ap detailed

### SHOW ROGUE CLIENT COMMANDS

Use the following show roque client commands:

- <u>show roque client detailed</u>
- show roque client summary

# show rogue client detailed

To show details of a rogue client detected by the Alcatel OmniAccess Switch or Appliance, use the show rogue client detailed command.

### >show rogue client detailed <MAC address>

Syntax	show	Display configurations.

rogue client Rogue client.

detailed Summary information. <MAC address> Client MAC address.

**Defaults** (none)

Examples >show rogue client detailed 00:40:96:90:d1:6a

Reported By
AP 1

MAC Address ... 00:0b:85:01:88:b0

Name ... AP1

Radio Type ... 802.11b

 SSID.
 Chichen

 Channel.
 6

 RSSI.
 -60 dBm

 SNR.
 40 dB

**Related Commands** show rogue client summary

# show rogue client summary

To display a summary of the rogue clients detected by the Alcatel OmniAccess Switch or Appliance, use the show rogue client summary command.

>show rogue client summary

**Syntax** show Display configurations.

roque client Roque clients.

summary Summary information.

**Defaults** None.

Examples >show rogue client summary

MAC Address	State	# APs	Last Heard	l
00:02:6d:28:37:ab	Alert	1	Sat Aug 9	21:12:50 2003
00:09:6b:54:23:90	Alert	1	Sat Aug 9	21:12:50 2003
00:0b:65:00:80:40	Alert	1	Sat Aug 9	21:10:50 2003

**Related Commands** show rogue client detailed

# show route summary

To a show the routes assigned to the Alcatel OmniAccess Switch or Appliance Service port, use the show route summary command.

>show route summary

Syntax show route Command action

summary Summary information.

**Defaults** (none)

Examples >show route summary

**Related Commands** config route

#### show serial

To a show the serial (Console) port configuration, use the show serial command.

>show serial

**Syntax** show Display configurations. serial Console serial port.

**Defaults** 9600, 8, OFF, 1, None.

Examples >show serial

 Serial Port Login Timeout (minutes)
 0

 Baud Rate
 9600

 Character Size
 8

 Flow Control:
 Disable

 Stop Bits
 1

 Parity Type:
 none

Related Commands config serial baudrate, config serial timeout

#### show sessions

To a show the Console port login timeout and maximum number of simultaneous CLI sessions, use the show sessions command.

>show sessions

**Syntax** show Display configurations.

sessions CLI session limits.

**Defaults** 5 minutes, 5 sessions.

Examples >show sessions

which indicates that the CLI sessions never time out, and that the Alcatel Omni-Access Switch or Appliance can host up to five simultaneous CLI sessions.

Related Commands config sessions maxsessions, config sessions timeout

# show snmpcommunity

To a show the SNMP version 1/version 2c community configuration, use the show snmpcommunity command.

>show snmpcommunity

**Syntax** show Display configurations.

snmpcommunity SNMP version 1/version 2c community configuration.

**Defaults** (none)

Examples > show snmpcommunity

 SNMP Community Name
 Client IP Address
 Client IP Mask
 Access Mode
 Status

 \*\*\*\*\*\*\*\*\*\*
 0.0.0.0
 0.0.0.0
 Read/Write
 Enable

 public
 0.0.0.0
 0.0.0.0
 Read Only
 Enable

Related Commands config snmp version, config snmp community mode, config snmp community

accessmode, config snmp community create, config snmp community delete,

config snmp community ipaddr

### show snmptrap

To a show the Alcatel OmniAccess Switch or Appliance SNMP trap receivers and their status, use the show snmptrap command.

>show snmptrap

**Syntax** show Display configurations.

snmptrap SNMP trap receivers.

**Defaults** (none)

Examples >show snmptrap

**Related Commands** config snmp version, config snmp trapreceiver

### show snmpv3user

To a show the SNMP version 3 configuration, use the show snmpv3user command.

#### >show snmpv3user

**Syntax** show Display configurations.

snmpv3user SNMP version 3 configuration.

**Defaults** (none)

Examples >show snmpv3user

SNMP v3 User Name AccessMode Authentication Encryption
----default Read/Write HMAC-MD5 CBC-DES

Related Commands config snmp version, config snmp v3user

# show snmpversion

To a show the SNMP version status, use the show snmpversion command.

>show snmpversion

**Syntax** show Display configurations.

snmpversion SNMP states.

**Defaults** Enabled.

Examples >show snmpversion

 SNMP v1
 Mode
 Enable

 SNMP v2c
 Mode
 Enable

 SNMP v3
 Mode
 Enable

**Related Commands** config snmp version

### show spanningtree port

To a show the Alcatel OmniAccess Switch or Appliance spanning tree port configuration, use the show spanningtree port command.

#### >show spanningtree port <port>

**Syntax** show Display configurations.

spanningtree Spanning tree. Physical port.

<port> Physical port number:

1 through 13 on 40121 through 25 on 4024

- 1 or 2 on 4102

**Defaults** 800C, Disabled, 802.1D, 128, 100, Auto.

Examples > show spanningtree port 3

 STP Port ID.
 800C

 STP Port State.
 Disabled

 STP Port Administrative Mode
 802.1D

 STP Port Priority
 128

 STP Port Path Cost
 100

 STP Port Path Cost Mode
 Auto

**Related Commands** config spanningtree port

# show spanningtree switch

To a show the Alcatel OmniAccess Switch or Appliance network (DS Port) spanning tree configuration, use the show spanningtree switch command.

### >show spanningtree switch

**Syntax** show Display configurations.

spanningtree Spanning tree.

switch Alcatel OmniAccess Switch or Appliance

configuration.

<port> Physical port number:

1 through 13 on 40121 through 25 on 4024

- 1 or 2 on 4102

**Defaults** (none)

Examples > show spanningtree switch

 STP Specification
 IEEE 802.1D

 STP Base MAC Address
 00:0B:85:02:0D:20

**Related Commands** config spanningtree switch bridgepriority, config spanningtree switch forward-

delay, config spanningtree switch hellotime, config spanningtree switch

maxage, config spanningtree switch mode

#### SHOW STATS COMMANDS

Use the following show stats commands:

- show stats port
- show stats switch

### show stats port

To a show physical port receive and transmit statistics, use the show stats port command.

>show stats port detailed <port>
>show stats port summary <port>

**Syntax** show Display configurations.

stats Statistics. port Port.

detailed Details for a port.
summary Summary of all ports.
<port> Physical port number:
- 1 through 13 on 401

1 through 13 on 40121 through 25 on 4024

- 1 or 2 on 4102

**Defaults** (none)

Examples > show stats port summary 5

```
Packets Received Without Error..... 399958
Packets Received With Error......0
Broadcast Packets Received...... 8350
Packets Transmitted Without Error..... 106060
Collisions Frames...... 0
Time Since Counters Last Cleared...... 2 day 11 hr 16 min 23 sec
>show stats port detailed 5
PACKETS RECEIVED (OCTETS)
Total Bytes...... 32834575
                          128-255 byte pkts :2758
                         512-1023 byte pkts :1353
                         1519-1530 byte pkts :0
1024-1518 byte pkts :6
> 1530 byte pkts :2
PACKETS RECEIVED SUCCESSFULLY
Unicast Pkts :390007 Multicast Pkts:0 Broadcast Pkts:8321
PACKETS RECEIVED WITH MAC ERRORS
Total..... 0
Jabbers :0
                 Undersize :0
                                      Alignment :0
FCS Errors:0
                  Overruns :0
RECEIVED PACKETS NOT FORWARDED
Total..... 0
Local Traffic Frames:0 RX Pause Frames :0
Unacceptable Frames :0 VLAN Membership :0
VLAN Viable Discards:0 MulticastTree Viable:0
PACKETS TRANSMITTED (OCTETS)
Total Bytes..... 8955560
64 byte pkts :95330 65-127 byte pkts :1270 128-255 byte pkts :7369 256-511 byte pkts :510
512-1023 byte pkts :0
1519-1530 byte pkts :0
                         1024-1518 byte pkts :1172
                         Max Info
PACKETS TRANSMITTED SUCCESSFULLY
Unicast Pkts :44349 Multicast Pkts:40989 Broadcast Pkts:20315
TRANSMIT ERRORS
Total Errors..... 0
                                     Underrun Error:0
FCS Error :0 TX Oversized :0
TRANSMIT DISCARDS
Total Discards...... 0
Single Coll Frames : Multiple Coll Frames:0
Excessive Coll Frame:0 Port Membership:0
VLAN Viable Discards:0
Unicast Pkts :44349 Multicast Pkts:40989 Broadcast Pkts:20315
TRANSMIT ERRORS
Total Errors..... 0
FCS Error :0 TX Oversized :0 Underrun Error:0
TRANSMIT DISCARDS
```

Single Coll Frames :0 Multiple Coll Frames:0

Excessive Coll Frame:0 Port Membership :0

VLAN Viable Discards:0

PROTOCOL STATISTICS

BPDUs Received :9182 BPDUs Transmitted :0 802.3x RX PauseFrame:0 GVRP PDU Received :0 GVRP PDU Transmitted:40992 GVRP Failed Regs :0

Time Since Counters Last Cleared...... 2 day 11 hr 4 min 48 sec

Related Commands config port physical mode

### show stats switch

To a show the network (DS Port) receive and transmit statistics, use the show stats switch command.

# >show stats switch detailed

>show stats switch summary

**Syntax** show Display configurations.

stats Statistics.

switch Alcatel OmniAccess Switch or Appliance.

detailed Details for a port. summary Summary of all ports.

**Defaults** (none)

Examples >show stats switch summary

Time Since Counters Last Cleared...... 2 day 11 hr 22 min 17 sec

>show stats switch detailed

RECEIVE

 Octets.
 13973582

 Total Pkts.
 136441

 Unicast Pkts.
 117636

 Multicast Pkts.
 0

 Broadcast Pkts.
 18805

 Pkts Discarded.
 0

TRANSMIT

 Octets.
 5919784

 Total Pkts.
 78028

 Unicast Pkts.
 33448

 Multicast Pkts.
 41240

 Broadcast Pkts.
 3340

 Pkts Discarded.
 2

ADDRESS ENTRIES

VLAN ENTRIES

Time Since Ctrs Last Cleared...... 2 day 11 hr 23 min 43 sec

Related Commands config network dsport

# show switchconfig

To a show the network (DS Port) 802.3x flow control mode, use the show switchconfig command.

>show switchconfig

**Syntax** show Display configurations.

switchconfig Alcatel OmniAccess Switch or Appliance

configuration.

**Defaults** (none)

Examples >show switchconfig

802.3x Flow Control Mode...... Disable Current LWAPP Transport Mode...... Layer 2 LWAPP Transport Mode after next switch reboot.. Layer 2

**Related Commands** config switchconfig flowcontrol, config switchconfig mode

# show sysinfo

To a show high-level Alcatel OmniAccess Switch or Appliance information, use the show sysinfo command.

>show sysinfo

**Syntax** show Display configurations.

sysinfo Alcatel OmniAccess Switch or Appliance information.

**Defaults** (none)

Examples >show sysinfo

Product Name...... OmniAccess Wireless Switch Product Version...... 2.0.113.3

 Product Version
 2.0.113.3

 RTOS Version
 2.0.113.3

 Bootloader Version
 1.1.11.0

 System Name
 IT2003

 System Location
 Andrew 1

System Up Time...... 2 days 11 hrs 30 mins 1 secs

Configured Country...... United States

Internal Temp Alarm Limits...... 0 to 65  $\ensuremath{\text{C}}$ 

Internal Temperature.....+38 C

Number of Active Clients...... 1

Related Commands config country, config wlan, config ap

# show syslog

To a show the Alcatel OmniAccess Switch or Appliance SNMP trap logging status or target IP Address, use the show syslog command.

>show syslog

**Syntax** show Display configurations.

syslog Alcatel OmniAccess Switch or Appliance SNMP trap

logging status or target IP Address.

**Defaults** (none)

Examples >show syslog

Syslog destination..... disabled

>show syslog

Syslog destination...... 10.10.2.7

Related Commands config syslog

### show time

To a show the Alcatel OmniAccess Switch or Appliance time and date, use the show time command.

>show time

**Syntax** show Display configurations.

time Alcatel OmniAccess Switch or Appliance time and

date.

**Defaults** (none)

Examples >show time

Related Commands config time

# show trapflags

To a show the Alcatel OmniAccess Switch or Appliance SNMP trap flags, use the show trapflags command.

>show trapflags

**Syntax** show Display configurations.

trapflags Alcatel OmniAccess Switch or Appliance SNMP trap

flags.

# **Defaults** (none)

# Examples >show trapflags

> D110W (	erupriugb	
Authenti	cation Flag Enable	
Link Up/	Down Flag Enable	
Multiple	e Users Flag Enable	
Spanning	Tree Flag Enable	
Client R	Related Traps	
	802.11 Disassociation	Disable
	802.11 Deauthenticate	Disable
	802.11 Authenticate Failure	Disable
	802.11 Association Failure	Disable
	Blacklisted	Disable
OmniAcce	ess AP	
	Register	Enable
	<pre>InterfaceUp</pre>	Enable
Auto-RF	Profiles	
	Load	Enable
	Noise	Enable
	Interference	Enable
	Coverage	Enable
Auto-RF	Thresholds	
	tx-power	Enable
	channel	Enable
	antenna	Enable
AAA		
	auth	Enable
	servers	Enable
rogueap.	Enable	
configsa	ave Enable	
IP Secur	rity	
	esp-auth	Enable
	esp-replay	Enable
	invalidSPI	Enable
	ike-neg	Enable
	suite-neg	Enable
	invalid-cookie	Enable

### **Related Commands**

config trapflags authentication, config trapflags linkmode, config trapflags multiusers, config trapflags stpmode, config trapflags client, config trapflags ap, config trapflags rrm-profile, config trapflags rrm-params, config trapflags aaa, config trapflags rogueap, config trapflags configsave, config trapflags ipsec, show traplog

# show traplog

To a show the Alcatel OmniAccess Switch or Appliance SNMP trap log, use the show traplog command.

>show traplog

**Syntax** show Display configurations.

traplog Alcatel OmniAccess Switch or Appliance SNMP trap

log.

**Defaults** (none)

Examples >show traplog

Log System Time	Trap	
0 Sun Aug 10 03:13:03 2003	Rogue AP: 00:0b:85:01:2f:90 removed from AP:0 0:0b:85:01:18:b0 Interface no:1(unknowntype)	
1 Sun Aug 10 03:10:06 2003	Rogue AP: 00:0b:85:01:02:40 removed from AP:0 0:0b:85:01:18:b0 Interface no:1(unknowntype)	
2 Sun Aug 10 03:10:06 2003	Rogue AP: 00:0b:85:01:4c:90 removed from AP:0	
3 Sun Aug 10 03:07:53 2003	0:0b:85:01:18:b0 Interface no:1(unknowntype) Rogue AP: 00:0b:85:01:2e:30 detected on AP:00	
	:0b:85:01:18:b0 Interface no:1(unknown type) with RSSI: -66 and SNR: 29	
4 Sun Aug 10 03:05:53 2003	Rogue AP: 00:40:96:40:82:89 detected on AP:	
	00:0b:85:01:18:b0 Interface no:1(unknown type) with RSSI: -68 and SNR: 27	
Would you like to display more entries? (y/n)		

**Related Commands** show trapflags

### show watchlist

To display the client watchlist, use the show watchlist command.

>show watchlist

**Syntax** show Command action.

watchlist Display client watchlist entry.

**Defaults** None.

Examples >show watchlist

Related Commands config watchlist delete, config watchlist enable/disable, config watchlist add

### show wlan

To show a summary of the Alcatel OmniAccess Switch or Appliance WLANs and their status, use the show wlan summary command.

#### >show wlan <WLAN id> foreignAp

**Syntax** show Display configurations.

wlan Wireless LAN.

summary Displays a summary of all WLAN.

<WLAN id> Alcatel WLAN 1 through 17 (17 = foreignAp).

foreignAp Alcatel WLAN 17.

**Defaults** (none)

Examples >show wlan 1

Radio Policy	All
Security  802.11 Authentication: Static WEP Keys.  802.1X. Wi-Fi Protected Access. IP Security. IP Security Passthru. Web Based Authentication Cranite Passthru.	Disabled Disabled Disabled Disabled Disabled Disabled Disabled
>show wlan 17 (or show wlan foreignAp) WLAN Identifier Network Name (SSID) Status MAC Filtering Number of Active Clients Blacklist Timeout Session Timeout VLAN DHCP Server Quality of Service Radio Policy Security	Lobby Enabled Disabled 0 60 seconds Infinity Default Disabled Bronze (low)
802.11 Authentication: 802.1X Encryption: Wi-Fi Protected Access. IP Security. IP Security Passthru. Web Based Authentication. Cranite Passthru.	Enabled Unavailable Disabled Disabled Disabled Disabled Disabled

config wlan blacklist, config wlan create, config wlan delete, config wlan dhcp\_server, config wlan disable, config wlan enable, config wlan mac-filtering, config wlan qos, config wlan radio, config wlan security 802.1X, config wlan security 802.1X encryption, config wlan security cranite, config wlan security ipsec, config wlan security ipsec authentication, config wlan security ipsec encryption, config wlan security ipsec ike authentication, config wlan security ipsec ike DH-Group, config wlan security ipsec ike lifetime, config wlan security ipsec ike phase1, config wlan security passthru, config wlan security static-wep-key, config wlan security static-wep-key encryption, config wlan security wpa, config wlan security wpa encryption, config wlan timeout, config wlan vlan

# show wlan summary

To show a summary of the Alcatel OmniAccess Switch or Appliance WLANs and their status, use the show wlan summary command.

# >show wlan summary

**Syntax** show Display configurations.

wlan Wireless LAN.

summary Alcatel OmniAccess Switch or Appliance Virtual

Gateway IP Address.

**Defaults** (none)

Examples >show wlan summary

WLAN ID WLAN Name Status

1 Controller Enabled
2 Marketing Enabled

**Related Commands** config wlan summary

# show wps-peers summary

To show a summary of the Wireless Protection System (WPS) Peer Management Configuration, use the show wps-peers summary command.

Note: This command functions only when WPS has been installed.

>show wps-peers summary

**Syntax** show Display configurations.

wps-peers Wireless Protection System Peer Management.

summary Summary of WPS peer manager.

**Defaults** (none)

Example >show wps-peers summary

Switches configured in the WPS Peer Group
MAC Address WP Address
00:0b:85:82:0d:20
192.168.2.36

**Related Commands** config wps, config wps-peers

# **Setting Configurations**

Use the following config commands to configure Alcatel OmniAccess Switch or Appliance options and settings.

- config 802.11a
- config 802.11b
- config acl
- config advanced 802.11a
- config advanced 802.11b
- <u>config advanced timers</u>
- config ap
- <u>config blacklist</u>
- <u>config certificate</u>
- config client deauthenticate
- config country
- <u>config custom-web</u>
- <u>config interface</u>
- config load-balancing
- <u>config loginsession close</u>
- <u>config macfilter</u>
- <u>config mgmtuser</u>
- <u>config mirror</u>
- config mobility group
- config netuser
- <u>config network</u>
- config port
- <u>config prompt</u>
- config gos queu length
- <u>config radius acct</u>
- <u>config radius auth</u>
- <u>config roque ap</u>
- <u>config roque client</u>
- <u>config route</u>
- <u>config serial</u>
- <u>config sessions</u>
- config snmp community
- <u>config snmp syscontact</u>

- config snmp syslocation
- <u>config snmp trapreceiver</u>
- config snmp v3user
- config snmp version
- <u>config spanning tree port</u>
- config spanningtree switch
- config switchconfig
- config syslog
- config sysname
- config time
- <u>config trapflags</u>
- <u>config watchlist add</u>
- config watchlist
- config wlan
- config wlan security
- config wlan timeout
- config wlan vlan
- config wps
- <u>config wps-peers</u>

### **CONFIG 802.11A COMMANDS**

Use the following config 802.11a commands:

- config 802.11a antMode
- <u>config 802.11a beaconperiod</u>
- config 802.11a channel
- config 802.11a disable
- <u>config 802.11a dtim</u>
- config 802.11a enable
- <u>config 802.11a rate</u>
- config 802.11a txPower

# config 802.11a antMode

To configure the OmniAccess AP to use one internal antenna for an 802.11a sectorized 180-degree coverage pattern, or both internal antennas for an 802.11a 360-degree omnidirectional pattern, use the config 802.11a antMode command.

>config 802.11a antMode <OmniAccess AP> <omni/sectorA/sectorB>

**Syntax** config Configure parameters.

802.11a antMode Antenna for 802.11a OmniAccess Radio.

<OmniAccess AP> Alcatel OmniAccess Wireless Access Point name.

omni Use both internal antennas.

sectorA Use only the Side A internal antenna. sectorB Use only the Side B internal antenna.

**Defaults** internal

Examples >config 802.11a antMode AP1 omni

**Related Commands** show ap config 802.11a, config 802.11b antMode

# config 802.11a beaconperiod

In Alcatel 802.11a networks, all OmniAccess AP WLANs broadcast a beacon at regular intervals. This beacon notifies clients that 802.11a service is available, and allows the clients to synchronize with the OmniAccess AP. To change the 802.11a beacon period for the whole 802.11a network, use the config 802.11a beaconperiod command.

Before you change the beacon period using the config 802.11a beaconperiod command, make sure that you have disabled the 802.11a network using the config 802.11a disable command. When you are done changing the beacon period, remember to enable the 802.11a network using the config 802.11a enable command.

#### >config 802.11a beaconperiod <Time Units>

**Syntax** config Configure parameters.

802.11a 802.11a network parameters.

beaconperiod Send a beacon every 100 to 600 milliseconds.

<time units> Beacon interval in milliseconds.

**Defaults** 100 milliseconds

Examples >config 802.11a beaconperiod 120

to configure an 802.11a network for a beacon period of 120 milliseconds.

**Related Commands** show 802.11a, config 802.11b beaconperiod, config 802.11a disable, config

802.11a enable

# config 802.11a channel

To configure an 802.11a network for automatic or manual channel selection, use the config 802.11a channel command.

When configuring 802.11a channels for a single OmniAccess AP, use the config 802.11a disable command to disable the 802.11a network. Then use the config 802.11a channel command to set automatic channel selection by OmniVista AirView Software or manually set the channel for the 802.11a OmniAccess Radio. Then enable the 802.11a network using the config 802.11a enable command.

>config 802.11a channel {global <auto/once/off>}/{<OmniAccess AP> <global/
channel #>}

**Syntax** config Configure parameters.

802.11a channel OmniAccess Radio channel number.

global Global channel control.

<OmniAccess AP> Name of OmniAccess AP or global setting for all

OmniAccess APs.

**Defaults** (none)

Examples To have OmniVista AirView Software automatically configure all 802.11a

channels based on availability and interference: >config 802.11a channel global auto

To have OmniVista AirView Software automatically reconfigure all 802.11a

channels one time based on availability and interference:

>config 802.11a channel global once

To turn 802.11a OmniVista AirView Software automatic configuration off:

>config 802.11a channel global off

To configure all 802.11a channels in AP1: >config 802.11a channel AP1 global

To configure 802.11a channel 36 in AP1: >config 802.11a channel AP1 36

Related Commands show 802.11a, config 802.11a disable, config 802.11a enable, config 802.11b

channel

# config 802.11a disable

To disable 802.11a transmission, use the config 802.11a disable command.

Disable 802.11a transmissions for the whole network or for an individual OmniAccess Radio using the config 802.11a disable command.

Note that you must use this command to disable the network before using many config 802.11a commands.

This command can be used any time the CLI interface is active.

>config 802.11a disable {network/<OmniAccess AP>}

**Syntax** config Configure parameters.

802.11a 802.11a network parameters.

disable Disable 802.11a. network Whole network.

<OmniAccess AP> Override the network setting for an individual

<OmniAccess AP> OmniAccess Radio.

**Defaults** Network = enabled.

**Examples** To disable the whole 802.11 a network:

>config 802.11a disable network

To disable AP1 802.11a transmissions: >config 802.11a disable AP1

Related Commands show sysinfo, show 802.11a, config 802.11a enable, config 802.11b disable,

config 802.11b enable, config 802.11a beaconperiod

### config 802.11a dtim

In 802.11 networks, the OmniAccess AP WLANs broadcast a beacon at regular intervals, which coincides with the DTIM (Delivery Traffic Indication Map). After the DTIM, if the OmniAccess AP has any

frames buffered for broadcast or multicast, it transmits the buffered frames. This protocol allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast after every beacon) or 2 (transmit after every other beacon). For instance, if the beaconperiod is 100 ms, and the DTIM value is set to 1, the OmniAccess AP transmits buffered broadcast and multicast frames 10 times a second; if the beaconperiod is 100 ms, and the DTIM value is set to 2, the OmniAccess AP transmits buffered broadcast and multicast frames five times a second; either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast after every 255th beacon), if all 802.11a clients have power save enabled. Because the clients only have to listen when the DTIM time is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beaconperiod is 100 ms, and the DTIM value is set to 100, the OmniAccess AP transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power saving clients to sleep longer between periods when they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. A low DTIM value is indicated for 802.11a networks that support such clients.

To change the DTIM value for the whole 802.11a network, use the config 802.11a dtim command.

#### >config 802.11a dtim <value>

<b>Syntax</b> config Configure	parameters.
--------------------------------	-------------

802.11a 802.11a network parameters. dtim Delivery Traffic Indication Map.

<value> DTIM value in number of beaconperiods.

**Defaults** 1 (every beaconperiod)

Examples >config 802.11a dtim 2

to configure the 802.11a network to transmit multicast and broadcast

messages every other DTIM, or beaconperiod.

Related Commands show 802.11a, config 802.11a beaconperiod, config 802.11b dtim, config

802.11a disable, config 802.11a enable

# config 802.11a enable

Enable 802.11a transmissions for the whole network or for an individual OmniAccess AP using the config 802.11a enable command. You must use this command to enable the network after configuring other 802.11a parameters.

Note that this command only enables the Alcatel 802.11a network. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, use the config wlan radio command.

This command can be used any time the CLI interface is active.

### >config 802.11a enable {network/<OmniAccess AP>}

**Syntax** config Configure parameters.

802.11a 802.11a network parameters.

enable Enable 802.11a. network For the whole network.

<OmniAccess AP> Override the network setting for an individual

<OmniAccess AP> OmniAccess Radio.

**Defaults** Network = enabled.

**Examples** To enable the whole 802.11a network:

>config 802.11a enable network

To enable AP1 802.11a transmissions:

>config 802.11a enable AP1

Related Commands show sysinfo, show 802.11a, config wlan radio, config 802.11a disable, config

802.11b disable, config 802.11b enable, config 802.11b 11gSupport enable,

config 802.11b 11gSupport disable

# config 802.11a rate

To set 802.11a mandatory and supported operational rates, use the config 802.11a rate command.

>config 802.11a rate <mandatory/supported> <rate>

Note: The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate.

**Syntax** config Configure parameters.

802.11a 802.11a network parameters.

rate Data rate.
mandatory/supported See Note above.

rate 6000, 9000, 12000, 18000, 24000, 36000, 48000,

or 54000 Kbps.

**Defaults** (none)

**Examples** To set 802.11a transmission at a mandatory rate at 12000 Kbps:

>config 802.11a rate mandatory 12000

**Related Commands** show ap config 802.11a, config 802.11b rate

# config 802.11a txPower

To configure the 802.11a Tx (Transmit) Power Level, use the config 802.11a txPower command.

>config 802.11a txPower {global <auto/once/power level #>}/{<OmniAccess AP>
<global/power level #>}

**Syntax** config Configure parameters.

802.11a 802.11a network parameters. txPower Transmit power parameter.

global All OmniAccess APs.

auto/once Periodic or one-time OmniVista AirView Software

automatic configuration.

<OmniAccess AP> Alcatel OmniAccess Wireless Access Point name.

power level # Transmit power level number.

Note: The 802.11a OmniAccess Radio currently supports five transmit power levels:

1 = Maximum transmit power level allowed per Country Code setting, 2 = 50% power,
3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power.

Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel
OmniAccess Wireless Product Guide for the maximum regulatory Transmit Power Level Limits published for each Country Code. Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Also note that the actual maximum transmit power levels may be less than the published regulatory limits.

**Defaults** Global, Auto.

**Examples** To have OmniVista AirView Software automatically set the transmit power for

all 802.11a OmniAccess Radios at periodic intervals:

>config 802.11a txPower global auto

To have OmniVista AirView Software automatically reset the transmit power for all 802.11a OmniAccess Radios one time:

>config 802.11a txPower global once

To set transmit power for all 802.11a OmniAccess AP OmniAccess Radios to

power level 5 (lowest):

>config 802.11a txPower global 5

To set transmit power for 802.11a AP1 to global:

>config 802.11a txPower AP1 global

To set transmit power for 802.11a AP1 to power level 2:

>config 802.11a txPower AP1 2

**Related Commands** show ap config 802.11a, config 802.11b txPower, config country

#### **CONFIG 802.11B COMMANDS**

Use the following config 802.11b command:

- config 802.11b 11qSupport
- <u>config 802.11b antenna</u>
- config 802.11b beaconperiod
- config 802.11b channel
- config 802.11b disable
- <u>config 802.11b diversity</u>
- <u>config 802.11b dtim</u>
- config 802.11b enable
- config 802.11b rate
- config 802.11b txPower

# config 802.11b 11gSupport

After enabling the Alcatel 802.11b network using the config 802.11b enable command, enable or disable the Alcatel 802.11g network using the config 802.11b 11gSupport command. Note that you must use this command to enable the network after configuring other 802.11b parameters.

Note that this command only enables the Alcatel 802.11g network after the Alcatel 802.11b network is enabled using the config 802.11b enable command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, use the config wlan radio command.

This command can be used any time the CLI interface is active.

>config 802.11b 11gSupport {enable/disable}

**Syntax** config Configure parameters.

802.11b 802.11b network parameters.

11qSupport Support for the 802.11q network.

enable Enable 802.11b/g. network For the whole network.

<OmniAccess AP> To override the network setting for individual

<OmniAccess AP> OmniAccess Radio.

**Defaults** Enabled.

Examples >config 802.11b 11gSupport enable

to enable the Alcatel 802.11g network.

>config 802.11b 11gSupport disable to disable the Alcatel 802.11g network.

**Related Commands** show sysinfo, show 802.11b, config 802.11b enable, config wlan radio, config

802.11b disable, config 802.11a disable, config 802.11a enable

### config 802.11b antenna

To configure the 802.11b/g antenna, use the config 802.11b antenna command.

Use the config 802.11b disable command to disable the 802.11b/g OmniAccess Radio before using the config 802.11b antenna command. Then use the config 802.11b antenna command to configure the OmniAccess AP to use internal or external antennas. Then use the config 802.11b enable command to enable the 802.11b/g OmniAccess Radio.

>config 802.11b antenna <OmniAccess AP> <internal/external>

**Syntax** config Configure parameters.

802.11b antenna Antennas for 802.11b/g OmniAccess Radio.

<OmniAccess AP > OmniAccess AP name.

<internal/external> Configure for internal or external antennas.

**Defaults** Internal.

Examples >config 802.11b antenna AP1 internal

to set AP1 to use the 802.11b/g internal antennas.

Related Commands config 802.11b disable, config 802.11b enable, config 802.11a antMode

# config 802.11b beaconperiod

In Alcatel 802.11b/g networks, all OmniAccess AP WLANs broadcast a beacon at regular intervals. This beacon notifies clients that 802.11b/g service is available, and allows the clients to synchronize with the OmniAccess AP. To change the 802.11b/g beacon period for the whole 802.11b/g network, use the config 802.11b beaconperiod command.

Before you change the beacon period using the config 802.11b beaconperiod command, make sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the beacon period, remember to enable the 802.11b/g network using the config 802.11b enable command.

#### >config 802.11b beaconperiod <Time Units>

**Syntax** config Configure parameters.

802.11b 802.11b/g network parameters.

beaconperiod Send a beacon every 100 to 600 milliseconds.

<time units> Beacon interval in milliseconds.

**Defaults** 100 milliseconds.

**Examples** To configure an 802.11b/g network for a beacon period of 180 milliseconds.

>config 802.11b beaconperiod 180

Related Commands show 802.11a, config 802.11a beaconperiod, config 802.11b disable, config

802.11b enable

## config 802.11b channel

To configure the 802.11b/g network for automatic or manual channel selection, use the config 802.11b channel command.

When configuring 802.11b/g channels for a single OmniAccess AP, use the config 802.11b disable command to disable the 802.11b/g network. Then use the config 802.11b channel command to set automatic channel selection by OmniVista AirView Software or manually set the channel for the 802.11b/g OmniAccess Radio. Then enable the 802.11b/g network using the config 802.11b enable command.

>config 802.11b channel {global <auto/once/off>}/{<OmniAccess AP> <global/
channel #>}

**Syntax** config Configure parameters.

802.11b channel 802.11b/g OmniAccess Radio channel number.

global Global channel control.

<OmniAccess AP> Name of OmniAccess AP or global setting for all

OmniAccess APs.

**Defaults** None.

**Examples** To have OmniVista AirView Software automatically configure all 802.11b/g

channels based on availability and interference:

>config 802.11b channel global auto

To have OmniVista AirView Software automatically reconfigure all 802.11b/g

channels one time based on availability and interference:

>config 802.11b channel global once

To turn 802.11b/g OmniVista AirView Software automatic configuration off:

>config 802.11b channel global off

To have AP1 use the global (whole network) settings.

>config 802.11b channel AP1 global

To have AP1 start and continue using channel 11. >config 802.11b channel AP1 channel 11

Note: Only channels 1, 6 and 11 are nonoverlapping.

Related Commands show 802.11b, config 802.11b disable, config 802.11b enable, config 802.11a

channel

### config 802.11b disable

Disable 802.11b/g transmissions for the whole network or for an individual OmniAccess Radio using the config 802.11b disable command.

Note that you must use this command to disable the network before using other config 802.11b commands.

This command can be used any time the CLI interface is active.

>config 802.11b disable {network/<OmniAccess AP>}

**Syntax** config Configure parameters.

802.11b 802.11b/g network parameters.

disable Disable 802.11b/g. network Whole network.

<OmniAccess AP> Override the network setting for an individual

<OmniAccess AP> OmniAccess Radio.

**Defaults** Enabled.

Examples >config 802.11b disable network

to disable the whole 802.11b/g network.

>config 802.11b disable AP1

to disable AP1 802.11b/g transmissions.

**Related Commands** show sysinfo, show 802.11b, config 802.11a disable, config 802.11a enable,

config 802.11b enable, config 802.11b beaconperiod

### config 802.11b diversity

To configure the diversity option for 802.11b/g antennas, use the config 802.11b diversity command.

>config 802.11b diversity <OmniAccess AP> <enable/sideA/sideB>

**Syntax** config Configure parameters.

802.11b diversity Diversity antennas for 802.11b/g.

<OmniAccess AP > OmniAccess AP name.

enable Between the two internal antennas.

sideA Between the internal antennas and an external

antenna connected to the OmniAccess AP Left port.

sideB Between the internal antennas and an external

antenna connected to the OmniAccess AP Right port.

**Defaults** Enabled.

**Examples** To enable diversity for AP1:

>config 802.11b diversity AP1 enable

To enable diversity for AP1 using an external antenna connected to the Omni-

Access AP Left port (sideA).

>config 802.11b diversity AP1 sideA

**Related Commands** show ap config 802.11b

## config 802.11b dtim

In 802.11 networks, the OmniAccess AP WLANs broadcast a beacon at regular intervals, which coincide with the DTIM (Delivery Traffic Indication Map). After the DTIM, if the OmniAccess AP has any frames buffered for broadcast or multicast, it transmits the buffered frames. This protocol allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast after every beacon) or 2 (transmit after every other beacon). For instance, if the 802.11b/g beaconperiod is 100 ms, and the DTIM value is set to 1, the OmniAccess AP transmits buffered broadcast and multicast frames 10 times a second; if the beaconperiod is 100 ms, and the DTIM value is set to 2, the OmniAccess AP transmits buffered broadcast and multicast frames five times a second; either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast after every 255th beacon), if all 802.11a clients have power save enabled. Because the clients only have to listen when the DTIM time is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the 802.11b/g beaconperiod is 100 ms, and the DTIM value is set to 100, the OmniAccess AP transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power saving clients to sleep longer between periods when they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Note that many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. A low DTIM value is indicated for 802.11b/g networks that support such clients.

To change the DTIM value for the whole 802.11b/g network, use the config 802.11b dtim command.

Before you change the 802.11b/g DTIM value using the config 802.11b dtim command, make sure that you have disabled the 802.11b/g network using the config 802.11b disable command. When you are done changing the DTIM value, remember to enable the 802.11b/g network using the config 802.11b enable command.

#### >config 802.11b dtim <value>

Svntax	confia	Configure parameters.
Sylicax	COLLIG	Continual e parameters.

802.11b 802.11b/g network parameters. dtim Delivery Traffic Indication Map.

<value> DTIM value in number of beaconperiods.

**Defaults** 1 (every beaconperiod)

Examples >config 802.11b dtim 1

to configure the 802.11b/g network to transmit multicast and broadcast

messages every DTIM, or beaconperiod.

**Related Commands** show 802.11b, config 802.11b beaconperiod, config 802.11a dtim, config

802.11b disable, config 802.11b enable

### config 802.11b enable

Note that you must use this command to enable the network after configuring other 802.11b parameters.

Note that this command only enables the Alcatel 802.11b network. To enable the Alcatel 802.11g network, you MUST have the 802.11b network enabled, and then use the config 802.11b 11gSupport enable command. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, use the config wlan radio command.

This command can be used any time the CLI interface is active.

>config 802.11b enable {network/<OmniAccess AP>}

**Syntax** config Configure parameters.

802.11b 802.11b network parameters.

enable Enable 802.11b. Allow support for 802.11g.

network For the whole network.

<OmniAccess AP> To override the network setting for individual

<OmniAccess AP> OmniAccess Radio.

**Defaults** Enabled.

Examples >config 802.11b enable network

to enable the whole 802.11b network and provide support for the 802.11g

network.

>config 802.11b enable AP1

to enable AP1 802.11b transmissions and support AP1 802.11g transmissions.

**Related Commands** show sysinfo, show 802.11b, config 802.11b 11gSupport, config wlan radio,

config 802.11b disable, config 802.11a disable, config 802.11a enable

### config 802.11b rate

To configure 802.11b/g mandatory and supported operational rates, use the config 802.11b rate command.

>config 802.11b rate <mandatory/supported> <rate>

Þ

**Note:** The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate.

**Syntax** config Configure parameters.

802.11b 802.11b/g network parameters.

mandatory/supported See the Note above.

rate 1, 2, 5.5, or 11 Mbps data rate.

**Defaults** (none)

**Examples** To set 802.11b/g transmission at a mandatory rate at 5.5 Mbps:

>config 802.11b rate mandatory 5.5

**Related Commands** show ap config 802.11b, config 802.11a rate

# config 802.11b txPower

To configure the 802.11b/g Tx (Transmit) Power Level, use the config 802.11b txPower command.

>config 802.11b txPower {global <auto/once/powerLevel #>}/{<OmniAccess AP>
<global/powerLevel #>}

**Syntax** config Configure parameters.

802.11b 802.11b/g network parameters. txPower Transmit power parameter.

global All OmniAccess APs.

auto/once Periodic or one-time OmniVista AirView Software

automatic configuration.

<OmniAccess AP> Alcatel OmniAccess Wireless Access Point name.

power level # Transmit power level number.

Note: The OmniAccess AP 802.11b OmniAccess Radio currently supports five transmit power levels: 1 = Maximum transmit power level allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power.

Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum regulatory Transmit Power Level Limits published for each Country Code. Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Also note that the actual maximum transmit power levels may be less than the published regulatory limits.

**Defaults** Global, Auto.

**Examples**To have OmniVista AirView Software automatically set the transmit power for

all 802.11b/g OmniAccess Radios at periodic intervals:

>config 802.11a txPower global auto

To have OmniVista AirView Software automatically reset the transmit power for

all 802.11b/g OmniAccess Radios one time: >config 802.11b txPower global once

To set transmit power for all 802.11b/g OmniAccess Radios to power level 5

(lowest):

>config 802.11b txPower global 5

To set transmit power for 802.11b/g AP1 to global:

>config 802.11b txPower AP1 global

To set transmit power for 802.11b/g AP1 to power level 2:

>config 802.11b txPower AP1 2

**Related Commands** show ap config 802.11b, config 802.11a txPower, config country

# config acl

To configure Access Control Lists, use the config acl command.

>config acl [apply/create/delete/rule] [name]

**Syntax** config acl Command action.

apply <name> Applies the ACL (name with up to 32 alphanumeric

characters) to the data path.

create Create a new ACL. delete Delete an ACL.

rule Configure rules in the ACL.

Name ACL name

Defaults N/A

Examples >config acl create acl01

Related Commands show acl

#### **CONFIG ADVANCED 802.11A COMMANDS**

Use the following advanced 802.11a commands:

- config advanced 802.11a channel foreign
- config advanced 802.11a channel load
- config advanced 802.11a channel noise
- config advanced 802.11a channel update
- config advanced 802.11a factory
- <u>config advanced 802.11a group-mode</u>
- <u>config advanced 802.11a logging channel</u>
- config advanced 802.11a logging coverage
- <u>config advanced 802.11a logging foreign</u>
- <u>config advanced 802.11a logging load</u>
- config advanced 802.11a logging noise
- <u>config advanced 802.11a logging performance</u>
- config advanced 802.11a logging power
- config advanced 802.11a monitor coverage
- config advanced 802.11a monitor load
- <u>config advanced 802.11a monitor noise</u>
- <u>config advanced 802.11a monitor signal</u>
- <u>config advanced 802.11a power-update</u>
- config advanced 802.11a profile clients
- <u>config advanced 802.11a profile coverage</u>
- config advanced 802.11a profile customize
- <u>config advanced 802.11a profile exception</u>
- config advanced 802.11a profile foreign
- <u>config advanced 802.11a profile level</u>
- config advanced 802.11a profile noise
- <u>config advanced 802.11a profile throughput</u>
- config advanced 802.11a profile utilization

# config advanced 802.11a channel foreign

To have OmniVista AirView Software consider or ignore foreign 802.11a interference in making channel selection updates for all 802.11a OmniAccess APs, use the config advanced 802.11a channel foreign command.

>config advanced 802.11a channel foreign [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

channel OmniVista AirView Software channel selections.

foreign Foreign interference. [enable/disable] Consider or ignore.

**Defaults** Enabled.

Examples >config advanced 802.11a channel foreign enable

to have OmniVista AirView Software consider foreign 802.11a interference when making channel selection updates for all 802.11a OmniAccess APs.

**Related Commands** show advanced 802.11a channel, config advanced 802.11b channel foreign

### config advanced 802.11a channel load

To have OmniVista AirView Software consider or ignore traffic load in making channel selection updates for all 802.11a OmniAccess APs, use the config advanced 802.11a channel load command.

>config advanced 802.11a channel load [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

channel OmniVista AirView Software channel selections.

load Traffic load.

[enable/disable] Consider or ignore.

**Defaults** Disabled.

Examples >config advanced 802.11a channel load enable

to have OmniVista AirView Software consider traffic load when making channel

selection updates for all 802.11a OmniAccess APs.

Related Commands show advanced 802.11a channel, config advanced 802.11b channel load

### config advanced 802.11a channel noise

To have OmniVista AirView Software consider or ignore non-802.11a noise in making channel selection updates for all 802.11a OmniAccess APs, use the config advanced 802.11a channel noise command.

>config advanced 802.11a channel noise [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

channel OmniVista AirView Software channel selections.

noise Non-802.11a noise. [enable/disable] Consider or ignore.

**Defaults** Disabled.

Examples >config advanced 802.11a channel noise enable

to have OmniVista AirView Software consider non-802.11a noise when making

channel selection updates for all 802.11a OmniAccess APs.

Related Commands show advanced 802.11a channel, config advanced 802.11b channel noise

# config advanced 802.11a channel update

To have OmniVista AirView Software initiate a channel selection update for all 802.11a OmniAccess APs, use the config advanced 802.11a channel update command.

>config advanced 802.11a channel update

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

channel update Have OmniVista AirView Software update the

channel selections.

**Defaults** (none)

Examples >config advanced 802.11a channel update

**Related Commands** show advanced 802.11a channel, config advanced 802.11b channel update

# config advanced 802.11a factory

To reset 802.11a advanced settings back to the factory defaults, use the config advanced 802.11a factory command.

>config advanced 802.11a factory

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

factory Return all 802.11a advanced settings to their factory

defaults.

**Defaults** (none)

Examples >config advanced 802.11a factory

**Related Commands** show advanced 802.11a channel

# config advanced 802.11a group-mode

To set the 802.11a automatic RF group selection mode on or off, use the config advanced 802.11a group-mode command.

>config advanced 802.11a group-mode <auto/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. group-mode OmniAccess Radio RF grouping.

**Defaults** Auto.

**Examples** To turn the 802.11a automatic RF group selection mode on:

>config advanced 802.11a group-mode auto

To turn the 802.11a automatic RF group selection mode off:

>config advanced 802.11a group-mode off

**Related Commands** show advanced 802.11a group, config advanced 802.11b group-mode

# config advanced 802.11a logging channel

To turn the channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging channel <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging channel Log channel changes. <on/off> Enable or Disable logging.

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging channel on

**Related Commands** show advanced 802.11a logging, config advanced 802.11b logging channel

### config advanced 802.11a logging coverage

To turn the channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging coverage <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging coverage Log coverage changes. <on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging coverage on

Related Commands show advanced 802.11a logging, config advanced 802.11b logging coverage

## config advanced 802.11a logging foreign

To turn the channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging foreign <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging foreign Log foreign changes. <on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging foreign on

Related Commands show advanced 802.11a logging, config advanced 802.11b logging foreign

# config advanced 802.11a logging load

To turn the channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging load <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging load Log load changes.

<on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging load on

Related Commands show advanced 802.11a logging, config advanced 802.11b logging load

### config advanced 802.11a logging noise

To turn the channel change logging mode on or off, use the config advanced 802.11a logging channel command.

>config advanced 802.11a logging noise <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging noise Log noise changes. <on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging noise on

**Related Commands** show advanced 802.11a logging, config advanced 802.11b logging noise

### config advanced 802.11a logging performance

To turn the channel change logging mode on or off, use the config advanced 802.11a logging performance command.

>config advanced 802.11a logging performance <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.
logging performance Log performance changes.
<on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples > config advanced 802.11a logging performance on

Related Commands show advanced 802.11a logging, config advanced 802.11b logging performance

### config advanced 802.11a logging power

To turn the transmit power change logging mode on or off, use the config advanced 802.11a logging power command.

>config advanced 802.11a logging power <on/off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

logging power changes. <on/off> Log power changes. <nylength series to power changes. <nylength series to power changes.

**Defaults** Off (disabled).

Examples >config advanced 802.11a logging power off

Related Commands show advanced 802.11a logging, config advanced 802.11b logging power

# config advanced 802.11a monitor coverage

To set the coverage measurement interval between 60 and 3600 seconds, use the config advanced 802.11a monitor coverage command.

>config advanced 802.11a monitor coverage <seconds>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.
monitor coverage Monitor coverage interval.
<seconds> 60 to 3600 seconds.

**Defaults** 180 seconds.

Examples >config advanced 802.11a monitor coverage 60

to set the coverage measurement interval to 60 seconds.

Related Commands show advanced 802.11a monitor, config advanced 802.11b monitor coverage

### config advanced 802.11a monitor load

To set the load measurement interval between 60 and 3600 seconds, use the config advanced 802.11a monitor load command.

>config advanced 802.11a monitor load <seconds>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

monitor load Monitor load interval. <seconds> 60 to 3600 seconds

**Defaults** 60 seconds.

Examples >config advanced 802.11a monitor load 60

to set the load measurement interval to 60 seconds.

Related Commands show advanced 802.11a monitor, config advanced 802.11b monitor load

### config advanced 802.11a monitor noise

To set the noise measurement interval between 60 and 3600 seconds, use the config advanced 802.11a monitor noise command.

>config advanced 802.11a monitor noise <seconds>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

monitor noise Monitor noise interval. <seconds> 60 to 3600 seconds

**Defaults** 180 seconds.

Examples >config advanced 802.11a monitor noise 120

to set the noise measurement interval to 120 seconds.

Related Commands show advanced 802.11a monitor, config advanced 802.11b monitor noise

# config advanced 802.11a monitor signal

To set the signal measurement interval between 60 and 3600 seconds, use the config advanced 802.11a monitor signal command.

>config advanced 802.11a monitor signal <seconds>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

monitor signal Monitor signal interval. <seconds> 60 to 3600 seconds

**Defaults** 60 seconds.

Examples >config advanced 802.11a monitor signal 120

to set the signal measurement interval to 120 seconds.

Related Commands show advanced 802.11a monitor, config advanced 802.11b monitor signal

# config advanced 802.11a power-update

To initiate a transmit power update for all 802.11a OmniAccess APs, use the config advanced 802.11a power-update command.

>config advanced 802.11a power-update

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

power-update Update transmit power.

**Defaults** (none)

Examples >config advanced 802.11a power-update

Related Commands show advanced 802.11a power, config advanced 802.11b power-update

# config advanced 802.11a profile clients

To set the Alcatel OmniAccess Wireless Access Point clients threshold between 1 and 75 clients, use the config advanced 802.11a profile clients command.

>config advanced 802.11a profile clients <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile clients OmniAccess AP Client profile

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 1 to 75 clients.

**Defaults** 12 clients.

**Examples** To set all OmniAccess AP clients thresholds to 25 clients:

>config advanced 802.11a profile clients global 25

To set the AP1 clients threshold to 75 clients:

>config advanced 802.11a profile clients AP1 75

Related Commands show advanced 802.11a profile, config advanced 802.11b profile clients

# config advanced 802.11a profile coverage

To set the OmniAccess AP coverage threshold between 3 and 50 dB, use the config advanced 802.11a profile coverage command.

>config advanced 802.11a profile coverage <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile coverage OmniAccess AP profile coverage

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 3 to 50 dB.

**Defaults** 12 dB.

**Examples** To set all OmniAccess AP coverage thresholds to 30 dB:

>config advanced 802.11a profile coverage global 30

To set AP1 coverage thresholds to 50 dB:

>config advanced 802.11a profile coverage AP1 50

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile coverage

#### config advanced 802.11a profile customize

To turn customizing on or off for an 802.11a OmniAccess AP performance profile, use the config advanced 802.11a profile customize command.

>config advanced 802.11a profile customize <OmniAccess AP> <on|off>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

customize Performance profile.
OmniAccess AP OmniAccess AP.
on/off Enable or disable.

**Defaults** Off.

**Examples** To turn performance profile customization on for 802.11a OmniAccess AP AP1:

>config advanced 802.11a profile customize AP1 on

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile customize

# config advanced 802.11a profile exception

To set the OmniAccess AP coverage exception level between 0 and 100 percent, use the config advanced 802.11a profile exception command.

>config advanced 802.11a profile exception <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile exception OmniAccess AP profile exception

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 0 to 100 percent.

**Defaults** 25 percent.

**Examples** To set all OmniAccess AP coverage exception levels to 0 percent:

>config advanced 802.11a profile exception global 0

To set the AP1 coverage exception level to 100 percent: >config advanced 802.11a profile exception AP1 100

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile exception

### config advanced 802.11a profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the config advanced 802.11a profile foreign command.

>config advanced 802.11a profile foreign {global/<OmniAccess AP>} <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile foreign foreign interference profile.

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 0 to 100 percent.

**Defaults** 10 percent.

**Examples**To set the Other 802.11a transmitter interference threshold for all OmniAccess

APs to 50 percent:

>config advanced 802.11a profile foreign global 50

To set the Other 802.11a transmitter interference threshold for AP1 to 0

percent:

>config advanced 802.11a profile foreign AP1 0

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile foreign

# config advanced 802.11a profile level

To set the OmniAccess AP client minimum exception level between 1 and 75 clients, use the config advanced 802.11a profile level command.

>config advanced 802.11a profile level <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile level OmniAccess AP profile level

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 1 to 75 clients.

**Defaults** 3 clients.

Examples >config advanced 802.11a profile level global 10

to set all OmniAccess AP client minimum exception levels to 10 clients.

>config advanced 802.11a profile level AP1 25 to set the AP1 client minimum exception level to 25 clients.

Related Commands show advanced 802.11a profile, config advanced 802.11b profile level

### config advanced 802.11a profile noise

To set the 802.11a foreign noise threshold between -127 and 0 dBm, use the config advanced 802.11a profile noise command.

>config advanced 802.11a profile noise <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

profile noise Profile noise limits

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> -127 to 0 dBm.

**Defaults** -70 dBm.

**Examples** To set the 802.11a foreign noise threshold for all OmniAccess APs to -127 dBm:

>config advanced 802.11a profile noise global -127

To set the 802.11a foreign noise threshold for AP1 to 0 dBm:

>config advanced 802.11a profile noise AP1 0

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile noise

#### config advanced 802.11a profile throughput

To set the OmniAccess AP data-rate throughput threshold between 1000 and 10000000 bytes per second, use the config advanced 802.11a profile throughput command.

>config advanced 802.11a profile throughput {global/<OmniAccess AP>} <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters.

profile throughput Data rate threshold

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 1,000 to 10,000,000 bps.

**Defaults** 1,000,000 bps.

**Examples** To set all OmniAccess AP data-rate thresholds to 1000 bytes per second.

>config advanced 802.11a profile data-rate global 1000

To set the AP1 data-rate threshold to 10000000 bytes per second. >config advanced 802.11a profile data-rate AP1 10000000

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile data-rate

# config advanced 802.11a profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the config advanced 802.11a profile utilization command. AWOS generates a trap when this threshold is exceeded.

>config advanced 802.11a profile utilization <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11a Advanced 802.11a parameters. profile utilization OmniAccess AP profile utilization

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 0 to 100 percent.

**Defaults** 80 percent.

**Examples** To set the RF utilization threshold for all OmniAccess APs to 0 percent:

>config advanced 802.11a profile utilization global 0

To set the RF utilization threshold for AP1 to 100 percent >config advanced 802.11a profile utilization AP1 100

**Related Commands** show advanced 802.11a profile, config advanced 802.11b profile utilization

#### **CONFIG ADVANCED 802.11B COMMANDS**

Use the following config advanced 802.11b commands:

- config advanced 802.11b channel foreign
- config advanced 802.11b channel load
- config advanced 802.11b channel noise
- <u>config advanced 802.11b channel update</u>
- config advanced 802.11b factory
- config advanced 802.11b group-mode
- config advanced 802.11b logging channel
- config advanced 802.11b logging coverage
- config advanced 802.11b logging foreign
- <u>config advanced 802.11b logging load</u>
- config advanced 802.11b logging noise
- <u>config advanced 802.11b logging performance</u>
- config advanced 802.11b logging power
- config advanced 802.11b monitor coverage
- config advanced 802.11b monitor load
- config advanced 802.11b monitor noise
- config advanced 802.11b monitor signal
- config advanced 802.11b power-update
- config advanced 802.11b profile clients
- config advanced 802.11b profile coverage

- config advanced 802.11b profile customize
- <u>config advanced 802.11b profile exception</u>
- config advanced 802.11b profile foreign
- config advanced 802.11b profile level
- config advanced 802.11b profile noise
- config advanced 802.11b profile throughput
- <u>config advanced 802.11b profile utilization</u>

# config advanced 802.11b channel foreign

To have OmniVista AirView Software consider or ignore foreign 802.11b/g interference in making channel selection updates for all 802.11b/g OmniAccess APs, use the config advanced 802.11b channel foreign command.

>config advanced 802.11b channel foreign [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

channel OmniVista AirView Software channel selections.

foreign Foreign interference. [enable/disable] Consider or ignore.

**Defaults** Enabled.

Examples >config advanced 802.11b channel foreign enable

to have OmniVista AirView Software consider foreign 802.11b/g interference when making channel selection updates for all 802.11b/g OmniAccess APs.

**Related Commands** show advanced 802.11b channel, config advanced 802.11a channel foreign

### config advanced 802.11b channel load

To have OmniVista AirView Software consider or ignore traffic load in making channel selection updates for all 802.11b/g OmniAccess APs, use the config advanced 802.11b channel load command.

>config advanced 802.11b channel load [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

channel OmniVista AirView Software channel selections.

load Traffic load.

[enable/disable] Consider or ignore.

**Defaults** Disabled.

Examples >config advanced 802.11b channel load enable

to have OmniVista AirView Software consider traffic load when making channel

selection updates for all 802.11b/g OmniAccess APs.

Related Commands show advanced 802.11b channel, config advanced 802.11a channel load

# config advanced 802.11b channel noise

To have OmniVista AirView Software consider or ignore non-802.11b/g noise in making channel selection updates for all 802.11b/g OmniAccess APs, use the config advanced 802.11b channel noise command.

>config advanced 802.11b channel noise [enable/disable]

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

channel OmniVista AirView Software channel selections.

noise Non-802.11b/g noise. [enable/disable] Consider or ignore.

**Defaults** Disabled.

Examples >config advanced 802.11b channel noise enable

to have OmniVista AirView Software consider non-802.11b/g noise when making channel selection updates for all 802.11b/g OmniAccess APs.

**Related Commands** show advanced 802.11b channel, config advanced 802.11a channel noise

### config advanced 802.11b channel update

To have OmniVista AirView Software initiate a channel selection update for all 802.11b/g OmniAccess APs, use the config advanced 802.11b channel update command.

>config advanced 802.11b channel update

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. Channel update Update the channel selections.

**Defaults** (none)

Examples >config advanced 802.11b channel update

Related Commands show advanced 802.11b channel, config advanced 802.11a channel update

### config advanced 802.11b factory

To reset 802.11b/g advanced settings back to the factory defaults, use the config advanced 802.11b factory command.

>config advanced 802.11b factory

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

factory Return all 802.11b/g advanced settings to their

factory defaults.

**Defaults** (none)

Examples >config advanced 802.11b factory

to reset all 802.11b/g advanced settings back to the factory defaults.

**Related Commands** show advanced 802.11b channel

# config advanced 802.11b group-mode

To set the 802.11b/g RF group selection mode on or off, use the config advanced 802.11b group-mode command.

>config advanced 802.11b group-mode <auto/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.
group-mode OmniAccess Radio RF grouping.
<auto/off> Automatic selection or off.

**Defaults** Auto.

**Usage** Use to enable or disable 802.11b/g automatic RF group selection mode.

Examples >config advanced 802.11b group-mode auto

to set the 802.11b/g RF group selection mode to automatic.

>config advanced 802.11b group-mode off to disable the 802.11b/g RF group selection mode.

**Related Commands** show advanced 802.11b group, config advanced 802.11a group-mode

## config advanced 802.11b logging channel

To turn the 802.11b/g channel change logging mode on or off, use the config advanced 802.11b logging channel command.

>config advanced 802.11b logging channel <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

logging channel Log channel changes. <on/off> Enable or Disable logging.

**Defaults** Disabled.

Examples >config advanced 802.11b logging channel on

Related Commands show advanced 802.11b logging, config advanced 802.11a logging channel

# config advanced 802.11b logging coverage

To turn the 802.11b/g channel change logging mode on or off, use the config advanced 802.11b logging channel command.

>config advanced 802.11b logging coverage <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

logging coverage Log coverage changes. <on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging coverage on

**Related Commands** show advanced 802.11b logging, config advanced 802.11a logging coverage

# config advanced 802.11b logging foreign

To turn the 802.11b/g channel foreign logging mode on or off, use the config advanced 802.11b logging foreign command.

>config advanced 802.11b logging foreign <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging foreign on

Related Commands show advanced 802.11b logging, config advanced 802.11a logging foreign

## config advanced 802.11b logging load

To turn the 802.11b/g channel load logging mode on or off, use the config advanced 802.11b logging load command.

>config advanced 802.11b logging load <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

logging load Log load changes.

<on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging load on

**Related Commands** show advanced 802.11b logging, config advanced 802.11a logging load

# config advanced 802.11b logging noise

To turn the 802.11b/g channel noise logging mode on or off, use the config advanced 802.11b logging noise command.

>config advanced 802.11b logging noise <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

logging noise Log noise changes. <on/off> Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging noise on

Related Commands show advanced 802.11b logging, config advanced 802.11a logging noise

# config advanced 802.11b logging performance

To turn the 802.11b/g channel performance logging mode on or off, use the config advanced 802.11b logging performance command.

>config advanced 802.11b logging performance <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. Log performance changes.

<on/off>

Enable or Disable logging

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging performance on

Related Commands show advanced 802.11b logging, config advanced 802.11a logging performance

## config advanced 802.11b logging power

To turn the 802.11b/g transmit power logging mode on or off, use the config advanced 802.11b logging power command.

>config advanced 802.11b logging power <on/off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

logging power changes. <on/off> Log power changes. <nable or Disable logging.

**Defaults** Off (disabled).

Examples >config advanced 802.11b logging power off

**Related Commands** show advanced 802.11b logging, config advanced 802.11a logging power

## config advanced 802.11b monitor coverage

To set the 802.11b/g coverage measurement interval between 60 and 3600 seconds, use the config advanced 802.11b monitor coverage command.

>config advanced 802.11b monitor coverage <seconds>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

monitor coverage Monitor coverage interval. <seconds> 60 to 3600 seconds.

**Defaults** 180 seconds.

Examples >config advanced 802.11b monitor coverage 60

to set the coverage measurement interval to 60 seconds.

**Related Commands** show advanced 802.11b monitor, config advanced 802.11a monitor coverage

# config advanced 802.11b monitor load

To set the 802.11b/g load measurement interval between 60 and 3600 seconds, use the config advanced 802.11b monitor load command.

>config advanced 802.11b monitor load <seconds>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

monitor load Monitor load interval. <seconds> 60 to 3600 seconds

**Defaults** 60 seconds.

Examples >config advanced 802.11b monitor load 60

to set the load measurement interval to 60 seconds.

Related Commands show advanced 802.11b monitor, config advanced 802.11a monitor load

### config advanced 802.11b monitor noise

To set the 802.11b/g noise measurement interval between 60 and 3600 seconds, use the config advanced 802.11b monitor noise command.

>config advanced 802.11b monitor noise <seconds>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

monitor noise Monitor noise interval. <seconds 60 to 3600 seconds

**Defaults** 180 seconds.

Examples >config advanced 802.11b monitor noise 120

to set the noise measurement interval to 120 seconds.

**Related Commands** show advanced 802.11b monitor, config advanced 802.11a monitor noise

## config advanced 802.11b monitor signal

To set the 802.11b/g signal measurement interval between 60 and 3600 seconds, use the config advanced 802.11b monitor signal command.

>config advanced 802.11b monitor signal <seconds>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

monitor signal Monitor signal interval. <seconds> 60 to 3600 seconds

**Defaults** 60 seconds.

Examples >config advanced 802.11b monitor signal 120

to set the signal measurement interval to 120 seconds.

**Related Commands** show advanced 802.11b monitor, config advanced 802.11a monitor signal

#### config advanced 802.11b power-update

To initiate 802.11b/g transmit power update for all OmniAccess APs, use the config advanced 802.11b power-update command.

>config advanced 802.11b power-update

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

power-update Update transmit power

**Defaults** (none)

Examples >config advanced 802.11b power-update

**Related Commands** show advanced 802.11b power, config advanced 802.11a power-update

### config advanced 802.11b profile clients

To set the number of 802.11b/g OmniAccess AP clients threshold between 1 and 75 clients, use the config advanced 802.11b profile clients command.

>config advanced 802.11b profile clients <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

profile clients Client profiles.

global/<OmniAccess AP> Global or OmniAccess AP specific profile.

<value> 1 to 75 clients.

**Defaults** 12 clients

Examples >config advanced 802.11b profile clients global 25

to set the OmniAccess AP clients threshold for all OmniAccess Radios to 25.

>config advanced 802.11b profile clients AP1 75 to set the OmniAccess AP clients threshold for AP1 to 75.

**Related Commands** config advanced 802.11a profile clients

## config advanced 802.11b profile coverage

To set the 802.11b/g OmniAccess AP coverage threshold between 3 and 50 dB, use the config advanced 802.11b profile coverage command.

>config advanced 802.11b profile coverage <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. profile coverage OmniAccess AP profile coverage

global/<OmniAccess AP> global or OmniAccess AP specific profile

<value> 3 to 50 dB

**Defaults** 12 dB

Examples >config advanced 802.11b profile coverage global 30

to set the OmniAccess AP coverage threshold for all OmniAccess APs to 30 dB.

>config advanced 802.11b profile coverage AP1 50 to set the OmniAccess AP coverage threshold for AP1 to 50 dB.

**Related Commands** config advanced 802.11a profile coverage

## config advanced 802.11b profile customize

To turn customization on or off for an 802.11b/g OmniAccess AP performance profile, use the config advanced 802.11b profile customize command.

>config advanced 802.11b profile customize <OmniAccess AP> <on|off>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

**Defaults** Off

Example: >config advanced 802.11b profile customize on

to turn customization on for the AP1 performance profile.

**Related Commands** config advanced 802.11a profile customize

## config advanced 802.11b profile exception

To set the 802.11b/g OmniAccess AP coverage exception level between 0 and 100 percent, use the config advanced 802.11b profile exception command.

>config advanced 802.11b profile exception <global/OmniAccess AP> <value=0 to 100 percent>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

profile exception OmniAccess AP profile exception
global/<OmniAccess AP> global or OmniAccess AP specific profile

<value> 0 to 100 percent

Defaults 25%

Examples >config advanced 802.11b profile exception global 0

to set the OmniAccess AP coverage exception level for all OmniAccess APs to 0

percent.

>config advanced 802.11b profile exception AP1 100

to set the OmniAccess AP coverage exception level for AP1 to 100 percent.

**Related Commands** config advanced 802.11a profile exception

### config advanced 802.11b profile foreign

To set the foreign 802.11b/g transmitter interference threshold between 0 and 100 percent, use the config advanced 802.11b profile foreign command.

>config advanced 802.11b profile foreign {global/<OmniAccess AP>} <value> (0
to 100 percent)

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. profile foreign foreign interference profile.

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 0 to 100 percent.

**Defaults** 802.11b/g foreign profile = (tbd) percent.

Examples >config advanced 802.11b profile foreign global 50

to set the foreign 802.11b/g transmitter interference threshold for the whole

802.11b/g network to 50 percent.

>config advanced 802.11b profile foreign AP1 0

to set the foreign 802.11b/g transmitter interference threshold for AP1 to

0 percent.

**Related Commands** config advanced 802.11b profile foreign

### config advanced 802.11b profile level

To set the 802.11b/g OmniAccess AP client minimum exception level between 1 and 75 clients, use the config advanced 802.11b profile level command.

>config advanced 802.11b profile level <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. profile minimum OmniAccess AP profile level

global/<OmniAccess AP> global or OmniAccess AP specific profile

<value> 1 to 75 clients

**Defaults** 3 clients

Examples >config advanced 802.11b profile level global 75

to set the OmniAccess AP client minimum exception level for all OmniAccess

Radios to 75 clients.

>config advanced 802.11b profile level AP1 25

to set the OmniAccess AP client minimum exception level for AP1 to 25 clients.

**Related Commands** config advanced 802.11a profile level

### config advanced 802.11b profile noise

To set the 802.11b/g foreign noise threshold between -127 and 0 dBm, use the config advanced 802.11b profile noise command.

>config advanced 802.11b profile noise <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. profile noise OmniAccess AP profile noise

global/<OmniAccess AP> global or OmniAccess AP specific profile

<value> -127 to 0 dBm

**Defaults** -70 dB

Examples >config advanced 802.11b profile noise global -90

to set the 802.11b/g foreign noise threshold for the whole 802.11b/g network

to -90 dBm.

>config advanced 802.11b profile noise AP1 -30

to set the 802.11b/g foreign noise threshold for AP1 to -30 dBm.

**Related Commands** config advanced 802.11a profile noise

#### config advanced 802.11b profile throughput

To set the 802.11b/g OmniAccess AP throughput threshold between 1000 and 10000000 bytes per second, use the config advanced 802.11b profile throughput command.

>config advanced 802.11b profile throughput <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters.

global/<OmniAccess AP> global or OmniAccess AP specific profile.

<value> 1,000 to 10,000,000 bps.

**Defaults** 1,000,000 bps

Examples >config advanced 802.11b profile throughput global 1000

to set the OmniAccess AP throughput threshold for all OmniAccess Radios to

1000 bytes per second.

>config advanced 802.11b profile throughput AP1 10000000

to set the OmniAccess AP throughput threshold for AP1 to 10000000 bytes per

second.

Related Commands config advanced 802.11a profile throughput

# config advanced 802.11b profile utilization

To set the 802.11b/g RF utilization threshold between 0 and 100 percent, use the config advanced 802.11b profile utilization command.

>config advanced 802.11b profile utilization <global/OmniAccess AP> <value>

**Syntax** config Configure parameters.

advanced 802.11b Advanced 802.11b/g parameters. profile utilization OmniAccess AP profile utilization

global/<OmniAccess AP> global or OmniAccess AP specific profile

<value> 0 to 100 percent

Defaults 80%

Examples >config advanced 802.11b profile utilization global 100

to set the RF utilization threshold for the whole 802.11b/g network to 100

percent.

>config advanced 802.11b profile utilization AP1 50 to set the RF utilization threshold for the AP1 to 50 percent.

**Related Commands** config advanced 802.11a profile utilization

## **CONFIG ADVANCED TIMERS COMMANDS**

User the following config advanced timers commands:

- <u>config advanced timers auth-timeout</u>
- <u>config advanced timers roque-ap</u>

# config advanced timers auth-timeout

To configure the authentication timeout, and use the config advanced timers auth-timeout command.

>config advanced timers auth-timeout <seconds>

**Syntax** config Configure parameters.

advanced Advanced parameters.

timers Network timers.

auth-timeout Authentication response timeout <seconds> Timeout period in seconds

**Defaults** 10 seconds

Example >config advanced timers auth-timeout 20

**Related Commands** show advanced timers

### config advanced timers rogue-ap

To configure the rogue AP expiration timeout, use the config advanced timers rogue-ap command. Use this command to configure the duration that rogue APs are displayed by the Alcatel OmniAccess Switch or Appliance within a range of 1 to 3600 seconds.

#### >config advanced timers rogue-ap <seconds>

**Syntax** config Configure parameters.

advanced Advanced parameters. timers Network timers.

rogue-ap Rogue AP

<seconds> Timeout period in seconds

**Defaults** 1200 seconds

Example >config advanced timers rogue-ap 1500

**Related Commands** show advanced timers rogue-ap

#### **CONFIG AP COMMANDS**

Use the following config ap commands:

- config ap add
- config ap delete
- <u>config ap disable</u>
- <u>config ap enable</u>
- config ap location
- <u>config ap name</u>
- config ap port
- <u>config ap primary-base</u>
- config ap reset
- <u>config ap stats-timer</u>

#### config ap add

To add a third-party access point, use the config ap add command. This command only applies to third-party APs as OmniAccess APs are automatically detected and added to the Alcatel OmniAccess Switch or Appliance.

>config ap add <MAC address> <port>

**Syntax** config Configure parameters.

ap Access point.

add Add a third-party AP.

<MAC address > MAC address of the third-party AP.

<port> Port number of the Alcatel OmniAccess Switch or

Appliance where AP is connected.

**Defaults** (none)

Example >config ap add ac:10:02:72:2f:bf 12

Related Commands config 802.11a antenna, config 802.11b antenna

# config ap delete

To delete a third-party access point from the Alcatel OmniAccess Switch or Appliance, use the config ap delete command.

>config ap delete <MAC address>

**Syntax** config Configure parameters.

ap Access point.

delete Delete a third-party AP.

<MAC address > MAC address of the third-party AP.

**Defaults** (none)

Examples >config ap delete ac:10:02:72:2f:bf

Related Commands config 802.11a antenna, config 802.11b antenna

# config ap disable

To disable an OmniAccess AP, use the config ap disable command.

>config ap disable <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP. disable Disable command.

<OmniAccess AP> Name of the OmniAccess AP.

**Defaults** (none)

Examples >config ap disable AP1

**Related Commands** config ap enable

# config ap enable

To enable an OmniAccess AP, use the config ap enable command.

>config ap enable <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP. enable Enable command.

<OmniAccess AP> Name of the OmniAccess AP.

**Defaults** (none)

Examples >config ap enable AP1

**Related Commands** config ap disable

## config ap location

To modify the descriptive location of an OmniAccess AP, use the config ap location command. The OmniAccess AP must be disabled before changing this parameter.

>config ap location "<name>" <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP. location Descriptive location.

<name> Location name (enclosed by double quotation

marks)

<OmniAccess AP> Name of the OmniAccess AP

**Defaults** (none)

Examples >config ap location "Building 1" AP1

**Related Commands** show ap summary

## config ap name

To modify the name of an OmniAccess AP, use the config ap name command.

>config ap name <Old AP name> <New AP name>

**Syntax** config Configure parameters.

ap OmniAccess AP.

name Name of the OmniAccess AP.
<Old AP name> Current OmniAccess AP name.
<New AP name> Desired OmniAccess AP name.

**Defaults** (none)

Examples >config ap name AP1 AP2

**Related Commands** show ap config

### config ap port

To configure the port of a third-party access point, use the config ap port command.

>config ap port <MAC address>

**Syntax** config Configure parameters.

ap Access point.

port Alcatel OmniAccess Switch or Appliance port.

<MAC address > MAC address of the third-party AP.

**Defaults** (none)

Examples >config ap port ac:10:02:72:2f:bf

Related Commands show ap config

# config ap primary-base

To set the OmniAccess AP primary Alcatel OmniAccess Switch or Appliance, use the config ap primary-base command. The OmniAccess AP associates with this Alcatel OmniAccess Switch or Appliance for all network operation and in the event of a hardware reset.

>config ap primary-base <Switch name> <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP.

primary-base OmniAccess AP primary Alcatel OmniAccess Switch

or Appliance.

<Switch name> Name of Alcatel OmniAccess Switch or Appliance.

<OmniAccess AP> OmniAccess AP name.

**Defaults** (none)

Examples >config ap primary-base SW\_1 AP2

**Related Commands** show sysinfo, config sysname

# config ap reset

To reset an OmniAccess AP, use the config ap reset command.

>config ap reset <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP.
reset Reset command.
<OmniAccess AP> OmniAccess AP name.

**Defaults** (none)

Example >config ap reset AP2

Related Commands show ap config

### config ap stats-timer

Use this command to set the time in seconds that the OmniAccess AP sends its DOT11 statistics to the Alcatel OmniAccess Switch or Appliance. A value of 0 (zero) means the OmniAccess AP will not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the OmniAccess AP must be disabled to set this value.

>config ap stats-timer <seconds> <OmniAccess AP>

**Syntax** config Configure parameters.

ap OmniAccess AP.

stats-timer OmniAccess AP primary Alcatel OmniAccess Switch

or Appliance.

<seconds> Time in seconds. <OmniAccess AP> OmniAccess AP name

**Defaults** 0 (disabled)

Examples >config ap stats-timer 600 AP2

**Related Commands** config ap disable

# config blacklist

To create or delete a disabled (blacklisted) entry, use the config blacklist command.

>config blacklist [add/delete] <MAC addr> [description]

**Syntax** config blacklist Command action.

add/delete Creates/deletes a local Blacklist entry.

MAC addr MAC address of the local Blacklist entry.

description Sets the description for a Blacklist entry.

**Defaults** (none)

Examples >config blacklist add 0:0b:85:01:18:b0 lab

>config blacklist delete 0:0b:85:01:18:b0 lab

Related Commands show blacklist

### config certificate

To configures SSL Certificates, use the config certificate command.

>config certificate [generate/compatibility] [webadmin/webauth]

**Syntax** config certificate Command action.

generate Generates new certificates.

webadmin Generates a new web administration certificate webauth Generates a new web authentication certificate

compatibility Configure certificate compatibility mode.

Defaults N/A

Examples >config certificate generate webadmin

Creating a certificate may take some time. Do you wish to continue?  $(\mbox{y/n})$ 

>config certificate compatibility

**Related Commands** show certificate summary, show certificate compatibility

### config client deauthenticate

To deauthenticate a client, use the config client deauthenticate command.

>config client deauthenticate <MAC Address>

**Syntax** config Configure parameters.

client Network client.

deauthenticate Deauthenticate command. <MAC address> Client MAC address.

**Defaults** None.

Examples >config client deauthenticate 11:11:11:11:11:11

**Related Commands** show client summary, show client detail

# config country

To configure the country code, use the config country command. Use the show country command to display a list of supported countries.

>config country <country-code>

**Syntax** config Configure parameters.

country Set this Alcatel OmniAccess Switch or Appliance to

comply with selected country's regulations.

<country-code> Select country.

**Defaults** Country code = US (United States of America).

Examples >config country US

to configure the country code for use in the United States of America, which

allows 802.11a and 802.11b/g transmissions.

Related Commands show country

### config custom-web

To configure the custom-web authentication page, use the config custom-web command.

>config custom-web {redirectUrl <string>/weblogo [enable/disable]/web message
<string>/webtitle <string>}

**Syntax** config custom-web Command action.

redirectUrl <string> Enable/disable the custom redirect URL weblogo [enable/disable] Enable/disable the Web Authentication logo web message <string> Set the customer message text for Web

Authentication

webtitle <string> Set the custom title text for Web Authentication

**Defaults** None.

Examples >config custom-web redirectUrl abc.com

>config custom-web weblogo/weblogo enable
>config custom-web web message Thisistheplace

>config custom-web webtitle Helpdesk

**Related Commands** show custom-web

### **CONFIG INTERFACE COMMANDS**

Use the following config interface commands:

- <u>config interface acl</u>
- config interface address
- config interface create
- config interface delete
- config interface dhcp
- <u>config interface hostname</u>
- config interface port

<u>config interface vlan</u>

## config interface acl

To configure an interface's Access Control List, use the config interface acl command.

>config interface acl <management/vlan-intf-name> <ACL name/none>

**Syntax** config interface acl Command action

ap-manager Configures the AP Manager interface.
management Configures the management interface.

<interface-name> Enter interface name.

Defaults N/A

Examples >config interface acl management none

**Related Commands** show interface

### config interface address

To configure an interface's address information, use the config interface address command.

>config interface address [ap-manager <ipaddress>/management <addr> <netmask>
<gateway>/service port <addr> <netmask>/virtual <addr>] <interface-name>

**Syntax** config interface address Command action.

ap-manager <IP address>Configures the AP Manager interface.
management <addr> Configures the management interface.

<netmask> <gateway>

service-port <addr> Configures the out-of-band service Port.

<netmask>

virtual <addr> Configures the virtual gateway interface.

<interface-name> Enter interface name.

Defaults N/A

Examples >config interface address ap-manger 172.168.2.3

**Related Commands** show interface

### config interface create

To add a new dynamic interface, use the config interface create command.

>config interface create <interface-name> <vlan-id>

Syntax config interface create Command action

<interface-name> Interface name.

<vlan-id> VLAN id.

**Defaults** N/A

Examples >tbd

**Related Commands** show interface

# config interface delete

To delete a dynamic interface, use the config interface delete command.

>config interface delete <interface-name>

**Syntax** config interface delete Command action.

<interface-name> Interface name.

**Defaults** N/A

Examples >config interface delete VLAN501

**Related Commands** show interface

# config interface dhcp

To configure DHCP options on an interface, use the config interface dhcp command.

>config interface dhcp ap-manager/management/service-port <interface-name>

**Syntax** config interface dhcp Command action.

ap-manager Configures the AP Manager interface.
management Configures the Management Interface.

service-port Configures the out-of-band service Port with disable

or enable.

<interface-name> Enter interface name.

Defaults N/A

Examples >config interface dhcp service-port DHCP02

**Related Commands** show interface

### config interface hostname

To configure the virtual interface's virtual DNS host name, use the config interface hostname command.

>config interface hostname <virtual> <DNS Host Name>

**Syntax** config interface hostname Command action.

virtual Configures the virtual gateway interface.

(The Virtual Gateway IP Address is any fictitious, unassigned IP address, such as 1.1.1.1, to be used

by Layer 3 Security and Mobility managers.)

<DNS Host Name> DNS Host Name.

Defaults N/A

Examples >config interface hostname 1.1.1.1 DNS\_Host

**Related Commands** show interface

### config interface port

To assign an interface to a physical port, use the config interface port command.

>config interface port <management/vlan-intf-name> <port number>

**Syntax** config interface port Command action.

management The Management Interface.

vlan-intf-name VLAN or interface name

<port number> Port number for the interface.

Defaults N/A

Examples >config interface port management 3

**Related Commands** show interface

# config interface vlan

To configure an interface's VLAN Identifier, use the config interface vlan command.

>config interface vlan <management/vlan-intf-name> <vlan>

**Syntax** config interface vlan Command action.

management The management interface. Vlan-intf-name VLAN identifier name.

<vlan> VLAN id.

Defaults N/A

Examples >config interface vlan management 01

Request failed - Active WLAN using interface. Disable WLAN first.

**Related Commands** show interface

### config load-balancing

To change the state of the load-balancing feature, use the config load-balancing command.

>config load-balancing [enable/disable]

**Syntax** config Configure parameters.

load-balancingAggressive load-balancing[enable/disable]Enable or disable the feature

**Defaults** Enabled

Examples >config load-balancing enable

**Related Command** show load-balancing

#### config loginsession close

To close active telnet sessions, use the config loginsession close command. Use this command to terminate an individual or all active telnet sessions with the Alcatel OmniAccess Switch or Appliance. If you are using a telnet session for your CLI interface and terminate your session or all sessions, you will need to reconnect and log back into the Alcatel OmniAccess Switch or Appliance.

>config loginsession close [<session id>/ all]

**Syntax** config Configure parameters.

loginsession Telnet sessions. close Terminate session.

<session id> Terminate a specific telnet session. all Terminate all telnet sessions.

**Defaults** (none)

Examples >config loginsession close all

**Related Commands** show loginsession

#### **CONFIG MACFILTER COMMANDS**

Use the following config macfilter commands:

- <u>config macfilter add</u>
- <u>config macfilter delete</u>
- <u>config macfilter mac-delimiter</u>
- <u>config macfilter mac-delimiter</u>

# config macfilter add

To create a MAC filter entry on the Alcatel OmniAccess Switch or Appliance, use the config mac filter add command. Use this command to add a client locally to a WLAN on the Alcatel OmniAccess Switch or Appliance. This filter bypasses the RADIUS authentication process.

>config macfilter add <MAC address> <WLAN ID>

**Syntax** config Configure parameters.

macfilter Local MAC address filter

add Add a client

<WLAN ID> Client WLAN

**Defaults** (none)

Examples >config macfilter add 11:11:11:11:11 1

**Related Commands** show macfilter

# config macfilter delete

Use to remove a local client from the Alcatel OmniAccess Switch or Appliance.

>config macfilter delete <MAC address>

**Syntax** config Configure parameters.

macfilter Local MAC address filter

delete Delete a client <MAC address Client MAC address

**Defaults** (none)

Examples >config macfilter delete 11:11:11:11:11:11

Deleted user 111111111111

**Related Commands** show macfilter

# config macfilter mac-delimiter

To set the MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers, use the config macfilter mac-delimiter command.

>config macfilter mac-delimiter <colon|hyphen|none>

Syntax config Configure parameters.

macfilter Local MAC address filter.

mac-delimiter MAC address format for RADIUS servers.

<none|colon|hyphen> MAC delimiter format.

**Defaults** (none)

Examples >config macfilter mac-delimiter colon

To have AWOS send MAC address to RADIUS servers in the form

aa:bb:cc:dd:ee:ff.

>config macfilter mac-delimiter hyphen

To have AWOS send MAC address to RADIUS servers in the form

aa-bb-cc-dd-ee-ff.

>config macfilter mac-delimiter none

To have AWOS send MAC address to RADIUS servers in the form aabbccddeeff.

Related Commands show macfilter

## config macfilter wlan-id

To modify a client WLAN, use the config macfilter wlan-id command.

>config macfilter wlan-id <MAC address> <WLAN ID>

**Syntax** config Configure parameters.

macfilter Local MAC address filter Wlan-id Modify client WLAN < MAC address Client MAC address

<wl>New WLAN identification number

**Defaults** (none)

Examples >config macfilter wlanid 11:11:11:11:11:12

**Related Commands** show macfilter, show wlan

### **CONFIG MGMTUSER COMMANDS**

Use the following config mgmtuser commands:

- <u>config mgmtuser add</u>
- config mgmtuser delete
- config mgmtuser password

# config mgmtuser add

To add a management user login to the Alcatel OmniAccess Switch or Appliance, use the config mgmtuser add command.

>config mgmtuser add <username> <password> [read-write/read-only]

Syntax config Configure parameters.

mgmtuser Management user account add Add a management user account

<username> Account username
<password> Account password
[read-write/read-only] Account privileges

**Defaults** (none)

Examples >config mgmtuser add admin read-write

**Related Commands** show mgmtuser

## config mgmtuser delete

To delete a management user login to the Alcatel OmniAccess Switch or Appliance, use the config mgmtuser delete command.

>config mgmtuser delete <username>

**Syntax** config Configure parameters.

mgmtuser Management user account

delete Delete a management user account

<username> Account username

**Defaults** (none)

Examples >config mgmtuser delete admin

Deleted user admin

**Related Commands** show mgmtuser

#### config mgmtuser password

To change a management user password, use the config mgmtuser password command.

>config mgmtuser password <username> <password>

**Syntax** config Configure parameters.

mgmtuser Management user account password Add a management user account

<username> Account username
<password> New password

**Defaults** (none)

Examples >config mgmtuser password admin

**Related Commands** show mgmtuser

#### **CONFIG MIRROR COMMANDS**

Use the following config mirror commands:

- <u>config mirror ap</u>
- config mirror foreignap

- config mirror mac
- config mirror port

## config mirror ap

To have all OmniAccess AP transmit and receive data appear on the Mirror Port (see config mirror port) for troubleshooting, use the config mirror ap command.

>config mirror ap [enable/disable] <name>

**Syntax** Configure parameters. config

> Mirror command. mirror OmniAccess AP. ap

[enable/disable] Enable or Disable Mirroring for this OmniAccess AP.

<name> OmniAccess AP name.

**Defaults** (none)

**Examples** >config mirror ap enable AP5

configures the 4012 or 4024 OmniAccess Wireless Switch so the OmniAccess AP AP5 data stream is Mirrored on the port selected using the *config mirror port* 

command.

**Related Commands** config mirror foreignap, config mirror mac, config mirror port, show mirror ap,

show mirror foreignap, show mirror mac, show mirror port

## config mirror foreignap

To have all transmit and receive data from a third-party AP appear on the Mirror Port (see *config mirror port*) for troubleshooting, use the config mirror foreignap command.

>config mirror foreignap [enable/disable] <port>

**Syntax** config Configure parameters.

> Mirror command. mirror

Third-Party Access Point. foreignap

Enable or Disable Mirroring for this third-party AP. [enable/disable] <port> Front-panel port the third-party AP is connected to.

**Defaults** (none)

**Examples** >config mirror foreignap enable 3

> configures the 4012 or 4024 OmniAccess Wireless Switch so the data stream from the third-party AP on Port 3 is Mirrored on the port selected using the

config mirror port command.

**Related Commands** config mirror ap, config mirror mac, config mirror port, show mirror ap, show

mirror foreignap, show mirror mac, show mirror port

#### config mirror mac

To have all client transmit and receive data appear on the Mirror Port (see config mirror port) for troubleshooting, use the config mirror mac command.

>config mirror mac [enable/disable] <name>

**Syntax** config Configure parameters. mirror Mirror command. mac OmniAccess AP.

[enable/disable] Enable or Disable Mirroring for this OmniAccess AP.

<name> OmniAccess AP name.

**Defaults** (none)

Examples >config mirror mac enable 02:03:sd:66:85:4a

configures the 4012 or 4024 OmniAccess Wireless Switch so the data stream from client 02:03:sd:66:85:4a is Mirrored on the port selected using the *config* 

*mirror port* command.

**Related Commands** config mirror ap, config mirror foreignap, config mirror port, show mirror ap,

show mirror foreignap, show mirror mac, show mirror port

## config mirror port

To set up a Mirror Port on the OmniAccess Wireless Switch for troubleshooting using a protocol analyzer, use the config mirror port command.

>config mirror port <number>

**Syntax** config Configure parameters.

mirror Mirror command.

port Mirror client, OmniAccess AP, and/or third-party AP

data stream to this port.

<number> Front-panel port on a 4012 or 4024 OmniAccess

Wireless Switch.

**Defaults** (none)

Examples >config mirror port 23

configures the 4012 or 4024 OmniAccess Wireless Switch so all client, Omni-

Access AP, and/or third-party AP data stream is Mirrored to port 23.

To transfer the Mirrored data to another port, repeat the command with a new

port number.

**Related Commands** config mirror ap, config mirror foreignap, config mirror mac, show mirror ap,

show mirror foreignap, show mirror mac, show mirror port

#### **CONFIG MOBILITY GROUP COMMANDS**

Use the following config mobility group commands:

- config mobility group discovery
- <u>config mobility group member</u>

# config mobility group discovery

To activate or deactivate the dynamic discovery of mobility group members, use the config mobility group discovery command.

>config mobility group discovery [enable/disable]

Syntax config Configure parameters.
mobility group discover Mobility group discovery

[enable/disable] Enable or disable mobility group feature

**Defaults** (none)

Examples >config mobility group discovery enable

**Related Commands** show mobility summary

#### config mobility group member

To add or delete users from the mobility group member list, use the config mobility group member command.

>config mobility group member [add/delete] <MAC address>

**Syntax** config Configure parameters.

mobility group Mobility group member

[add/delete] Enable or disable mobility group feature

<MAC address> Client MAC address

**Defaults** (none)

Examples >config mobility group member add 11:11:11:11:11:11

**Related Commands** show mgmtuser

#### **CONFIG NETUSER COMMANDS**

Use the following config netuser commands:

• <u>config netuser add</u>

<u>config netuser delete</u>

config netuser password

• <u>config netuser wlan-id</u>

#### config netuser add

To add a user to the local network, use the config netuser add command.

>config netuser add <username> <password> <WLAN ID>

**Syntax** config Configure parameters.

netuser Local network user

add Add a user

<username> Network username <password> User password

<WLAN ID WLAN assigned to the user

**Defaults** (none)

Examples >config netuser add airel 1

**Related Commands** show netuser

#### config netuser delete

To delete an existing user from the local network, use the config netuser delete command.

>config netuser delete <username>

**Syntax** config Configure parameters. netuser Local network user

delete Add a user

<username> Network username

**Defaults** (none)

Examples >config netuser delete aire1

Deleted user airel

**Related Commands** show netuser

## config netuser password

To change a local network user password, use the config netuser password command.

>config netuser password <username> <password>

**Syntax** config Configure parameters.

netuser Local network user
password Modify the password
<username> Network username
<password> New user password

**Defaults** (none)

Examples >config netuser password aire1 aire2

**Related Commands** show netuser

#### config netuser wlan-id

To change a user WLAN ID, use the config netuser wlan-id command.

>config netuser wlan-id <username> <WAN ID>

**Syntax** config Configure parameters.

netuser Local network user wlan-id Modify the WLAN ID <username>

<WLAN ID New WLAN assigned to the user

**Defaults** (none)

Examples >config netuser wlan-id aire1 2

**Related Commands** show netuser, show wlan summary

### **CONFIG NETWORK COMMANDS**

Use the following config network commands:

- config network arptimeout
- <u>config network bcast-ssid</u>
- <u>config network dsport</u>
- <u>config network master-base</u>

- <u>config network mgmt-via-wireless</u>
- <u>config network params</u>
- config network rf-mobility-domain
- config network secureweb
- config network secweb-passwd
- config network ssh
- config network telnet
- <u>config network usertimeout</u>
- config network vlan
- <u>config network webmode</u>

# config network arptimeout

To set the ARP entry timeout value, use the config network arptimeout command.

>config network arptimeout <seconds>

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter

arptimeout Modify the ARP timeout value

<seconds> Timeout in seconds

Defaults 300

Examples >config network arptimeout 240

**Related Commands** show network

## config network bcast-ssid

To configure SSID broadcasts and probe request responses, use the config network bcast-ssid command. Use to enable or disable broadcast of the Alcatel OmniAccess Switch or Appliance SSID and to simultaneously enable or disable responses to probe requests.

#### >config network bcast-ssid enable

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

bcast-ssid Modify the broadcast SSID state.

[enable/disable] Change the state.

**Defaults** Enable

Examples >config network bcast-ssid enable

**Related Commands** show network

## config network dsport

To set the distribution port, use the config network dsport command.

Use to assign the interface port on the Alcatel OmniAccess Switch or Appliance to the distributed network. This hardwire connection to the Alcatel OmniAccess Switch or Appliance will use fast Ethernet ports 1-12 or 1-24 from the front panel of the Alcatel OmniAccess Switch or Appliance or a GigE port connection, either 1, 2, 13 or 25, depending on your network setup and the Alcatel OmniAccess Switch or Appliance model.

#### >config network dsport <port>

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

dsport Distribution port.

Ethernet port or 13 for 1000BASE-T/-SX GigE port. Model 4024: 1 through 24 for 10/100BASE-T Ethernet port or 25 for 1000BASE-T/-SX GigE port.

Model 4102: 1 for 1000BASE-SX GigE port.

**Defaults** Set during startup wizard installation.

Examples >config network dsport 7

to assign the Distribution System to use 4012 or 4024 OmniAccess Wireless

Switch Ethernet port 7.

**Related Commands** show network, show port, config network params, config network protocol

## config network master-base

To set the Alcatel OmniAccess Switch or Appliance as a master, use the config network master-base command. This setting is only used upon network installation and should be disabled after the initial network configuration.

#### >config network master-base

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

master-base Master Alcatel OmniAccess Switch or Appliance.

**Defaults** (none)

**Examples** >config network master-base

Related Commands None

## config network mgmt-via-wireless

To enable Alcatel OmniAccess Switch or Appliance management from an associated wireless client, use the config network mgmt-via-wireless command. Note that this feature allows wireless clients to manage only the Alcatel OmniAccess Switch or Appliance associated with the client AND the associated OmniAccess AP. That is, clients cannot manage another Alcatel OmniAccess Switch or Appliance with which they are not associated.

#### >config network mgmt-via-wireless [enable/disable]

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

mgmt-via-wireless Management sessions. [enable/disable] Enable or disable.

**Defaults** Disabled

Examples >config network mgmt-via-wireless enable

Related Commands show network

#### config network params

To set the Alcatel OmniAccess Switch or Appliance network parameters, use the config network params command.

>config network params <ipaddress> <ip mask> {gateway}

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

params Network parameters.

mask.

{gateway} Optional gateway address.

**Defaults** Set during startup wizard installation.

Examples >config network params 172.1.1.1 255.255.255.0

**Related Commands** config network protocol, show network

### config network rf-mobility-domain

To set the RF mobility group domain name, use the config network rf-mobility-domain command.

>config network rf-mobility-domain <name>

**Syntax** config Configure parameters.

network Alcatel OmniAccess Switch or Appliance network

parameter.

rf-mobility-domain Mobility group domain. <name> Mobility group name.

**Defaults** (none)

Examples >config network params 172.1.1.1 255.255.255.0

**Related Commands** show network

## config network secureweb

To change the state of the secure web (https = http + SSL) interface, use the config network secureweb command.

>config network secureweb [enable/disable]

**Syntax** config Configure parameters.

network Network parameters.

secureweb Secure web interface. [enable/disable] Change the interface state.

**Defaults** Enabled

**Examples** >config network secureweb enable

**Related Commands** show network

## config network secweb-passwd

To change the secure web interface SSL certificate password, use the config network secweb-passwd command.

>config network secweb-passwd <password>

**Syntax** Configure parameters. config

> network Network parameters. secweb-passwd Secure web password. <password> Change the password.

**Defaults** (none)

**Examples** >config network secweb-passwd admin

**Related Commands** show network

# config network ssh

To change the state of Secure Shell sessions, use the config network ssh command.

>config network ssh [enable/disable]

**Syntax** config Configure parameters.

> network Network parameters. ssh Secure Shell sessions

[enable/disable] Change the state of the SSH session.

**Defaults Enabled** 

**Examples** >config network ssh enable

**Related Commands** show network

#### config network telnet

To change the state of telnet sessions, use the config network telnet command.

>config network ssh [enable/disable]

**Syntax** config Configure parameters.

network Network parameters.

telnet Telnet sessions

[enable/disable] Change the state of the telnet session.

**Defaults** Disabled

**Examples** >config network telnet enable Related Commands show network

## config network usertimeout

To change the timeout for idle client sessions, use the config network usertimeout command. Use this command to set the idle client session duration on the Alcatel OmniAccess Switch or Appliance. The minimum duration is 10 seconds.

#### >config network usertimeout <seconds>

**Syntax** config Configure parameters.

network Network parameters. usertimeout Timeout for sessions. <seconds> Duration in seconds.

Defaults 300

Examples >config network usertimeout 1200

Related Commands show network

#### config network vlan

To set the management virtual LAN identification number, use the config network vlan command.

If you are logged in to the Alcatel OmniAccess Switch or Appliance remotely (that is, using any other connection than a serial connection), your session will be terminated.

#### >config network vlan <VLAN ID>

**Syntax** config Configure parameters.

network Network parameters.

vlan Virtual LAN.

<VLAN ID> Identification number.

**Defaults** Disabled

Examples >config network vlan 1

Related Commands show network

### config network webmode

To enable or disable web access, use the config network webmode command.

>config network webmode [enable/disable]

**Syntax** config Configure parameters.

network Network parameters.

webmode Web interface.

[enable/disable] Change the interface state.

**Defaults** Enabled

Examples >config network webmode disable

**Related Commands** show network

### **CONFIG PORT COMMANDS**

Use the following config port commands:

- <u>config port adminmode</u>
- <u>config port autoneg</u>
- config port linktrap
- config port physicalmode
- config port power

## config port adminmode

To configure the administration mode of a single port or all Alcatel OmniAccess Switch or Appliance ports, use the config port adminmode command.

>config port adminmode [<port number>/all] [enable/disable]

**Syntax** config Configure parameters.

port Port parameters adminmode Administrative mode

[<port number>/all] Individual port number or all ports

[enable/disable] Port state

**Default** Enabled

**Examples** To disable port 8:

>config port adminmode 8 disable

To enable all ports:

>config port adminmode all enable

Related Commands show port

### config port autoneg

To configure 10/100BASE-T Ethernet ports for physical port autonegotiation, use the config port autoneg command.

Note that port autoconfiguration must be disabled before you make physical mode manual settings using the config port physicalmode command. Also note that the config port autoneg command overrides settings made using the config port physicalmode command.

>config port autoneg [<port>/all] [enable/disable]

**Syntax** config Configure parameters.

port 10/100BASE-T Ethernet. <port> Physical port number.

all All Ports.

enable Turn autonegotiation on. disable Turn autonegotiation off.

**Defaults** All Ports = autonegotiation enabled.

**Examples** >config port autoneg all enable

to turn on physical port autonegotiation for all front-panel Ethernet ports.

>config port autoneg 19 disable

to disable physical port autonegotiation for front-panel Ethernet port 19.

**Related Commands** show port, config port physicalmode

## config port linktrap

To change trap settings for link status alert for a single port or all Alcatel OmniAccess Switch or Appliance ports, use the config port linktrap command.

>config port linktrap [<port number>/all] [enable/disable]

**Syntax** config Configure parameters.

port Port parameters. linktrap Link status alert.

[<port number>/all] Individual port number or all ports.

[enable/disable] Port state.

**Default** Enabled.

**Examples** To disable port 8 traps:

>config port linktrap 8 disable

To enable all port traps:

>config port linktrap all enable

Related Commands show port

## config port physicalmode

To set any or all front-panel 10/100BASE-T Ethernet ports for dedicated 10 Mbps or 100 Mbps, Half or Full Duplex operation, use the config port physicalmode command.

Note that you must disable autonegotiation using the config port autoneg command before manually configuring any port's physical mode. Also note that the config port autoneg command overrides settings made using the config port physicalmode command.

>config port physicalmode [<port>/all] [enable/disable] [100h/100f/10h/10f]

**Syntax** config Configure parameters.

port Port parameters. physicalmode Port physical mode.

[<port>/all] Individual port number or all ports

[enable/disable] Port state

[100h/100f/10h/10f] o 100h = 100 Mbps/Half Duplex operation

o 100f = 100 Mbps/Full Duplex operation o 10h = 10 Mbps/Half Duplex operation o 10f = 10 Mbps/Full Duplex operation

**Defaults** All Ports are set to auto negotiate.

**Examples** To set all ports to 100 Mbps/Full Duplex operation:

>config port physicalmode all 100f

To set port 20 to 100 Mbps/Half Duplex operation:

>config port physicalmode 20 100h

To set port 21 to 10 Mbps/Full Duplex operation:

>config port physicalmode 21 10f

To set port 22 to 10 Mbps/Half Duplex operation:

>config port physicalmode 22 10h

Related Commands config port autoneg, show port

#### config port power

To change Power over Ethernet (POE) settings for a single port or all Alcatel OmniAccess Switch or Appliance ports, use the config port power command. NOT ALL APs are POE (802.3af) compatible! If you are using third-party access points, refer to your user documentation to determine compatibility. Enabling POE to non-compatible APs can result in severe equipment damage including fire!

>config port power [<port number>/all] [enable/disable]

**Syntax** config Configure parameters.

port Port parameters power POE mode

[<port number>/all] Individual port number or all ports

[enable/disable] Port state

**Default** Enabled

**Examples** To disable POE on port 8:

>config port power 8 disable

To enable POE on all ports:

>config port power all enable

Related Commands show port

#### config prompt

To change the CLI system prompt, use the config prompt command.

This command can be used any time the CLI interface is active.

>config prompt <system prompt>

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

**Syntax** config Configure parameters.

prompt CLI system prompt, up to 31 alphanumeric

characters.

<system prompt> New CLI system prompt, in double guotes.

**Defaults** The system prompt is configured using the startup wizard.

Examples (old CLI prompt >config prompt "Type here"

Type here>

**Related Commands** None.

## config qos queu\_length

To configure the qos parameter, use the config qos command.

>config qos queue\_length [bronze/silver/gold] <length>

**Syntax** config qos Command action.

queue\_length Configure qos queue length bronze/silver/gold Level of quality of service

<length> Queue length

Defaults N/A

Examples >config qos queue\_length gold 12

**Related Commands** show gos queue\_length all

#### **CONFIG RADIUS ACCT COMMANDS**

Use the following config radius acct commands:

• <u>config radius acct add</u>

• config radius acct delete

<u>config radius acct disable</u>

config radius acct enable

## config radius acct add

To configure a RADIUS accounting server for the Alcatel OmniAccess Switch or Appliance, use the config radius acct add command.

>config radius acct add <index> <IP addr> <port> <secret>

**Syntax** config Configure parameters.

radius acct RADIUS accounting server. add Add a RADIUS server.

<index> Priority index (Alcatel OmniAccess Switch or Appli-

ance begins search with 1).

<IP addr> IP Address.

<port> Port number for the interface protocols

<secret> Login password

**Defaults** When added the port number defaults to 1813 and state is enabled.

Examples >config radius acct add 1 10.10.10.10 1813 admin

to configure a priority 1 RADIUS server at 10.10.10.10 using port 1813 with a

login password of admin.

**Related Commands** show radius acct statistics

## config radius acct delete

To delete a RADIUS accounting server for the Alcatel OmniAccess Switch or Appliance, use the config radius acct delete command.

>config radius acct add <index>

**Syntax** config Configure parameters.

radius acct RADIUS accounting server. delete Remove a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius acct delete 1

**Related Commands** show radius acct statistics

## config radius acct disable

To disable a RADIUS accounting server for the Alcatel OmniAccess Switch or Appliance, use the config radius acct disable command.

>config radius acct disable <index>

**Syntax** config Configure parameters.

radius acct RADIUS accounting server. disable Disable a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius acct disable 1

**Related Commands** show radius acct statistics

## config radius acct enable

To enable a RADIUS accounting server for the Alcatel OmniAccess Switch or Appliance, use the config radius acct enable command.

>config radius acct enable <index>

**Syntax** config Configure parameters.

radius acct RADIUS accounting server. enable Enable a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius acct enable 1

**Related Commands** show radius acct statistics

#### **CONFIG RADIUS AUTH COMMANDS**

Use the following config radius auth commands:

- <u>config radius auth add</u>
- <u>config radius auth delete</u>
- config radius auth disable
- config radius auth enable

### config radius auth add

To configure a RADIUS authentication server for the Alcatel OmniAccess Switch or Appliance, use the config radius auth add command.

>config radius auth add <index> <IP addr> <port> <secret>

**Syntax** config Configure parameters.

radius auth RADIUS authentication server.

add Add a RADIUS server.

<index> Priority index (Alcatel OmniAccess Switch or Appli-

ance begins search with 1).

<IP addr> IP Address.

<port> Port number for the interface protocols

<secret> Login password

**Defaults** When added the port number defaults to 1812 and state is enabled.

Examples >config radius auth add 1 10.10.10.10 1812 admin

to configure a priority 1 RADIUS server at 10.10.10.10 using port 1812 with a

login password of admin.

**Related Commands** show radius auth statistics

# config radius auth delete

To delete a RADIUS authentication server for the Alcatel OmniAccess Switch or Appliance, use the config radius auth delete command.

>config radius auth add <index>

**Syntax** config Configure parameters.

radius auth RADIUS authentication server. delete Remove a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius auth delete 1

**Related Commands** show radius auth statistics

### config radius auth disable

To disable a RADIUS authentication server for the Alcatel OmniAccess Switch or Appliance, use the config radius auth disable command.

>config radius auth disable <index>

**Syntax** config Configure parameters.

radius auth RADIUS authentication server. disable Disable a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius auth disable 1

**Related Commands** show radius auth statistics

## config radius auth enable

To enable a RADIUS authentication server for the Alcatel OmniAccess Switch or Appliance, use the config radius auth enable command.

>config radius acct enable <index>

**Syntax** config Configure parameters.

radius auth RADIUS authentication server. enable Enable a RADIUS server.

<index> Priority index.

**Defaults** (none)

Examples >config radius auth enable 1

**Related Commands** show radius auth statistics

# config rogue ap

To configure the status of a roque access point, use the config roque ap command.

>config rogue ap <acknowledged/alert/contain/known> <MAC address> <num of APs>

**Syntax** config Configure parameters.

rogue ap Rogue AP status.

acknowledged This AP has been identified and belongs to an

external network.

alert This AP has not been identified. Generates a trap

upon detection of this access point.

contain Start containing a rogue access point.

known This AP has been identified and is part of an internal

network

<MAC address> MAC address of the AP

<num of APs> Number of APs

**Defaults** (none)

Example >config rogue ap acknowledge 11:11:11:11:11:11

**Related Commands** show rogue ap summary, show rogue ap detailed

## config rogue client

To configure the status of a rogue clients, use the config rogue client command.

>config rogue client <alert/contain> <MAC address> <num of APs>

**Syntax** config Configure parameters.

rogue client Rogue client status.

alert This client has not been identified. Generates and

trap upon detection of this client.

contain Start containing a rogue client.

<MAC address> MAC address of the AP

<num of APs> Number of APs

**Defaults** (none)

Example >config rogue client acknowledge 11:11:11:11:11

**Related Commands** show rogue client summary, show rogue client detailed

### **CONFIG ROUTE COMMANDS**

Use the following config route commands:

- <u>config route add</u>
- config route delete

## config route add

To configure a network route, use the config route add command.

>config route add <IP address> <IP netmask> <gateway>

**Syntax** config Configure parameters.

route Network route. add Add a route.

<Network IP Address> Destination network IP Address range.

<IP netmask> Destination subnet mask.

<gateway> IP Address of the gateway router.

**Defaults** (none)

Examples >config route add 10.1.1.0 255.255.255.0 10.1.1.1

**Related Commands** show route all

## config route delete

To remove a network route, use the config route delete command.

>config route delete <network IP address>

**Syntax** config Configure parameters.

route Network route. delete Delete a route.

<Network IP Address> Destination network route.

**Defaults** (none)

Examples >config route delete 10.1.1.0 255.255.255.0 10.1.1.1

Related Commands show route all

#### **CONFIG SERIAL COMMANDS**

Use the following config serial commands:

- <u>config serial baudrate</u>
- <u>config serial timeout</u>

### config serial baudrate

To set the serial baud rate, use the config serial baudrate command.

>config serial [1200/2400/4800/9600/19200/38400/57600/115200]

**Syntax** config Configure parameters.

serial Serial connection settings

[1200/2400/4800/9600/ Connection speed

19200/38400/57600/

115200]

Defaults 9600

Examples >config serial baudrate 9600

**Related Commands** config serial timeout

## config serial timeout

To set the timeout of a serial session, use the config serial timeout command.

Use this command to set the timeout for a serial connection to the front of the Alcatel OmniAccess Switch or Appliance from 0 to 160 minutes where 0 is no timeout.

#### >config serial timeout <minutes>

**Syntax** config Configure parameters.

serial Serial connection settings. timeout Connection duration. <minutes> Timeout in minutes.

**Defaults** 0 (no timeout)

Examples >config serial timeout 10

Related Commands config serial timeout

### **CONFIG SESSIONS COMMANDS**

Use the following config sessions commands:

- config sessions maxsessions
- <u>config sessions timeout</u>

## config sessions maxsessions

To configure the number of telnet CLI sessions allowed by the Alcatel OmniAccess Switch or Appliance, use the config sessions maxsessions command. Up to five sessions are possible while a setting of zero prohibits any telnet CLI sessions.

### >config sessions maxsessions <0-5>

**Syntax** config Configure parameters.

sessions Telnet CLI session parameters.
maxsessions Number of allowed CLI sessions.
<0-5> Number of sessions from 0 to 5.

Defaults 5

Examples >config sessions maxsessions 2

**Related Commands** show sessions

# config sessions timeout

To configure the inactivity timeout for telnet CLI sessions, use the config sessions timeout command.

>config sessions timeout <0-160>

**Syntax** config Configure parameters.

sessions Telnet CLI session parameters.

timeout Duration of CLI sessions.

<0-160> Timeout of telnet session in minutes

Defaults 5

Examples >config sessions timeout 20

**Related Commands** show sessions

#### **CONFIG SNMP COMMUNITY COMMANDS**

Use the following config snmp community commands:

- config snmp community accessmode
- config snmp community create
- config snmp community delete
- config snmp community ipaddr
- <u>config snmp community mode</u>

# config snmp community accessmode

To modify the access mode (Read only or Read/Write) of an SNMP community, use the config snmp community accessmode command.

>config snmp community accessmode [ro/rw] <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.

community SNMP community parameters.

accessmode Access privileges.

ro/rw Read only or Read/Write.

<name> Community name.

**Defaults** Two communities are provided by default with the following parameters:

SNMP Community Name Client IP Address Client IP Mask Access Mode Status ----public 0.0.0.0 0.0.0.0 Read Only Enable private 0.0.0.0 0.0.0.0 Read/Write Enable

**Examples** >config snmp community accessmode rw private

**Related Commands** show snmp community, config snmp community mode, config snmp community

create, config snmp community delete, config snmp community ipaddr

# config snmp community create

To create a new SNMP community, use the config snmp community create command. Use this command to create a new community with the following default configuration:

name 0.0.0.0 0.0.0.0 Read Only Disable

>config snmp community create <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.

community SNMP community parameters. create Create a new community.

<name> Community name.

**Defaults** (none)

Examples >config snmp community create test

**Related Commands** show snmp community, config snmp community mode, config snmp community

accessmode, config snmp community delete, config snmp community ipaddr

## config snmp community delete

To delete an SNMP community, use the config snmp community delete command.

>config snmp community create <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.

community SNMP community parameters. delete Delete a new community.

<name> Community name.

Defaults N/A

Examples >config snmp community delete test

**Related Commands** show snmp community, config snmp community mode, config snmp community

accessmode, config snmp community create, config snmp community ipaddr

#### config snmp community ipaddr

To modify the IP Address of an SNMP community, use the config snmp community ipaddr command.

>config snmp community ipaddr <ipaddr> <ipmask> <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.

community SNMP community parameters. ipaddr Set IP Address parameters.

**Defaults** (none)

Examples >config snmp community ipaddr 10.10.10.2 255.255.255.0 public

**Related Commands** show snmp community, config snmp community mode, config snmp community

accessmode, config snmp community create, config snmp community delete,

config snmp community ipaddr

# config snmp community mode

To enable or disable an SNMP community, use the config snmp community mode command.

>config snmp community mode <enable/disable> <name>

**Syntax** config snmp community Configure SNMP community parameters.

mode Change the state.

<enable/disable> Enable or disable the community.

<name> Community name.

**Defaults** None.

Examples >config snmp community mode disable public

**Related Commands** show snmp community, config snmp community accessmode, config snmp

community create, config snmp community delete, config snmp community

ipaddr

## config snmp syscontact

To set the SNMP system contact name, use the config snmp syscontact command.

>config snmp syscontact <contact>

**Syntax** config Configure parameters.

snmp SNMP parameters. syscontact System contact.

<contact> Name (Up to 31 alphanumeric characters).

**Defaults** (none)

Examples >config snmp syscontact Alcatel\_administrator

Related Commands show snmpcommunity

#### config snmp syslocation

To set the SNMP system location name, use the config snmp syslocation command.

>config snmp syslocation <location>

**Syntax** config Configure parameters.

snmp SNMP parameters. syslocation System location.

<location> Name (Up to 31 alphanumeric characters).

**Defaults** (none)

Examples >config snmp syslocation Building\_2a

**Related Commands** show snmpcommunity

### **CONFIG SNMP TRAPRECEIVER COMMANDS**

Use the following config snmp trapreceiver commands:

- <u>config snmp trapreceiver create</u>
- config snmp trapreceiver delete

<u>config snmp trapreceiver mode</u>

### config snmp trapreceiver create

To add server to receive a SNMP traps, use the config snmp trapreceiver create command. The IP Address must be valid for the command to add the new server.

#### >config snmp trapreceiver create <name> <ipaddr>

**Syntax** config Configure parameters. snmp SNMP parameters.

trapreceiver SNMP trap server parameters.

create Create a new server.
<name> Server name.

<name> Server name.
<ipaddr> Server IP Address.

**Defaults** (none)

Examples >config snmp trapreceiver create test 10.1.1.1

**Related Commands** show snmp trap

### config snmp trapreceiver delete

To delete a server from the trap receiver list, use the config snmp trapreceiver delete command.

#### >config snmp trapreceiver delete <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.
trapreceiver Server to receive traps.
delete Remove a server.
<name> Server name

**Defaults** (none)

Examples >config snmp trapreceiver delete test

**Related Commands** show snmp trap

#### config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the config snmp trapreceiver mode command. This enables or disables the Alcatel OmniAccess Switch or Appliance from sending the traps to the selected server.

#### >config snmp trapreceiver mode <enable/disable> <name>

**Syntax** config Configure parameters.

snmp SNMP parameters.
trapreceiver Server to receive traps.
mode Change the state.
<enable/disable> Enable or disable.
<name> Server name.

**Defaults** (none)

Examples >config snmp trapreceiver mode disable server1

**Related Commands** show snmp trap

#### **CONFIG SNMP V3USER COMMANDS**

Use the following config snmp v3user commands:

- <u>config snmp v3user create</u>
- config snmp v3user delete

#### config snmp v3user create

To add a version 3 SNMP user, use the config snmp v3user create command.

>config snmp v3user <username> [rw/ro] [none/hmacmd5/hmacsha] [none/des]
<authkey> <encrypkey>

**Syntax** config Configure parameters.

snmp SNMP parameters. v3user Version 3 SNMP. <username> New user name.

[rw/ro] Read/write or read/only user privileges

[none/hmacmd5/hmacsha]Authentication protocol [none/des] Encryption protocol

<authkey> Authentication key, if enabled <encrypkey> Encryption key, if enabled

Defaults SNMP v3 User Name AccessMode Authentication Encryption

default Read/Write HMAC-MD5 CBC-DES

Examples >config snmp v3user test ro 3

to add an SNMP username test with read-only privileges and no encryption or

authentication.

**Related Commands** show snmp v3user

### config snmp v3user delete

To delete a version 3 SNMP user, use the config snmp v3user delete command.

>config snmp v3user delete <username>

**Syntax** config Configure parameters.

snmp SNMP parameters.
v3user Version 3 SNMP.
delete Remove user.
<username> Username to delete.

Defaults SNMP v3 User Name AccessMode Authentication Encryption

default Read/Write HMAC-MD5 CBC-DES

default Read/Write HMAC-MD5 CBC-DES

Examples >config snmp v3user delete test

This will remove an SNMP user named test.

**Related Commands** show snmp v3user

# config snmp version

To enable or disable selected SNMP versions, use the config snmp version command.

>config snmp version <v1/v2/v3> <enable/disable>

Syntax config Configure parameters.

snmp SNMP parameters. version Duration of CLI sessions.

<v1/v2/v3> SNMP version to enable or disable
<enable/disable> Enable or disable specified version

**Defaults** All versions enabled

Examples >config sessions timeout 20

**Related Commands** show snmpversion

#### **CONFIG SPANNINGTREE PORT COMMANDS**

Use the following config spanningtree port commands:

- config spanningtree port mode
- config spanningtree port pathcost
- config spanningtree port priority

# config spanningtree port mode

To turn fast or 802.1D Spanning Tree Protocol on or off for one or all Alcatel OmniAccess Switch or Appliance ports, use the config spanningtree port mode command.

Note that you must disable Alcatel OmniAccess Switch or Appliance STP using the config spanningtree switch mode command, select STP mode for all Ethernet ports using this command, and then enable Alcatel OmniAccess Switch or Appliance STP using the config spanningtree switch mode command. This procedure allows the Alcatel OmniAccess Switch or Appliance to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

#### >config spanningtree port mode [off/802.1d/fast] [<port>/all]

**Syntax** config Configure parameters.

spanningtree Spanning Tree Protocol.

port Alcatel OmniAccess Switch or Appliance Ethernet

port.

mode STP mode.

[off/802.1d/fast] STP off/802.1D/fast.

[<port>/all] Port 1 through 12 or 1 through 24, or all ports.

**Defaults** Port STP = off.

Examples >config spanningtree port mode off all

to disable STP for all Ethernet ports.

>config spanningtree port mode 802.1d 24 to turn on STP 802.1D mode for Ethernet port 24.

>config spanningtree port mode fast 2 to turn on fast STP mode for Ethernet port 2.

**Related Commands** show spanningtree port, config spanningtree switch mode, config spanningtree

port pathcost, config spanningtree port priority

## config spanningtree port pathcost

To set the STP path cost for an Ethernet port, use the config spanningtree port pathcost command.

>config spanningtree port pathcost [1-65535/auto] [<port>/all]

**Syntax** config Configure parameters.

spanning Tree Protocol.

port Alcatel OmniAccess Switch or Appliance Ethernet

port.

pathcost STP path cost.

[1-65535/auto] Port pathcost, as determined by the network

planner, or auto (default)

[<port>/all] Port 1 through 12 or 1 through 24, or all ports.

**Defaults** Pathcost = Automatic.

**Examples** >config spanningtree port pathcost auto all

to have the STP algorithm automatically assign a path cost for all ports.

>config spanningtree port pathcost 200 22

to have the STP algorithm use a port cost of 200 for port 22.

**Related Commands** show spanningtree port, config spanningtree port mode, config spanningtree

port priority

#### config spanningtree port priority

To configure the STP port priority, use the >config spanningtree port priority command.

>config spanningtree port priority [0-255] <port>

**Syntax** config Configure parameters.

spanning Tree Protocol.

port Alcatel OmniAccess Switch or Appliance Ethernet

port.

priority [0-255] STP priority, 0 through 255.

<port> Port 1 through 12 or 1 through 24.

**Defaults** STP Priority = 128.

Examples >config spanningtree port priority 100 2

to set Ethernet port 2 to STP priority 100.

**Related Commands** show spanningtree port, config spanningtree switch mode, config spanningtree

port mode, config spanningtree port pathcost

#### **CONFIG SPANNINGTREE SWITCH COMMANDS**

Use the following config spanningtree switch commands:

- config spanningtree switch bridgepriority
- config spanningtree switch forwarddelay
- <u>config spanningtree switch hellotime</u>

- <u>config spanningtree switch maxage</u>
- <u>config spanningtree switch mode</u>

## config spanningtree switch bridgepriority

To set the bridge ID, use the config spanningtree switch bridgepriority command. The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535.

#### >config spanningtree switch bridgepriority [0-65535]

Syntax config Configure parameters.

spanningtree Spanning Tree Protocol. switch Alcatel OmniAccess Switch or Appliance.

bridgepriority Bridge ID.

[0-65535] Decimal number range.

**Defaults** The factory default is 32768.

Examples >config spanningtree switch bridgepriority 40230

**Related Commands** show spanningtree switch, config spanningtree switch forwarddelay, config

spanningtree switch hellotime, config spanningtree switch maxage, config

spanningtree switch mode

## config spanningtree switch forwarddelay

To set the bridge timeout, use the config spanningtree switch forwarddelay command.

The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. The Factory default is 15. Valid values are 4 through 30 seconds.

#### >config spanningtree switch forwarddelay [4-30]

Syntax config Configure parameters.

spanningtree Spanning Tree Protocol.

switch Alcatel OmniAccess Switch or Appliance.

forwarddelay Forward delay setting. [4-30] Range in seconds.

**Defaults** The factory default is 15.

Examples >config spanningtree switch forwarddelay 20

**Related Commands** show spanningtree switch, config spanningtree switch bridgepriority, config

spanningtree switch hellotime, config spanningtree switch maxage, config

spanningtree switch mode

#### config spanningtree switch hellotime

To set the hello time, use the config spanningtree switch hellotime command.

This is the value all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be 1 second. Valid values are 1 through 10 seconds.

#### >config spanningtree switch hellotime [1 -10]

**Syntax** config Configure parameters.

spanningtree Spanning Tree Protocol.

switch Alcatel OmniAccess Switch or Appliance.

hellotime Hello time setting. [1-10] Range in seconds.

**Defaults** The factory default is 15.

Examples >config spanningtree switch hellotime 4

**Related Commands** show spanningtree switch, spanningtree switch bridgepriority, config span-

ningtree switch forwarddelay, config spanningtree switch maxage, config

spanningtree switch mode

## config spanningtree switch maxage

To set the maximum age, use the config spanningtree switch maxage command.

This is the value all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 4 through 30 seconds.

#### >config spanningtree switch maxage [4-30]

**Syntax** config Configure parameters.

spanning Tree Protocol.

switch Alcatel OmniAccess Switch or Appliance.

maxage Forward delay setting. [4-30] Range in seconds.

**Defaults** The factory default is 20.

Examples >config spanningtree switch maxage 30

**Related Commands** show spanningtree switch, config spanningtree switch bridgepriority, config

spanningtree switch forwarddelay, config spanningtree switch hellotime, config

spanningtree switch mode

#### config spanningtree switch mode

To turn Alcatel OmniAccess Switch or Appliance Spanning Tree Protocol on or off, use the config spanningtree switch mode command.

Note that you must disable the Alcatel OmniAccess Switch or Appliance STP using this command, select STP mode for all Ethernet ports using the config spanningtree port mode command, and then enable the Alcatel OmniAccess Switch or Appliance STP using this command. This procedure allows the Alcatel OmniAccess Switch or Appliance to most efficiently set up STP, detect logical network loops, place redundant ports on standby, and build a network with the most efficient pathways.

#### >config spanningtree switch mode [enable/disable]

**Syntax** config Configure parameters.

spanning Tree Protocol.

switch Alcatel OmniAccess Switch or Appliance.

mode STP mode. [enable/disable] Turn on/off.

**Defaults** STP = Disabled.

Examples >config spanningtree switch mode enable

to support STP on all Alcatel OmniAccess Switch or Appliance Ports.

**Related Commands** show spanningtree switch, config spanningtree switch bridgepriority, config

spanningtree switch forwarddelay, config spanningtree switch hellotime, config

spanningtree switch maxage, config spanningtree port mode

### **CONFIG SWITCHCONFIG COMMANDS**

Use the following config switchconfig commands:

- config switchconfig flowcontrol
- config switchconfig mode

# config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the config switchconfig flowcontrol command.

>config switchconfig flowcontrol [enable/disable]

**Syntax** config Configure parameters.

switchconfig Alcatel OmniAccess Switch or Appliance parameters.

flowcontrol Flow control. [enable/disable] Turn on/off.

**Defaults** Disabled

Examples >config switchconfig flowcontrol enable

Related Commands show switchconfig

### config switchconfig mode

To configure LWAPP transport mode for Layer 2 or Layer 3, use the config switchconfig flowcontrol command.

>config switchconfig mode [L2/L3]

**Syntax** config Configure parameters.

switchconfig Alcatel OmniAccess Switch or Appliance parameters.

mode [L2/L3] Layer 2 or Layer 3 mode.

**Defaults** L3

Examples >config switchconfig mode L3

Related Commands show switchconfig

### config syslog

To send or disable sending system logs, use the config syslog command.

>config syslog [<ipaddr>/disable]

**Syntax** config Configure parameters.

syslog System logs.

<ipaddr> Specify an IP Address to send logs.

disable Disable logs

**Defaults** Disable

Examples >config syslog 10.1.1.1

Sending logs to 10.1.1.1

>config syslog disable

Syslog disabled.

Related Commands show syslog

## config sysname

To set the Alcatel OmniAccess Switch or Appliance system name, use the config sysname command.

>config sysname <name>

**Syntax** config Configure parameters.

sysname Alcatel OmniAccess Switch or Appliance name. <name> Name (Up to 31 alphanumeric characters).

**Defaults** (none)

Examples >config sysname Ent\_01

Related Commands show sysinfo

### config time

To set the system time, use the config time command.

>config time MM/DD/YYYY HH:MM:SS

**Syntax** config Configure parameters.

time Alcatel OmniAccess Switch or Appliance time.

**Defaults** (none)

Examples >config time 02/11/2003 15:29:00

Related Commands show time

# **CONFIG TRAPFLAGS COMMANDS**

Use the following config trapflags commands:

- <u>config trapflags aaa</u>
- <u>config trapflags ap</u>
- <u>config trapflags authentication</u>
- <u>config trapflags client</u>
- config trapflags configsave
- <u>config trapflags ipsec</u>
- config trapflags linkmode

- <u>config trapflags multiusers</u>
- <u>config trapflags roqueap</u>
- config trapflags rrm-params
- config trapflags rrm-profile
- config trapflags stpmode

### config trapflags aaa

To enable or disable sending AAA server related traps, use the config trapflags aaa command.

>config trapflags aaa [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. aaa AAA traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags aaa disable

**Related Commands** show trapflags

### config trapflags ap

To enable or disable sending OmniAccess AP related traps, use the config trapflags ap command.

>config trapflags ap [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters.

ap OmniAccess AP traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags ap disable

**Related Commands** show trapflags

## config trapflags authentication

To enable or disable sending traps on invalid SNMP access, use the config trapflags authentication command.

>config trapflags authentication [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters.

authentication Authentication of SNMP access.
[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags authentication disable

Related Commands show trapflags

## config trapflags client

To enable or disable sending client related DOT11 traps, use the config trapflags client command.

>config trapflags client [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. client DOT11 traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Disabled

Examples >config trapflags client disable

**Related Commands** show trapflags

## config trapflags configsave

To enable or disable sending configuration saved trap, use the config trapflags configsave command.

>config trapflags configsave [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters.

configsave Saved configuration trap flag.
[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags configsave disable

**Related Commands** show trapflags

#### config trapflags ipsec

To enable or disable sending IPSec traps, use the config trapflags ipsec command.

>config trapflags ipsec [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. ipsec IPSec trap flags.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags ipsec disable

**Related Commands** show trapflags

#### config trapflags linkmode

To enable or disable Alcatel OmniAccess Switch or Appliance level Link Up/Down trap flag, use the config trapflags linkmode command.

>config trapflags linkmode [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. linkmode Link status flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags linkmode disable

**Related Commands** show trapflags

# config trapflags multiusers

To enable or disable sending traps when multiple logins active, use the config trapflags multiusers command.

>config trapflags multiusers [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. multiusers Multiple user flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags multiusers disable

**Related Commands** show trapflags

#### config trapflags roqueap

To enable or disable sending roque AP detection traps, use the config trapflags roqueap command.

>config trapflags rogueap [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters.

rogueap Rogue AP detection trap flag. [enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags rogueap disable

**Related Commands** show trapflags

#### config trapflags rrm-params

To enable or disable sending RRM profile related traps, use the config trapflags rrm-params command.

>config trapflags rrm-params [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters.

rrm-params RRM parameters traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags rrm-params disable

**Related Commands** show trapflags

## config trapflags rrm-profile

To enable or disable sending RRM profile related traps, use the config trapflags rrm-profile command.

>config trapflags rrm-profile [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. rrm-profile RRM profile traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags rrm-profile disable

**Related Commands** show trapflags

### config trapflags stpmode

To enable or disable sending spanning tree traps, use the config trapflags stpmode command.

>config trapflags stpmode [enable/disable]

**Syntax** config Configure parameters.

trapflags Trap parameters. stpmode Spanning traps flag.

[enable/disable] Modify the state of the parameter.

**Defaults** Enabled

Examples >config trapflags stpmode disable

**Related Commands** show trapflags

#### **CONFIG WATCHLIST COMMANDS**

Use the following config watchlist commands?

- config watchlist add
- <u>config watchlist delete</u>
- config watchlist enable/disable

#### config watchlist add

To add a watchlist entry for a wireless LAN, use the config watchlist add command.

>config watchlist add [mac <MAC addr>/username <User Name>]

**Syntax** config watchlist Command action.

add Add a watchlist entry.
mac <MAC addr> MAC address of new entry.

username < User Name > User name.

**Defaults** None.

Examples >config watchlist add a5:6b:ac:10:01:6b Able1

Related Commands config watchlist delete, config watchlist enable/disable, show watchlist

# config watchlist delete

To delete a watchlist entry for a wireless LAN, use the config watchlist delete command.

>config watchlist delete [mac <MAC addr>/username <User Name>]

**Syntax** config watchlist Command action.

delete Delete a watchlist entry.
mac <MAC addr> MAC address of new entry.

username <User Name> User name.

**Defaults** None.

Examples >config watchlist delete a5:6b:ac:10:01:6b Able1

Related Commands config watchlist add, config watchlist enable/disable, show watchlist

#### config watchlist enable/disable

To delete a watchlist entry for a wireless LAN, use the config watchlist delete command.

>config watchlist enable/disable

**Syntax** config watchlist Command action.

enable/disable Enable or disable the client watchlist.

**Defaults** None.

Examples >config watchlist enable

>config watchlist disable

Related Commands config watchlist add, config watchlist delete, show watchlist

#### config wlan blacklist

To modify the disable (blacklist) timeout for a wireless LAN, use the config wlan blacklist command.

Set the timeout in seconds for an automatically disabled client. Client machines are disabled by MAC address. A timeout setting of 0 indicates that the client is permanently disabled and that administrative control is required to remove the client from the automatic disable.

#### >config wlan blacklist [<WLAN id>/foreignAp] <seconds>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

blacklist Disable parameter.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points. <seconds> Timeout in seconds.

**Defaults** Not enabled

Examples >config wlan blacklist foreignAp 2

Related Commands show blacklist

#### **CONFIG WLAN COMMANDS**

Use the following config wlan commands:

- <u>config wlan create</u>
- config wlan delete
- <u>config wlan dhcp\_server</u>
- <u>config wlan disable</u>
- <u>config wlan enable</u>
- <u>config wlan mac-filtering</u>
- config wlan gos
- <u>config wlan radio</u>

# config wlan create

To create a wireless LAN, use the config wlan create command.

>config wlan create <WLAN id> [<SSID>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

create Add a WLAN.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan create 1 SSID01

**Related Commands** show trapflags

#### config wlan delete

To delete a wireless LAN, use the config wlan delete command.

>config wlan delete [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

delete Remove a WLAN.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan delete foreignAp

Related Commands show wlan, show wlan summary

#### config wlan dhcp server

To configure the DHCP server for a wireless LAN, use the config wlan dhcp\_server command.

>config wlan dhcp\_server [<WLAN id>/foreignAp] <ipaddr>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters. dhcp\_server Configure DHCP server.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.
<ipaddr> IP Address of the DHCP server

**Defaults** (none)

Examples >config wlan dhcp\_server foreignAp 10.10.2.1

Related Commands show wlan

# config wlan disable

To disable a wireless LAN, use the config wlan disable command.

>config wlan disable [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters. disable Change state of WLAN.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan disable foreignAp

Related Commands show wlan

## config wlan enable

To enable a wireless LAN, use the config wlan enable command.

>config wlan enable [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters. enable Change state of WLAN.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan enable foreignAp

**Related Commands** show wlan

#### config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the config wlan mac-filtering command.

>config wlan mac-filtering [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

mac-filtering MAC filtering feature. enable/disable Change state command.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan mac-filtering enable 1

Related Commands show wlan

# config wlan qos

To change the quality of service for a wireless LAN, use the config wlan gos command.

>config wlan qos [<WLAN id>/foreignAp] [bronze/silver/gold]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

qos Quality of service.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

bronze/silver/gold Grades of service

**Defaults** (none)

**Examples** To set the highest level of service on WLAN 1, use the following command:

>config wlan qos 1 gold

To set a lower level of service for third-party APs, use the following command:

>config wlan qos foreignAp bronze

Related Commands show wlan

#### config wlan radio

To the set the OmniAccess Radio policy on a wireless LAN, use the config wlan radio command. Set the WLAN policy to apply to 802.11a, 802.11g, 802.11b, 802.11a/g, 802.11b/g, or All = 802.11a/b/g OmniAccess Radios.

#### >config wlan radio <WLAN id> [all/802.11a/802.11bg/802.11g/802.11ag]

Syntax	config wlan radio <wlan id=""> 802.11a 802.11bg</wlan>	Configure parameters. Wireless LAN parameters. OmniAccess Radio policy. WLAN identifier between 1 and 16. Only 802.11a supported, when 802.11a is enabled. Only 802.11b supported, when 802.11b is enabled
	802.11g all	and 802.11g support is disabled. Only 802.11g supported, when 802.11b and 802.11g support are enabled. Only 802.11a/b supported, when 802.11a and
	802.11bg	802.11b are enabled and 802.11g support is disabled. Only 802.11b/g supported, when 802.11b and 802.11g support are enabled.

802.11ag Only 802.11a/g supported, when 802.11a, 802.11b

and 802.11g support are enabled.

all 802.11a/b/g supported, when 802.11a, 802.11b and

802.11g support are enabled.

**Defaults** (none)

Examples >config wlan radio 1 all

Related Commands config 802.11a enable, config 802.11a disable, config 802.11b enable, config

802.11b disable, config 802.11b 11gSupport enable, config 802.11b

11gSupport disable, show wlan

# **CONFIG WLAN SECURITY COMMANDS**

Use the following wlan security commands:

- config wlan security 802.1X
- <u>config wlan security 802.1X encryption</u>
- config wlan security cranite
- config wlan security ipsec
- <u>config wlan security ipsec authentication</u>
- config wlan security ipsec encryption
- config wlan security ipsec ike authentication
- config wlan security ipsec ike DH-Group
- <u>config wlan security ipsec ike lifetime</u>
- config wlan security ipsec ike phase1
- <u>config wlan security passthru</u>
- config wlan security static-wep-key
- config wlan security static-wep-key encryption
- <u>config wlan security web</u>
- config wlan security web passthru
- config wlan security wpa
- <u>config wlan security wpa encryption</u>

#### config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN OmniAccess Radios, use the config wlan security 802.1X command.

>config wlan security 802.1X [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. 802.1X 802.1X security.

enable/disable Change state command.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan security 802.1X enable foreignAp

Related Commands show wlan

## config wlan security 802.1X encryption

To change the state of 802.1X security on the wireless LAN OmniAccess Radios, use the config wlan security 802.1X encryption command.

Use to change the encryption level of 802.1X security on the WLAN OmniAccess Radios to:

- 40/64 bit key

- 104/128 bit key

- 128/152 bit key

>config wlan security 802.1X <WLAN id> [40/104/128]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. 802.1X 802.1X security.

<WLAN id> WLAN identifier between 1 and 16.

[40/104/128] Encryption level.

**Defaults** None.

Examples >config wlan security 802.1X encryption 01 40

Related Commands show wlan

#### config wlan security cranite

To change the state of the Cranite passthrough, use the config wlan security cranite command.

>config wlan security cranite [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
cranite Cranite passthrough.
enable/disable Change state command.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** (none)

Examples >config wlan security cranite enable foreignAp

**Related Commands** show wlan

#### config wlan security ipsec

To change the state of the IPSec security, use the config wlan security ipsec command.

>config wlan security ipsec [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
ipsec IPSec parameters.
enable/disable Change state command.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

Defaults N/A

Examples >config wlan security IPSec enable foreignAp

Related Commands show wlan

## config wlan security ipsec authentication

To modify the IPSec security authentication protocol used on the wireless LAN, use the config wlan security ipsec authentication command.

Use to change the authentication protocol for IPSec to:

hmac-md5
 hmac-sha-1
 Enables IPSec HMAC-MD5 authentication.
 Enables IPSec HMAC-SHA-1 authentication.

none Disables IPSec authentication.

>config wlan security ipsec authentication [hmac-md5/hmac-sha-1/none] [<WLAN
id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. ipsec IPSec security.

authentication Authentication parameter. [hmac-md5/hmac- Authentication protocol.

sha-1/none]

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

Defaults N/A

Examples >config wlan security ipsec authentication hmac-sha-1 1

Related Commands show wlan

#### config wlan security ipsec encryption

To modify the IPSec security encryption protocol used on the wireless LAN, use the config wlan security ipsec encryption command.

>config wlan security ipsec encryption [3des/aes/des/none] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
ipsec IPSec security.
encryption Encryption parameter.
[3des/aes/des/none] Encryption protocol.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

Defaults N/A

Examples >config wlan security ipsec encryption aes 1

**Related Commands** show wlan

#### config wlan security ipsec ike authentication

To modify the IPSec ike authentication protocol used on the wireless LAN, use the config wlan security ipsec ike authentication command.

>config wlan security ipsec ike authentication <certificates/pre-share-key/
xauth-psk> [<WLAN id>/foreignAp] [<key>]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. ipsec IPSec security. ike IKE protocol.

authentication Authentication parameter.

certificates Certificate authentication (no key required).

pre-share-key Pre-shared key xauth-psk XAuth pre-shared key.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

<key> Key required for pre-share and xauth-psk.

Defaults N/A

Examples >config wlan security ipsec ike authentication certificates

 ${\tt foreignAp}$ 

Related Commands show wlan

# config wlan security ipsec ike dh-group

To modify the IPSec IKE Diffie Hellman group used on the wireless LAN, use the config wlan security ipsec ike authentication command.

>config wlan security ipsec ike dh-group [<WLAN id>/foreignAp] <group-id>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. ipsec IPSec security. ike IKE protocol.

dh-group Diffie Hellman group parameter. <WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

<group-id> Group 1, 2 or 5

Defaults N/A

Examples >config wlan security ipsec ike dh-group 1 1

Related Commands show wlan

## config wlan security ipsec ike lifetime

To modify the IPSec IKE timeout used on the wireless LAN, use the config wlan security ipsec ike lifetime command.

>config wlan security ipsec ike lifetime [<WLAN id>/foreignAp] <group-id>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
ipsec IPSec security.
ike IKE protocol.
lifetime IKE timeout.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points. <seconds> Timeout in seconds

Defaults N/A

Examples >config wlan security ipsec ike lifetime 1 10

**Related Commands** show wlan

# config wlan security ipsec ike phase1

To modify IPSec IKE Phase 1 used on the wireless LAN, use the config wlan security ipsec ike phase1 command.

>config wlan security ipsec ike phasel [aggressive/main] [<WLAN id>/
foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
ipsec IPSec security.
ike IKE protocol.
phase1 Phase 1 command.
[aggressive/main] Phase 1 setting.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

Defaults N/A

Examples >config wlan security ipsec ike phasel aggressive foreignAp

**Related Commands** show wlan

# config wlan security passthru

To modify IPSec IKE Phase 1 used on the wireless LAN, use the config wlan security passthru command.

Use this command to enable Layer 3 passthrough. When you select Layer 3 VPN Pass Through, fill in the VPN Gateway IPSec Pass Through Address. With VPN Pass Through, but not with IPSec, you may also enable Web Authentication, also known as Web Auth

>config wlan security passthru [enable/disable] [<WLAN id>/foreignAp]
[gateway]

Syntax config Configure parameters.

wlan Wireless LAN parameters.

security Security policy. passthru VPN passthrough.

enable/disable Modify passthrough status.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points. gateway VPN gateway IP Address.

Defaults N/A

Examples >config wlan security passthru enable 1 10.10.2.1

Related Commands show wlan

## config wlan security static-wep-key

To change the status of static WEP key authentication, use the config wlan security static-wep-key command.

>config wlan security static-wep-key [enable/disable] <WLAN id>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.

static-wep-key Static WEP key authentication.

enable/disable Modify status.

<WLAN id> WLAN identifier between 1 and 16.

Defaults N/A

Examples >config wlan security static-wep-key enable 1

Related Commands config wlan security wpa encryption

#### config wlan security static-wep-key encryption

To change the status of static WEP key authentication, use the config wlan security static-wep-key encryption command.

Use to enable or disable static wep key authentication. Static WEP encryption parameters:

- Key sizes: 40/64, 104/128 and 128/152 bit key sizes
- Key Index: 1 to 4 (Note 2)
- Enter encryption key
- Select encryption key format in ASCII or HEX

One unique WEP Key Index can be applied to each WLAN. As there are only four WEP Key Indexes, only four WLANs can be configured for Static WEP Layer 2 encryption.

>config wlan security static-wep-key encryption <WLAN id> [40/104/128] [hex/ascii] <key> <key-index>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.

static-wep-key Static WEP key authentication.

encryption Encryption setting.

<WLAN id> WLAN identifier between 1 and 16.

[40/104/128] Encryption level.
hex/ascii Key format
<key> Hex or ASCII key
<key-index> Key index (see below)

Defaults N/A

Examples >config wlan security wpa encryption 1 40 hex 0201702001 2

Related Commands show wlan

## config wlan security web

To change the status of Web authentication used on the wireless LAN, use the config wlan security web command.

>config wlan security web [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
web Web authentication.
enable/disable Modify status.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

Defaults N/A

Examples >config wlan security web enable

Related Commands show wlan

#### config wlan security web passthru

To change the status of Web authentication using Microsoft NETBIOS configuration, use the config wlan security web passthru command.

>config wlan security web passthru [enable/disable] [<WLAN id>/foreignAp]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
web Web authentication.
passthru NetBIOs passthrough.

enable/disable Modify status.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

**Defaults** N/A

Examples >config wlan security web passthru enable 1

Related Commands show wlan

# config wlan security wpa

To change the status of WPA authentication, use the config wlan security wpa command.

>config wlan security wpa [enable/disable] <WLAN id>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
wpa WPA authentication.
enable/disable Modify status.

<WLAN id> WLAN identifier between 1 and 16.

Defaults N/A

Examples >config wlan security wpa enable 1

Related Commands show wlan

# config wlan security wpa encryption

To change the encryption of WPA authentication, use the config wlan security wpa encryption command.

Use to enable or disable WPA authentication. Wi-Fi Protected Access 802.11 data encryption types:

- TKIP-MIC

- WEP: 40/64, 104/128, and 128/152 bit key sizes

>config wlan security wpa encryption [aes-ocb/wep/tkip] <WLAN id> [40/104/ 128]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

security Security policy.
wpa WPA authentication.
encryption Encryption setting.
aes-ocb/wep/tkip Type of encryption.

<WLAN id> WLAN identifier between 1 and 16.

[40/104/128] Encryption level.

Defaults N/A

Examples >config wlan security wpa encryption tkip 1 40

Related Commands show wlan

### config wlan timeout

To change the timeout of WLAN clients, use the config wlan timeout command.

>config wlan timeout [<WLAN id>/foreignAp] <seconds>

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

timeout Client timeout.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points. <seconds> Timeout in seconds.

Defaults N/A

Examples >config wlan timeout 1 6000

Related Commands show wlan

## config wlan vlan

To add a Virtual LAN, use the config wlan vlan command.

>config wlan vlan [<WLAN id>/foreignAp] [<VLAN id/untagged> [<IP Address>
<Netmask> <Gateway>]/default]

**Syntax** config Configure parameters.

wlan Wireless LAN parameters.

vlan Virtual LAN.

<WLAN id> WLAN identifier between 1 and 16.

foreignAp Third-party access points.

<VLAN id/untagged> VLAN ID or untagged

<IP Address> <Netmask>If untagged, enter the IP Address, netmask and

<Gateway> gateway

Defaults N/A

Examples >config wlan vlan 1 untagged default

Related Commands show wlan

#### **CONFIG WPS COMMANDS**

Use the following config wps commands:

- <u>config wps contain-adhoc</u>
- config wps dot11
- config wps deny-invalid-ap
- config wps encryption
- config wps invalid-ssid
- config wps misconfigured-ap
- config wps missing-ap
- <u>config wps preamble</u>
- <u>config wps radio</u>
- <u>config wps rldp</u>

#### config wps contain-adhoc

To configure the auto-contain ad-hoc feature, use the config wps contain adhoc command.

>config wps contain-adhoc <disable/enable>

Alternate command:

>config rogue-ap ips contain-adhoc <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system. contain-adhoc Auto-contain ad-hoc feature.

<enable/disable> Enable or disable.

Defaults N/A

Examples >config rogue-ap ips contain-adhoc enable

**Related Commands** config wps dot11, config wps deny-invalid-ap, config wps encryption, config

wps invalid-ssid, config wps misconfigured-ap, config wps missing-ap, config

wps preamble, config wps radio, config wps rldp, show wps.

# config wps dot11

To configures the trusted AP 802.11 mode policy to be enforced, use the config wps dot11 command.

>config wps dot11 <dcf/none/pcf>

Alternate command:

>config rogue-ap ips dot11 <dcf/none/pcf>

**Syntax** config Configure parameters.

wps Wireless protection system.

dot11 802.11 mode

dcf Enforce DCF on trusted APs.

none Disable 802.11 mode policy enforcement.

pcf Enforce PCF on trusted APs.

Defaults N/A

**Examples** >config rogue-ap ips dot11 none

Related Commands config wps contain-adhoc, config wps deny-invalid-ap, config wps encryption,

config wps invalid-ssid, config wps misconfigured-ap, config wps missing-ap,

config wps preamble, config wps radio, config wps rldp, show wps.

# config wps deny-invalid-ap

To configure auto-contain of valid mobile units associating with rogue AP, use the config wps deny-invalid-ap command.

>config wps deny-invalid-ap <disable/enable>

Alternate command:

>config rogue-ap ips deny-invalid-ap <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system.

deny-invalid-ap Auto-contain valid mobile units associated with a

rogue AP.

<enable/disable> Enable or disable.

Defaults N/A

Examples >config rogue-ap ips deny-invalid-ap enable

#### **Related Commands**

config wps contain-adhoc, config wps dot11, config wps encryption, config wps invalid-ssid, config wps misconfigured-ap, config wps missing-ap, config wps preamble, config wps radio, config wps rldp, show wps.

#### config wps encryption

To configure the trusted AP encryption policy to be enforced, use the config wps encryption command.

>config wps encryption <open/none/wep/wpa>

Alternate command:

>config rogue-ap ips encryption <open/none/wep/wpa>

**Syntax** config Configure parameters.

wps Wireless protection system.

encryption AP encryption policy.

none Disable encryption policy enforcement.
open Enforce open mode on trusted APs.
wep Enforce WEP encryption on trusted APs.
wpa Enforce WPA encryption on trusted APs.

Defaults N/A

Examples >config wps encryption open

**Related Commands** config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps invalid-ssid, config wps misconfigured-ap, config wps missing-ap, config

wps preamble, config wps radio, config wps rldp, show wps.

## config wps invalid-ssid

To configure auto-contain of an invalid SSID on trusted AP, use the config wps invalid-ssid command.

>config wps invalid-ssid <disable/enable>

Alternate command:

>config rogue-ap ips invalid-ssid <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system.

invalid-ssid Invalid SSID. <enable/disable> Enable or disable.

Defaults N/A

**Examples** >config wps invalid-ssid enable

**Related Commands** config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps encryption, config wps misconfigured-ap, config wps missing-ap, config

wps preamble, config wps radio, config wps rldp, show wps.

#### config wps misconfigured-ap

To configure auto-contain of misconfigured trusted AP, use the config wps misconfigured-ap command.

>config wps misconfigured-ap <disable/enable>

Alternate command:

>config rogue-ap ips misconfigured-ap <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system.

misconfigured-ap Misconfigured AP. <enable/disable> Enable or disable.

Defaults N/A

Examples >config wps misconfigured-ap enable

Related Commands config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps encryption, config wps invalid-ssid, config wps missing-ap, config wps

preamble, config wps radio, config wps rldp, show wps.

# config wps missing-ap

To configure alert of a missing trusted AP, use the config wps missing-ap command.

>config wps missing-ap <disable/enable>

Alternate command:

>config rogue-ap ips missing-ap <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system.

missing-ap Missing AP.

<enable/disable> Enable or disable.

Defaults N/A

Examples >config wps missing-ap enable

Related Commands config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps encryption, config wps invalid-ssid, config wps misconfigured-ap, config

wps preamble, config wps radio, config wps rldp, show wps.

#### config wps preamble

To configure the trusted AP preamble policy to be enforced, use the config wps preamble command.

>config wps preamble <long/none/short>

Alternate command:

>config rogue-ap ips ips preamble <long/none/short>

**Syntax** config Configure parameters.

wps Wireless protection system.

preamble Preamble policy.

long Enforce long preamble on trusted APs.
none Disable preamble policy enforcement.
short Enforce short preamble on trusted APs.

Defaults N/A

Examples >config wps preamble short

#### **Related Commands**

config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config wps encryption, config wps invalid-ssid, config wps misconfigured-ap, config wps missing-ap, config wps radio, config wps rldp, show wps.

#### config wps radio

To configure the trusted AP OmniAccess Radio policy to be enforced., use the config wps radio command.

>config wps radio <802.11a/802.11b/802.11bg/none>

Alternate command:

>config rogue-ap ips radio <802.11a/802.11b/802.11bg/none>

**Syntax** config Configure parameters. wps Wireless protection system.

radio OmniAccess Radio policy.
802.11a Enforce 802.11a only on trusted APs.
802.11b Enforce 802.11b only on trusted APs.
802.11bg Enforce 802.11bg only on trusted APs.

none Disable OmniAccess Radio policy enforcement.

Defaults N/A

Examples >config wps radio 802.11a

**Related Commands** config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps encryption, config wps invalid-ssid, config wps misconfigured-ap, config

wps missing-ap, config wps preamble, config wps rldp, show wps.

#### config wps rldp

To configure Rogue Location Discovery Protocol, use the config wps rldp command.

>config wps rldp <disable/enable>

Alternate command:

>config rogue-ap ips rldp <disable/enable>

**Syntax** config Configure parameters.

wps Wireless protection system.

rldp Rogue Location Discovery Protocol.

<enable/disable> Enable or disable.

Defaults N/A

Examples >config wps rldp enable

**Related Commands** config wps contain-adhoc, config wps dot11, config wps deny-invalid-ap, config

wps encryption, config wps invalid-ssid, config wps misconfigured-ap, config

wps missing-ap, config wps preamble, config wps radio, show wps.

#### **CONFIG WPS-PEERS COMMANDS**

Use the following config wps-peers commands to configure the inter-Alcatel OmniAccess Switch and Appliance Mobility manager:

• <u>config wps-peers group member</u>

<u>config wps-peers secure-mode</u>

## config wps-peers group member

To configure the group members of the inter-Alcatel OmniAccess Switch and Appliance mobility manager, use the config wps-peers group member command.

Note: This command functions only when WPS has been installed.

>config wps-peers group member add/delete <MAC addr>

**Syntax** show Display configurations.

wps-peers Wireless Protection System Peer Management.

group The WPS peer group parameters

add/delete a WPS Peer group member to/from the

list.

MAC addr MAC address of the member to be added/deleted

**Defaults** (none)

Examples >config wps-peers group member add 00:0b:85:00:02:5

>config wps-peers group member delete 00:0b:85:00:02:5

Related Commands show wps, show wps-config, config wps, config wps-peers

# config wps-peers secure-mode

To configure the security of WPS peer messages between Alcatel OmniAccess Switches or Appliances, use the config wps-peers secure-mode command.

Note: This command functions only when WPS has been installed.

>config wps-peers secure-mode [enable/disable] <MAC addr>

**Syntax** show Display configurations.

wps-peers Wireless Protection System Peer Management.

secure-mode The WPS peer group parameters

OmniAccess Switches and Appliances.

**Defaults** (none)

Examples >config wps-peers secure-mode enable

**Related Commands** show wps, show wps-config, config wps, config wps-peers

# **Saving Configurations**

Use the save config command before you log out of the Command Line Interface to save all previous configuration changes.

save config

# save config

To save Alcatel OmniAccess Switch or Appliance configurations, use the save config command.

>save config

**Syntax** save Save

config Configuration changes.

**Defaults** (none)

Examples >save config

Are you sure you want to save? y/n

Y

Configuration Saved!

Related Commands show sysinfo

# **Clearing Configurations, Logfiles, and Other Actions**

To clear existing configurations, logfiles, and other functions, use the clear commands.

- clear ap-config
- clear arp
- <u>clear config</u>
- clear stats
  - clear stats port
  - clear stats switch
- <u>clear redirect-url</u>
- clear transfer
- clear traplog
- <u>clear webimage</u>
- <u>clear webmessage</u>
- clear webtitle

#### clear ap-config

To restore an OmniAccess AP configuration database to its factory default, use the clear ap-config command.

>clear ap-config <OmniAccess AP>

**Syntax** clear Clear.

ap-config OmniAccess AP configuration. <OmniAccess AP> Name of the OmniAccess AP.

Defaults N/A

Examples >clear ap-config aire1

Related Commands clear transfer, clear download filename, clear download mode, clear download

path, clear download serverip, clear download start, clear upload datatype, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

#### clear arp

To clear the ARP table to an OmniAccess AP its factory default, use the clear arp command.

>clear arp

Syntax clear arp Command action

Defaults N/A

Examples >clear arp

Are you sure you want to clear the ARP cache? (y/n)

Related Commands clear transfer, clear download filename, clear download mode, clear download

path, clear download serverip, clear download start, clear upload datatype,

clear upload filename, clear upload mode, clear upload path, clear upload serverip, clear upload start

## clear config

To remove the Alcatel OmniAccess Switch or Appliance configuration, use the clear config command.

>clear config

**Syntax** clear Clear.

config Alcatel OmniAccess Switch or Appliance

configuration.

Defaults N/A

Examples >clear config

Are you sure you want to clear the configuration? y/n

n

Configuration not cleared!

Related Commands clear transfer, clear download filename, clear download mode, clear download

path, clear download serverip, clear download start, clear upload datatype, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

#### clear stats port

To clear the statistics counters for a specific port, use the clear stats port command.

>clear stats port <port>

**Syntax** clear Clear.

stats Statistics counters.

port Port level.

<port> Alcatel OmniAccess Switch or Appliance port.

Defaults N/A

Examples >clear stats port 9

Are you sure you want to clear the port stats? y/n

У

Port stats cleared!

Related Commands clear transfer, clear download datatype, clear download filename, clear

download mode, clear download serverip, clear download start, clear upload datatype, clear upload filename, clear upload mode, clear upload path, clear

upload serverip, clear upload start

#### clear stats switch

To clear all statistics counters on the Alcatel OmniAccess Switch or Appliance, use the clear stats switch command.

>clear stats switch

Syntax clear Clear.

stats Statistics counters.

switch Alcatel OmniAccess Switch or Appliance.

Defaults N/A

Examples >clear stats switch

Are you sure you want to clear the switch stats? y/n

У

Switch stats cleared!

**Related Commands** clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download start, clear upload datatype, clear upload filename, clear upload mode, clear upload path, clear

upload serverip, clear upload start

#### clear redirect-url

To clear the custom Web Authentication Redirect URL on the Alcatel OmniAccess Switch or Appliance, use the clear redirect-url command.

>clear redirect-url

Syntax clear redirect-url Command action

Defaults N/A

Examples >clear redirect-url

URL cleared.

**Related Commands** clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download start, clear upload datatype, clear upload filename, clear upload mode, clear upload path, clear

upload serverip, clear upload start

#### clear transfer

To clear transfer information, use the clear transfer command.

>clear transfer

Syntax clear Clear.

transfer Transfer data

Defaults N/A

Examples >clear transfer

Are you sure you want to clear the transfer information? (y/n)

Y

Transfer Information Cleared!

**Related Commands** clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download serverip, clear upload datatype, clear download filename, clear download mode, clear download path,

clear download serverip, clear download start

# clear traplog

To clear traplog information, use the clear traplog command.

>clear traplog

**Syntax** clear Clear.

traplog Trap logs.

Defaults N/A

Examples >clear traplog

Are you sure you want to clear the trap log? (y/n)

У

Trap Log Cleared!

**Related Commands** clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download serverip, clear download start, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

# clear webimage

To clear the custom Web Authentication Image, use the clear webimage command.

>clear webimage

**Syntax** clear webimage Command action

Defaults N/A

Examples >clear webimage

Logo not installed.

**Related Commands** clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download serverip, clear download start, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

#### clear webmessage

To clear the custom Web Authentication Message, use the clear webmessage command.

>clear webmessage

**Syntax** clear webmessage Command action

Defaults N/A

Examples >clear webmessage

Message cleared.

Related Commands clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download serverip, clear download start, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

#### clear webtitle

To clear the custom Web Authentication Title, use the clear webtitle command.

>clear webtitle

Syntax clear webtitle Command action

Defaults N/A

Examples >clear webtitle

Title cleared.

Related Commands clear transfer, clear download datatype, clear download filename, clear

download mode, clear download path, clear download serverip, clear download start, clear upload filename, clear upload mode, clear upload path, clear upload

serverip, clear upload start

# **Uploading and Downloading Files and Configurations**

To transfer files to or from the Alcatel OmniAccess Switch or Appliance, use the transfer commands.

- transfer download
  - transfer download certpassword
  - transfer download datatype
  - <u>transfer download filename</u>
  - transfer download mode
  - <u>transfer download path</u>
  - <u>transfer download serverip</u>
  - <u>transfer download start</u>
  - <u>transfer download tftpPktTimeout</u>
  - transfer download tftpMaxRetries
- transfer upload
  - transfer upload datatype
  - <u>transfer upload filename</u>
  - transfer upload mode
  - <u>transfer upload path</u>
  - transfer upload serverip
  - transfer upload start

#### transfer download certpassword

To set a certificate's private password, use the transfer download certpassword command.

#### >transfer download certpassword [password]

**Syntax** transfer Move a file or configuration.

download Download operation to Alcatel OmniAccess Switch or

Appliance.

certpassword Certificate's private key password password Password or blank to clear password

Defaults N/A

Examples >transfer download certpassword

Clearing Password

**Related Commands** clear transfer, transfer download filename, transfer download mode, transfer

download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer

upload path, transfer upload serverip, transfer upload start

## transfer download datatype

To set the download data type, use the transfer download datatype command.

>transfer datatype [code/config/webauthcert/webadmincert]

**Syntax** transfer Move a file or configuration.

download Download operation to Alcatel OmniAccess Switch or

Appliance.

datatype Type of data.

code Alcatel OmniAccess Switch or Appliance code.

config Configuration file.

webauthcert Authentication certificate. webadmincert Administration certificate.

Defaults N/A

Examples >transfer datatype code

Related Commands clear transfer, transfer download filename, transfer download mode, transfer

download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start, transfer download

datatype image, transfer download start

#### transfer download filename

To download a specific file, use the transfer download filename command.

>transfer download filename <filename>

**Syntax** transfer Move a file

download Download operation to Alcatel OmniAccess Switch or

**Appliance** 

filename <filename> Enter filename up to 16 alphanumeric characters.

Defaults N/A

Examples >transfer download filename build603

**Related Commands** clear transfer, transfer download datatype, transfer download mode, transfer

download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer

upload path, transfer upload serverip, transfer upload start

#### transfer download mode

To download a specific file, use the transfer download mode command.

>transfer download mode <mode>

**Syntax** transfer Move a file.

download mode Download mode for <mode> Enter mode of tftp.

**Defaults** N/A

Example >transfer download mode tftp

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start

# transfer download path

To set a specific path, use the transfer download path command.

>transfer download filename <filename>

**Syntax** transfer Move a file

> download Download operation for path <path> Enter filename directory path.

**Defaults** N/A

Example >transfer download c:\install\version2

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

> transfer download mode, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start

#### transfer download serverip

To download a specific server, use the transfer download serverip command.

>transfer download serverip <ip addr>

**Syntax** transfer Move a file

> download Download operation for

serverip <IP addr> Enter IP address of the server.

**Defaults** N/A

**Examples** >transfer download serverip 175.34.56.78

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

> transfer download mode, transfer download path, transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start

#### transfer download start

To start a download transfer, use the transfer download start command.

>transfer download start

**Syntax** transfer Move a file

> download start Download start operation for

**Defaults** N/A

Example >transfer download start

> Mode..... TFTP Data Type..... Code TFTP Server IP...... 172.16.16.78

TFTP Packet Timeout..... 6

TFTP Filename..... wps\_2\_0\_75\_0.aes

This may take some time.

Are you sure you want to start? (y/n) n

Transfer Cancelled

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer upload datatype, transfer download filename, transfer download mode, transfer download path, transfer download serverip, transfer download start

#### transfer download tftpPktTimeout

To enter the tftp Packet Timeout in secs between 1 and 254, use the transfer download tftpPktTimeout command.

>transfer download tftpPktTimeout <time out>

**Syntax** transfer Move a file

download tftpPktTimeout The tftp Packet Timeout in secs between 1 and 254.

**Defaults** N/A

Example >transfer download tftpPktTimeout 55

Related Commands clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer upload datatype, transfer download filename, transfer download mode, transfer download path, transfer download serverip, transfer download start

## transfer download tftpMaxRetries

To enter the tftp Packet Max Retries in secs between 1 and 254, use the transfer download tftpMax Timeout command.

>transfer download tftpPktMaxTimeout <time out>

**Syntax** transfer Move a file

download tftpPktMaxTimeoutThe tftp Packet Maximum timeout in secs between

1 and 254.

Defaults N/A

Example >transfer download tftpPktMaxTimeout 55

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer upload datatype, transfer download filename, transfer download mode, transfer download path, transfer download serverip, transfer download start

#### transfer upload datatype

To set the upload data type, use the transfer upload datatype command.

>transfer upload datatype [errorlog/crashfile/systemtrace/messagelog/traplog]

**Syntax** transfer Move a file or configuration.

upload Upload operation to Alcatel OmniAccess Switch or

Appliance.

datatype Type of data errorlog Error log file

crashfile Crash file

systemtrace System trace file messagelog Message log traplog Trap log

Defaults: N/A

Examples >transfer upload datatype errorlog

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start

## transfer upload filename

To upload a specific file, use the transfer upload filename command.

>transfer upload filename <filename>

**Syntax** transfer Move a file

upload Upload operation to Alcatel OmniAccess Switch or

**Appliance** 

filename <filename > Enter filename up to 16 alphanumeric characters.

Defaults N/A

Examples >transfer upload filename build603

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload mode, transfer upload path, transfer upload serverip, transfer upload start

#### transfer upload mode

To upload a specific file, use the transfer upload mode command.

>transfer upload mode <mode>

**Syntax** transfer Move a file

upload mode Download mode for <mode> Enter mode of tftp.

Defaults N/A

Examples >transfer upload mode tftp

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename,

transfer upload path, transfer upload serverip, transfer upload start

## transfer upload path

To set a specific upload path, use the transfer upload path command.

>transfer upload filename <filename>

**Syntax** transfer Move a file

upload Upload operation for

path <path> Enter filename directory path.

Defaults N/A

Examples >transfer upload c:\install\version2

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename, transfer upload serverip, transfer upload start

transfer upload mode, transfer upload serverip, transfer upload start

#### transfer upload serverip

To upload a specific server, use the transfer upload serverip command.

>transfer upload serverip <ip addr>

**Syntax** transfer Move a file

upload Upload operation for

serverip <IP addr> Enter IP address of the server.

Defaults N/A

Examples >transfer upload serverip 175.34.56.78

Related Commands clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip, transfer download start, transfer upload datatype, transfer upload filename,

transfer upload mode, transfer upload path, transfer upload start

#### transfer upload start

To start an upload transfer, use the transfer upload start command.

>transfer download start

**Syntax** transfer Move a file

upload start Download start operation for

Defaults N/A

Examples >transfer upload start

TFTP Path...... c:\find\off/
TFTP Filename...... wps\_2\_0\_75\_0.aes

This may take some time.

Are you sure you want to start? (y/n) n

Transfer Cancelled

**Related Commands** clear transfer, transfer download datatype, transfer download filename,

transfer download mode, transfer download path, transfer download serverip,

transfer download start, transfer upload datatype, transfer upload filename, transfer upload mode, transfer upload path, transfer upload serverip

# **Troubleshooting**

Use the debug commands to manage system debugging.

- <u>debug aaa</u>
- <u>debug airewave-director</u>
- <u>debug arp</u>
- <u>debug bcast</u>
- <u>debug crypto</u>
- debug dhcp
- <u>debug disable-all</u>
- debug 80211
  - <u>debug 80211-events</u>
  - debug 80211-frames
- <u>debug dot1x</u>
- debug l2age
- <u>debug lwapp</u>
- debug mac
  - <u>debug mac addr</u>
  - debug mac disable
- <u>debug ntp</u>
- <u>debug pem</u>
- debug pm
- <u>debug poe</u>
- <u>debug transfer</u>

#### debug aaa

To configure AAA debug options, use the debug aaa command.

#### >debug aaa [keyword] [enable/disable]

Syntax	debug aaa	Debug aaa

all Configures debug of all AAA messages.
trace Configures debug of AAA trace messages.
file Configures debug of AAA usmdb database.
radius Configures debug of AAA RADIUS database.
Idap Configures debug of AAA LDAP database.
smb Configures debug of AAA SMB database.
[enable/disable] Enable or disable the selected keyword action.

Defaults N/A

Example >debug aaa trace enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames,

debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe, debug transfer

# debug airewave-director

To configure the OmniVista AirView Software debug options, use the debug airwave-director command.

debug airewave-director [all/channel/error/group/message/packet/detail/
rf-change/profile/power] [enable/disable]

**Syntax** debug airewave-director Command action

all Configures debug of all OmniVista AirView Software

logs

channel Configures debug of OmniVista AirView Software

channel assignment protocol

error Configures debug of OmniVista AirView Software

error logs

detail Configures debug of OmniVista AirView Software

detail logs

group Configures debug of OmniVista AirView Software

grouping protocol

manager Configures debug of OmniVista AirView Software

manager

message Configures debug of OmniVista AirView Software

messages

packet Configures debug of OmniVista AirView Software

packets

power Configures debug of OmniVista AirView Software

power assignment protocol

rf-change Configures logging of OmniVista AirView Software rf

changes

profile Configures logging of OmniVista AirView Software

profile events

[enable/disable] Enable or disabled the selected activity

Defaults N/A

**Example** >debug airwave-director error enable

Related Commands debug aaa, debug arp, debug bcast, debug crypto, debug dhcp, debug

disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe, debug

transfer

## debug arp

To configure debug of ARP, use the debug arp command.

debug arp [all/error/message/detail] [enable/disable]

Syntax debug arp Command action

all Configures debug of all arp logs.
error Configures debug of arp Errors.
message Configures debug of arp Messages.

detail Configures debug of arp Detail Messages. [enable/disable] Enable or disable the selected keyword action.

Defaults N/A

Example >debug arp error enable

**Related Commands** debug aaa, debug airewave-director, debug bcast, debug crypto, debug dhcp,

debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug bcast

To configure debug of broadcast packets, use the debug bcast command.

debug bcast [all/error/message/detail] [enable/disable]

Syntax debug bcast Command action

all Configures debug of all broadcast logs.
error Configures debug of broadcast Errors.
message Configures debug of broadcast Messages.
detail Configures debug of broadcast Detail Messages.

[enable/disable] Enable or disable the selected option.

Defaults N/A

Example >debug bcast message enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug crypto, debug dhcp,

debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

#### debug crypto

To configure the Hardware Crypto debug options, use the debug crypto command.

**Note:** This command is only valid if the ESM Module is present in the system.

debug crypto [all/sessions/trace/warnings] [enable/disable]

Syntax debug crypto Command action

all Configures debug of all Hardware Crypto messages.
sessions Configures debug of Hardware Crypto Sessions.
trace Configures debug of Hardware Crypto trace

messages.

warnings Configures debug of Hardware Crypto warning

messages.

enable/disable Enable or disable the selected action.

Defaults N/A

**Examples** >debug crypto trace enable/disable

Related Commands debug aaa, debug airewave-director, debug arp, debug bcast, debug dhcp,

debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug dhcp

To configure the DHCP debug options, use the debug dhcp command.

debug dhcp [message/packet] [enable/disable]

Syntax debug dhcp Command Action

message Configures debug of DHCP error messages.

packet Configures debug of DHCP packets. enable/disable Enable or disable the selected option.

Defaults N/A

Examples >debug dhcp message enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug disable-all

To disable all debug messages, use the disable-all command.

debug disable-all

**Syntax** debug disable-all Command action

Defaults N/A

Example >debug disable-all

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe, debug

transfer

## debug 80211-events

To configure the 802.11 events debug options, use the debug 80211-events command.

debug 80211-events [all/client] [enable/disable]

Syntax debug 80211-events Command action

[all/client]

all Configures debug of all 802.11 messages.
mobile Configures debug of 802.11 mobile events.
rldp Configures debug of 802.11 Rogue Location

Discovery.

rogue Configures debug of 802.11 rogue events.

state Configures debug of 802.11 mobile state transitions.

[enable/disable] Enable or disable the selected action.

**Defaults** N/A

Examples >debug 80211-events mobile enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-frames, debug l2age, debug

lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe, debug transfer

## debug 80211-frames

To configure the 802.11 frame debug options, use the debug 80211-frames command.

debug 80211-frames [all/control/data/errors/management] [enable/disable]

**Syntax** debug 80211-frames Command actions

all Configures debug of all 802.11 messages.

control Configures debug of 802.11 control messages.

data Configures debug of 802.11 data messages.

errors Configures debug of malformed 802.11 messages.

management Configures debug of 802.11 management messages.

enable/disable Enable or disable the selected option.

Defaults N/A

Examples >debug 80211-frames control enable

Related Commands debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe, debug

transfer

## debug dot1x

To configure the dot1x, use the debug dot1x command.

debug dot1x [all/packet] [enable/disable]

**Syntax** debug doy1x Command actions

all Configures debug of all 802.1X messages.
packet Configures debug of 802.1X packets.
trace Configures debug of 802.1X packets.
enable/disable Enable or disable the selected option.

Defaults N/A

Examples >debug dot1x all enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-frames, debug 80211-events, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm,

debug poe, debug transfer

## debug l2age

To configure debug of Layer 2 Age Timeout Messages, use the debug I2age command.

debug 12age [enable/disable]

**Syntax** debug I2age Command action

[enable/disable] Enable or disable the messages.

Defaults N/A

Examples >debug 12age enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug lwapp

To configure the LWAPP debug options, use the debug lwapp command.

debug lwapp [all/error/messages/detail/packet] [enable/disable]

**Syntax** debug Iwapp Command action

all Configures debug of all LWAPP logs
error Configures debug of LWAPP error logs
messages Configures debug of LWAPP messages
packet Configures debug of LWAPP Packet trace
enable/disable Enable or disable the selected action.

Defaults N/A

Examples >debug lwapp all enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug mac, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug mac addr

To configure MAC debugging, use the debug mac addr command. The purpose of this command is to limit the number of debug messages being output to those that are relevant to the specified MAC address.

debug mac addr <MAC addr>

**Syntax** debug mac Command action.

addr Configure the MAC address <MAC addr> Specific MAC address

Defaults N/A

Examples >debug mac addr 00:0b:85:00:02:5

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug mac disable

To disable MAC debugging, use the debug mac disable command.

debug mac disable <MAC addr>

**Syntax** debug mac Command action.

disable Disable the MAC address

<MAC addr> Specific MAC address

Defaults N/A

Examples >debug mac disable 00:0b:85:00:02:5

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mobility, debug pem, debug pm, debug poe,

debug transfer

## debug ntp

To configure debug of NTP, use the debug ntp command.

debug ntp [detail/low/packet]

**Syntax** debug ntp Command action.

detail Configures debug of detailed NTP messages.

low Configures debug of NTP messages. packet Configures debug of NTP packets.

Defaults N/A

Examples >debug ntp low

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pm, debug poe,

debug transfer

## debug pem

To configure the access policy manager debug options, use the debug pem command.

debug pem [events/state] [enable/disable]

**Syntax** debug pem Command action.

events Configures debug of policy manager events.

state Configures debug of policy manager State Machine.

enable/disable Enable or disable the selected action.

Defaults N/A

Examples >debug pem state enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pm, debug poe,

debug transfer

## debug pm

To configure debug of the security policy manager module, use the debug pm command.

debug pm [<keyword>] [enable/disable]

**Syntax** debug pm Command action.

keywords:

all Used to disable all debug in policy manager module init Configures debug of policy manager initialization

events

config Configures debug of policy manager configuration

rules Configures debug of Layer 3 policy events

message Configures debug of policy manager message queue

events

pki Configures debug of PKI-related events sa-export Configures debug of SA export (mobility) Configures debug of SA import (mobility) sa-import Configures debug of hardware offload events hwcrypto Configures debug of random number generation rng Configures debug of the policy manager policy mgr ssh-pmgr Configures debug of the policy manager engine ssh-engine Configures debug of the policy manager interceptor ssh-int

ssh-appgw Configures debug of application gateways

ssh-tcp Configures debug of policy manager tcp handling list Configures debug of policy manager list mgmt enable/disable Enable of disable the selected command action.

Defaults N/A

Example >debug pm pki enable

**Related Commands** debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto,

debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug poe,

debug transfer

## debug poe

To configure the power over ethernet debug options, use the debug poe command.

#### debug poe [error/message/detail] [enable/disable]

Syntax debug poe Command action

detail Configures debug of poe detail logs error Configures debug of poe error logs message Configures debug of poe messages enable/disable Enable or disable the selected action.

Defaults N/A

#### Examples >debug poe detail enable

debug>poe Mon Dec 29 12:38:52 2003: avpPtr = 0x129d4b6c, blockPtr = 0

x129d4b8c (32 bytes into block, 12 bytes of room)

Mon Dec 29 12:38:52 2003: Queueing Authentication Message: Mon Dec 29 12:38:52 2003: AuthenticationRequest: 0x775fdb90

Mon Dec 29 12:38:52 2003: Callback......0x1

0259d94

Mon Dec 29 12:38:52 2003: protocolType................0x4

0000001

Mon Dec 29 12:38:53 2003: proxyState......00:

00:00:C4:00:00

Mon Dec 29 12:38:53 2003: Packet contains 2 AVPs:

Mon Dec 29 12:38:53 2003: AVP[01] User-Name.....

.....admin (5 bytes)

```
Mon Dec 29 12:38:53 2003:
                              AVP[02] User-Password.....
....admin (5 bytes)
Mon Dec 29 12:38:53 2003: Found a service (File Database), sending request to it
Mon Dec 29 12:38:53 2003: avpPtr = 0x781ff698, blockPtr = 0x781ff6b8 (32 bytes i
nto block, 10 bytes of room)
Mon Dec 29 12:38:53 2003: Sending result 0
Mon Dec 29 12:38:53 2003: AuthorizationResponse: 0x781ff680
Mon Dec 29 12:38:53 2003:
                          structureSize......66
Mon Dec 29 12:38:53 2003:
                          resultCode.....0
Mon Dec 29 12:38:53 2003:
                          protocolUsed.....0x0
0000008
Mon Dec 29 12:38:53 2003:
                          proxyState.....00:
00:00:C4:00:00
Mon Dec 29 12:38:54 2003:
                          Packet contains 2 AVPs:
Mon Dec 29 12:38:54 2003:
                              AVP[01]
                         Service-Type......0x00000006
                         (6) (4 bytes)
Mon Dec 29 12:38:54 2003:
                              AVP[02]
                         Vap-Id.....0x00000000
                         (0) (4 bytes)
Mon Dec 29 12:38:54 2003: Calling callback 0x10259d94 with result 0x781ff680
Mon Dec 29 12:38:54 2003: avpPtr = 0x129d4b6c, blockPtr = 0x129d4b8c (32 bytes i
nto block, 12 bytes of room)
Mon Dec 29 12:38:54 2003: Queueing Authentication Message:
Mon Dec 29 12:38:54 2003: AuthenticationRequest: 0x775fdb90
Mon Dec 29 12:38:54 2003:
                          Callback......0x1
0259d94
Mon Dec 29 12:38:54 2003:
                          protocolType.....0x4
0000001
Mon Dec 29 12:38:54 2003:
                          proxyState......00:
00:00:C5:00:00
Mon Dec 29 12:38:54 2003:
                          Packet contains 2 AVPs:
                             AVP[01] User-Name.....
Mon Dec 29 12:38:55 2003:
....admin (5 bytes)
Mon Dec 29 12:38:55 2003:
                              AVP[02] User-Password.....
....admin (5 bytes)
Mon Dec 29 12:38:55 2003: Found a service (File Database), sending request to it
Mon Dec 29 12:38:55 2003: avpPtr = 0x781ff698, blockPtr = 0x781ff6b8 (32 bytes i
nto block, 10 bytes of room)
Mon Dec 29 12:38:55 2003: Sending result 0
Mon Dec 29 12:38:55 2003: AuthorizationResponse: 0x781ff680
Mon Dec 29 12:38:55 2003:
                       structureSize......66
Mon Dec 29 12:38:55 2003:
                          resultCode.....0
Mon Dec 29 12:38:55 2003:
                          protocolUsed......0x0
0000008
Mon Dec 29 12:38:55 2003:
                          proxyState.....00:
00:00:C5:00:00
Mon Dec 29 12:38:55 2003:
                          Packet contains 2 AVPs:
Mon Dec 29 12:38:55 2003:
                             AVP[01]
                         Service-Type......0x00000006
                         (6) (4 bytes)
Mon Dec 29 12:38:56 2003:
                              AVP[02]
                         Vap-Id.....0x00000000
                         (0) (4 bytes)
Mon Dec 29 12:38:56 2003: Calling callback 0x10259d94 with result 0x781ff680
Mon Dec 29 12:38:56 2003: avpPtr = 0x129d4b6c, blockPtr = 0x129d4b8c (32 bytes i
nto block, 12 bytes of room)
Mon Dec 29 12:38:56 2003: Queueing Authentication Message:
Mon Dec 29 12:38:56 2003: AuthenticationRequest: 0x775fdb90
```

```
Mon Dec 29 12:38:56 2003:
                         Callback.....0x1
0259d94
Mon Dec 29 12:38:56 2003:
                         protocolType.....0x4
0000001
Mon Dec 29 12:38:56 2003:
                         proxyState......00:
00:00:C6:00:00
Mon Dec 29 12:38:56 2003:
                         Packet contains 2 AVPs:
                            AVP[01] User-Name.....
Mon Dec 29 12:38:56 2003:
.....admin (5 bytes)
Mon Dec 29 12:38:56 2003:
                            AVP[02] User-Password.....
....admin (5 bytes)
Mon Dec 29 12:38:57 2003: Found a service (File Database), sending request to it
Mon Dec 29 12:38:57 2003: avpPtr = 0x781ff698, blockPtr = 0x781ff6b8 (32 bytes i
nto block, 10 bytes of room)
Mon Dec 29 12:38:57 2003: Sending result 0
Mon Dec 29 12:38:57 2003: AuthorizationResponse: 0x781ff680
Mon Dec 29 12:38:57 2003:
                         structureSize......66
Mon Dec 29 12:38:57 2003:
                         resultCode.....0
Mon Dec 29 12:38:57 2003:
                         protocolUsed.....0x0
0000008
Mon Dec 29 12:38:57 2003:
                         proxyState......00:
00:00:C6:00:00
Mon Dec 29 12:38:57 2003:
                         Packet contains 2 AVPs:
Mon Dec 29 12:38:57 2003:
                            AVP[01]
                        Service-Type......0x00000006
                        (6) (4 bytes)
Mon Dec 29 12:38:57 2003:
                            AVP[02]
                        Vap-Id.....0x00000000
                        (0) (4 bytes)
Mon Dec 29 12:38:57 2003: Calling callback 0x10259d94 with result 0x781ff680
```

#### **Related Commands**

debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto, debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames, debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug transfer

## debug transfer

To configure the transfer debug options, use the debug transfer command.

**Warning:** Using this command should be done with great care. Its use will cause the Alcatel Omni-Access Switch or Appliance to reboot.

#### debug transfer [all/tftp/trace] [enable/disable]

Syntax	debug transfer all tftp trace enable/disable	Command action Configures debug of all transfer messages. Configures debug of tftp transfers. Configures debug of transfer/upgrade. Enable or disable the selected action.
Defaults	N/A	

Examples >debug transfer tftp disable

**Related Commands**debug aaa, debug airewave-director, debug arp, debug bcast, debug crypto, debug dhcp, debug disable-all, debug 80211-events, debug 80211-frames,

debug l2age, debug lwapp, debug mac, debug mobility, debug pem, debug pm, debug poe

Notes:

# Alcatel OmniAccess Wireless System Web Browser Online Help

System Release 2.0

Welcome to the Alcatel OmniAccess Wireless System Web Browser Online Help! This help system is designed for use with Alcatel OmniAccess Wireless Switches and Appliances and comes bundled with the Alcatel Wireless Operating System software. You can find additional documentation for all Alcatel products and interfaces in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

- Note: The Web Browser Online Help pages require that cookies be enabled on your Web Browser. If the Web Browser fails to appear when you attempt to log on, make sure that cookies are enabled on your Web Browser.
- Note: The Web Browser Online Help pages can be blocked by Internet Explorer Content Advisor. If the Web Browser Online Help pages fail to appear when you click the **Help...** button, make sure Internet Explorer Content Advisor is disabled.
- Note: The Web Browser Online Help pages refer to "Switches". The term Switches generally applies to all Alcatel OmniAccess Wireless Switches and OmniAccess Wireless Appliances, unless expressly called out.

Similarly, the Web Browser Online Help pages refer to "APs". The term APs generally applies to all Alcatel OmniAccess Wireless Access Points (OmniAccess APs) and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs), unless expressly called out.

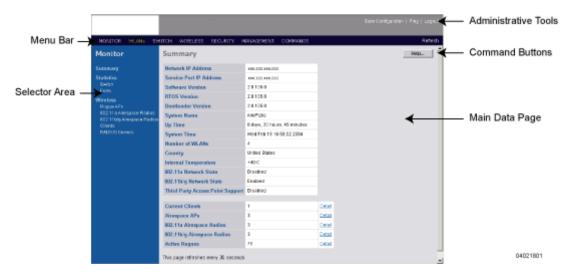
This Online Help document consists of the following sections:

- <u>Using the Web Browser Interface</u>
- Monitor Menu Bar Selection
- WLANs Menu Bar Selection
- Switch Menu Bar Selection
- Wireless Menu Bar Selection
- Security Menu Bar Selection
- Management Menu Bar Button
- Commands Menu Bar Selection
- <u>Using the Configuration Wizard</u>

## **Using the Web Browser Interface**

The typical Web interface page consists of five areas. The following figure illustrates them.

Figure - Web Browser Interface



The following sections describe the Web Browser interface page areas and how to use them:

- Menu Bar
- Selector Area
- Main Data Page
- Administrative Tools
- **Button Area**
- Applying Parameters
- Refreshing the Screen
- **Troubleshooting**

#### Menu Bar

The menu bar shows the names of the main configuration areas of the Alcatel OmniAccess Switch or Appliance. The menu bar in white accented characters on a black background. Refer to the following for available menu bar selections:

- Using the Web Browser Interface
- Monitor Menu Bar Selection
- WLANs Menu Bar Selection
- Switch Menu Bar Selection
- Wireless Menu Bar Selection
- Security Menu Bar Selection
- Management Menu Bar Button
- Commands Menu Bar Selection

## **Selector Area**

The selector area allows you to select a new configuration panel under the menu area that you have selected. You may select a single choice from several available for data to be displayed or configured. The selector area options vary based on the menu you select.

## Main Data Page

The main data page depends on what information the menu requires. Input fields are of two basic types:

- Text Fields into which data may be entered using the keyboard.
- Pulldowns from which one of several options may be chosen.

Input fields are black text on a white background. When you enter or select data, it does not go to the Alcatel OmniAccess Switch or Appliance, but is saved in the field until you click the **Apply** button. There may be fields that contain buttons. Selecting a button does take immediate effect. Data may also be displayed.



**Note:** Microsoft Internet Explorer generates a submit action on the next available button when you press the enter key while in an input field. On most menus this triggers the apply function.

#### **Administrative Tools**

This area provides shortcuts to Administration functions used on a regular basis when configuring an Alcatel OmniAccess Switch or Appliance through the Web Interface.

- **Save Configuration:** Data is saved to the Alcatel OmniAccess Switch or Appliance in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If you reboot the Alcatel OmniAccess Switch or Appliance, all applied changes are lost unless the configuration has been saved. Click on the **Save** button to save the current configuration.
- Ping: Send a Ping to a network element.

This pop-up window allows the you to tell the Alcatel OmniAccess Switch or Appliance to send a Ping request to a specified IP address. This can help you determine if there is connectivity between the Alcatel OmniAccess Switch or Appliance and a particular IP station. Once the operator clicks the Submit button, three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it shows No Reply Received from IP xxx.xxx.xxx.xxx, otherwise it shows Reply received from IP xxx.xxx.xxx.xxx (send count = 3, receive count = n).

Logout: Exit the current Web Browser Interface session.

## **Button Area**

At the right side of the main data area are command buttons to apply or refresh the data displayed in the main data area or request a help window.

Buttons take immediate effect when you select them and information goes to the Alcatel OmniAccess Switch or Appliance about the state of the menu at that time. The most commonly used buttons are:

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Refresh: Update the data on the current screen from the Alcatel OmniAccess Switch or Appliance.
- Help: Request that the help page be displayed in a new browser window.

There are additional buttons to perform other actions and not all main data areas have all buttons. The functionality of these buttons are described under the respective help topics.

## **Applying Parameters**

After submitting the new parameters or settings entered the page is refreshed. However, in some cases, the settings may appear different than specified by the operator. This happens where timers are involved and the affected code takes some period of time to execute. Refreshing the menu or tree shows the expected results. An example of this occurs when you enable the spanning tree mode or disabled on the Alcatel OmniAccess Switch or Appliance.

## **Refreshing the Screen**

Using the refresh function from the web browser refreshes all screens and displays the default initial screen in the main data area.

If you want to refresh a screen in the main data area, and there is no Refresh button present on that screen, use your mouse to right-click on the main data area screen, then select the refresh option.

## **Troubleshooting**

Note that some popup window filters can be configured to block the Alcatel Web Browser Online Help windows. If your system cannot display the Online Help windows, disable or reconfigure your browser popup filter software.

## Monitor Menu Bar Selection

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance and OmniAccess AP summary details. Use the selector area to access the respective network details. Making this selection from the menu bar displays the system *Summary* page.

The following pages can be accessed from the Monitor Menu Bar Selection:

- Summary
- Switch Statistics
- Ports Statistics
- <u>Ports > Statistics</u>
- Third-Party APs
- <u>Third-Party APs > New</u>
- Third-Party APs > Edit
- Rogue APs
- Roque AP Detail
- <u>802.11a OmniAccess Radios</u>
- Radio > Statistics
- 802.11b OmniAccess Radios
- Clients
- <u>Clients > Detail</u>
- RADIUS Servers
- RADIUS Servers > Authentication Stats
- RADIUS Servers > Accounting Stats

## **Summary**

Use MONITOR/Summary to navigate to this page.

This summary page provides a top level description of your Alcatel OmniAccess Switch or Appliance. Configure the parameters listed on this page by selecting the appropriate page from links on the left of the summary page. The following table describes each of the these read-only fields and is refreshed every 30 seconds.

**Table - Summary Parameters** 

Parameter	Description	
Network IP Address	Local network IP address of the Alcatel OmniAccess Switch or Appliance as described in <u>Management Interface</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> .	
Service Port IP Address	The IP address of the Alcatel OmniAccess Switch or Appliance front-panel Service port.	

Table - Summary Parameters (Continued)

Parameter	Description
Software Version	The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
RTOS Version	Alcatel Wireless Operating System RTOS (real-time operating system) version number.
Bootloader Version	Alcatel Wireless Operating System bootloader version number.
System Name	Name assigned to the Alcatel OmniAccess Switch or Appliance.
Up Time	Time in days, hours and minutes since the last reboot.
System Time	Current time set on the Alcatel OmniAccess Switch or Appliance.
Number of WLANs	1 (one) is the default.
Country	Identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide.
Internal Temperature	Current internal chassis temperature.
802.11a Network State	Enabled or disabled.
802.11b/g Network State	Enabled or disabled.
Third Party Access Point Support	Enabled or disabled.
Current Clients	Number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
OmniAccess APs	Number of Alcatel OmniAccess Wireless Access Points associated with this Alcatel OmniAccess Switch or Appliance.
802.11a OmniAccess Radios	Number of 802.11a OmniAccess Radios.
802.11b/g OmniAccess Radios	Number of 802.11b/g OmniAccess Radios.
Active Rogues	Number of unauthorized access points detected by Alcatel OmniAccess Switch or Appliance.

Select the **Detail** links to take you to the following main data page:

- <u>Clients</u>
- OmniAccess APs
- 802.11a OmniAccess Radios
- 802.11b OmniAccess Radios
- Rogue APs

• **Help:** Request that the help page be displayed in a new browser window.

## **Switch Statistics**

Use MONITOR/Statistics/Switch to navigate to this page.

The following table describes Alcatel OmniAccess Switch or Appliance statistics provided on this page.

 Table - Alcatel OmniAccess Switch or Appliance Summary Statistics

Parameter	Description
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	The total number of packets received by the processor.
Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets	The total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

 Table - Alcatel OmniAccess Switch or Appliance Summary Statistics (Continued)

Parameter	Description
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this Alcatel OmniAccess Switch or Appliance since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this Alcatel OmniAccess Switch or Appliance.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this Alcatel OmniAccess Switch or Appliance.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this Alcatel OmniAccess Switch or Appliance since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this Alcatel OmniAccess Switch or Appliance that have been created statically.
VLAN Deletes	The number of VLANs on this Alcatel OmniAccess Switch or Appliance that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this Alcatel OmniAccess Switch or Appliance were last cleared.

- **Clear Counters:** Sets all summary and detailed Alcatel OmniAccess Switch or Appliance statistics counters to zero; also resets the "Time Since Counters Last Cleared" field.
- **Help:** Request that the help page be displayed in a new browser window.

## **Ports Statistics**

Use MONITOR/Statistics/Ports to navigate to this page.

This page displays the status of each port on the Alcatel OmniAccess Switch or Appliance. View detailed statistics for each port by selecting the **view stats** link ( $\underline{Ports} > \underline{Statistics}$ ). The following table provides a description and the range for each parameter.

**Table -** Summary Parameters

Parameter	Description	Range
Port No	Port number on the Alcatel OmniAccess Switch or Appliance.	<ul> <li>1-12 for 10/100Base-T, 13 for 1000Base-T or -SX on a 4012 OmniAccess Wireless Switch</li> <li>1-24 for 10/100Base-T, 25 for 1000Base-T or -SX on a 4024 OmniAccess Wireless Switch</li> <li>1 for 1000Base-SX on a (UNUSED DEVICE) OmniAccess Wireless Appliance</li> <li>1 for 1000Base-SX on a 4102 OmniAccess Wireless Appliance</li> </ul>

Table - Summary Parameters (Continued)

Parameter	Description	Range
Admin Mode	State of the port.	Enable; Disable
Physical Mode	Displays the configuration of the port physical interface.	<ul> <li>Auto</li> <li>100 Mbps Full Duplex;</li> <li>100 Mbps Half Duplex;</li> <li>10 Mbps Full Duplex;</li> <li>10 Mbps Half Duplex;</li> <li>1000 Mbps Full Duplex</li> </ul>
Physical Status	Displays the actual port physical interface.	<ul> <li>Auto</li> <li>100 Mbps Full Duplex;</li> <li>100 Mbps Half Duplex;</li> <li>10 Mbps Full Duplex;</li> <li>10 Mbps Half Duplex;</li> <li>1000 Mbps Full Duplex</li> </ul>
Link Status	Displays the status of the link.	Link Up; Link Down

The physical mode and status may reflect different values depending on the link status. For example, the physical mode may be set to "Auto" while the link actually runs at "10 Mbps Half Duplex".

The **view stats** links in the ports table takes you to the respective <u>Ports > Statistics</u> page when selected.

## **Command Buttons**

• **Help:** Request that the help page be displayed in a new browser window.

## **Ports > Statistics**

Use MONITOR/Statistics/Ports and then view stats to navigate to this page.

This page displays statistics on a per port basis. The **port number** appears on the main data page directly below the page title and above the Traffic Statistics tables. The following tables explain the port statistics.

Table - Traffic Statistics

Parameter	Received Description	Transmitted Description
Total Bytes	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the ether-StatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets (64 Octets)	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets (65-127 Octets)	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (128-255 Octets)	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (256-511 Octets)	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (512-1023 Octets)	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (1024-1518 Octets)	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Table - Traffic Statistics (Continued)

Parameter	Received Description	Transmitted Description
Packets (1519-1530 Octets)	The total number of packets (including bad packets) received that were between 1519 and 1530 octets in length inclusive (excluding framing bits but including FCS octets).	The total number of packets (including bad packets) received that were between 1519 and 1530 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (> 1530 Octets)	The total number of packets received that were longer than 1530 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	The total number of packets transmitted that were longer than 1530 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

**Maximum Info size allowed** - The maximum size of the Info (non-MAC) field that this port receives or transmits.

Table - Successful Packets

Parameter	Received Description	Transmitted Description
Total	The total number of packets received that were without errors.	The number of frames that have been transmitted by this port to its segment.
Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address.	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Table - Protocol Statistics

Parameter	Received Description	Transmitted Description
BPDUs	The count of BPDU's (Bridge Protocol Data Units) received in the spanning tree layer.	The count of BPDU's (Bridge Protocol Data Units) transmitted from the spanning tree layer.

Table - Protocol Statistics (Continued)

Parameter	Received Description	Transmitted Description
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface operates in half-duplex mode.	N/A.

**Time Since Counters Last Cleared:** The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

Click **Clear Counters** to set all summary and Alcatel OmniAccess Switch or Appliance detailed statistics counters to zero; also resets the "Time Since Counters Last Cleared" field.

Table - Received Packets with MAC Errors

Parameter	Description
Total	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber differs from the definition in IEEE-802.3 section 8.2.1.5 (10Base-5) and section 10.3.1.4 (10Base-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments/ Undersize	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Table - Received Packets Not Forwarded

Parameter	Description
Total	A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.

Table - Received Packets Not Forwarded (Continued)

Parameter	Description	
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface operates in half-duplex mode.	
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.	
VLAN Membership Mismatch	The number of frames discarded on this port due to ingress filtering.	
VLAN Viable Discards	The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.	
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.	
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.	
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.	
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.	

Table - Transmit Errors

Parameter	Description
Total Errors	The sum of Single, Multiple, and Excessive Collisions.
FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Oversized	The total number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

## Table - Transmit Discards

Parameter	Description
Total Discards	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Table - Transmit Discards (Continued)

Parameter	Description
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Port Membership	The number of frames discarded on egress for this port due to egress filtering being enabled.
VLAN Viable Discards	The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or when the VLAN has not been configured.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

- **< Back:** Return to the previous window.
- Help: Request that the help page be displayed in a new browser window.

## **Rogue APs**

Use MONITOR/Summary/Active Rogues Detail or MONITOR/Wireless/Rogue APs or WIRELESS/Rogue APs to navigate to this page.

This page displays access points in your air space which are not part of your configured network. These rogue access point radios may be one of the following four types:

- An unknown radio: This type of radio presents a threat to the integrity and security of your network. It has not been identified as an accepted internal radio or as a radio belonging to another company located near your premises.
- An internal radio: This radio has been identified and accepted as being secure. This radio is being used for accepted company functions, but is not part of the internal network.
- An acknowledged radio: This radio is transmiting from a known source outside of the company network. This radio may be part of another company's LAN which is located on another floor or in close proximity to your network. This radio does not present a security threat to your network.
- A contained radio: Between one and four OmniAccess APs are transmitting de-authorization and disassociate messages to clients associated with the rogue access point.

The following information is provided when a rogue access point radio is detected:

**Table - Rogue Access Point Radios** 

Parameter	Description
MAC Address	Media Access Control of the access point.

Table - Rogue Access Point Radios (Continued)

Parameter	Description
Туре	Rogue Access Point Type:  • AP = Infrastructure Access Point  • Ad Hoc (Peer to Peer, or Client to Client)
# Detecting Radios	Number of OmniAccess Radios detecting the rogue access point radio.
First Seen On	Date and time the radio was first scanned by the Alcatel OmniAccess Switch or Appliance.
Last Seen On	Date and time the radio was last scanned by the Alcatel OmniAccess Switch or Appliance.
Status	Configurable state of this radio relative to the network or Alcatel OmniAccess Switch or Appliance. Rogue access point radios appear as "Alert" when first scanned by the Alcatel OmniAccess Switch or Appliance, or as "Pending" when Alcatel Wireless Operating System identification is still underway.

This page reports rogue access points until the "Expiration Timeout for Rogue AP Entries" (set on the <u>Timers</u> page) expires.

The **Edit** links in the rogue access point radios table takes you to the respective <u>Rogue AP Detail</u> page when selected.

#### **Command Buttons**

• **Help:** Request that the help page be displayed in a new browser window.

## **Rogue AP Detail**

Use MONITOR/Summary/Active Rogues Detail and then Edit to navigate to this page.

This page displays the access points details of the unauthorized or unknown radio. The following information is provided when a rogue access point radio is detected:

**Table - Rogue Access Point Radio Details** 

Parameter	Description
MAC Address	Media Access Control of the rogue access point.
Туре	Rogue Access Point Type:  • AP = Infrastructure Access Point  • Ad Hoc = Client-to-Client
First Time Reported On	Date and time the radio was first scanned by the Alcatel OmniAccess Switch or Appliance.
Last Time Reported On	Date and time the radio was last scanned by the Alcatel OmniAccess Switch or Appliance.

Table - Rogue Access Point Radio Details (Continued)

Parameter	Description
Current Status	The status of this radio is:  • Alert (Unknown AP)  • Known (Internal AP)  • Acknowledge (External AP)  • Contain (Rogue Access Point)  • Pending (unidentified)
Update Status (Note)	Configurable state of this rogue access point in the Alcatel OmniAccess Switch or Appliance. You may set the status to:  • Alert (Unknown AP)  • Known (Internal AP)  • Acknowledge (External AP)  • Contain (Rogue Access Point) discourage all rogue access point clients.
Maximum number of OmniAccess APs to contain the rogue	When Update Status parameter is set to Contain (Rogue Access Point), choose the number of OmniAccess APs to contain the rogue access point clients:  1 OmniAccess AP - Gently discourage rogue access point clients on current channel using one OmniAccess AP limited discouragement.  2 OmniAccess APs - Discourage rogue access point clients on current channel using two OmniAccess APs, if available.  3 OmniAccess APs - Discourage rogue access point clients on current channel using three OmniAccess APs, if available.  4 OmniAccess APs - Aggressively discourage rogue access point clients on current channel using four OmniAccess APs, if available.

**Note:** Make sure you do not attempt to contain rogue access points operated by other establishments, such as the cafe hotspot across the street!

#### OmniAccess APs that Detected this Rogue

This table provides a detailed list of OmniAccess APs that detect the unauthorized radio as well as the transmit characteristics of the radio. The following information physically identifies the location of the rogue access point.

- OmniAccess AP MAC address that identified the rogue access point radio.
- Name of the OmniAccess AP that identified the roque access point radio.
- SSID Service Set Identifier being broadcast by the rogue access point radio.
- Channel Which channel the roque access point is broadcasting on.
- Radio Type Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g.
- WEP Whether WEP is enabled or disabled.
- Pre-Amble Whether the Preamble is Short or Long.
- RSSI (receive signal strength indicator) of rogue access point radio at the OmniAccess AP
   (-80 dBm or lower, the rogue access point is far away or transmitting at a low signal strength;
   -60 dBm or higher, the rogue access point is close and/or transmitting at a high signal strength).
- SNR (signal to noise ratio) of rogue access point radio at the OmniAccess AP.

- Containment Type 'Contained' if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status Maximum Number, otherwise blank.
- Containment Channels Current channel or channels if the roque access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise blank.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

## 802.11a OmniAccess Radios

Use MONITOR/Wireless/802.11a OmniAccess Radios or MONITOR/Summary/802.11a Omni-**Access Radios** to navigate to this page.

This page displays the OmniAccess Radio profile for your 802.11a RF network. It shows the status of each 802.11a OmniAccess Radio configured on this Alcatel OmniAccess Switch or Appliance and its profile.

Table - 802,11a OmniAccess Radio Profile

Parameters	Description
AP Name	This is the name assigned to the OmniAccess AP.
MAC Address	Media Access Control of the OmniAccess AP.
Operational Status	Displays the operational status of the OmniAccess Radios.
Load Profile	
Noise Profile	The OmniVista AirView Software profile for the OmniAccess Radio is displayed for these characteristics. The profile status is dis-
Interference Profile	played as a pass or fail with details provided on <u>OmniAccess APs &gt; Details</u> data page.
Coverage Profile	

To access details for each OmniAccess Radio, select the **details** link (*Radio > Statistics*).

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

## Radio > Statistics

Use MONITOR/Wireless/802.11a OmniAccess Radios and then details to navigate to this page.

This page displays the RF (Radio Frequency) statistics for the selected OmniAccess Radio. You can alternate between the Graphics View and the Text View using the Graphics View and the Text View buttons. You can view and refresh the following Statistics by selecting them (using the checkboxes) and then clicking the **Refresh** button on the data page:

- Profile Information.
- Rx Neighbors.

802.11 MAC Counters.

This page also displays the following OmniAccess AP variables:

- AP Name.
- AP MAC Address.
- AP IP Address Only shows an IP address if the Alcatel OmniAccess Switch or Appliance LWAPP protocol is set for Layer 3 on the <u>General</u> page, otherwise Disabled.
- Radio Type (802.11a or 802.11b/g).
- Operational Status Displays the operational status of the OmniAccess Radios, either UP or DOWN.
- Monitor Only Mode (OmniAccess AP) Status Local (OmniAccess AP), OmniAccess AP 1200R (Alcatel OmniAccess Remote Edge Access Point), or Monitor (OmniAccess AP in monitor-only mode).
- Current Channel Number.

#### **Profile Information/Graphics View and Text View**

The RF statistics are used to derive the OmniVista AirView Software profile for each OmniAccess Radio in your network. The Alcatel OmniAccess Switch or Appliance uses the OmniVista AirView Software profile to adjust the OmniAccess Radio transmit and receive levels in order to maintain the most efficient configuration for your network. This data view also displays the RF properties of the Alcatel OmniAccess Switch or Appliance and its clients.

- The OmniVista AirView Software PASSED/FAILED thresholds are Globally set for all OmniAccess
   APs in the <u>802.11a Global Parameters > Auto RF</u> and <u>802.11b/g Global Parameters > Auto RF</u>
   pages.
- The OmniVista AirView Software PASSED/FAILED thresholds are Individually set for this OmniAccess AP in the <u>802.11 AP Interfaces > Performance Profile</u> page.



Figure - Profile Information in Graphics View

The following sections describe each of the Graphical and Text results.

## **Noise by Channel**

Each channel of the OmniAccess AP appears along with the corresponding non-802.11 noise interfering with the currently-assigned channel.

#### Interference by Channel

Each channel of the OmniAccess AP appears with the corresponding traffic interference from other 802.11 sources.

#### **Load Statistics**

Total bandwidth and channel utilization appears for transmitting and receiving traffic on this Omni-Access Radio. Attached clients are also displayed.

#### Client RSS

The Received Signal Strength appears for each attached client.

## Client SNR

The Signal to Noise Ratio appears for each attached client.

## **Rx Neighbors Information**

This area displays the OmniAccess Radio's neighboring APs, and their IP address and RSSI values. These details are used for channel allotment and RF coverage area shaping.

This information is displayed similar to the following:

```
AP 00:0b:85:00:83:00 172.16.16.10
```

#### where:

- AP is an access point.
- 00:0b:85:00:83:00 is the MAC address of the neighboring AP.
- 172.16.16.10 is the IP address of the AP's Alcatel OmniAccess Switch or Appliance.

## 802.11 MAC Counters

The following table describes the 802.11 MAC counters.

Table - 802.11 MAC Counters

Counter	Description
Tx Fragment Count	This counter is incremented for an acknowledged MPDU with an individual address in the address 1 field.
Tx Failed Count	This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
Multiple Retry Count	This counter increments when an MSDU is successfully transmitted after more than one retransmission.
RTS Success Count	This counter increments when a CTS is received in response to an RTS.
ACK Failure Count	This counter increments when an ACK is not received when expected.
Multicast Rx Frame Count	This counter increments when a MSDU is received with the multicast bit set in the destination MAC address.
Tx Frame Count	This counter increments for each successfully transmitted MSDU.
Multicast Tx Frame Count	This counter increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the OmniAccess AP, this implies having received an acknowledgment to all associated MPDUs.
Retry Count	This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
Frame Duplicate Count	This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.
RTS Failure Count	This counter increments when a CTS is not received in response to an RTS.
Rx Fragment Count	This counter shall be incremented for each successfully received MPDU of type Data or Management.
FCS Error Count	This counter increments when an FCS error is detected in a received MPDU.

Table - 802.11 MAC Counters (Continued)

Counter	Description
WEP Undecryptable Count	This counter increments when a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the TA's MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

- < Back: Return to the previous window.
- Graphics View/Text View: Move back and forth between the graphics and text views of the Radio > Statistics page.
- **Help:** Request that the help page be displayed in a new browser window.

#### 802.11b OmniAccess Radios

Use MONITOR/Wireless 802.11b OmniAccess Radios or MONITOR/Summary/802.11b Omni-**Access Radios** to navigate to this page.

This page displays the OmniAccess Radio profile for your 802.11b/802.11g RF network. It shows the status of each 802.11b/g OmniAccess Radio configured on this Alcatel OmniAccess Switch or Appliance and its profile.

Table - 802.11a OmniAccess Radio Profile

Parameters	Description
AP Name	This is the name assigned to the OmniAccess AP.
MAC Address	Media Access Control of the OmniAccess AP.
Operational Status	Displays the operational status of the OmniAccess Radios.
Load Profile	The OmniVista AirView Software profile for the OmniAccess Radio is displayed for these characteristics. The profile status is displayed as a pass or fail with details provided on the <u>Radio &gt; Statistics</u> data page.
Noise Profile	
Interference Profile	
Coverage Profile	

Access details for each OmniAccess Radio by selecting the **details** link (*Radio > Statistics*).

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

#### Clients

Use MONITOR/Wireless/Clients or MONITOR/Summary/Current Clients Detail or WIRELESS/ **Clients** to navigate to this page.

#### **MAC Address Search**

You can search the client list by MAC address.

Enter the MAC address as 6 two-digit hexadecimal numbers separated by colons--for example, 01:23:45:67:89:AB. Then click the **Search** button. If the address exists, that entry is displayed as the first entry followed by the remaining (greater) MAC addresses. An exact match is required.

#### **Client Information Table**

This table displays a list of all clients attached to the Alcatel OmniAccess Switch or Appliance. Client information includes:

- MAC Address of the client.
- Name of the AP to which client is attached.
- MAC Address of the AP.
- Name of WLAN used by the client.
- The type of client (802.11a, 802.11b or 802.11g).
- Status of the client connection.
- Authorization status.
- Alcatel OmniAccess Switch or Appliance port number of the client's associated access point.

Select the **Detail** link to display the *Clients > Detail* page.

Select **LinkTest** to test the link to the Client, and determine Client signal strength, Local signal strength, and Local signal to noise ratio in a popup window. Note that the **LinkTest** *does not* work for IPSec links, and may not work for some clients.

Select **Disable** to manually disable a client on the <u>Disabled Client > New page</u>.

Select the Remove link to dissociate the Client.

#### **Command Buttons**

• **Help:** Request that the help page be displayed in a new browser window.

## Clients > Detail

Use **MONITOR/Wireless/Clients** then **Detail** to navigate to this page.

This page displays the details of the select client's session. Information is display for both the client and its associated AP.

**Table - Client Properties** 

Parameter	Description
MAC Address	MAC address of the client station.
IP Address	IP address of the client station.
User Name	Login client name from RADIUS or Alcatel OmniAccess Switch or Appliance authentication.
Port Number	Alcatel OmniAccess Switch or Appliance port used for the client's associated access point.

Table - Client Properties (Continued)

Parameter	Description
Mobility Role	<ul> <li>Local when the client has not roamed from its original Alcatel Omni-Access Switch or Appliance, or when the client has roamed to another Alcatel OmniAccess Switch or Appliance on the same subnet.</li> <li>Foreign when the client has roamed from its original Alcatel Omni-Access Switch or Appliance to another Alcatel OmniAccess Switch or Appliance on a different subnet.</li> <li>Anchor when the client has roamed back to its original Alcatel Omni-Access Switch or Appliance after roaming to another Alcatel OmniAccess Switch or Appliance on a different subnet.</li> </ul>
Mobility Peer IP Address	<ul> <li>N/A when the client is Local (has not roamed from its original subnet).</li> <li>Anchor IP Address (the IP address of the original Alcatel OmniAccess Switch or Appliance) when the client is Foreign (has roamed to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> <li>Foreign IP Address (the IP address of the original Alcatel OmniAccess Switch or Appliance) when the client is Anchor (has roamed back to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> </ul>
Security Policy Completed	No, when the security policy checks have not been completed, or Yes, when the security policy checks have been completed.
Policy Manager State	<ul> <li>DHCP_REQD when a DHCP server is required to complete the security policy.</li> <li>Other messages, to be determined.</li> </ul>
Mirror Mode	• Enable or disable Mirror mode, as described in the <u>Alcatel OmniAccess</u> <u>Wireless Product Guide</u> .

**Table - Quality of Service Properties** 

Parameter	Description
QoS Level	Gold, Silver, or Bronze.

**Table - Client Statistics** 

Parameter	Description
Bytes Received	Total number of bytes received by the Alcatel OmniAccess Switch or Appliance from the client.
Bytes Sent	Total number of bytes sent to the client from the Alcatel OmniAccess Switch or Appliance.
Packets Received	Total number of packets received by the Alcatel OmniAccess Switch or Appliance from the client.
Packets Sent	Total number of packets sent to the client from the Alcatel OmniAccess Switch or Appliance.
Policy Errors	Number of policy errors for the client.

Table - Client Statistics (Continued)

Parameter	Description
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal to noise ratio of the client RF session.

The AP Properties table identifies the properties of the client's access point and of the client's negotiated session.

**Table -** AP Properties

Parameter	Description
AP Address	MAC address of the access point.
AP Name	Name of the access point.
AP Type	Access point's RF type.
WLAN SSID	Name of the WLAN.
Status	Status of client from status code (see Status Code below).
Association ID	Client's AP association identification number.
802.11 Authentication	Authentication algorithm of client.
Reason Code	The client reason code may be one of the following:  • no reason code (0) normal operation  • unspecified reason (1) client associated but no longer authorized  • previousAuthNotValid (2) client associated but not authorized  • deauthenticationLeaving (3) the OmniAccess AP went offline, de-authenticating the client  • disassociationDueToInactivity (4) client session timeout exceeded  • disassociationAPBusy (5) the OmniAccess AP is busy, performing load balancing, for example  • class2FrameFromNonAuthStation (6) client attempted to transfer data before it was authenticated  • class2FrameFromNonAssStation (7) client attempted to transfer data before it was associated  • disassociationStaHasLeft (8) Alcatel Wireless Operating System moved the client to another OmniAccess AP using non-aggressive load balancing  • staReqAssociationWithoutAuth (9) client not authorized yet, still attempting to associate with an Alcatel  • missingReasonCode (99) client momentarily in an unknown state

Table - AP Properties (Continued)

Parameter	Description
Status Code	Client status may be one of the following:  • idle (0) normal operation: no rejections of client association requests  • aaaPending (1) completing an aaa transaction  • authenticated (2) 802.11 authentication completed  • associated (3) 802.11 association completed  • powersave (4) client in powersave mode  • disassociated (5) 802.11 disassociation completed  • tobedeleted (6) to be deleted after disassociation  • probing (7) client not associated or authorized yet  • disabled (8) automatically disabled by Alcatel Wireless Operating  System for an operator-defined time
CF Pollable	When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Specifies whether CFP is requested by the client.
Short Preamble	This attribute, when true, indicates that the short preamble option as defined in subclause 18.2.2.2 is implemented. This parameter must be Disabled to optimize this Alcatel OmniAccess Switch or Appliance for some clients, including SpectraLink NetLink Telephones.
PBCC	This attribute, when true, indicates that the PBCC modulation option as defined in subclause 18.4.6.6 is implemented. The default value of this attribute is not implemented.
Channel Agility	Physical channel agility functionality is or is not implemented.
Timeout	Client Session timeout. Sets the maximum amount of time allowed a client before it is forced to re-authenticate.
WEP State	WEP security state of the client.

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Link Test:** Use the built-in test circuitry to test the link between the client and the Alcatel OmniAccess Switch or Appliance.
- **Remove:** Disconnect the client.
- **Help:** Request that the help page be displayed in a new browser window.

## **RADIUS Servers**

Use MONITOR/Wireless/RADIUS Servers to navigate to this page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers. Configure the authentication and accounting servers by selecting the Security option from the Menu Bar.

Table - Authentication Servers and Accounting Servers Status

Parameter	Description
Index	Access priority number for RADIUS servers. Up to four Authentication and four Accounting servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the Alcatel OmniAccess Switch or Appliance.
Address	IP address of the RADIUS server.
Port	Communication port.
Admin Status	Enabled or disabled.

Select the **Stats...** link to display the statistics page for the selected server (*RADIUS Servers > Authen*tication Stats or RADIUS Servers > Accounting Stats).

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

## **RADIUS Servers > Authentication Stats**

Use MONITOR/Wireless/RADIUS Servers then Stats... in a RADIUS Authentication entry to navigate to this page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers as follows.

Table - Authentication Server Addressing

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1 first, Index 2 second, etc. Index number is based on the order in which the servers were added to the Alcatel OmniAccess Switch or Appliance.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

**Table - Authentication Server Statistics** 

Parameter	Description
Msg Round Trip Time	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Retry Requests	The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Messages	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.
Bad Authenticator Msgs	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout, or retransmission.
Timeout Requests	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Other Drops	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

- < Back: Return to the previous window.
- **Help:** Request that the help page be displayed in a new browser window.

# **RADIUS Servers > Accounting Stats**

Use **MONITOR/Wireless/RADIUS Servers** then **Stats...** in a RADIUS Accounting entry to navigate to this page.

This page displays addressing and status information for your Remote Authentication Dial-In User Servers as follows:

Table - Accounting Server Addressing

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1 first, Index 2 second, etc. Index number is based on the order in which the servers were added to the Alcatel OmniAccess Switch or Appliance.
Server Address	IP address of the RADIUS server.
Admin Status	State of the server.

Table - Accounting Server Statistics

Parameter	Description
Msg Round Trip Time	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retry Requests	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Messages	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticator Msgs	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.

Table - Accounting Server Statistics (Continued)

Parameter	Description
Timeout Requests	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Other Drops	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.

- < Back: Return to the previous window.
- **Help:** Request that the help page be displayed in a new browser window.

# WLANs Menu Bar Selection

This menu bar selection provides access to the system <u>WLANs</u> page.

Access the following pages from the WLANs Menu Bar Selection:

- **WLANs**
- WLANs > New
- WLANs > Edit

### **WLANs**

Click **WLANs** to navigate to this page.

This page shows a summary of the wireless local access networks (WLANs) that you have configured on your network. From this page, you may add, remove or edit WLANs.

Table - Timer Descriptions

Parameter	Description
WLAN ID	Identification number of the WLAN.
WLAN SSID	Definable name of the WLAN (text string).
Admin Status	Status of the WLAN is either enabled or disabled.
Security Policies	Security policies enabled on the WLAN.

From the summary table, select **Edit** to modify the selected WLAN characteristics and the WLANs > Edit page is displayed.

Select **Remove** from the summary table to delete the selected WLAN. You are prompted to confirm the removal of the selected WLAN.

#### **Command Buttons**

- New: Select to add a WLAN.
- **Help:** Request that the help page be displayed in a new browser window.

### WLANs > New

Use **WLANs** and then **New...** to navigate to this page.

To add a new wireless LAN:

- Select an unused WLAN ID from the drop-down menu. To add a WLAN for third-party APs, select 17.
- Note: Third-party APs must be connected directly to the front panel of 4012 and 4024 Alcatel OmniAccess Wireless Switches for the Alcatel Wireless Operating System to control them using WLAN 17. Because the (UNUSED DEVICE) and 4102 OmniAccess Wireless Appliances do not have front-panel AP ports, WLAN 17 is not supported on the (UNUSED DEVICE) or 4102 OmniAccess Wireless Appliances as described in *Third-Party Access Points* in the *Alcatel Omni*-Access Wireless Product Guide.
  - Enter a text name for the WLAN in the WLAN SSID box. (This is the SSID broadcast name for the WLAN.)

3. Click the **Apply** button to bring up the <u>WLANs > Edit</u> page and continue configuring the WLAN.

### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### WLANs > Edit

For existing WLANs, use **WLANs** and then **Edit** to navigate to this page.

This page allows you to edit the configurable parameters for a WLAN. The **WLAN ID** and **WLAN SSID** are displayed at the top of the page. The following tables describe the WLAN parameters.

Table - General Policies

Parameter	Description
Radio Policy	Set the WLAN radio policy to apply to All = 802.11a/b/g, 802.11a only, 802.11b only, 802.11g only, 802.11b/g only, 802.11a/b only, or 802.11a/g only. This setting requires that the selected bands be enabled on the 802.11a Global Parameters and 802.11b/g Global Parameters pages.
Admin Status	Set the status of the WLAN to either enabled or disabled.
Session Timeout	Set the maximum time for a client session before requiring reauthorization.
Quality of Service (QoS)	Set QoS to: Gold (Highest); Silver (Mid-range); Bronze (Low). Services such as VoIP should be set to Gold while non-discriminating services such as text messaging can be set to Bronze.
Allow AAA Override	<ul> <li>Enable or disable AAA override for global WLAN parameters.</li> <li>When AAA Override is enabled, and a client has conflicting AAA and Alcatel OmniAccess Switch or Appliance WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the Alcatel Wireless Operating System will move clients from the default Alcatel WLAN VLAN to a VLAN returned by the AAA server and predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Alcatel Wireless Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)</li> <li>For instance, if the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the Alcatel Wireless Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</li> <li>When AAA Override is disabled, all client authentication defaults to the Alcatel OmniAccess Switch or Appliance authentication parameter settings, and authentication is only performed by the AAA server if the Alcatel OmniAccess Switch or Appliance WLAN do not contain any client-specific authentication parameters.</li> <li>The AAA override values may come from a RADIUS server, for example.</li> </ul>

Table - General Policies (Continued)

Parameter	Description
Blacklisting	Enable or disable automatic client disabling (blacklisting), as described in the Alcatel OmniAccess Wireless Product Guide.
Blacklist Timeout	When automatic disabling (blacklisting) is enabled, set the timeout in seconds for disabled client machines. Client machines are disabled by MAC address and their status can be observed on the <u>Clients &gt; Detail</u> page. A timeout setting of 0 indicates that administrative control is required to re-enable the client.
DHCP Server (Override)	<ul> <li>When selected, you can enter the IP address of your DHCP server. This is a required field for some WLAN configurations. There are three valid configurations:</li> <li>DHCP Server Override ON, a valid DHCP Server IP address, and DHCP Address Assignment Required: Requires all WLAN clients to obtain an IP address from the DHCP Server.</li> <li>DHCP Server Override ON, a valid DHCP Server IP address, and DHCP Address Assignment Not Required: Allows all WLAN clients to obtain an IP address from the DHCP Server or use a static IP address.</li> <li>DHCP Server Override OFF: Forces all WLAN clients to use a static IP address. All DHCP requests are dropped.</li> </ul>
Interface Name	Limited to the non-service-port and non-virtual Interface Names configured on the <i>Interfaces</i> page.

You can choose both Layer 2 and Layer 3 security policies from the drop down list under the Security Policies heading. The selected security policy options are at the bottom of the page with the appropriate parameters listed. The following tables describe these parameters.

Table - Layer 2 Security Policies

Parameter	Description
None	No Layer 2 security selected.
WPA	Wi-Fi Protected Access 802.11 data encryption type, TKIP-MIC.
802.1X	WEP 802.1X data encryption type (Note 1):  • 40/64 bit key  • 104/128 bit key  • 128/152 bit key.
Static WEP	Static WEP encryption parameters:  • Key sizes: 40/64, 104/128 and 128/152 bit key sizes  • Key Index: 1 to 4 (Note 2)  • Enter encryption key  • Select encryption key format in ASCII or HEX.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite WirelessWall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Alcatel OmniAccess Wireless System. (Note 3).
Fortress	Layer 2 security feature.

Table - Layer 2 Security Policies (Continued)

Parameter	Description
MAC Filtering	Select to filter clients by MAC address. Locally configure clients by MAC address in the <u>MAC Filters &gt; New</u> page. Otherwise, configure the clients on a RADIUS server.

**Note 1:** The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop down configurable 802.1X parameters are not available for this WLAN.

**Note 2:** One unique WEP Key Index can be applied to each WLAN. As there are only four WEP Key Indexes, only four WLANs can be configured for Static WEP Layer 2 encryption.

**Note 3:** When Cranite is selected as the Layer 2 security policy, no Layer 3 security policies are allowed.

 Layer 3 security is available via VPN Pass Through or IPSec. Check software availability and client hardware compatibility before implementing IPSec. Layer 3 IPSec parameters are described in the following table.

**Table -** Layer 3 IPSec Parameters

Parameter (Note 1)	Range
IPSec Authentication	None; HMAC MD5; HMAC SHA1.
IPSec Encryption	None; DES; Triple DES; AES CBC.
IKE Authentication	Certificates, Pre Shared Key, or XAuth Pre Shared Key (NoteS 2, 3).
IKE Phase 1	Aggressive or Main.
Lifetime	Timeout in seconds.
IKE Diffie-Hellman Group	Group 1, 2 or 5.

**Note 1:** You must have the optional Enhanced Security Module (crypto processor card) installed to enable IPSec. Verify it is installed on your Alcatel OmniAccess Switch or Appliance on the *Inventory* page.

**Note 2:** When you select IKE Authentication Pre Shared Key or XAuth Pre Shared Key, you must also enter a key.

**Note 3:** When you select XAuth Pre Shared Key, the key must be at least eight bytes to interoperate with Cisco clients. Other tested clients function with a key of less than eight bytes.

- When you select Layer 3 VPN Pass Through, fill in the VPN Gateway IPSec Pass Through Address.
- With VPN Pass Through, but not with IPSec, you may also enable Web Authentication, also known as Web Auth.
- When you have Web Auth enabled, you can also Select a Preauthentication ACL, which
  allows you to assign any of the Access Control List Names currently available on the <u>Access</u>
  <u>Control Lists</u> page.
- **Note:** To enable Web Auth, you MUST configure the Virtual Gateway Address in the <u>Interfaces</u> page.

- **< Back:** Return to the previous window.
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Switch Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance configuration details. Use the selector area to access specific Alcatel OmniAccess Switch or Appliance parameters. Making this selection from the menu bar opens the <u>General</u> page.

Access the following pages from the Switch Menu Bar Selection:

- General
- <u>Inventory</u>
- <u>Interfaces</u>
- <u>Interfaces > New</u>
- Interfaces > Edit
- <u>Network Routes</u>
- Network Routes > New
- Static Mobility Group Members
- <u>Mobility Group Member > New</u>
- <u>Mobility Group Member > Edit All</u>
- <u>Mobility Statistics</u>
- Switch Spanning Tree Configuration
- Ports
- <u>Ports > Configure</u>
- <u>Port > Configure</u>
- Master Switch Configuration

## General

Use **SWITCH/General** to navigate to this page.

The following tables explain the Alcatel OmniAccess Switch or Appliance configuration general parameters.

Table - Alcatel OmniAccess Switch or Appliance Configuration Parameters

Parameter	Description
802.3x Flow Control Mode	May be enabled or disabled by selecting the corresponding line on the pulldown entry field. The factory default is disabled.

 Table - Alcatel OmniAccess Switch or Appliance Configuration Parameters (Continued)

Parameter	Description
LWAPP Transport Mode	Layer 2 or Layer 3 Lightweight Access Point Protocol transport mode. When set to Layer 3, the LWAPP uses IP addresses to communicate with the OmniAccess APs; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the LWAPP uses proprietary code to communicate with the OmniAccess APs.  Use the <b>Save Configuration</b> Administrative Tool to save the configuration after changing this parameter. Then use the <u>System Reboot</u> page to restart the Alcatel OmniAccess Switch or Appliance with a configuration save after changing this parameter.
Ethernet Multicast Support	Enable or disable multicast support.
Aggressive Load Balancing	Enable or disable aggressive load balance algorithm.
Broadcast SSID	Enable or disable to start or stop SSID broadcasts. Note that you must disable 802.11a, 802.11b, and 802.11g global before changing this value.
Peer to Peer Blocking Mode	Enable or disable peer to peer blocking mode. Disabled (default) allows same-subnet clients to communicate through the Alcatel OmniAccess Switch or Appliance. Enable forces same-subnet clients to communicate through a higher-level router.
Over the Air Provisioning of AP	Enable or disable over-the-air OmniAccess AP and Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R) configuration.
RF Mobility Domain Name	Operator-defined Mobility Group Name. Refer to the <u>Alcatel Mobility Group</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
User Idle Timeout	Set time out for idle clients in seconds. The factory default is 300. When timeout expires, client loses authentication, briefly disassociates from the OmniAccess AP, reassociates, and re-authenticates.
ARP Timeout	Timeout in seconds for the Address Resolution Protocol. The factory default is 300.

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# Inventory

Use **SWITCH/Inventory** to navigate to this page.

This page identifies Alcatel product information assigned by the manufacturer. These read-only fields are described in the following table.

**Table - Inventory Parameters** 

Parameter	Description
System Description	Product name of this Alcatel OmniAccess Switch or Appliance.
Machine Model	Specifies the Machine Model as defined by the factory.
Serial Number	Unique Serial Number for this Alcatel OmniAccess Switch or Appliance.
Burned-in MAC Address	The burned-in Medium Access Control address for this Alcatel OmniAccess Switch or Appliance.
Gig Ethernet/Fiber Card	Displays the presence or absence of the optional 1000Base-T/ 1000Base-SX GigE card.
Crypto Accelerator	Displays the presence or absence of an optional Enhanced Security Module (Crypto card) which enables IPSec security and which provides enhanced processing power.

• **Help:** Request that the help page be displayed in a new browser window.

## Interfaces

Use **SWITCH/Interfaces** to navigate to this page.

The following table shows Alcatel OmniAccess Switch or Appliance interface general parameters.

To edit the parameters for an interface, select the **Edit** link (*Interfaces > Edit*).

Remove an interface by selecting the appropriate **Remove** link. You are prompted for confirmation of the interface removal.

Table - Alcatel OmniAccess Switch or Appliance Interface Parameters

Parameter	Description
Interface Name	Name of the interface:  • management 802.11 Distribution System wired network.  • service-port System Service (management) interface.  • virtual Unused IP address used as the Virtual Gateway Address.  • ap-manager Only used when the LWAPP protocol is run across Layer 3. Can be on the same subnet as the management IP address, but must have a different IP address than the management interface.  • <name> An Operator-Defined Interface assignment, without any spaces.</name>
VLAN Identifier	Virtual LAN assignment of the interface.
IP Address	The IP address of the Alcatel OmniAccess Switch or Appliance and its distribution port.

 Table - Alcatel OmniAccess Switch or Appliance Interface Parameters (Continued)

Parameter	Description
Interface Type	Static - Configured with a static IP address.  Dynamic - Obtain an IP address from a DHCP server.

- New: Click to add a new interface.
- **Help:** Request that the help page be displayed in a new browser window.

### Interfaces > New

Use **SWITCH/Interfaces** then **New...** to navigate to this page.

Add a new Alcatel OmniAccess Switch or Appliance Operator-Defined Interface by adding the following parameters:

- Interface Name Enter the name of the new Operator-Defined Interface, without any spaces.
- VLAN Id Enter the VLAN identifier for this new interface.

Click **Apply** to display the <u>Interfaces > Edit</u> page and continue configuring the new Operator-Defined Interface.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

### Interfaces > Edit

Use **SWITCH/Interfaces** then **Edit** or **SWITCH/Interfaces**, **New...**, and **Apply** to navigate to this page.

The top of this page displays the **Interface Name**, and may include the interface **MAC Address**. Edit Alcatel OmniAccess Switch or Appliance Management, VLAN, Service port, Virtual, and AP-Manager interfaces as described in the following tables.

Table - Alcatel OmniAccess Switch or Appliance Management or Operator-Defined Interface Parameters

Parameter	Description
VLAN Identifier	Virtual LAN assigned to the interface.
IP Address	The IP address of the Alcatel OmniAccess Switch or Appliance and its distribution port.
Netmask	Interface subnet mask.
Gateway	Interface gateway router IP address.
Port Number	The Alcatel OmniAccess Switch or Appliance physical port for this interface.

Table - Alcatel OmniAccess Switch or Appliance Management or Operator-Defined Interface Parameters

Parameter	Description
Primary DHCP Server	The interface uses this DHCP server first to obtain an IP address.
Secondary DHCP Server	The interface uses this DHCP server as a backup to obtain an IP address.
ACL Name	Any of the Access Control List Names currently available on the Access Control Lists page.

Table - Alcatel OmniAccess Switch or Appliance Service Port Interface Parameters

Parameter	Description
DHCP Protocol	Whether or not the Service port uses a DHCP server to obtain an IP address.
IP Address	The IP address of the Alcatel OmniAccess Switch or Appliance front-panel Service port.
Netmask	Service Port subnet mask.
Note: The service port cannot be configured with the same IP address or on the same subnet as the	

**Note:** The service port cannot be configured with the same IP address or on the same subnet as the network distribution system.

Table - Alcatel OmniAccess Switch or Appliance Virtual Interface Parameters

Parameter	Description
IP Address	Gateway IP address. Any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers. Reboot the Alcatel OmniAccess Switch or Appliance to have this change take effect.
DNS Host Name	Gateway host name. Used by Layer 3 Security and Mobility managers to verify the source of certificates when Web Auth is enabled. Reboot the Alcatel OmniAccess Switch or Appliance to have this change take effect.

**Note:** You must configure the Virtual Gateway Address to enable Layer 3 Web Auth, configured on the  $\underline{WLANs} > \underline{Edit}$  page.

Table - Alcatel OmniAccess Switch or Appliance Layer 3 Access Point Management Interface Parameters

Parameter	Description
VLAN Identifier	Virtual LAN assigned to the interface.
IP Address	The IP address of the Alcatel OmniAccess Switch or Appliance Layer 3 LWAPP protocol manager. Note that this IP address cannot be the same as used by the Management Interface.
Netmask	Interface subnet mask.
Gateway	Interface gateway router IP address.
Port Number	The Alcatel OmniAccess Switch or Appliance physical port for this interface.
Primary DHCP Server	The interface uses this DHCP server first to obtain an IP address.
Secondary DHCP Server	The interface uses this DHCP server as a backup to obtain an IP address.
ACL Name	Any of the Access Control List Names currently available on the Access Control Lists page.

**Note:** You may only create a Layer 3 LWAPP Access Point manager after the Alcatel OmniAccess Switch or Appliance has been rebooted to use Layer 3 LWAPP protocol.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
  Applying Interface changes may cause WLANs to temporarily drop client connections. You will be prompted to confirm the changes if this is the case.
- Help: Request that the help page be displayed in a new browser window.

### **Network Routes**

Use **SWITCH/Network Routes** to navigate to this page.

This page provides a summary of existing Service port Network Routes to Network or Element Management systems on a different subnet by **IP Address**, **IP Netmask**, and **Gateway IP Address**.

Remove a Network Route by selecting the appropriate **Remove** link. You are prompted for confirmation of the Network Route removal.

### **Command Buttons**

- New: Select to add a new Network Route.
- **Help:** Request that the help page be displayed in a new browser window.

### **Network Routes > New**

Use **SWITCH/Network Routes** then **New...** to navigate to this page.

Add a new Network Route for the Service port by entering the Route:

- **IP Address**
- **IP Netmask**
- Gateway IP Address

#### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Static Mobility Group Members**

Use **SWITCH/Mobility Management/Mobility Groups** to navigate to this page.

This page lists existing Mobility Group members by MAC Address and IP Address, and also indicates whether the Mobility Group member is Local (this Alcatel OmniAccess Switch or Appliance) or remote (any other Mobility Group member). The first entry is the local Alcatel OmniAccess Switch or Appliance, which cannot be deleted. The following entries are other Alcatel OmniAccess Switch or Appliance in the mobility group, that can be deleted at any time using the **Remove** link. Note that you can ping any of the Static Mobility Group Members using the Ping link.

The RF Mobility Group Domain Name is set on the *General* page.

For more information on mobility groups, refer to the Alcatel Mobility Group section in the Alcatel Omni-Access Wireless Product Guide.

#### **Command Buttons**

- New: Select to add a new Mobility Group member.
- Edit All: Display the Mobility Group Member > Edit All page.
- **Help:** Request that the help page be displayed in a new browser window.

### **Mobility Group Member > New**

Use **SWITCH/Mobility Management/Mobility Groups** then **New...** to navigate to this page.

This page allows you to add Mobility Group members by IP Address and MAC Address. For more information on mobility groups, refer to the Alcatel Mobility Group section in the Alcatel OmniAccess Wireless Product Guide.

#### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Mobility Group Member > Edit All**

Use SWITCH/Mobility Management/Mobility Groups then Edit All to navigate to this page.

This page allows you to edit all the existing Mobility Group members' **MAC Addresses** and **IP Addresses** in a text box, and then to cut and paste all the entries from one Alcatel OmniAccess Switch or Appliance to the other Alcatel OmniAccess Switches and Appliances in the Mobility Group.

You can edit existing entries and/or paste new entries directly into the box. In all cases, leave one space between the MAC address and IP address on each line.

The text box on this page makes it easy to avoid data-entry errors while copying the Mobility Group Members List to all the Alcatel OmniAccess Switches and Appliances in the same mobility group:

- Notice that the text box starts with the local Alcatel OmniAccess Switch or Appliance MAC address and IP address.
- 2. In the text box, add the MAC addresses and IP addresses for the rest of the Alcatel OmniAccess Switches and Appliances in the same geographical location (such as a campus or building) you want to add to the Static Mobility Group.
- 3. When you have added all the Alcatel OmniAccess Switch and Appliance MAC addresses and IP addresses to the Static Mobility Group, you can cut and paste the complete list into the corresponding boxes in the <u>Mobility Group Member > Edit All</u> pages in other mobility group member Alcatel OmniAccess Switch or Appliance Web Browser Interfaces.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Mobility Statistics**

Use **SWITCH/Mobility Management/Mobility Statistics** to navigate to this page.

This page displays the statistics for Mobility Group events, and is divided into three sections: Global Mobility Statistics, Mobility Initiator Statistics, and Mobility Responder Statistics.

- Global Statistics are those that affect all mobility transactions.
- Mobility Initiator Statistics are those that are generated by an Alcatel OmniAccess Switch or Appliance initiating the mobility event.
- Mobility Responder Statistics are those generated by an Alcatel OmniAccess Switch or Appliance responding to a mobility event.

The following tables list parameters and descriptions or each of these Statistics:

Table - Global Mobility Statistics

Parameter	Description
Rx Errors	Generic protocol packet receive errors, such as packet too short or format incorrect.
Tx Errors	Generic protocol packet transmit errors, such as packet transmission fail.

Table - Global Mobility Statistics (Continued)

Parameter	Description
Responses Retransmitted	The Mobility protocol uses UDP and it resends requests several times if it doesn't receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This is a count of the response resends.
Handoff Requests Received	Total number of handoff requests received, ignored or responded.
Handoff End Requests Received	Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.
State Transitions Disallowed	PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.

**Table - Mobility Initiator Statistics** 

Parameter	Description
Handoff Requests Sent	Number of client clients that have associated with an Alcatel OmniAccess Switch or Appliance and have been 'announced' to the mobility group.
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.
Handoff Denys Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. Handoff was received from another foreign and the new Alcatel OmniAccess Switch or Appliance is requesting the anchor to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.

Table - Mobility Initiator Statistics (Continued)

Parameter	Description
Anchor Transfer Received	Number of anchor requests that 'closed' the session on the current anchor and transferred the anchor back to the requestor.

Table - Mobility Responder Statistics

Parameter	Description
Handoff Requests Ignored	Number of handoff requests/client announces that were ignored. The Alcatel OmniAccess Switch or Appliance simply had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 sec).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the 'local' role.
Client Handoff as Foreign	Number of handoffs responses sent while in the 'foreign' role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client has moved from a foreign Alcatel OmniAccess Switch or Appliance to an Alcatel OmniAccess Switch or Appliance on the same subnet as the current anchor.

- Clear Stats: Deletes all Mobility statistics entries.
- **Help:** Request that the help page be displayed in a new browser window.

# **Switch Spanning Tree Configuration**

Use **SWITCH/Spanning Tree** to navigate to this page.

The Spanning Tree Protocol (STP) is a link management protocol. Alcatel implements the IEEE 802.1D standard for media access control bridges.

Using the spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time

between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

This page allows you to Enable or Disable the Spanning Tree Algorithm, modify its characteristics and view statistics as described in the following tables.

Table - STP Parameters

Parameter	Description
Spanning Tree Algorithm	Specifies if this Alcatel OmniAccess Switch or Appliance participates in the spanning tree protocol. May be enabled or disabled by selecting the corresponding line on the pulldown entry field. The factory default is disabled.
Priority	The value of the writable portion of the Bridge ID, i.e., the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535. The factory default is 32768.
Maximum Age (seconds)	The value that all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (seconds)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Forward Delay (seconds)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. Valid values are 4 through 30 seconds. The Factory default is 15.
Spanning Tree Specification	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version a new value will be defined.

Table - STP Statistics

Parameter	Description
Base MAC Address	The MAC address used by this bridge when it must be referred to in a unique fashion. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Table - STP Statistics (Continued)

Parameter	Description	
Time Since Topology Changed	The time (in days, hours, minutes and seconds) since the last time a topology change was detected by the bridge entity.	
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.	
Root Port	The port number of the port that offers the lowest cost path from this bridge to the root bridge.	
Root Cost	The cost of the path to the root as seen from this bridge.	
Max Age (seconds)	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.	
Hello Time (seconds)	The amount of time between the transmission of Configuration Bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so. This is the actual value that this bridge is currently using.	
Forward Delay (seconds)	This time value controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, that precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. [This value is the one that this bridge is currently using, in contrast to Stp Bridge Forward Delay that is the value that this bridge and all others would start using if/when this bridge were to become the root.]	
Hold Time (seconds)	The minimum time period to elapse between the transmission of Configuration BPDUs through a given LAN Port: at most one Configuration BPDU shall be transmitted in any Hold Time period.	

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **Ports**

Use **SWITCH/Ports** to navigate to this page.

This page displays the status of each physical port on the Alcatel OmniAccess Switch or Appliance, and also indicates whether **Port Mirroring** is enabled or disabled. The following table provides a description and the range for each parameter.

**Table - Summary Parameters** 

Parameter	Description	Range
Port No	Port number on the Alcatel OmniAccess Switch or Appliance.	<ul> <li>1 to 12 for 4012, and 13 for optional 1000Base-T or 1000Base-SX module</li> <li>1 to 24 for 4024, and 25 for optional 1000Base-T or 1000Base-SX module</li> <li>1 for 4102 1000Base-SX ports</li> </ul>
STP Status	State of the Spanning Tree Protocol Administrative Mode associated with the port.	<ul><li>Enabled</li><li>Disabled</li><li>Forwarding</li></ul>
Admin Mode	Displays the state of the port.	Enable     Disable
Physical Mode	Displays the configuration of the port physical interface.	<ul><li>Auto</li><li>100 Mbps Full Duplex</li><li>100 Mbps Half Duplex</li><li>10 Mbps Full Duplex</li><li>10 Mbps Half Duplex</li></ul>
Physical Status	Displays the actual port physical interface.	<ul><li>Auto</li><li>100 Mbps Full Duplex</li><li>100 Mbps Half Duplex</li><li>10 Mbps Full Duplex</li><li>10 Mbps Half Duplex</li></ul>
Link Status	Displays the status of the link.	Link Up     Link Down
Link Trap	Displays if the port is set to send a trap when link status changes.	Enable     Disable
POE	Displays status of Power over Ethernet functionality.	Enable     Disable

The physical mode and status may reflect different values depending on the link status. For example, the physical mode may be set to "Auto" while the actual link is running at "10 Mbps Half Duplex".

To edit global parameters across all ports, click the **ConfigureAll** command button to open the <u>Ports > Configure</u> page.

To edit the parameters for a single port, select the **Edit** link for the port you wish to configure. This brings up a <u>Port > Configure</u> page.

### **Command Buttons**

- **ConfigureAll:** Open the Global Port configuration data page.
- **Help:** Request that the help page be displayed in a new browser window.

# **Ports > Configure**

Use **SWITCH/Ports** then **ConfigureAll** to navigate to this page.

This page allows you to change the parameters of all front-panel physical ports on the Alcatel Omni-Access Switch or Appliance simultaneously. The following table describes these parameters.

**Table - Port Configuration Details** 

Parameter	Description	Range
Admin Mode	Sets the state of all ports to	Don't Apply, Enable or Disable.
Physical Mode	Sets the physical mode of all ports.	<ul> <li>Don't Apply</li> <li>Auto</li> <li>100 Mbps Full Duplex</li> <li>100 Mbps Half Duplex</li> <li>10 Mbps Full Duplex</li> <li>10 Mbps Half Duplex</li> <li>10 Mbps Half Duplex</li> </ul>
Link Trap	Sets all ports to send or not to send a trap when link status changes. The factory default is Don't Apply.	
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port. The possible values are:	<ul> <li>Don't Apply</li> <li>802.1D - all ports participate in the spanning tree and goes through all of the spanning tree states when the link state transitions from Down to Up.</li> <li>Off - spanning tree is disabled for all ports.</li> <li>Fast - all ports participate in the spanning tree and are put in the forwarding state when the link state transitions from Down to Up faster than when STP Mode is 802.1D. In this state, the Forwarding Delay timer is ignored on Link Up.</li> </ul>

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Port > Configure**

Use **SWITCH/Ports** then **Edit...** to navigate to this page.

This page allows you to change the parameters of a single physical port on the Alcatel OmniAccess Switch or Appliance. The following table describes these parameters.

**Table -** General Port Configuration

Parameter	Description	Range
Port No	Identifies the current port.	<ul> <li>1 to 12 for 4012, and 13 for optional 1000Base-T or 1000Base-SX module</li> <li>1 to 24 for 4024, and 25 for optional 1000Base-T or 1000Base-SX module</li> <li>1 for 4102 1000Base-SX ports</li> </ul>
Admin Mode	Sets the state of the port.	Enable     Disable
Mirror Mode	Sets the Port Mirroring mode, as described in the Alcatel OmniAccess Wireless Product Guide.	Enable     Disable
Physical Mode	Sets the physical mode of the port.	<ul> <li>Auto</li> <li>100 Mbps Full Duplex</li> <li>100 Mbps Half Duplex</li> <li>10 Mbps Full Duplex</li> <li>10 Mbps Half Duplex</li> </ul>
Physical Status	Displays the current physical port interface status.	<ul><li>100 Mbps Full Duplex</li><li>100 Mbps Half Duplex</li><li>10 Mbps Full Duplex</li><li>10 Mbps Half Duplex</li></ul>
Link Status	Displays the status of the link.	Link Up     Link Down
Link Trap	Sets port to send or not to send a trap when link status changes. The factory default is enabled.	Enable     Disable
Power over Ethernet (PoE)	Detects if connecting device is equipped to receive power via the Ethernet cable and if so provides -48 VDC per 802.3af. (Note.)	<ul><li>Enable</li><li>Disable</li></ul>

**Note:** Some Cisco APs **do not conform** to the 802.3af specification. Some older Cisco APs do not draw PoE, even if it is enabled on the Alcatel OmniAccess Switch or Appliance port. Please contact Alcatel Technical Support.

**Table - Spanning Tree Protocol Configuration** 

Parameter	Description
STP Port ID	The port number of the port for which this entry contains Spanning Tree Protocol management information.

Table - Spanning Tree Protocol Configuration (Continued)

Parameter	Description
STP Mode	<ul> <li>The Spanning Tree Protocol Administrative Mode associated with the port or trunk. The possible values are:</li> <li>802.1D - this port participates in the spanning tree and goes through all of the spanning tree states when the link state transitions from Down to Up.</li> <li>Fast - this port participates in the spanning tree and is put in the forwarding state when the link state transitions from Down to Up faster than when STP Mode is 802.1D. In this state, the Forwarding Delay timer is ignored on Link Up.</li> <li>Off - spanning tree is disabled for this port. This is also referred to as manual spanning tree.</li> </ul>
STP State	The port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning it places that port into the broken state. For ports disabled by Spanning Tree mode, this object has a value of disabled. The valid values are:  • Disabled • Blocking • Listening • Learning • Forwarding • Broken
STP Port Designated Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
STP Port Designated Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received Bridge PDUs.
STP Port Designated Bridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
STP Port Designated Port	The Port Identifier of the port on the Designated Bridge for this port's segment.
STP Port Forward Transitions Count	The number of times this port has transitioned from the Learning state to the Forwarding state.
STP Port Priority	The value of the priority field contained in the first (in network byte order) octet of the (2 octet long) Port ID. The other octet of the Port ID is given by the value of the Port id. Valid values are from 0 to 255. The factory default is 128.
STP Port Path Cost Mode	Auto (use the STP Port Path Cost parameter) or User Configured.

**Table - Spanning Tree Protocol Configuration (Continued)** 

Parameter	Description
STP Port Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root that includes this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. Valid values are from 0 to 65535. The factory default is 0, which means the cost is adjusted for the speed of the port when the link comes up. The value used is 100 for 10 Mbps ports, and 19 for 100 Mbps ports.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Master Switch Configuration**

Use **SWITCH/Master Switch Mode** to navigate to this page.

This page enables the Alcatel OmniAccess Switch or Appliance to be configured as the Master Alcatel OmniAccess Switch or Appliance for your Alcatel OmniAccess Wireless Access Points connected in Appliance Mode, as described in the Alcatel OmniAccess Wireless Product Guide. When there is a Master Alcatel OmniAccess Switch or Appliance enabled, all newly-added OmniAccess APs with no Primary Alcatel OmniAccess Switch or Appliance assigned associate with the Master Alcatel OmniAccess Switch or Appliance on the same subnet. This allows the operator to verify the OmniAccess AP configuration and assign a Primary Alcatel OmniAccess Switch or Appliance to the OmniAccess AP using the Omni-Access APs > Details page.



Note: The Master Alcatel OmniAccess Switch or Appliance is normally used only while adding new OmniAccess APs to the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel Omni-Access Wireless System). When no more OmniAccess APs are being added to the network. Alcatel recommends that you disable the Master Alcatel OmniAccess Switch or Appliance.

Refer to the Alcatel OmniAccess Switch and Appliance Failover Protection section in the Alcatel Omni-Access Wireless Product Guide for more information.

#### **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# Wireless Menu Bar Selection

This menu bar selection provides access to the Alcatel wireless network configuration details. Use the selector area to access specific wireless network parameters. Making this selection from the menu bar opens the *OmniAccess APs* page.

Access the following pages from the Wireless Menu Bar Selection:

- OmniAccess APs
- OmniAccess APs > Details
- 802.11a OmniAccess Radios
- 802.11a OmniAccess Radios > Configure
- 802.11 AP Interfaces > Performance Profile
- 802.11a AP Interfaces > Details
- 802.11b/g OmniAccess Radios
- 802.11b/g OmniAccess Radios > Configure
- <u>802.11b/g AP Interfaces > Details</u>
- <u>Third-Party APs</u>
- Third-Party APs > New
- Roque APs
- Clients
- 802.11a Global Parameters
- 802.11a Global Parameters > Auto RF
- 802.11b/g Global Parameters
- 802.11b/g Global Parameters > Auto RF
- <u>Country</u>
- <u>Timers</u>

#### **OmniAccess APs**

Use WIRELESS/Access Points/OmniAccess APs or MONITOR/Summary/OmniAccess APs Detail to navigate to this page.

This page displays OmniAccess APs associated with this Alcatel OmniAccess Switch or Appliance. For details on a particular OmniAccess AP, select the **Detail** link to open the <u>OmniAccess APs > Details</u> page for that OmniAccess AP.

Table - OmniAccess AP Summary

Parameter	Description
AP Name	Customer definable name of the OmniAccess AP.
AP ID	Identification number automatically assigned by the Alcatel OmniAccess Switch or Appliance when the OmniAccess AP is configured.
MAC Address	Media Access Control Address of the OmniAccess AP.

Table - OmniAccess AP Summary (Continued)

Parameter	Description
Admin Status	Administration state of the OmniAccess AP is either enabled or disabled.
Operational Status	Operational status of the OmniAccess AP is either registered (REG) or not registered (DEREG).
Port Number	OmniAccess AP is connected to this Alcatel OmniAccess Switch or Appliance port.

• **Help:** Request that the help page be displayed in a new browser window.

# **OmniAccess APs > Details**

Use WIRELESS/Access Points/OmniAccess APs and then Detail to navigate to this page.

This page shows the details of the selected OmniAccess AP including the hardware, Alcatel Wireless Operating System software and boot version details.

Table - General Details

Parameter	Description
AP Name	Set the customer definable name of the OmniAccess AP.
AP MAC Address	Media Access Control of the OmniAccess AP.
AP IP Address	IP address of the OmniAccess AP.
AP ID	Identification number automatically assigned by the Alcatel OmniAccess Switch or Appliance when the OmniAccess AP is configured.
Admin Status	Set the administration state of the OmniAccess AP to either enabled or disabled.
AP Mode	Set the OmniAccess AP operation to Local (normal operation), Monitor (monitor-only mode), or OmniAccess AP 1200R. In order for Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) to operate correctly, this must be set to OmniAccess AP 1200R.
Mirror Mode	Port Mirroring mode, either enabled or disabled, as described in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
Operational Status	The operational status of the OmniAccess AP comes up as either registered (REG) or not registered (DEREG) automatically by the Alcatel OmniAccess Switch or Appliance.
Port Number	The OmniAccess AP is connected to this Alcatel OmniAccess Switch or Appliance port.
Location	Customer-definable location name for the OmniAccess AP.

Table - General Details (Continued)

Parameter	Description
Primary Switch Name	This is the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance SNMP name. The OmniAccess AP attempts to associate with this Alcatel OmniAccess Switch or Appliance first for all network operations and in the event of a hardware reset (Note).
Statistics Timer	This counter sets the time in seconds that the OmniAccess AP sends its DOT11 statistics to the Alcatel OmniAccess Switch or Appliance.

**Note:** After the OmniAccess AP is reset, it attempts to connect with its Primary Alcatel OmniAccess Switch or Appliance as configured on this page. If the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance is not available, it searches for the Master Alcatel OmniAccess Switch or Appliance (*Master Switch Configuration*) and finally the least loaded Alcatel OmniAccess Switch or Appliance on the network.

Table - AP Interface Details

Parameter	Description
Number of interfaces	One or Two 802.11a and/or 802.11b/g interfaces.
Interface Type	Displays the OmniAccess Radio type: either 802.11a or 802.11b/g.
Admin Status	Displays the OmniAccess Radio interface status: either enabled or disabled.
Oper Status	Displays the OmniAccess Radio operational status: either UP or DOWN.

#### **Hardware Reset Button**

Click the Reset AP Now button to reset the OmniAccess AP.

#### **Versions**

Displays the Alcatel Wireless Operating System Software and Boot ROM versions.

#### **Inventory Information**

- Displays the OmniAccess AP Model Number.
- Displays the OmniAccess AP Serial Number.
- Displays whether or not OmniAccess AP 1200R (Alcatel OmniAccess Remote Edge Access Point)
   Mode is supported.

#### **Set to Factory Defaults Button**

Click the Clear Config button to reset the OmniAccess AP parameters to the factory defaults.

### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# 802.11a OmniAccess Radios

Use WIRELESS/Access Points/802.11a Radios to navigate to this page.

This page displays an overview of your 802.11a OmniAccess Radio network. The status of each 802.11a OmniAccess Radio configured on this Alcatel OmniAccess Switch or Appliance and its profile as detailed in the following table.

Table - 802.11a OmniAccess Radio Summary

Parameter	Description
AP Name	Set the customer definable name of the OmniAccess AP.
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Channel Number	Channel number of the OmniAccess AP.
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Antenna	Internal or external antennas.
Diversity	Diversity enabled or external antennas identified by connectors.

Details for each OmniAccess Radio may be accessed by selecting the Configure or Details link located next to the OmniAccess Radio summary.

- The Configure link opens a list of configurable parameters for the identified OmniAccess Radio (802.11a OmniAccess Radios > Configure).
- The **Details** link opens a list of primarily read-only OmniAccess Radio attributes (802.11a AP Interfaces > Details).

### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

# 802.11a OmniAccess Radios > Configure

Use WIRELESS/Access Points/802.11a Radios and then Configure to navigate to this page.

This page allows you to configure parameters specifically for this OmniAccess Radio including antenna type, RF channel and Tx power level assignments. The performance profile for this OmniAccess Radio is also accessed through this page. Reference the following tables for these parameters.

Table - 802.11a General Parameters

Parameter	Description
AP Name	Set the customer definable name of the OmniAccess AP.
Admin Status	Set the interface status to either enabled or disabled.

Table - 802.11a General Parameters (Continued)

Parameter	Description
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Site Config ID	Site identification number.

#### Table - Antenna

Parameter	Description
Antenna Type	Internal.
Antenna Mode	Sector A, Sector B, or OMNI ( = Sector A and Sector B).

### Table - WLAN Override

Parameter	Description
WLAN Override	Enable or disable WLAN Override for this 802.11a OmniAccess Radio.

Note: When you enable WLAN Override, the Alcatel Wireless Operating System displays a table showing all current Alcatel WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a OmniAccess Radio.

Table - RF Channel Assignment

Parameter	Description
Current Channel	Channel number of the OmniAccess AP.
Assignment Method	Channels may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally using the custom option.

Note: The assignment method should normally be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the channel number as determined by the OmniVista AirView Software.

Table - Tx Power Level Assignment

Parameter	Description
Current Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.

Table - Tx Power Level Assignment (Continued)

Parameter	Description
Assignment Method	Transmit power may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally using the custom option.

**Note:** The assignment method should be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the transmit power level based on the OmniVista AirView Software.

Use the **Performance Profile** button to view and edit the Performance Profile for this OmniAccess AP (802.11 AP Interfaces > Performance Profile).

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### 802.11 AP Interfaces > Performance Profile

Use WIRELESS/Access Points/802.11a Radios or WIRELESS/Access Points/802.11b/g Radios, Configure and then Performance Profile to navigate to this page.

This page shows the details of the performance profile of the selected OmniAccess Radio. The profile parameters are detailed in the following table and should be enabled for global control.

Table - 802.11 General Parameters

Parameter	Description
Interface Type	Displays the OmniAccess Radio type: 802.11a or 802.11b/g.
AP Name	Displays the customer definable name of the OmniAccess AP.
AP ID	Displays the OmniAccess AP identification number automatically assigned by the Alcatel OmniAccess Switch or Appliance.
Profile Parameters Globally Controlled	<b>Note:</b> You cannot change the following parameters if the Profile Parameters Globally Controlled checkbox is selected.
Interference (0 to 100%)	Foreign 802.11a or 802.11b/g interference threshold between 0 and 100 percent. Globally set on 802.11a Global Parameters > Auto RF and 802.11b/g Global Parameters > Auto RF pages.
Clients (1 to 75)	Client threshold between 1 and 75 clients. Globally set on <u>802.11a Global Parameters &gt; Auto RF</u> and <u>802.11b/g Global Parameters &gt; Auto RF</u> pages.
Noise (-127 to 0 dBm)	Noise threshold between -127 and 0 dBm. Globally set on <u>802.11a Global Parameters &gt; Auto RF</u> and <u>802.11b/g Global Parameters &gt; Auto RF</u> pages.

Table - 802.11 General Parameters (Continued)

Parameter	Description
Coverage (3 to 50 dBm)	802.11a or 802.11b/g coverage threshold between 3 and 50 dBm. Globally set on 802.11a Global Parameters > Auto RF and 802.11b/g Global Parameters > Auto RF pages.
Utilization (0 to 100%)	802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent. Globally set on 802.11a Global Parameters > Auto RF and 802.11b/g Global Parameters > Auto RF pages.
Coverage Exception Level (0 to 100%)	Coverage exception level between 0 and 100 percent. Globally set on 802.11a Global Parameters > Auto RF and 802.11b/g Global Parameters > Auto RF pages.
Data Rate (1 to 1000 Kbps)	802.11a or 802.11b/g throughput threshold between 1 Kbps and 1000 Kbps. Globally set on 802.11a Global Parameters > Auto RF and 802.11b/g Global Parameters > Auto RF pages.
Client Min Exception Level (1 to 75)	Client minimum exception level. Globally set on <u>802.11a Global Parameters &gt; Auto RF</u> and <u>802.11b/g Global Parameters &gt; Auto RF</u> pages.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# 802.11a AP Interfaces > Details

Use WIRELESS/Access Points/802.11a Radios and then Details to navigate to this page.

This page lists primarily read-only attributes of the selected OmniAccess Radio.

Table - AP Details

Parameters	Description
Interface Type	Displays the OmniAccess Radio type as 802.11a.
AP Name	This is the name assigned to the OmniAccess AP.
AP ID	Identification number automatically assigned when the OmniAccess AP is configured.
Admin Status	Displays the interface status either enabled or disabled.
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Monitor Mode	Displays the OmniAccess AP Monitor mode: Local (normal operation), OmniAccess AP 1200R (Alcatel OmniAccess Remote Edge Access Point), or Monitor (monitor-only mode).
Location	Customer definable location.

**Table - Station Configuration Parameters** 

Parameters	Description
Configuration Type	Automatic or Custom.
Number of WLANs	1 (one) is the default.
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the OmniAccess AP.
Beacon Period	The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
Country String	Identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide.

Table - Operation Rate Set for 802.11a OmniAccess Radios

Parameter	Range (Note)
6000 Kilo Bits	Mandatory, Supported or Disabled.
9000 Kilo Bits	Mandatory, Supported or Disabled.
12000 Kilo Bits	Mandatory, Supported or Disabled.
18000 Kilo Bits	Mandatory, Supported or Disabled.
24000 Kilo Bits	Mandatory, Supported or Disabled.
36000 Kilo Bits	Mandatory, Supported or Disabled.
48000 Kilo Bits	Mandatory, Supported or Disabled.
54000 Kilo Bits	Mandatory, Supported or Disabled.

Table - Operation Rate Set for 802.11a OmniAccess Radios (Continued)

Parameter	Range (Note)
-----------	--------------

**Note:** The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network

If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match Client settings.

Table - Multi Domain Capability

Parameter	Description
Configuration Type	Automatic or Custom.
Implemented	TRUE indicates that the station implementation is capable of supporting multiple regulatory domains. FALSE indicates the capability is disabled.
Enabled	TRUE indicates that the capability of the station to operate in multiple regulatory domains is enabled. The capability is disabled if set to FALSE.
First Channel Number	The value of the lowest channel number in the subband for the associated domain country string.
Number of Channels	The value of the total number of channels allowed in the subband for the associated domain country string.

**Table - MAC Operation Parameters** 

Parameter	Description
Configuration Type	Automatic or Custom.
RTS Threshold	This attribute shall indicate the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size shall have the effect of turning off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero shall have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
Short Retry Limit	The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 7.

Table - MAC Operation Parameters (Continued)

Parameter	Description
Long Retry Limit	The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.
Fragmentation Threshold	The current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.
Max. Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.
Max Rx Life Time	The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Table - Tx Power

Parameter	Description
# Supported Power Levels	Five or fewer power levels, depending on operator preference.
Tx Power Level (1, highest through 5, lowest)	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, $2 = 50\%$ power, $3 = 25\%$ power, $4 = 12.5\%$ power, and $5 = 6.25\%$ power).
	Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Tx Power Configuration	Globally controlled or Customized for this OmniAccess AP.
Current Tx Power Level	Displays the operating transmit power level from the transmit power table.

**Table - Physical Channel Parameters** 

Parameter	Description
Current Channel	Current operating frequency channel.

Table - Physical Channel Parameters (Continued)

Parameter	Description
Configuration	Locally customized or globally controlled.
Current CCA Mode	<ul> <li>CCA method in operation. Valid values are:</li> <li>Energy detect only (edonly) = 01,</li> <li>Carrier sense only (csonly) = 02,</li> <li>Carrier sense and energy detect (edandcs) = 04</li> <li>Carrier sense with timer (cswithtimer) = 08</li> <li>High rate carrier sense and energy detect (hrcsanded) = 16.</li> </ul>
ED/TI Threshold	The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.

**Table - Physical Antenna Parameters** 

Parameter	Description
Antenna Type	Internal
Diversity	Enabled via the internal antennas or via either Connector A or Connector B.

Table - RF Recommendation Parameters

Parameter	Description
Channel	802.11a Low Band, Medium Band, and High Band     802.11b/g Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide.
Tx Power Level	0 if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled.
RTS/CTS Threshold	0 if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled. Refer to RTS Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.
Antenna Pattern	0 if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.

- < Back: Return to the previous window.
- **Help:** Request that the help page be displayed in a new browser window.

# 802.11b OmniAccess Radios

Use WIRELESS/Access Points/802.11b/g Radios to navigate to this page.

This page displays an overview of your 802.11b/802.11g OmniAccess Radio network. The status of each 802.11b/g OmniAccess Radio configured on this Alcatel OmniAccess Switch or Appliance and its profile as detailed in the following table.

Table - Alcatel 802.11b/g OmniAccess Radio Summary

Parameter	Description
AP Name	Set the customer definable name of the OmniAccess AP.
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Channel Number	Channel number of the OmniAccess AP. Note that only channels 1, 6, and 11 are non-overlapping.
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Antenna	Internal or external antennas.
Diversity	Diversity Enabled or external antennas identified by connectors.

Details for each OmniAccess Radio may be accessed by selecting the Configure or Details link located next to the OmniAccess Radio summary.

- The Configure link opens a list of configurable parliamentary for the identified OmniAccess Radio (802.11b/g OmniAccess Radios > Configure).
- The **Details** link opens a list of primarily read-only OmniAccess Radio attributes (802.11a AP Interfaces > Details)

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

# 802.11b/g OmniAccess Radios > Configure

Use WIRELESS/Access Points/802.11b/g Radios and then Configure to navigate to this page.

This page allows you to configure parameters specifically for this OmniAccess Radio including antenna type, RF channel and Tx power level assignments. The performance profile for this OmniAccess Radio is also accessed through this page. Reference the following tables for these parameters.

Table - General

Parameter	Description
AP Name	Displays the customer definable name of the OmniAccess AP.

# Table - General (Continued)

Parameter	Description
Admin Status	Set the interface status to either enabled or disabled.
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Site Config ID	Site identification number.

## Table - Antenna

Parameter	Description
Antenna Type	Internal or External.
Diversity	For internal antennas, Enable diversity, or select Side A for the front (door) antenna, or select Side B for the rear antenna.  For External antennas, Enable diversity, or select Right for the Right (Connector B) antenna, or select Left for the Left (Connector A) antenna.

#### Table - WLAN Override

Parameter	Description
WLAN Override	Enable or disable WLAN Override for this 802.11b/g OmniAccess Radio.

Note: When you enable WLAN Override, the Alcatel Wireless Operating System displays a table showing all current Alcatel WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11b/g OmniAccess Radio.

## Table - RF Channel Assignment

Parameter	Description	
Current Channel	Channel number of the OmniAccess AP. Note that only channels 1, 6, and 11 are non-overlapping.	
Assignment Method	Channels may be set either Globally by the Alcatel OmniAccess Switch or Appliance or locally using the Custom option.	

Note: The assignment method should normally be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the channel number based OmniVista AirView Software directives.

Table - Tx Power Level Assignment

Parameter	Description
Current Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Assignment Method	Transmit power may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally using the custom option.

Note: The assignment method should be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the transmit power level based on the OmniVista AirView Software.

Use the **Performance Profile** button to view and edit the Performance Profile for this OmniAccess AP on the <u>802.11 AP Interfaces > Performance Profile</u> page.

#### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# 802.11b/g AP Interfaces > Details

Use WIRELESS/Access Points/802.11b/g Radios and then Details to navigate to this page.

This page lists primarily read-only attributes of the selected OmniAccess Radio.

Table - AP Details

Parameters	Description
Interface Type	Displays the OmniAccess Radio type as 802.11b/g.
AP Name	This is the name assigned to the OmniAccess AP.
AP ID	Identification number automatically assigned when the OmniAccess AP is configured.
Admin Status	Displays the interface status either enabled or disabled.
Operational Status	Displays the OmniAccess Radio operational status: either UP or DOWN.
Monitor Mode	Displays the OmniAccess AP Monitor mode: Local (normal operation), OmniAccess AP 1200R (Alcatel OmniAccess Remote Edge Access Point), or Monitor (monitor-only mode).

Table - AP Details (Continued)

Parameters	Description
Location	Customer definable location.

**Table -** Station Configuration Parameters

Parameters	Description
Configuration Type	Automatic or Custom.
Number of WLANs	1 (one) is the default.
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
BSSID	MAC address of the OmniAccess AP.
Beacon Period	The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
Country String	Identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide.

Table - Operation Rate Set for 802.11b/g OmniAccess Radios

Parameter	Band	Range (Note)
1000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported or Disabled.
2000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported or Disabled.
5500 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported or Disabled.
11000 Kilo Bits	802.11b or 802.11g.	Mandatory, Supported or Disabled.
6000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
9000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
12000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.

Table - Operation Rate Set for 802.11b/g OmniAccess Radios (Continued)

Parameter	Band	Range (Note)
18000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
24000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
36000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
48000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.
54000 Kilo Bits	802.11g only.	Mandatory, Supported or Disabled.

Note: The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network.

If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. Each data rate can also be set to Disabled to match Client settings.

Table - Multi Domain Capability

Parameter	Description
Configuration Type	Automatic or Custom.
Implemented	TRUE indicates that the station implementation is capable of supporting multiple regulatory domains. FALSE indicates the capability is disabled.
Enabled	TRUE indicates that the capability of the station to operate in multiple regulatory domains is enabled. The capability is disabled if set to FALSE.
First Channel Number	The value of the lowest channel number in the subband for the associated domain country string.
Number of Channels	The value of the total number of channels allowed in the subband for the associated domain country string.

**Table - MAC Operation Parameters** 

Parameter	Description
Configuration Type	Automatic or Custom.

Table - MAC Operation Parameters (Continued)

Parameter	Description
RTS Threshold	This attribute shall indicate the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size shall have the effect of turning off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero shall have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
Short Retry Limit	The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 7.
Long Retry Limit	The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.
Fragmentation Threshold	The current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.
Max. Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.
Max Rx Life Time	The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Table - Tx Power

Parameter	Description
# Supported Power Levels	Five or fewer power levels, depending on operator preference.

Table - Tx Power (Continued)

Parameter	Description
Tx Power Level (1, highest through 5, lowest)	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, $2 = 50\%$ power, $3 = 25\%$ power, $4 = 12.5\%$ power, and $5 = 6.25\%$ power).
	Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Tx Power Configuration	Globally controlled or Customized for this OmniAccess AP.
Current Tx Power Level	Displays the operating transmit power level from the transmit power table.

Table - Physical Channel Parameters

Parameter	Description
Current Channel	Current operating frequency channel.
Configuration	Locally customized or globally controlled.
Current CCA Mode	<ul> <li>CCA method in operation. Valid values are:</li> <li>Energy detect only (edonly) = 01,</li> <li>Carrier sense only (csonly) = 02,</li> <li>Carrier sense and energy detect (edandcs) = 04</li> <li>Carrier sense with timer (cswithtimer) = 08</li> <li>High rate carrier sense and energy detect (hrcsanded) = 16.</li> </ul>
ED/TI Threshold	The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.

Table - Physical Antenna Parameters

Parameter	Description
Antenna Type	Internal
Diversity	Enabled via the internal antennas or via either Connector A or Connector B.

Table - RF Recommendation Parameters

Parameter	Description
Channel	<ul> <li>802.11a Low Band, Medium Band, and High Band</li> <li>802.11b/g</li> <li>Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.</li> </ul>
Tx Power Level	0 if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled.
RTS/CTS Threshold	O if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled. Refer to RTS Threshold in MAC Operation Parameters above.
Fragmentation Threshold	0 if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.
Antenna Pattern	0 if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.

- < Back: Return to the previous window.</li>
- **Help:** Request that the help page be displayed in a new browser window.

# **Third-Party APs**

Use **WIRELESS/Access Points/Third Party APs** to navigate to this page. Refer to <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information.

This page lists the Cisco 1200, Cisco 350 and ORINOCO 2000 Access Points directly connected to your 4012 or 4024 OmniAccess Wireless Switch, listed by:

- AP MAC address.
- Interface Number, or front-panel port number.
- IP Address -- Blank if obtaining IP address from a DHCP server.
- Whether 802.1X is enabled or disabled.

Click an **Edit** link to go to the *Third-Party APs > Edit* page.

Click **Remove** to remove a third-party AP from the Alcatel Wireless Operating System database.

### **Command Buttons**

- New: Select to add a new third-party access point (Third-Party APs > New).
- **Help:** Request that the help page be displayed in a new browser window.

# **Third-Party APs > New**

Use WIRELESS/Access Points/Third Party APs and then New... to navigate to this page.

Use this page to enter the Cisco 1200, Cisco 350 and ORiNOCO 2000 Access Points connected to your 4012 or 4024 OmniAccess Wireless Switch by:

- AP MAC address.
- Interface Number is the front-panel physical port on the 4012 or 4024 OmniAccess Wireless Switch.
- IP Address (leave blank to have the AP obtain its IP address from a DHCP server).
- Whether 802.1X is enabled or disabled.
- Whether Port Mirroring Mode is enabled or disabled, as described in the <u>Port Mirroring</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

Refer to <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the OmniAccess Wireless Switch and made to take effect, but not
  preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **Third-Party APs > Edit**

Use WIRELESS/Access Points/Third Party APs and then Edit to navigate to this page.

Use this page to configure parameters for the Cisco 1200, Cisco 350 and ORiNOCO 2000 Access Points connected to your 4012 or 4024 OmniAccess Wireless Switch by:

- AP MAC address (read only).
- Interface Number (read only).
- IP address (read only).
- Whether 802.1X is enabled or disabled (read only).
- Set Port Mirroring Mode to enabled or disabled, as described in the <u>Port Mirroring</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

Refer to <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information.

# **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the OmniAccess Wireless Switch and made to take effect, but not
  preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### 802.11a Global Parameters

Use **WIRELESS/Global RF/802.11a Network** to navigate to this page.

This page allows you to change the global parameters of your 802.11a network.

• Enable or Disable the 802.11a network.

- Note: You must use this command to enable the 802.11a network after configuring other 802.11a parameters. Note that this command only enables the global Alcatel 802.11a network. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, refer to the <u>WLANs > Edit</u> page.
  - Status of the 802.11a Network and the 802.11a low, mid and high bands are displayed.
  - The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match Client settings.
- The beacon period is rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Auto RF: Opens the <u>802.11a Global Parameters > Auto RF</u> page for the 802.11a network.
- Help: Request that the help page be displayed in a new browser window.

### 802.11a Global Parameters > Auto RF

Use WIRELESS/Global RF/802.11a Network then Auto RF to navigate to this page.

Use this page to modify the Auto RF characteristics.

Table - RF Group

Parameter	Description
Group Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is on, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Update Interval	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Leader	This is the MAC address of the group leader for the group containing this Alcatel OmniAccess Switch or Appliance.
Is this Switch Group Leader?	Yes this Alcatel OmniAccess Switch or Appliance is the group leader or No the Alcatel OmniAccess Switch or Appliance is not the group leader. This leader is automatically determined by the OmniVista AirView Software within the <u>Alcatel Mobility Group</u> as described in the <u>Alcatel OmniAccess Wireless Product Guide</u> .

Table - RF Group (Continued)

Parameter	Description
Last Group Update	The elapsed time since the last group update in seconds. This is only valid if this Alcatel OmniAccess Switch or Appliance is a group leader.

Table - RF Channel Assignment

Parameter	Description
Channel Assignment Method	<ul> <li>Dynamic channel assignment has three modes.</li> <li>Automatic - The channel assignment is periodically updated for all OmniAccess APs that permit this operation.</li> <li>On Demand - Channel assignments are updated when the <b>Assign Now</b> button is clicked.</li> <li>OFF - No dynamic channel assignments occur and value are set to their global default.</li> <li>Default is Automatic.</li> </ul>
Avoid Foreign AP Interference	Enabled or Disabled.
Avoid OmniAccess AP Load	Enabled or Disabled.
Avoid non-802.11a Noise	Enabled or Disabled.
Signal Strength Contribution	Enabled or Disabled. Assigned elsewhere.
Channel Assignment Leader	MAC address of the channel assignment leader.
Last Channel Assignment	Time since last channel assignment.

**Table -** Tx Power Level Assignment

Parameter	Description
Power Level Assignment Method	<ul> <li>Dynamic transmit power assignment has three modes.</li> <li>Automatic - The transmit power is periodically updated for all OmniAccess APs that permit this operation.</li> <li>On Demand - Transmit power is updated when the <b>Assign Now</b> button is selected.</li> <li>Fixed - No dynamic transmit power assignments occur and value are set to their global default.</li> <li>Default is Automatic.</li> </ul>
Power Threshold	These read-only parameters are used to fine tune the power control.  The transmit power control is trying to limit power so that at most <neighbor count=""> OmniAccess APs receive the signal of each  OmniAccess AP above a <power threshold="">.</power></neighbor>
Power Neighbor Count	

Table - Tx Power Level Assignment (Continued)

Parameter	Description
Power Update Contribution	This read-only field displays the factors used for changing channel assignments. The factors are:  • L (Load)  • S (Signal)  • N (Noise)  • I (Interference)  For each factor listed, the corresponding measurement is used in the assignment algorithm.
Power Assignment Leader	MAC address of the power level assignment leader.
Last Power Level Assignment	The elapsed time since the last transmit power assignment in seconds.

Table - Profile Thresholds

Parameter	Description
Interference (0 to 100%)	Foreign 802.11a interference threshold between 0 and 100 percent.
Clients (1 to 75)	Client threshold between 1 and 75 clients.
Noise (-127 to 0 dBm)	Foreign noise threshold between -127 and 0 dBm.
Coverage (3 to 50 dBm)	802.11a coverage threshold between 3 and 50 dB.
Utilization (0 to 100%)	802.11a RF utilization threshold between 0 and 100 percent.
Coverage Exception Level (0 to 100%)	Coverage exception level between 0 and 100 percent.
Data Rate (1 to 1000 Kbps)	802.11a throughput threshold between 1 Kbps and 1000 Kbps.
Client Min Exception Level (1 to 75)	Client minimum exception level.

Table - Monitor Intervals

Parameter	Description
Noise Measurement	The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
Load Measurement	The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
Signal Measurement	The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
Coverage Measurement	The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.
Note: Intervals from 60 to 3600 seconds.	

Use **Set to Factory Default** to set all Auto RF 802.11a parameters to the Factory Defaults.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# 802.11b/g Global Parameters

Use WIRELESS/Global RF/802.11b/g Network to navigate to this page.

Use this page to change the global parameters of your 802.11b/g network.

- Enable or Disable the 802.11b/g network.
- Enable or Disable 802.11g network support. (Only available if the 802.11b/g network is Enabled.)
- Note: You must use these commands to enable the 802.11b/g networks after configuring other 802.11b/g parameters. Note that this command only enables the global Alcatel 802.11b/g networks. To disable the 802.11a, 802.11b and/or 802.11g networks for an individual WLAN, refer to the <u>WLANs > Edit</u> page.
- The data rates set here are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, the client may negotiate for the respective rate. Each data rate can also be set to Disabled to match Client settings.
- The beacon period is rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
- Enable or disable the Short Preamble. This parameter must be disabled to optimize this Alcatel OmniAccess Switch or Appliance for some clients, including SpectraLink NetLink Telephones.

### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Auto RF: Opens the <u>802.11b/g Global Parameters</u> > <u>Auto RF</u> page for the 802.11b/g network.
- **Help:** Request that the help page be displayed in a new browser window.

### 802.11b/g Global Parameters > Auto RF

Use WIRELESS/Global RF 802.11b/g Network then Auto RF to navigate to this page.

The Auto RF characteristics may be modified on this page.

Table - RF Group

Parameter	Description
Group Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is on, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Update Interval	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Leader	This is the MAC address of the group leader for the group containing this Alcatel OmniAccess Switch or Appliance.
Is this Switch Group Leader?	Yes this Alcatel OmniAccess Switch or Appliance is the group leader or No the Alcatel OmniAccess Switch or Appliance is not the group leader. This leader is automatically determined by the OmniVista AirView Software within the <u>Alcatel Mobility Group</u> as described in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
Last Group Update	The elapsed time since the last group update in seconds. This is only valid if this Alcatel OmniAccess Switch or Appliance is a group leader.

Table - RF Channel Assignment

Parameter	Description
Channel Assignment Method	<ul> <li>Dynamic channel assignment has three modes.</li> <li>Automatic - The channel assignment is periodically updated for all OmniAccess APs that permit this operation.</li> <li>On Demand - Channel assignments are updated when the <b>Assign Now</b> button is selected.</li> <li>OFF - No dynamic channel assignments occur and value are set to their global default.</li> <li>Default is Automatic.</li> </ul>
Avoid Foreign AP Interference	Enabled or Disabled.
Avoid Foreign AP Load	Enabled or Disabled.
Avoid non-802.11b/g Noise	Enabled or Disabled.
Signal Strength Contribution	Enabled or Disabled. Assigned elsewhere.
Channel Assignment Leader	MAC address of the channel assignment leader.
Last Channel Assignment	Time since last channel assignment.

**Table -** Tx Power Level Assignment

Parameter	Description
Power Level Assignment Method	Dynamic transmit power assignment has three modes.  Automatic - The transmit power is periodically updated for all OmniAccess APs that permit this operation.  On Demand - Transmit power is updated when the <b>Assign Now</b> button is selected.  Fixed - No dynamic transmit power assignments occur and value are set to their global default.  Default is Automatic.
Power Threshold	These read-only parameters are used to fine tune the power control.
Power Neighbor Count	The transmit power control is trying to limit power so that at most <neighbor count=""> OmniAccess APs receive the signal of each OmniAccess AP above a <power threshold="">.</power></neighbor>
Power Update Contribution	This read-only field displays the factors used for changing channel assignments. The factors are:  • L (Load)  • S (Signal)  • N (Noise)  • I (Interference) For each factor listed, the corresponding measurement is used in the assignment algorithm.
Power Assignment Leader	MAC address of the power level assignment leader.
Last Power Level Assignment	The elapsed time since the last transmit power assignment in seconds.

**Table - Profile Thresholds** 

Parameter	Description
Interference (0 to 100%)	Foreign 802.11b/g interference threshold between 0 and 100 percent.
Clients (1 to 75)	Client threshold between 1 and 75 clients.
Noise (-127 to 0 dBm)	Foreign noise threshold between -127 and 0 dBm.
Coverage (3 to 50 dBm)	802.11b/g coverage threshold between 3 and 50 dB.
Utilization (0 to 100%)	802.11b/g RF utilization threshold between 0 and 100 percent.
Coverage Exception Level (0 to 100%)	Coverage exception level between 0 and 100 percent.
Data Rate (1 to 1000 Kbps)	802.11b/g throughput threshold between 1 Kbps and 1000 Kbps.
Client Min Exception Level (1 to 75)	Client minimum exception level.

Table - Monitor Intervals

Parameter	Description
Noise Measurement	The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds, range is from 60 to 3600 seconds.
Load Measurement	The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds, range is from 60 to 3600 seconds.
Signal Measurement	The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds, range is from 60 to 3600 seconds.
Coverage Measurement	The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds, range is from 60 to 3600 seconds.

Use **Set to Factory Default** to set all Auto RF 802.11b/g parameters to the Factory Defaults.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# Country

Use **WIRELESS/Country** to navigate to this page.

On this page, enter the country code where the Alcatel OmniAccess Switch or Appliance and associated Access Points are installed and operational. This selection ensures that the listed broadcast frequency bands, interfaces, channels and transmit power levels are compliant with country-specific regulations.

The currently-supported countries are:

- AT (Austria), which allows 802.11a and 802.11b/g.
- AU (Australia), which allows 802.11a and 802.11b.
- BE (Belgium), which allows 802.11a and 802.11b/g.
- CA (Canada), which allows 802.11b/g.
- CH (Switzerland and Liechtenstein), which allows 802.11a and 802.11b/g.
- DE (Germany), which allows 802.11a and 802.11b/g.
- DK (Denmark), which allows 802.11a and 802.11b/g.
- ES (Spain), which allows 802.11a and 802.11b/g.
- FI (Finland), which allows 802.11a and 802.11b/g.
- FR (France), which allows 802.11a and 802.11b/g.
- GB (United Kingdom), which allows 802.11a and 802.11b/g.
- GR (Greece), which allows 802.11b/g.

- HK (Hong Kong), which allows 802.11a and 802.11b/g.
- IE (Ireland), which allows 802.11a and 802.11b/g.
- IN (India), which allows 802.11a and 802.11b.
- IS (Iceland), which allows 802.11a and 802.11b/g.
- IT (Italy), which allows 802.11a and 802.11b/g.
- JP (Japan), which allows 802.11a and 802.11b/g.
- KR (Republic of Korea), which allows 802.11a and 802.11b/g.
- LU (Luxembourg), which allows 802.11a and 802.11b/g.
- NL (Netherlands), which allows 802.11a and 802.11b/g.
- NO (Norway), which allows 802.11a and 802.11b/g.
- PT (Portugal), which allows 802.11a and 802.11b/g.
- SE (Sweden), which allows 802.11a and 802.11b/g.
- SG (Singapore), which allows 802.11a and 802.11b/g.
- TH (Thailand), which allows 802.11b/g.
- TW (Taiwan), which allows 802.11a and 802.11b/g.
- US (United States of America), which allows 802.11b/g operation and 802.11a Low, Medium, and High bands.
- USL (US Low), which allows 802.11b/g operation and 802.11a Low and Medium bands. (Used for legacy 802.11a interface cards that do not support 802.11a High band.)

Note that both 802.11a and 802.11b/g bands must be disabled in order to change the country code.

### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

#### **Timers**

Use WIRELESS/Timers to navigate to this page.

The timers listed on this page are described in the following table.

Table - Timer Descriptions

Timer	Description
802.11 Authentication Response Timeout	Configures 802.11 authentication response timeout in seconds.

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **Security Menu Bar Selection**

This menu bar selection provides access to the security configuration details. Use the selector area to access specific security parameters. Making this selection from the menu bar opens the <u>RADIUS</u> <u>Authentication Servers</u> page.

Access the following pages from the Security Menu Bar Selection:

- RADIUS Authentication Servers
- RADIUS Authentication Servers > New
- RADIUS Authentication Servers > Edit
- RADIUS Accounting Servers
- RADIUS Accounting Servers > New
- RADIUS Accounting Servers > Edit
- Local Net Users
- <u>Local Net Users > New</u>
- <u>Local Net Users > Edit</u>
- MAC Filtering
- MAC Filters > New
- MAC Filters > Edit
- Disabled Clients
- Disabled Client > New
- Disabled Client > Edit
- Access Control Lists
- <u>Access Control Lists > New</u>
- Access Control Lists > Edit
- Access Control Lists > Rules > Edit
- <u>CA Certification</u>
- <u>ID Certificate</u>
- ID Certificate > New
- Web Authentication Certificate
- Roque Policy

### **RADIUS Authentication Servers**

Use **SECURITY/AAA/RADIUS Authentication** to navigate to this page.

This page displays Server Index, Server Address, Port and Admin Status information for your configured Remote Authentication Dial-In User Servers.

- Server Index The RADIUS server Index. The Alcatel OmniAccess Switch or Appliance tries Index 1 first, then Index 2 through 4, in descending order. Should be 1 if your network is using only one Authentication server.
- Server Address IP address of the RADIUS server.

- Port Communication port number for the interface protocols.
- Admin Status Whether the interface is Enabled or Disabled.
- The **Edit** link opens the *RADIUS Authentication Servers > Edit* page.
- The **Remove** link allows you to delete an existing RADIUS Authentication server.
- Click the **Ping** link to send ping packets to the RADIUS Server to verify that you have a working connection between the Alcatel OmniAccess Switch or Appliance and the RADIUS Server

- New: Select to add a new RADIUS Authentication server (RADIUS Authentication Servers > New).
- **Help:** Request that the help page be displayed in a new browser window.

### **RADIUS Authentication Servers > New**

Use **SECURITY/AAA/RADIUS Authentication** then **New...** to navigate to this page.

This page allows you to add a new Remote Authentication Dial-In User Servers. The following information is required:

- Server Index (Priority) Index of the RADIUS server. The Alcatel OmniAccess Switch or Appliance tries Index 1 first, then Index 2 through 4, in descending order. Set to 1 if your network is using only one Authentication server.
- Server IP Address IP address of the RADIUS server.
- Shared Secret/Confirm Shared Secret RADIUS server login Shared Secret.
- Port Number Communication port number for the interface protocols.
- Note: DO NOT assign the Port Number to one used by another application. Use the default (1812) or any other port unused by any other application.
- Server Status Set the interface to Enabled or Disabled.

### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **RADIUS Authentication Servers > Edit**

Use **SECURITY/AAA/RADIUS Authentication** then **Edit** to navigate to this page.

This page allows you to change the following parameters on an existing Remote Authentication Dial-In User Servers:

- Server Shared Secret/Confirm Shared Secret RADIUS server login Shared Secret.
- Server Status Set the interface to enabled or disabled.

# **Command Buttons**

< Back: Return to the previous window.

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **RADIUS Accounting Servers**

Use **SECURITY/AAA/RADIUS Accounting** to navigate to this page.

This page displays Server Index, Server Address, Port and Admin Status information for your existing Remote Accounting Dial-In User Servers.

- Server Index The RADIUS server Index. The Alcatel OmniAccess Switch or Appliance tries Index 1 first, then Index 2 through 4, in descending order. Should be 1 if your network is using only one Accounting server.
- Server Address IP address of the RADIUS server.
- Port Alcatel OmniAccess Switch or Appliance port number for the interface protocols.
- Admin Status Whether the interface is enabled or disabled.
- The Edit link opens the <u>RADIUS Accounting Servers > Edit</u> page.
- The Remove link allows you to delete an existing RADIUS Accounting server.
- Click the **Ping** link to send ping packets to the RADIUS Server to verify that you have a working connection between the Alcatel OmniAccess Switch or Appliance and the RADIUS Server

#### **Command Buttons**

- New: Select to add a new RADIUS Accounting server (<u>RADIUS Accounting Servers > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

## **RADIUS Accounting Servers > New**

Use **SECURITY/AAA/RADIUS Accounting** then **New...** to navigate to this page.

This page allows you to add a new Remote Accounting Dial-In User Server. The following information is required:

- Server Index (Priority) Index of the RADIUS server. The Alcatel OmniAccess Switch or Appliance tries Index 1 first, then Index 2 through 4, in descending order. Set to 1 if your network is using only one Accounting server.
- Server IP Address IP address of the RADIUS server.
- Shared Secret/Confirm Shared Secret RADIUS server login Shared Secret.
- Port Number Port number for the interface protocols.
- Note: DO NOT assign the Port Number to one used by another application. Use the default (1813) or any other port unused by any other application.
  - Server Status Set the interface to enabled or disabled.

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **RADIUS Accounting Servers > Edit**

Use **SECURITY/AAA/RADIUS Accounting** then **New...** to navigate to this page.

This page allows you to change the following parameters on an existing Remote Accounting Dial-In User Server:

- Server Shared Secret/Confirm Shared Secret RADIUS server login Password.
- Server Status Set the interface to enabled or disabled.

#### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **Local Net Users**

Use **SECURITY/AAA/Local Net Users** to navigate to this page.

This page presents a summary of the existing local network users who are allowed to access a specific Alcatel WLAN sorted by User Name. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication located on the WLANs > Edit page must be enabled.

Client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

Use the **Remove** link to remove an existing local network client.

#### **Command Buttons**

- **New:** Select to add a new local network client (<u>Local Net Users > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

### **Local Net Users > New**

Use **SECURITY/AAA/Local Net Users** then **New...** to navigate to this page.

This page allows you to add a local network user. Layer 3 Web Authentication located on WLANs > Edit page must be enabled.

- Add the User Name, Password and Password Confirmation.
- Enter the Alcatel WLAN ID that the user is allowed to access.
- If desired, enter a user description.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

## Local Net Users > Edit

Use **SECURITY/AAA/Local Net Users** then **Edit** to navigate to this page.

This page allows you to edit a local network user definition. Layer 3 Web Authentication located on <u>WLANs > Edit</u> page must be enabled.

- Confirm or change the Password and Password Confirmation.
- Enter the Alcatel WLAN ID that the user is allowed to access.
- If desired, enter a user description.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **MAC Filtering**

Use **SECURITY/AAA/MAC Filtering** to navigate to this page.

This page presents the RADIUS Compatibility Mode and MAC Delimiters for MAC Filtering, and also presents a summary of the client machines allowed to access network services via a specific Alcatel WLAN and through a specific interface. The client machine access is determined by its MAC address. This is an administrative bypass of the RADIUS authentication process.

- Select the required RADIUS Compatibility Mode for MAC Filtering: Cisco ACS, ORINOCO RADIUS, or Other.
- Select the required **MAC Delimiters** for MAC Filtering. The MAC delimiters can be colon (xx:xx:xx:xx:xx), hyphen (xx-xx-xx-xx-xx), single hyphen (xxxxxxxxxx), or none (xxxxxxxxxxxx), as required by the RADIUS server.

This page lists the current Local MAC Filters by MAC address, WLAN ID, Interface, and optional Description.

- Use the **Edit** link to change a current local MAC filter definition on the <u>MAC Filters > Edit</u> page.
- Use the **Remove** link to remove a current local MAC filter.

#### **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- New: Select to add a new client by MAC address (<u>MAC Filters > New</u>).
- Help: Request that the help page be displayed in a new browser window.

## **MAC Filters > New**

Use **SECURITY/AAA/MAC Filtering** then **New...** to navigate to this page.

This page allows you to add a client by MAC address.

- Add the client MAC Address
- Add the WLAN ID to which the client has access.
- If desired, add a client Description.

Select the associated Interface Name, as defined in the <u>Interfaces</u> page.

### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

### MAC Filters > Edit

Use **SECURITY/AAA/MAC Filtering** then **Edit** to navigate to this page.

This page allows you to change a MAC Filter definition for an existing client MAC Address.

- Change the WLAN ID to which the client has access.
- If desired, add a filter Description.
- Select the associated Interface Name, as defined in the *Interfaces* page.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **Disabled Clients**

Use SECURITY/AAA/Disabled Clients to navigate to this page.

This page presents a summary of existing disabled (blacklisted) clients manually barred by MAC address from access to network services.

- The Edit link opens the <u>Disabled Client > Edit</u> page.
- The Remove link allows you to enable a client that was formerly disabled.

#### **Command Buttons**

- **New:** Select to manually disable a client (<u>Disabled Client > New</u>).
- Help: Request that the help page be displayed in a new browser window.

# **Disabled Client > New**

Use **SECURITY/AAA/Disabled Client** then **New...** or **MONITOR/Clients** then **Disable** to navigate to this page.

This page allows you to manually disable (blacklist) a client by MAC address.

- Add the MAC Address and an optional Client Description for the client to be disabled.
- Note: When you enter a client MAC address to be disabled, the Alcatel Wireless Operating System checks that the MAC address is not one of the known Local Net clients (<u>Local Net Users</u>), Authorized clients (<u>MAC Filtering</u>), or Local Management users (<u>Local Management Users</u>) MAC addresses. If the entered MAC address is on one of these three lists, the Alcatel Wireless Operating System does not allow the MAC address to be manually disabled.

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

### Disabled Client > Edit

Use **SECURITY/AAA/Disabled Clients** then **Edit** to navigate to this page.

This page allows you to change a manually disabled (blacklisted) client description.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **Access Control Lists**

Use **SECURITY/Access Control Lists** to navigate to this page.

This page allows you to view current Access Control Lists, similar to standard firewall Access Control Lists.

Note that the Alcatel Wireless Operating System allows you to define up to 64 ACLs, with up to 64 Rules (filters) per ACL.

- Use the Edit link to open the <u>Access Control Lists > Edit</u> page.
- Use the Remove link to remove an existing local MAC filter.

### **Command Buttons**

- New: Select to add a new Access Control List (<u>Access Control Lists > New</u>).
- Help: Request that the help page be displayed in a new browser window.

### **Access Control Lists > New**

Use **SECURITY/Access Control Lists** then **New...** to navigate to this page.

This page allows you to add an Access Control List by Name.

#### **Command Buttons**

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Access Control Lists > Edit**

Use **SECURITY/Access Control Lists** then **Edit** to navigate to this page.

This page allows you to view and/or change an Access Control List definition, similar to standard firewall Access Control Lists. Note that the Alcatel Wireless Operating System allows you to define up to 64 ACLs, with up to 64 Rules (filters) per ACL.

Use the **Remove** link to remove an existing Access Control List rule.

Table - Current Rules

Parameter	Description
Access List Name	The name of the Access Control List.
Sequence	The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is added as Rule 5. Note that if you add or change a Sequence number, the Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, the Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
Action (Note)	Deny or Permit.
Source IP/Mask	Any or IP Address and Netmask.
Destination IP/Mask	Any or IP Address and Netmask.
Protocol	Protocol to use for this ACL:  Any - All protocols  TCP - Transmission Control Protocol  UDP - User Datagram Protocol  ICMP - Internet Control Message Protocol  ESP - IP Encapsulating Security Payload  AH - Authentication Header  GRE - Generic Routing Encapsulation  IP - Internet Protocol  Eth Over IP - Ethernet over Internet Protocol  OSPF - Open Shortest Path First  Other - Any other IANA protocol ( <a href="http://www.iana.org/">http://www.iana.org/</a> )
Source Port	Any or IP Address and Netmask.
Dest Port	Any or IP Address and Netmask.
DSCP	Any or Specific (from 0 - 63). Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client) or Outbound (to client).
Note: The default filter is to deny all access unless a Rule explicitly permits it.	

When the ACL contains one or more ACL Rule, click **Edit** to modify the rule on the <u>Access</u> <u>Control Lists > Rules > Edit</u> page.

Table - New Rule Parameters

Parameter	Description
Sequence	The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is be added as Rule 5. Note that if you add or change a Sequence number, the Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, the Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IP Address and Netmask.
Destination	Any or IP Address and Netmask.
Protocol (Note 1)	Protocol to use for this ACL:  • Any - All protocols  • TCP - Transmission Control Protocol  • UDP - User Datagram Protocol  • ICMP - Internet Control Message Protocol  • ESP - IP Encapsulating Security Payload  • AH - Authentication Header  • GRE - Generic Routing Encapsulation  • IP - Internet Protocol  • Eth Over IP - Ethernet over Internet Protocol  • OSPF - Open Shortest Path First  • Other - Any other IANA protocol ( <a href="http://www.iana.org/">http://www.iana.org/</a> )
DSCP	Any or Specific (from 0 - 63). Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client) or Outbound (to client).
Action (Note 2)	Deny or Permit.

Note 1: When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.

Note 2: The default filter is to deny all access unless a Rule explicitly permits it.

Use **Add New Rule** to add the new rule to the Access Control List.

# **Command Buttons**

- < Back: Return to the previous window.
- **Help:** Request that the help page be displayed in a new browser window.

## Access Control Lists > Rules > Edit

Use **SECURITY/Access Control Lists** then **Edit** and then **Edit** again to navigate to this page.

This page allows you to change an Access Control List Rule definition. Note that the Alcatel Wireless Operating System allows you to define up to 64 ACLs, with up to 64 Rules (filters) per ACL.

Table - Rule Edit Parameters

Parameter	Description
Sequence	The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is be added as Rule 5. Note that if you add or change a Sequence number, the Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, the Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IP Address and Netmask.
Destination	Any or IP Address and Netmask.
Protocol (Note 1)	Protocol to use for this ACL:  • Any - All protocols  • TCP - Transmission Control Protocol  • UDP - User Datagram Protocol  • ICMP - Internet Control Message Protocol  • ESP - IP Encapsulating Security Payload  • AH - Authentication Header  • GRE - Generic Routing Encapsulation  • IP - Internet Protocol  • Eth Over IP - Ethernet over Internet Protocol  • OSPF - Open Shortest Path First  • Other - Any other IANA protocol (http://www.iana.org/)
DSCP	Any or Specific (from 0 - 63). Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client) or Outbound (to client).
Action (Note 2)	Deny or Permit.

Note 1: When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.

Note 2: The default filter is to deny all access unless a Rule explicitly permits it.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **CA Certification**

Use **SECURITY/IPSec Certificates/CA Certificate** to navigate to this page.

This page contains the current CA certificate information. If you choose to add an operator-generated or purchased CA Certificate, paste the new CA certificate ASCII text into the Certificate box and click **Apply**.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Delete Certificate:** Deletes the current CA Certification. You are prompted to confirm if you select this option.
- **Help:** Request that the help page be displayed in a new browser window.

# **ID Certificate**

Use **SECURITY/IPSec Certificates/ID Certificate** to navigate to this page.

This page summarizes existing network ID certificates by ID Certificate name and Valid Period. An ID Certificate can used by Web server operators to ensure secure server operation. Refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information about this and other feature descriptions.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

### **Command Buttons**

- **New:** Open the <u>ID Certificate > New</u> page to add a new ID certificate.
- Help: Request that the help page be displayed in a new browser window.

# **ID Certificate > New**

Use **SECURITY/IPSec Certificates/ID Certificate** then **New...** to navigate to this page.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

Use this page to add new ID certificates, in addition to the factory-supplied ID certificate. For each new ID certificate, add:

- Certificate Name.
- Certificate Password (Private Key).
- Paste the new ID certificate ASCII text into the Certificate box.
- Click Apply.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **Web Authentication Certificate**

Use **SECURITY/Web Auth Certificate** to navigate to this page.

Use this page to view the current Web Authentication certificate type, download an SSL certificate, or regenerate a new locally- generated Web Auth certificate.

Note that the Alcatel Wireless Operating System automatically generates a fully-functional Web Authentication certificate as it is loaded onto your Alcatel OmniAccess Switch or Appliance. This means that you do not have to do anything to use certificates with Layer 3 Web Authentication.

- However, if you would like to use a new Alcatel Wireless Operating System-generated Web Authentication certificate, click the Regenerate Certificate button. The Alcatel Wireless Operating System generates a new Web Auth certificate, and displays a Successfully generated Web Authentication Certificate message, Reboot the Alcatel OmniAccess Switch or Appliance to register the new certificate.
- If you would prefer to use an externally-generated Web Authentication certificate, verify that the Alcatel OmniAccess Switch or Appliance can ping the TFTP server, and then click the **Download SSL Certificate** box, and fill in the following:
- Note: The TFTP server cannot run on the same computer as the OmniVista Air Control System, because the ACS and the TFTP server use the same communication port.



CAUTION: Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

- TFTP Server IP Address.
- Maximum Retries: Maximum number of times each download can be attempted.
- Timeout: The amount of time allowed for each download.
- Certificate File Path: usually "/" so the TFTP software can use its default directory.
- Certificate File Name: The Web Authentication Certificate filename in encrypted .PEM (Privacy Enhanced Mail) format.
- Certificate Password.

When you have filled in the required information, click Apply and the Alcatel Wireless Operating System collects the new certificate from the TFTP server. Reboot the Alcatel OmniAccess Switch or Appliance to register the new certificate.

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Regenerate Certificate: Direct the Alcatel Wireless Operating System to internally generate a new Web Authentication certificate.
- **Help:** Request that the help page be displayed in a new browser window.

# **Rogue Policy**

Use **SECURITY/Rogue Policy** to navigate to this page.

This page allows you to select global parameters for rogue access point detection and containment.

- Enable Rogue Location Discovery Protocol to have the Alcatel OmniAccess Wireless System
  automatically detect rogue access points on your wired network. Enabling this feature allows
  the Automatically contain rogues on my network function to contain only the rogue access
  points on your wired network, while ignoring the rogue access points on other floors or across
  the street.
- Enable **Automatically contain rogues on my network** to have the Alcatel OmniAccess Wireless System automatically contain rogue access point clients on the local subnet as described in *Rogue AP Location, Tagging and Containment* in the *Alcatel OmniAccess Wireless Product Guide*.
- Expiration Timeout for Rogue AP Entries: The number of seconds an automatically-contained rogue access point will continue to be contained.

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **Management Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance management details. Use the selector area to access specific management parameters. Making this selection from the menu bar opens the <u>Summary</u> page.

- Summary
- SNMP System Summary
- SNMP V3 Users
- <u>SNMP V3 Users > New</u>
- SNMP v1/v2c Community
- SNMP v1/v2c Community > New
- SNMP v1/v2c Community > Edit
- <u>SNMP Trap Receiver</u>
- <u>SNMP Trap Receiver > New</u>
- SNMP Trap Receiver > Edit
- <u>SNMP Trap Controls</u>
- Trap Logs
- HTTP Configuration
- <u>Telnet-SSH Configuration</u>
- Serial Port Configuration
- Local Management Users
- <u>Local Management Users > New</u>
- CLI Sessions
- Syslog Configuration
- Mgmt Via Wireless
- Message Logs
- System Resource Information
- Switch Crash
- AP Crash
- AP Crash Information

# **Summary**

Use **MANAGEMENT/Summary** to navigate to this page.

This page displays the network summary of this Alcatel OmniAccess Switch or Appliance.

**Table - Summary Parameters** 

Parameter	Description
SNMP Protocols	SNMP protocols supported.

Table - Summary Parameters (Continued)

Parameter	Description
Syslog	Log of system events.
HTTP Mode	Access mode for web and secure web.
HTTPS Mode	Enable or Disable the https Secure Shell (SSL) interface using secure certificate authentication
New Telnet Sessions Allowed	Whether or not additional telnet sessions are permitted.
New SSH Sessions Allowed	Whether or not additional SSH-enabled sessions are permitted.
Management via Wireless	Whether Alcatel OmniAccess Switch or Appliance management from a wireless client is enabled or disabled.

• **Help:** Request that the help page be displayed in a new browser window.

# **SNMP System Summary**

Use MANAGEMENT/SNMP/General to navigate to this page.

This page allows you to change some of the SNMP system parameters.

**Table - SNMP System Parameters** 

Parameter	Description
Name	Customer definable name of the Alcatel OmniAccess Switch or Appliance.
Location	Customer definable Alcatel OmniAccess Switch or Appliance location.
Contact	Customer definable contact details.
System Description	Read-only Alcatel OmniAccess Switch or Appliance description.
System Object ID	Read-only object ID.
SNMP Port Number	Read-only SNMP port number.
Trap Port Number	Definable trap port number; Default is 162.
SNMP v1 Mode	Enable or disable SNMP v1; Default is disable.
SNMP v2c Mode	Enable or disable SNMP v2c; Default is disable.
SNMP v3 Mode	Enable or disable SNMP v3; Default is enable.

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **SNMP V3 Users**

Use MANAGEMENT/SNMP/SNMP V3 Users to navigate to this page.

This page provides a summary of the SNMP users as described in the following table.

Table - SNMP User Summary

Parameter	Range
User Name	Name of the user profile.
Access Level	Read Only; Read Write.
Auth Protocol	None; HMAC-MD5; HMAC-SHA.
Privacy Protocol	None; CBC-DES.

Remove a user profile by selecting the appropriate **Remove** link. You are prompted for confirmation of the user removal.

#### **Command Buttons**

- New: Select to add a new SNMP user (<u>SNMP V3 Users > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

### SNMP V3 Users > New

Use MANAGEMENT/SNMP/SNMP V3 Users then New... to navigate to this page.

This page provides a summary of the SNMP users as described in the following table.

Table - SNMP User Details

Parameter	Range
User Profile Name	Name of the user profile.
Access Mode	Read Only or Read Write.
Authentication Protocol	None, HMAC-MD5, or HMAC-SHA. For HMAC-MD5 or HMAC-SHA, enter and confirm an Authentication Password.
Privacy Protocol	None or CBC-DES. For CBC-DES, enter and confirm a Privacy Password.

If you select an authentication or privacy protocol, you must enter a password for each.

- < Back: Return to the previous window.</li>
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# SNMP v1/v2c Community

Use MANAGEMENT/SNMP/Communities to navigate to this page.

This page provides a summary of the SNMP community as described in the following table.

Table - SNMP Community Summary

Parameter	Range
Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address	An IP address from which this device accepts SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address.  Note: If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, that is, the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string. May be specified by selecting Read/Write or Read Only from the pulldown.
Status	The status of this community access entry. When this object is set to enabled, if the Community Name for this row is not unique among all valid rows, the set request is rejected.

Edit a user profile by selecting the **Edit** link (<u>SNMP v1/v2c Community > Edit</u>).

Remove a user profile by selecting the appropriate **Remove** link. You are prompted for conformation of the user removal.

### **Command Buttons**

- New: Select to add a new community user profile (<u>SNMP v1/v2c Community > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

# **SNMP v1/v2c Community > New**

Use MANAGEMENT/SNMP Communities then New... to navigate to this page.

Use this page to add a new SNMP community profile as described in the following table.

Table - SNMP Community Summary

Parameter	Range
Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address	An IP address from which this device accepts SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address.  Note: If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, that is, the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string. May be specified by selecting Read/Write or Read Only from the pulldown.
Status	The status of this community access entry. When this object is set to enabled, if the Community Name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by selecting disable.

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **SNMP v1/v2c Community > Edit**

Use MANAGEMENT/SNMP Communities then Edit to navigate to this page.

Use this page to Enable or Disable an SNMP community profile. All fields are read-only except the Status field.

Table - SNMP Community Summary

Parameter	Range
Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.

Table - SNMP Community Summary (Continued)

Parameter	Range
IP Address	An IP address from which this device accepts SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address.  Note: If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, that is, the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string. May be specified by selecting Read/Write or Read Only from the pulldown.
Status	Set the status of this community access entry. When this object is set to enabled, if the Community Name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by selecting disable.

- **< Back:** Return to the previous window.
- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

# **SNMP Trap Receiver**

Use MANAGEMENT/SNMP/Trap Recipients to navigate to this page.

This page provides a summary of existing SNMP trap receivers as described in the following table.

**Table - SNMP Trap Receiver Summary** 

Parameter	Range
Trap Receiver Name	The name of the server where the traps are sent.
IP Address	The IP address of the server.
Status	Status must be enabled for the SNMP traps to be sent to the server.

Edit a user profile by selecting the **Edit** link (<u>SNMP Trap Receiver > Edit</u>).

Remove a user profile by selecting the appropriate **Remove** link. You are prompted for conformation of the trap removal.

- **New:** Select to add a new trap receiver (<u>SNMP Trap Receiver > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

# **SNMP Trap Receiver > New**

Use **MANAGEMENT/SNMP Trap Recipients** then **New...** to navigate to this page.

Use this page to add a server to receive SNMP traps from this Alcatel OmniAccess Switch or Appliance as described in the following table.

**Table - SNMP Trap Receiver Details** 

Parameter	Range
Trap Receiver Name	The name of the server where the traps are sent.
IP Address	The IP address of the server.
Status	Status must be enabled for the SNMP traps to be sent to the receiver.

### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

# **SNMP Trap Receiver > Edit**

Use MANAGEMENT/SNMP Trap Recipients then Edit to navigate to this page.

You can use this page to Enable or Disable sending traps to a particular server. Only the Status field can be modified.

### **Command Buttons**

- < Back: Return to the previous window.
- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

## **SNMP Trap Controls**

Use MANAGEMENT/SNMP Trap Controls to navigate to this page.

This page allows you to select which traps logs should be captured. Select the applicable logs and select Apply.

Table - Miscellaneous Traps

Trap Name	Description	
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated.	
Link (Port) Up/Down	Port changes status from up or down.	
Multiple Users	Two users login with the same login ID.	
Spanning Tree	Spanning Tree traps. Refer to the STP specifications for descriptions of individual parameters.	
Rogue AP	Whenever a rogue access point is detected this trap is sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.	
Config Save	Notification sent when the configuration is modified.	

Table - 802.11 Station Traps

Trap Name	Description	
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.	
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.	
802.11 Failed Authentication	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.	
802.11 Failed Association	The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.	
Blacklisting	The associate failure notification is sent when a client is disabled (blacklisted).	

Table - OmniAccess AP Traps

Trap Name	Description
AP Register	Notification sent when the OmniAccess AP associates or disassociates with the Alcatel OmniAccess Switch or Appliance.
AP Interface Up/Down	Notification sent when the OmniAccess AP interface (802.11a or 802.11b/g) status changes to up or down.

Table - Auto RF Profile Traps

Trap Name	Description
Load Profile	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Profile	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Profile	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Profile	Notification sent when Coverage Profile state changes between PASS and FAIL.

## **Table -** Auto RF Update Traps

Trap Name	Description	
Channel Update	Notification sent when the OmniAccess AP's dynamic channel algorithm is updated.	
Tx Power Update	Notification sent when the OmniAccess AP's dynamic transmit power algorithm is updated.	
Antenna Update	Notification sent when the OmniAccess AP's dynamic antenna algorithm is updated.	

## Table - AAA Traps

Trap Name	Description
User Authentication	This trap is to inform that a client RADIUS authentication failure has occurred.
RADIUS Servers Not Responding	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

## Table - IP Security Traps

Trap Name	Description
ESP Authentication Failure	IPSec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPSec packets with invalid sequence numbers were found in an inbound ESP SA.
Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.

Table - IP Security Traps (Continued)

Trap Name	Description
IKE Negotiation Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
IKE Suite Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.

Table - 802.11 Security Traps

Trap Name	Description	
WEP Decrypt Error	This trap is to inform that an error has occurred while a WEP entity is being decrypted.	

#### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

## **Trap Logs**

Use **MANAGEMENT/SNMP Trap Logs** to navigate to this page.

You can view the traps logs which have been captured by the Alcatel OmniAccess Switch or Appliance. Each trap entry includes the Log Number, System Time, and Trap Description.

This screen also displays the Number of Traps Since Last Reset and Number of Traps Since Log Last Viewed.



**Note:** Please find below the Client Reason and Status Codes you are likely to encounter when reviewing the Trap Logs.

Table - Client Reason Code Descriptions and Meanings

Client Reason Code	Description	Meaning
0	noReasonCode	normal operation
1	unspecifiedReason	client associated but no longer authorized
2	previousAuthNotValid	client associated but not authorized

Table - Client Reason Code Descriptions and Meanings (Continued)

Client Reason Code	Description	Meaning
3	deauthenticationLeaving	the OmniAccess AP went offline, de-authenticating the client
4	disassociationDueToInactivity	client session timeout exceeded
5	disassociationAPBusy	the OmniAccess AP is busy, performing load balancing, for example
6	class2FrameFromNonAuthStation	client attempted to transfer data before it was authenticated
7	class2FrameFromNonAssStation	client attempted to transfer data before it was associated
8	disassociationStaHasLeft	the Alcatel Wireless Operating System moved the client to another OmniAccess AP using non-aggressive load balancing
9	staReqAssociationWithoutAuth	client not authorized yet, still attempting to associate with an OmniAccess AP
99	missingReasonCode	client momentarily in an unknown state

Table - Client Status Code Descriptions and Meanings

Client Status Code	Description	Meaning
0	idle	normal operation no rejections of client association requests
1	aaaPending	completing an aaa transaction
2	authenticated	802.11 authentication completed
3	associated	802.11 association completed
4	powersave	client in powersave mode
5	disassociated	802.11 disassociation completed
6	tobedeleted	to be deleted after disassociation
7	probing	client not associated or authorized yet
8	disabled	automatically disabled by the Alcatel Wireless Operating System for an operator-defined time

### **Command Buttons**

• Clear Log: Deletes all log entries. You are prompted for confirmation to delete the logs.

**Help:** Request that the help page be displayed in a new browser window.

## **HTTP Configuration**

Use **MANAGEMENT/HTTP** to navigate to this page.

This page allows you to enable or disable Web Mode or Secure Web Mode.

- HTTP Access: This is the HTTP Web interface which is accessible using a login and password. If vou disable HTTP Web Mode, vou need Secure Web Mode enabled, or must use the CLI or OmniVista Air Control System Software interface to configure the Alcatel OmniAccess Switch or Appliance. If you disable Web Mode and Secure Web Mode, and must use the CLI interface to configure the Alcatel OmniAccess Switch or Appliance.
- HTTPS Access: This is the HTTPS Secure Shell (SSL) interface accessible using secure certificate authentication (configured below). If you disable HTTPS Secure Web Mode, you need Web Mode enabled or need to use the CLI or OmniVista Air Control System Software interface to configure the Alcatel OmniAccess Switch or Appliance.
- **Current Certificate Information.**
- Download SSL Certificate: Use to download an SSL Web Admin Certificate from a local TFTP server. Select the Download SSL Certificate checkbox to display the following entries:
- Note: The TFTP server cannot run on the same computer as the OmniVista Air Control System, because the ACS and the TFTP server use the same communication port.



CAUTION: Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

- Server IP Address: The IP address of the local TFTP server.
- Maximum Retries: Maximum number of times each download can be attempted.
- Timeout: The amount of time allowed for each download.
- Certificate File Path: Usually either \ or /, as most TFTP servers automatically determine the path to their default file location. Otherwise, the TFTP server absolute file path.
- Certificate File Name: The Web Administration Certificate filename in encrypted .PEM (Privacy Enhanced Mail) format.
- Certificate Password: To decrypt the SSL Web Admin Certificate, enter the SSL certificate password.

Click **Apply** and **Yes** to download the SSL Web Admin Certificate. The Alcatel Wireless Operating System informs you of the file transfer and the Certificate installation progress.

The SSL password decrypts the certificate, and the certificate is used for Secure Web Mode access when activated.



## **Command Buttons**

- Apply: Data or a Download SSL Certificate request is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but the result is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Delete Certificate: Instruct the Alcatel Wireless Operating System to delete the current SSL Certificate.

- **Regenerate Certificate:** Instruct the Alcatel Wireless Operating System to generate a new SSL Certificate to replace any existing Certificate; the Web Browser Interface displays the Successfully Generated SSL Web Admin Certificate message when done.
- Help: Request that the help page be displayed in a new browser window.

## **Telnet-SSH Configuration**

Use MANAGEMENT/Telnet-SSH to navigate to this page.

Use this page to modify Telnet accessibility to the Alcatel OmniAccess Switch or Appliance.

- **Telnet Login Timeout (minutes):** This object indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. May be specified as a number from 0 to 160. The factory default is 5.
- Maximum Number of Telnet Sessions: Selectable from a pulldown menus for values of from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The factory default is 5.
- **Allow New Telnet Sessions:** Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no.
- Note: New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.
  - **Allow New SSH Sessions:** Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

#### **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **Serial Port Configuration**

Use MANAGEMENT/Serial Port to navigate to this page.

Use this page to modify configurable serial session properties.

Table - Serial Session Properties

Parameter	Description	Range
Serial Port Login Timeout	Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Alcatel OmniAccess Switch or Appliance closes the connection.	Any numeric value between 0 and 160 is allowed. The default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port tries to connect. This is selected from a pull-down menu.	The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The Default is 9600 baud.
Character Size	The number of bits in a character.	8 (read-only).

Table - Serial Session Properties (Continued)

Parameter	Description	Range
Flow Control	Whether hardware flow-control is enabled or disabled.	Disabled (read-only).
Stop Bits	The number of Stop bits per character.	1 (read-only).
Parity	The parity method used on the Serial Port.	None (read-only).

#### **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

## **Local Management Users**

Use MANAGEMENT/Local Management Users to navigate to this page.

This page lists current management user logins on the Alcatel OmniAccess Switch or Appliance and the users' access privileges.

You may remove a user account by selecting **Remove**. Removing the default admin user prohibits both Web and CLI access to the Alcatel OmniAccess Switch or Appliance, so you must create a user provide with administrative (read/write) privileges BEFORE you remove the default user.

### **Command Buttons**

- New: Select to add a new management user (<u>Local Management Users > New</u>).
- **Help:** Request that the help page be displayed in a new browser window.

## **Local Management Users > New**

Use **MANAGEMENT/Local Management Users** then **New...** to navigate to this page.

Use this page to add management user accounts on the Alcatel OmniAccess Switch or Appliance and the user's access privileges.

Table - Management User Details

Parameter	Description
User Name	Login user name.
Password	Enter the user password. (Default = admin.)
Confirm Password	Confirm the user password. (Default = admin.)
User Access Mode	User privilege assignment can be ReadOnly or ReadWrite.

## **Command Buttons**

< Back: Return to the previous window.</li>

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

### **CLI Sessions**

Use **MANAGEMENT/User Sessions** to navigate to this page.

This page provides a list of open Command Line Interface Sessions. It details the following information.

Table - CLI Session Details

Parameter	Description
ID	Session identification.
User Name	Login user name.
Login Type	Telnet or serial session.
Connection From	Name of the client computer system or the physical port.
Idle time	Elapsed inactive session time.
Session Time	Elapsed active session time.

Select **Close** to halt an existing Telnet session.

### **Command Buttons**

• **Help:** Request that the help page be displayed in a new browser window.

## **Syslog Configuration**

Use **MANAGEMENT/Syslog** to navigate to this page.

- Use this page to Enable or Disable system logs.
- If you enable syslogs, enter the Syslog Server IP address.

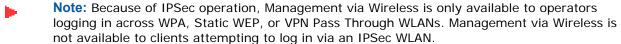
## **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

## **Mgmt Via Wireless**

Use MANAGEMENT/Mgmt Via Wireless to navigate to this page.

Use this page to enable or disable access to the Alcatel OmniAccess Switch or Appliance management interface from wireless clients. The default setting is disabled.



#### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Help: Request that the help page be displayed in a new browser window.

## Message Logs

Use **MANAGEMENT/Message logs** to navigate to this page.

This page allows you to set the Message Log filter to include the following or more critical messages:

- Critical Failure
- Software Error
- Authentication or Security Errors
- Unexpected Software Events
- Significant System Events

Click **Apply** to implement the desired Message Log filter level.

You can view the message logs which have been captured by the Alcatel OmniAccess Switch or Appliance, last to first message. Each trap entry includes the System Time, Filename and Line, Message Type and Message.

#### **Command Buttons**

- **Apply:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- **Help:** Request that the help page be displayed in a new browser window.

## **System Resource Information**

Use MANAGEMENT/Tech Support/System Resource Information to navigate to this page.

You can view the current Alcatel OmniAccess Switch or Appliance CPU usage, system buffer, and Web server buffers parameters on this page.

Click **Refresh** to update the values displayed on this page.

#### **Command Buttons**

Help: Request that the help page be displayed in a new browser window.

### **Switch Crash**

Use MANAGEMENT/Tech Support/Switch Crash to navigate to this page.

You can view the most recent Alcatel OmniAccess Switch or Appliance CPU crash files on this page, from most to least recent.

### **Command Buttons**

Help: Request that the help page be displayed in a new browser window.

### **AP Crash**

Use MANAGEMENT/Tech Support/AP Crash to navigate to this page.

This page allows you to select the OmniAccess AP to collect any available OmniAccess AP crash information on the AP Crash Information page.

Click the Get Crash link to view available crash information for the selected OmniAccess AP.

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

### **AP Crash Information**

Use MANAGEMENT/Tech Support/AP Crash and then Get Crash to navigate to this page.

You can view the most recent OmniAccess AP crash files on this page, from most to least recent.

#### **Command Buttons**

**Help:** Request that the help page be displayed in a new browser window.

## **Commands Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance Alcatel Wireless Operating System software management commands. Use the selector area to access the Alcatel Wireless Operating System software management data pages. Making this selection from the menu bar opens the *Download File to Switch* page.

Access the following pages from the Commands Menu Bar Selection:

- Download File to Switch
- Upload File from Switch
- System Reboot
- System Reboot > Save?
- System Reboot > Confirm
- Reset to Factory Default
- Set Time

### **Download File to Switch**

Use **COMMANDS/Download File** to navigate to this page.

Use this page to download and install new Alcatel OmniAccess Switch or Appliance Alcatel Wireless Operating System software or a configuration file to your Alcatel OmniAccess Switch or Appliance from a local TFTP (trivial file transfer protocol) server.

- Note: The TFTP server cannot run on the same computer as the OmniVista Air Control System, because the ACS and the TFTP server use the same communication port.
  - Select Code to download and automatically install new Alcatel OmniAccess Switch or Appliance Alcatel Wireless Operating System software. This process takes at least three minutes and overwrites your existing code and configuration. You must reboot the Alcatel OmniAccess Switch or Appliance after the new Alcatel Wireless Operating System software is installed.
  - Select Configuration to download a backup configuration file to the Alcatel OmniAccess Switch or Appliance.
  - Configure the IP address of the TFTP server, the Maximum Retries, the Timeout (in seconds), the directory path on the server (default = /), and the name of the file to be transferred.

#### **Command Buttons**

- Clear: Entries in the TFTP data fields are deleted.
- **Download:** Begin the download from the TFTP server; you are prompted to continue.
- **Help:** Request that the help page be displayed in a new browser window.

## **Upload File from Switch**

Use **COMMANDS/Upload File** to navigate to this page.

Use this page to upload files from your Alcatel OmniAccess Switch or Appliance to a local TFTP (trivial file transfer protocol) server. You can upload the following files:

- Configuration file
- Event Log
- Message Log

- Trap Log
- Crash file

Enter the IP address of the TFTP server, the directory path on the server (default = /), and a name for the file you have selected for upload.

Note: The TFTP server cannot run on the same computer as the OmniVista Air Control System, because the ACS and the TFTP server use the same communication port.

When you click **Upload**, the selected file is uploaded to your TFTP server and named what you entered in the File Name field.

#### **Command Buttons**

- Clear: Entries in the TFTP data fields are deleted.
- **Upload:** Begin the upload to the TFTP server; you are prompted for confirmation.
- Help: Request that the help page be displayed in a new browser window.

## **System Reboot**

Use **COMMANDS/Reboot** to navigate to this page.

This page allows you to restart the Alcatel OmniAccess Switch or Appliance. You are prompted to save your configuration changes on the next page, if you have not already saved configuration changes using the Save Configuration Administrative Tool at the top right of your screen.

### **Command Buttons**

- Reboot: Restart the Alcatel OmniAccess Switch or Appliance. (You are prompted for confirmation (<u>System Reboot > Save?</u>).
- Help: Request that the help page be displayed in a new browser window.

### **System Reboot > Save?**

Use **COMMANDS/Reboot** then **Reboot** to navigate to this page.

This page prompts you to restart the Alcatel OmniAccess Switch or Appliance after saving your configuration changes or restart without saving. Select the appropriate command button.

## **Command Buttons**

- **Save and Reboot:** Restart the Alcatel OmniAccess Switch or Appliance after saving your existing applied changes (<u>System Reboot > Confirm</u>).
- **Reboot Without Saving:** Restart the Alcatel OmniAccess Switch or Appliance using the existing configuration. All "Applied" changes are lost.
- Help: Request that the help page be displayed in a new browser window.

### System Reboot > Confirm

Use **COMMANDS/Reboot** then **Reboot** to navigate to this page.

This page allows you to confirm the restart of your Alcatel OmniAccess Switch or Appliance after saving your configuration changes. All system connections are lost so you must open a new session and log back into the Alcatel OmniAccess Switch or Appliance.

### **Command Buttons**

- Reboot: Restart the Alcatel OmniAccess Switch or Appliance.
- **Help:** Request that the help page be displayed in a new browser window.

## **Reset to Factory Default**

Use **COMMANDS/Reset to Factory Default** to navigate to this page.

This page allows you to reset the Alcatel OmniAccess Switch or Appliance configuration to the factory default. This overwrites all applied and saved configuration parameters! You are prompted for confirmation to re-initialize your Alcatel OmniAccess Switch or Appliance.

All configuration data files are deleted, and upon reboot, the Alcatel OmniAccess Switch or Appliance is restored to its original unconfigured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.



**Note:** After confirming configuration removal, you must reboot the Alcatel OmniAccess Switch or Appliance and select the "Reboot Without Saving" option.



**CAUTION:** Have a serial session active to complete <u>Using the Startup Wizard</u> as described in the <u>Alcatel OmniAccess Wireless Product Guide</u>!

#### **Command Buttons**

- Reset: Return configuration to factory default.
- **Help:** Request that the help page be displayed in a new browser window.

### **Set Time**

Use **COMMANDS/Set Time** to navigate to this page.

Use this page to set the current time and date on the Alcatel OmniAccess Switch or Appliance. Select the date and time from the drop-down menus and select **Apply**.

#### **Command Buttons**

- Apply: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect.
- Help: Request that the help page be displayed in a new browser window.

# **Using the Configuration Wizard**

When the Alcatel OmniAccess Switch or Appliance is activated for the first time from the factory, or when it has been rebooted after a *Reset to Factory Default*, the Web Browser interface displays the Web Configuration Wizard. Use the Configuration Wizard to configure the Alcatel OmniAccess Switch or Appliance for initial operation.

Perform the following steps to enter the initial Alcatel OmniAccess Switch or Appliance configuration:

- Collect the Initial Configuration Settings
- Connect Your Web Browser to the Alcatel OmniAccess Switch or Appliance
- Configuration Wizard System Information
- Service Interface Configuration
- Management Interface Configuration
- Miscellaneous Configuration
- Virtual Interface Configuration
- WLAN Policy Configuration
- RADIUS Server Configuration
- 802.11 Configuration
- Configuration Wizard Completed

## **Collect the Initial Configuration Settings**

Collect the high-level Alcatel OmniAccess Wireless Switch or Appliance parameters:

#### **System Parameters**

- Alcatel OmniAccess Switch or Appliance name.
- Supported protocols: 802.11a and/or 802.11b/g.
- New usernames and passwords (optional).

### **Network (Distribution System) Parameters**

- Distribution System (network) port static IP Address, netmask, and optional default gateway IP Address from the network planner.
- Service port static IP Address and netmask from the network planner (optional).
- Distribution System physical port (1000Base-T, 1000Base-SX, or 10/100Base-T).
- Distribution System port VLAN assignment (optional).
- Distribution System port Web and Secure Web mode settings, enabled or disabled.
- Distribution System port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age.

#### **WLAN Parameters**

WLAN Configuration: VLAN assignments, Layer 2 Security settings, Layer 3 Security settings, QoS assignments.

### **Mobility Parameters**

Mobility Settings: Mobility Group Name (optional).

#### **RADIUS Parameters**

RADIUS Settings.

#### **SNMP Parameters**

SNMP Settings.

#### **Other Parameters**

Other Port and Parameter Settings: Service port, OmniVista AirView Software, third-party APs, Serial/CLI Console port, 802.3x Flow Control, and System Logging.

#### **Other Actions**

Collect all files that may need uploading or downloading to the Alcatel OmniAccess Switch or Appliance, including the latest AWOS code.

Continue with Connect Your Web Browser to the Alcatel OmniAccess Switch or Appliance.

## Connect Your Web Browser to the Alcatel OmniAccess Switch or Appliance

- Temporarily configure your Web Browser device with a 192.168.1.2 IP address. Connect your Web Browser device to the Alcatel OmniAccess Switch or Appliance front-panel Service (Management) Port, either using a crossover ethernet cable or through an ethernet hub or switch.
- 2. Type 192.168.1.1 into the address line of your Web Browser to log into the Alcatel Web Browser Interface as described in the *Using the Web Browser Interface* section. The Web server built into the Alcatel OmniAccess Switch or Appliance responds with the login prompt.
- 3. Enter admin and admin as the login and password, respectively. The Alcatel OmniAccess Switch or Appliance displays the Configuration Wizard System Information page, in which you will configure the Alcatel OmniAccess Switch or Appliance name and administrative user login.

## **Configuration Wizard System Information**

- In the Configuration Wizard System Information page, enter the Alcatel OmniAccess Switch or Appliance name.
- Also in the Configuration Wizard page, enter a new administrative user name and password. 2. (Default = admin and admin, respectively.)
- Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the Service Interface Configuration page, in which you will configure the Service Port Interface.

## **Service Interface Configuration**

- Click the DHCP Protocol **Enable** box when the Service Port Interface is to obtain an IP address from a DHCP server. When the Service Port Interface is to use a fixed IP address, leave this box unchecked.
- The IP Address box contains the current Service Port Interface IP address. If desired, enter a different Service Port Interface IP address.
- The Netmask box contains the current Service Port IP netmask. If desired, enter a different Service Port Interface IP netmask.

4. Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the <u>Management Interface Configuration</u> page, in which you will configure the Management Interface.

## **Management Interface Configuration**

- 1. The VLAN Identifier box contains the current VLAN assignment (0 if untagged). If desired, enter a different Management Interface VLAN assignment (or 0 if untagged).
- 2. The IP Address box contains the current Management Interface IP address. If desired, enter a different Management Interface IP address.
- 3. The Netmask box contains the current Management Interface netmask. Enter a different Management Interface netmask.
- 4. The Gateway box contains the default Management Interface gateway. If desired, enter a different Management Interface gateway.
- 5. The Port Number box contains the current Management Interface physical port. If desired, enter a different Management Interface physical port.
- 6. The Primary DHCP Server box contains the default Management Interface primary DHCP server IP address. If necessary, enter a valid primary DHCP server IP address for the Management Interface.
- 7. The Secondary DHCP Server box contains the default Management Interface secondary DHCP server IP address. If necessary, enter a valid secondary DHCP server IP address for the Management Interface.
- 8. Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the <u>Miscellaneous Configuration</u> page, in which you will configure some Alcatel OmniAccess Wireless System parameters.

## **Miscellaneous Configuration**

- 1. The LWAPP Transport Mode box contains the current LWAPP Transport Mode (default = Layer 2). When you plan to use the Alcatel OmniAccess Switch or Appliance in an existing Layer 3 Alcatel OmniAccess Wireless System, enter Layer 3. Otherwise, leave as Layer 2.
- 2. The RF Mobility Domain Name box contains the default RF Mobility Domain Name. If desired, enter a different RF Mobility Domain Name.
- 3. The Country Code box contains the current Country Code. If desired, enter a different Country Code.
- 4. Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the *Virtual Interface Configuration* page, in which you will configure the Virtual Interface parameters.

## **Virtual Interface Configuration**

- 1. The IP Address box contains the default Virtual Interface IP address. Enter a different Virtual Interface IP address. Note that the Virtual Interface uses any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- 2. The DNS Host Name box contains a space for a Web Auth ID Certificate DNS Host Name. If the Alcatel OmniAccess Switch or Appliance will use an externally-generated Web Auth ID Certificate that includes a DNS Host Name, enter the DNS Host Name here.

3. Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the <u>WLAN Policy Configuration</u> page, in which you will configure the WLAN 1 parameters.

## **WLAN Policy Configuration**

Refer to the <u>WLANs > Edit</u> page for a description of these parameters.

- 1. The WLAN SSID box contains the current WLAN 1 SSID. If desired, enter a different SSID.
- The Radio Policy box contains the default bands controlled by the WLAN 1 policy. If desired, enter a different WLAN 1 policy: 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only, or All.
- The Admin Status box contains the default administrative status (unchecked, or disabled). If desired, enable the WLAN 1 policy by checking the Admin Status box.
- 4. The Session Timeout box contains the default 802.11 session timeout (0, or no timeout). If desired, enter a different 802.11 session timeout in minutes.
- 5. The Quality of Service (QoS) box contains the default QoS status (Bronze, or lowest QoS). If desired, enter a different QoS: Gold = highest, Silver, or leave as Bronze = lowest.
- 6. The Allow AAA Override box contains the default AAA Override status (unchecked, or disabled). If desired, enable AAA Override by checking the AAA Override box.
- 7. The Blacklist Timeout box contains the default client disable (blacklist) timeout status (checked, or enabled). If desired, disable Blacklist Timeout by unchecking the Blacklist Timeout box.
- 8. When Blacklist Timeout is enabled, enter the number of seconds a client is disabled (black-listed) upon failing to authenticate three consecutive times.
- 9. The DHCP Server Override box contains the current status (unchecked, or disabled). If desired, enable DHCP Server Override by checking the Override box.
- 10. The DHCP Addr. Assignment Required box contains the current status (unchecked, or not required). If desired, enable DHCP Address Assignment Required parameter by checking the Required box.
- 11. The Interface Name box contains the current WLAN 1 Interface (management). Leave this setting unchanged.
- 12. The Layer 2 Security box contains the default Layer 2 Security setting (802.1X). If desired, select a different Layer 2 Security setting: None, WPA, 802.1X, Static WEP, Cranite, or Fortress. Refer to the <u>WLANs > Edit</u> page for a description of these parameters, and the related parameters that can be set for Layer 2 Security.
- 13. The Layer 3 Security box contains the default Layer 3 Security setting (None). If desired, select a different Layer 3 Security setting: None, IPSec, or VPN Pass Through. Refer to the <u>WLANs > Edit</u> page for a description of these parameters, and the related parameters that can be set for Layer 3 Security.
- 14. Click **Next** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the <u>RADIUS Server Configuration</u> page, in which you will configure the RADIUS server parameters.

## **RADIUS Server Configuration**

If you do not want to configure a RADIUS server at this time, click **Skip** to ignore this section, and continue with the 802.11 Configuration section. If you do want to configure a RADIUS server, continue with this section.

1. If required, enter a RADIUS Server IP address.

- 2. If required, enter a RADIUS Server Shared Secret (password) in the Shared Secret and Confirm Shared Secret boxes.
- 3. The Port Number box contains the default communication port number (1812). If required, enter a different, unused communication port number.
- 4. The Server Status box contains the default RADIUS server status (Disabled). If desired, enable the RADIUS configuration by selecting Enabled.
- 5. Click **Apply** to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the <u>802.11 Configuration</u> page, in which you will activate or deactivate the different 802.11 bands and the OmniVista AirView Software (RRM software).

## **802.11 Configuration**

- The 802.11a Network Status box contains the current status (unchecked = disabled). If desired, check the box to activate the 802.11a Network in the Alcatel OmniAccess Wireless System
- 2. The 802.11b Network Status box contains the current status (unchecked = disabled). If desired, check the box to activate the 802.11b Network in the Alcatel OmniAccess Wireless System.
- 3. The 802.11g Network Status box contains the current status (unchecked = disabled). If desired, check the box to activate the 802.11g Network in the Alcatel OmniAccess Wireless System.
- 4. The AireView Director box contains the current AireView Director, or Radio Resource Management, status (checked = enabled). If desired, uncheck the box to disable the AireView Director dynamic channel number and transmit power level assignment functions.
- 5. Click Next to have the Alcatel OmniAccess Switch or Appliance save your inputs and display the Configuration Wizard Completed page, in which the Alcatel OmniAccess Switch or Appliance saves your changes in nonvolatile RAM and reboots the Alcatel OmniAccess Switch or Appliance.

## **Configuration Wizard Completed**

- Click the Save and Reboot button to have the Alcatel OmniAccess Switch or Appliance save your changes in nonvolatile RAM and reboot.
- The Alcatel Wireless Operating System prompts you to confirm the operation. Click **OK** to continue.

You have configured the Alcatel OmniAccess Switch or Appliance using the Web Browser Interface. If desired, continue with the *Alcatel OmniAccess Wireless Product Guide*.

Notes:

3/17/04 Notes 90-100778-300 Rev 1Alcatel OmniAccess Wireless System Web Browser Online Help

# **OmniVista Air Control System Online Help**

System Release 2.0

The OmniVista Air Control System (ACS Software) is a management tool that extends the capabilities of the Alcatel Web Browser and the Alcatel OmniAccess Wireless System Command Line Interface from an individual Alcatel OmniAccess Wireless Switch or Appliance to a network of Alcatel OmniAccess Switches and Appliances.

You can access the ACS Software Server through the ACS Software Java Admin Client which allows the ACS Software Server administrator to administer user accounts and schedule periodic maintenance tasks, and the ACS Software Browser Client, which allows ACS Software Server operators to control all other permitted ACS Software functions.

This help system is for ease-of-use of the ACS Software Browser Client. It is designed for use with Alcatel OmniAccess Switch or Appliance. Additional documentation for all Alcatel products and interfaces is available in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

This Online Help document is comprised of the following sections:

- <u>Logging into ACS</u>
- Using the ACS Interface
- Viewing System Maps, Devices, Templates and Reports
- Adding Maps, Devices and Templates
- Editing Templates, Maps and Devices
- Operating Devices

Refer to the <u>Glossary</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for definitions of common networking terms.

Refer to *Map Icons* for an explanation of the icons on the map displays.

# **Logging into ACS**

Use the login page shown below to log into ACS as follows:

- 1. Enter your user name.
- 2. Enter your password.
- 3. Click Submit.

Figure - Login Page



# **Using the ACS Interface**

The typical ACS interface page consists of the areas illustrated in the following figure.

Figure - ACS Interface



The following sections describe the ACS interface page areas and how to use them:

- Tabs/Menu Bar
- Sidebar Area
- Alarm Monitor
- Command Buttons
- Main Data Page
- Administrative Tools
- Applying Parameters
- Refreshing the Screen
- Map Icons

### Tabs/Menu Bar

There are two tabs shown on each screen: MONITOR and CONFIGURE. When you move the mouse over either one, the menu bar for that tab appears. The menu bar shows the names of the main monitoring and configuration areas of the Alcatel OmniAccess Switch or Appliance. The menu bar in white accented characters on a blue background. When you select either tabs or menu bar items they turn green.

#### **MONITOR Tab**

Refer to the following for available menu bar selections for the MONITOR tab:

- <u>MONITOR/Network Menu Bar Selection</u>
- MONITOR/Maps Menu Bar Selection
- <u>MONITOR/Switches Menu Bar Selection</u>
- MONITOR/Access Points Menu Bar Selection
- MONITOR/Clients Menu Bar Selection
- MONITOR/Alarms Menu Bar Selection
- MONITOR/Events Menu Bar Selection

#### **CONFIGURE Tab**

Refer to the following for available menu bar selections for the CONFIGURE tab:

- CONFIGURE/Templates Menu Bar Selection
- CONFIGURE/Switches Menu Bar Selection
- <u>CONFIGURE/Access Points Menu Bar Selection</u>

## Logo Rectangle

To the far left side of the menu bar is a rectangle with the Alcatel log. Click on this area to reveal the following information:

- Name of Product: OmniVista Air Control System
- Version Number, for example, 2.0.67.0
- Copyright (c) 2004 Alcatel Internetworking, Inc. All Rights Reserved.
- This product includes software developed by the Apache Software Foundation (http://www.apache.org)

### Sidebar Area

The sidebar area allows you to select a new configuration panel under the menu area that you have selected. You may select a single choice from several available for data that is to be displayed or configured. The selector area options will vary based on the menu that you have selected.

Some screens contain a group of menus in this area. Click the menu item to reveal a sub-menu and then click the item to select it.

Make a selection from the pulldown menus and click **Search**.

### **Alarm Monitor**

When the ACS Software receives a "rogue AP" message from an Alcatel OmniAccess Switch or Appliance, ACS Software generates an alarm, with an indicator visible in the lower left corner of any main ACS Software window.

Alarms are color coded as follows:

- Clear = No Alarm
- Red = Critical Alarm
- Orange = Major Alarm
- Yellow = Minor Alarm

Click any of these alarms to display details about the alarm(s) as follows:

- Rogues: Displays <u>Monitor Rogue AP Alarms</u>.
- Coverage: Displays <u>Monitor Coverage Holes on Floor Map</u>.
- Security: Displays Security Alarms. Refer to <u>MONITOR/Alarms Menu Bar Selection</u>.
- Switches: Displays Alcatel OmniAccess Switch and Appliance Alarms. Refer to <u>MONITOR/Alarms</u> <u>Menu Bar Selection</u>.
- Access Points: Displays Access Point Alarms. Refer to <u>MONITOR/Alarms Menu Bar Selection</u>.

## **Command Buttons**

ACS uses a number of command buttons throughout its screens. The most common of these are as follows:

- Apply to Switches: Apply the selected information to the Alcatel OmniAccess Switches and Appliances.
- Delete: Delete the selected information.
- Cancel: Cancel new information entered on the current screen and return to the previous screen.
- Save: Save the current settings.
- Audit: Discover the present status of this AP.
- Place AP: Fixes the position of the AP on the graphic map display and updates the display of its
  coordinates.

## **Main Data Page**

The main data page will depend on what information is required by the menu. Input fields on the data pages selected from the menu bar are of two basic types:

- Text Fields into which data may be entered using the keyboard.
- Pulldowns from which one of several options may be chosen.

Input fields are black text on a white background. When data is entered or selected, it is not sent to the Alcatel OmniAccess Switch or Appliance, but is saved in the field until the **GO** button is selected. There may be fields that contain buttons. Selecting a button does take immediate effect.

#### **Administrative Tools**

This area provides shortcuts to Administration functions that are used on a regular basis when configuring an Alcatel OmniAccess Switch or Appliance through the Web Interface.

- Logged in as: Displays the current user login.
- Logout: Click to log out.
- Refresh: Update the data on the current screen from the Alcatel OmniAccess Switch or Appliance.
- **Help:** Request that the help page be displayed in a new browser window.

## **Applying Parameters**

After submitting the new parameters or settings entered the page is refreshed. However, in some cases, the settings may appear different than specified by the operator. This happens where timers are involved and the affected code takes some period of time to execute. Refreshing the menu or tree will show the expected results. An example of this occurs when the spanning tree mode is enabled or disabled on the Alcatel OmniAccess Switch or Appliance.



**Note:** The exception is on the Maps pages. On these pages, use the Place command button to position the image before saving it.

## **Refreshing the Screen**

Using the refresh function from the web browser will refresh all screens and display the default initial screen in the main data area.

If you want to refresh a screen in the main data area, and there is no Refresh button present on that screen, use your mouse to right-click the main data area screen, then select the refresh option.

## Map Icons

The circular part of the OmniAccess AP icon can be split in half. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.



**Note:** When the icon is representing 802.11a and 802.11b, the top half displays the 802.11a status, and the bottom half displays the 802.11b/g status. When the icon is representing only 802.11a, the whole icon displays the 802.11a status. When the icon is representing only 802.11b/g, the whole icon displays the 802.11b/g status.

The following table shows the icons used on the ACS map displays.

Icon	Description
<b>\$</b>	The green icon indicates an OmniAccess AP (AP) with an operational state with no faults. The top half of the circle represents the 802.11a OmniAccess Radio. The bottom half of the circle represents the state of the 802.11b/g OmniAccess Radio.
<b>⇔</b>	The amber icon indicates an OmniAccess AP (AP) with an operational state with a minor fault. The top half of the circle represents the 802.11a OmniAccess Radio. The bottom half of the circle represents the state of the 802.11b/g OmniAccess Radio.  Note: A flashing yellow icon indicates there has been an 802.11a or 802.11b/g interference, noise, coverage or load Profile Failure. A flashing amber icon indicates there have been 802.11a and 802.11b/g Profile Failures.
<b>\$</b>	The red icon indicates an OmniAccess AP (AP) with an operational state with a major or critical fault. The top half of the circle represents the 802.11a OmniAccess Radio. The bottom half of the circle represents the state of the 802.11b/g OmniAccess Radio.
	The grayed-out icon with a question mark in the middle represents an unreachable OmniAccess AP. It is gray since its status cannot be known.
*	The icon with a red "x" in the center of the circle represents an OmniAccess AP that has been administratively disabled.
<b>\$</b>	The icon with the top half green and the lower half amber indicates that the 802.11a OmniAccess Radio (top) is operational with no faults, and the 802.11b/g OmniAccess Radio (bottom) has a minor fault. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.

Icon	Description
<b>\$</b>	The icon with the top half green and the lower half red indicates that the 802.11a OmniAccess Radio (top) is operational with no faults, and the 802.11b/g OmniAccess Radio (bottom) has a major or critical fault. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.
<b>(3</b>	The icon with the top half amber and the lower half red indicates that the 802.11a OmniAccess Radio (top) has a minor fault, and the 802.11b/g OmniAccess Radio (bottom) has a major or critical fault. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.
<b>\$</b>	The icon with the top half amber and the lower half green indicates that the 802.11a OmniAccess Radio (top) has a minor fault, and the 802.11b/g OmniAccess Radio (bottom) is operational with no faults. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.
<b>\$</b>	The icon with the top half red and the lower half green indicates that the 802.11a OmniAccess Radio (top) has a major or critical fault, and the 802.11b/g OmniAccess Radio (bottom) is operational with no faults. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.
<b>\$</b>	The icon with the top half red and the lower half amber indicates that the 802.11a OmniAccess Radio (top) has major or critical faults, and the 802.11b/g OmniAccess Radio (bottom) has a minor fault. The 'worst' of the two OmniAccess Radio colors determines the color of the triangle-shaped pointer.
*	The icon with a red "x" on the top half (802.11a) shows that the indicated OmniAccess Radio has been administratively disabled. The rest of the color coding is as described above. There are six possibilities as shown.
₩	
*	
<b>*</b>	
<b>☆</b>	
<b>₽</b>	

# Viewing System Maps, Devices, Templates and Reports

You can view Alcatel OmniAccess Wireless System Maps, Device Configurations, Templates, and AP and Audit Reports from the following:

- Monitor Predicted Coverage (RSSI)
- Monitor Channels on Floor Map
- Monitor Tx Power Levels on Floor Map
- Monitor Coverage Holes on Floor Map
- Monitor Users on Floor Map
- Monitor Clients From Floor Map
- MONITOR/Alarms Menu Bar Selection
- Monitor Alarms
- Monitor Roque AP Alarms
- <u>Monitor Alarms > Roque AP <MACaddress> > Detecting APs</u>
- <u>Monitor Roque Alarm > Events</u>
- Monitor Alarm > Events > Rogue AP < MACaddress >
- <u>MONITOR/Events Menu Bar Selection</u>
- Monitor Events
- Monitor Alarm > Events > <device name> <MACaddress>
- <u>Monitor Link Test Results</u>
- MONITOR/Network Menu Bar Selection
- Monitor Network Summary
- MONITOR/Maps Menu Bar Selection
- Monitor Maps
- Monitor Maps > Campus
- Monitor Maps > Campus > Building
- <u>Monitor Maps > Campus > Building > Floor</u>
- Monitor Maps > Building
- <u>Monitor Maps > Building > Floor</u>
- <u>Monitor Maps > Campus > <outdoor area></u>
- Monitor Alarms > Roque AP < MACaddress >
- Monitor Alarms > Roque AP < MACaddress > 2
- MONITOR/Switches Menu Bar Selection
- Monitor Switches > Search Results
- Monitor Switches > < IPaddress > Summary
- Monitor Switches > <IPaddress> > Ports > n
- Monitor Switches > <IPaddress> > Spanning Tree Protocol

- <u>Monitor Switches > <IPaddress> > CLI Sessions</u>
- <u>Monitor Switches > <IPaddress> > WLANs</u>
- Monitor Switches > <IPaddress> > Ports
- Monitor Switches > <IPaddress> > RADIUS Authentication Servers
- Monitor Switches > <IPaddress> > RADIUS Accounting Servers
- Monitor <IPaddress> > Local Authentication
- Monitor Switches > <IPaddress> > Mobility Stats
- <u>Monitor Switches > <IPaddress> > 802.11a Parameters</u>
- Monitor Switches > <IPaddress> > 802.11a RRM Groups
- <u>Monitor Switches > <IPaddress> > Switch 802.11b/g Parameters</u>
- Monitor Switches > <IPaddress> > 802.11b/q RRM Groups
- Monitor <IPaddress> > Interface
- Monitor <IPaddress> > Network Route
- Monitor <IPaddress> > Mobility Group <name> > Group Members
- Monitor WLAN
- Monitor <IPaddress> > WLANs > <WLAN ID>
- <u>Monitor Client <client name></u>
- Monitor Disabled Clients
- Monitor Access Control List
- Monitor Access Control List Template
- <u>Monitor <IPaddress> > Certificate</u>
- Monitor < IPaddress > Trap Receivers
- MONITOR/Access Points Menu Bar Selection
- Monitor Access Points > Search Results
- Monitor Access Points > <name>
- <u>Monitor Access Points > <name> > <Radio Type></u>
- Monitor RADIUS Authentication Server
- Configure RADIUS Accounting Server
- Monitor Local Authentication
- <u>Monitor Local Authentication > Template < name > </u>
- MONITOR/Clients Menu Bar Selection
- Monitor Clients Summary
- Monitor Watch Lists
- <u>Configure Watch Lists > New Watch List</u>
- Monitor Watch Lists > < list name >
- Monitor 802.11a Parameters

- Monitor 802.11a RRM Thresholds
- Monitor 802.11b/g Parameters
- Monitor 802.11b/g RRM Thresholds Template
- Monitor 802.11b/g RRM Intervals Template
- Monitor Historically Known Roque AP
- Monitor TFTP Server
- Monitor Trap Receiver
- Monitor Trap Controls
- Monitor Telnet SSH Template
- Monitor Syslog Configuration
- Monitor Access Points > Load
- Monitor Access Points > Dynamic Power Control
- Monitor Access Points > Noise
- Monitor Access Points > Interference
- Monitor Access Points > Coverage (RSSI)
- Monitor Access Points > Coverage (SNR)
- <u>Monitor Access Points > Up Time</u>
- Monitor <IPaddress> > Audit Reports
- Monitor <IPaddress> > Audit Report

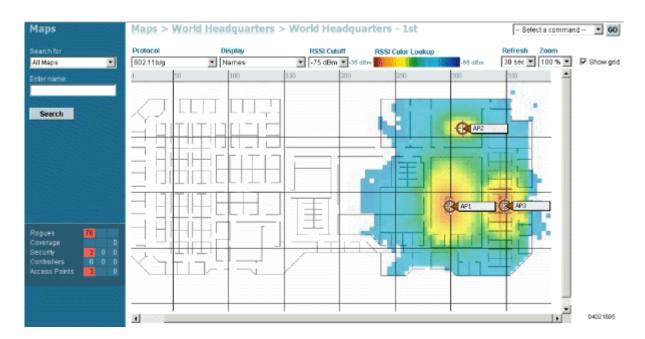
## **Monitor Predicted Coverage (RSSI)**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Protocol pulldown menu, select a protocol to access this page.

The display of predicted RF coverage on the map is determined by the selection you make from the Protocol pulldown:

- For 802.11a and 802.11b/g: This information is displayed in the panel next to the OmniAccess AP icon as follows: n% Failed (a+b), where n is the percentage of OmniAccess Radios that failed.
- For 802.11a: A colored overlay appears on the map displaying the coverage patterns for the 802.11a OmniAccess Radios. A Received Signal Strength Indicator (RSSI) Color Lookup appears at the top of the map indicating the meaning of the colors. The colors show the signal strength form RED (-35 dBm) through DARK BLUE (-85 dBm). Next to each OmniAccess AP is a percentage of failure.
- For 802.11b/g: A colored overlay appears on the map displaying the coverage patterns for the 802.11b/g OmniAccess Radios. Received Signal Strength Indicator (RSSI) Color Lookup appears at the top of the map indicating the meaning of the colors. The colors show the signal strength form RED (-35 dBm) through DARK BLUE (-85 dBm). Next to each OmniAccess AP is a percentage of failure.

A sample RF Prediction Heat Map with OmniAccess APs providing coverage at one end of a building appears in the following figure:



Refer to <u>Adding OmniAccess APs to an Alcatel OmniAccess Switch or Appliance</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## **Monitor Channels on Floor Map**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Channel** to access this page.

When you select this option, the channel number being used by the OmniAccess Radio is displayed on the panel next to each OmniAccess AP. This display depends upon the selection made from the Protocol pulldown as follows:

- 802.11a: The display shows the channel in the following format: Ch#n, where n is the channel number.
- 802.11b/g: The display shows the channel in the following format: Ch#n, where n is the channel number.
- 802.11a and 802.11b/g: The display shows the channels in the following format: Ch#n/x, where n represents the channel being used by the 802.11a OmniAccess Radio and x represents the channel being used by the 802.11b/g OmniAccess Radio.

## **Monitor Tx Power Levels on Floor Map**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Tx Power Level** to access this page.

When you select this option, the power level number being used by the OmniAccess Radio is displayed on the panel next to each OmniAccess AP.

Power Level (1, highest through 5, lowest) OmniAccess AP transmit power level are as follows:

- 1 = Maximum power allowed per Country Code setting
- 2 = 50% power
- 3 = 25% power

- 4 = 12.5% power
- 5 = 6.25% power)

The power levels and available channels are defined by the Country Code setting and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory</u> <u>Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

## **Monitor Coverage Holes on Floor Map**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Coverage Holes** to access this page.

In the Alarm Monitor, click on a colored Coverage alarm to access this page.

Coverage holes are areas where clients cannot receive a signal from the wireless network. When deploying wireless networks, there is a trade-off between the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations may receive marginal service. After launch, the Alcatel OmniVista AirView Software identifies these coverage areas and reports them to the IT manager, allowing the IT manager to fill holes based on user demand. This percentage is shown in the panel next to each OmniAccess AP on the map. They are displayed as follows:

- 802.11a: The display shows the coverage hole percentage for this OmniAccess Radio.
- 802.11b/g: The display shows the coverage hole percentage for this OmniAccess Radio.
- 802.11a and 802.11b/g: The display shows the total coverage hole percentage for both OmniAccess Radios.

### **Monitor Users on Floor Map**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Users** to access this page.

When you select this option, the number of clients being used by the OmniAccess Radio is displayed on the panel next to each OmniAccess AP. This display depends upon the selection made from the Protocol pulldown as follows:

- 802.11a: The display shows the number of clients using this protocol in the form n clients, where n is the number of clients. Click "n clients" to display a list of clients. Refer to <u>Monitor Clients From Floor Map</u>.
- 802.11b/g: The display shows the number of clients using this protocol. Click "n clients" to display a list of clients. Refer to <u>Monitor Clients From Floor Map</u>.
- 802.11a and 802.11b/g: The display shows the total number of clients using a combination of both protocols. Click "n clients" to display a list of clients. Refer to <u>Monitor Clients From Floor Map</u>.

## **Monitor Clients From Floor Map**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Users**, click **n clients** to access this page.

This page displays client parameters.

Table - Clients

Parameter	Description
Checkbox	Click to select, so that a command can be applied.
User Name	Name of the user. Refer to <u>Monitor Client <client name=""></client></u> .
IP Address	IP Address of the client.
MAC Address	MAC address of the client.
Access Point	Access Point Name. Refer to <u>Monitor Access Points &gt; <name></name></u> .
Switch	IP Address of Alcatel OmniAccess Switch or Appliance to which this OmniAccess AP is attached. Refer to <u>Monitor Switches &gt; <ipaddress> Summary</ipaddress></u> .
Port	Port number of the Alcatel OmniAccess Switch or Appliance to which this OmniAccess AP is attached.
Status	Associated or non-associated.
SSID	Service Set Identifier being broadcast by the OmniAccess Radio.
Auth	Authentication enabled. Yes or No.
Protocol	802.11a or 802.11b/g.

#### Select a command

Add to Watch List: Make sure a checkbox is selected, select this command and click **GO**. Refer to <u>Configure Clients</u> > <u>Add to Watch List</u> > <u><MAC address</u>>.

### **MONITOR/Alarms Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance alarms summary details. Use the selector area to access the respective alarms details.

Making this selection from the menu bar displays the *Monitor Alarms*.

## **Monitor Alarms**

### Use MONITOR/Alarms to access this page.

This page displays alarm information.

The data area of this screen contains a table with the following columns:

Table - Alarms

Parameter	Description
(checkbox)	Use this checkbox to select an alarm so you can take action on it.
Severity	Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

Table - Alarms (Continued)

Parameter	Description
Failure Object	Click the title to toggle between the name and the object in the Message column. Click a list item to display parameter details. Refer to <u>Monitor Alarms &gt; Rogue AP &lt; MACaddress &gt;</u> .
Owner	Name of person to whom this alarm is assigned.
Date/Time	When the alarm occurred. Click the title to toggle between ascending and descending order.
Message	Message explaining why the alarm occurred. Click the title to toggle between ascending and descending order (alphabetical).

If there are more than one page of alarms, the number of pages is displayed with a scroll arrow on each side. Use this to view additional alarms.

### Select a command pulldown

(Assign to me, Unassign, Delete, Clear and click GO.

#### Left sidebar

- Severity (pulldown): (All Severities, Critical, Major, Minor, Warning, Clear, Info).
- Alarm Category: (All Types, AP, Switch, Security, Coverage, Rogue AP).
- Search (button).

## **Monitor Rogue AP Alarms**

Click an alarm square in the Alarm Monitor (lower left-hand side of the screen) to access this page.

Rogue access point radios are unauthorized access points detected by Alcatel OmniAccess Switch or Appliance. This page displays rogue access point alarms based on the severity you clicked in the Alarm Monitor.

If there are more than one page of alarms, the number of pages is displayed with a scroll arrow on each side. Use this to view additional alarms.

This page contains the following parameters:

Table - Rogue Access Point AP Alarms

Parameter	Description
Checkbox	Select the alarms upon which you want to take action. See <u>Select a command</u> below.
Severity	The severity of the alarm: Critical, Major, Minor. Color coded. Refer to Alarm Monitor.
Rogue MAC Address	Media Access Control of the rogue access point. Refer to <u>Monitor Alarms &gt; Rogue AP &lt; MACaddress &gt;</u> .
Туре	Alarm type, for example AP.
Owner	Name of person to which this alarm is assigned.

Table - Rogue Access Point AP Alarms (Continued)

Parameter	Description
Date/Time	Date and time the alarm occurred.
State	State of the alarm, for example Alert.
SSID	Service Set Identifier being broadcast by the rogue access point radio.

#### Select a command

Select one or more alarms by checking its checkbox, select one of the following commands and click **GO**.

- Assign to me: Assign the selected alarm to the current user.
- Unassign: Unassign the selected alarm.
- Delete: Delete the selected alarm.
- Clear: Clears the selected alarm.

## Monitor Alarms > Rogue AP < MACaddress > Detecting APs

Use **MONITOR/Alarms** and click an item under Failure Object, from the Select a command pulldown, select **Detecting APs** to access this page.

Click an alarm square in the **Alarm Monitor** (lower left-hand side of the screen) click a list item under **Rogue MAC Addresses**, from the Select a command pulldown, select **Detecting APs** to access this page.

This page allows you to view information about the OmniAccess APs that are detecting a rogue access point.

Click a list item to display data about that item:

- AP Name: Refer to <u>Monitor Access Points > <name></u>.
- Radio: Refer to <u>Monitor Access Points</u> > <<u>name</u>> > <<u>Radio Type</u>>.
- Location: Refer to Monitor Maps > Campus > Building > Floor.
- SSID: Service Set Identifier being broadcast by the roque access point radio.
- Channel Number: Which channel the rogue access point is broadcasting on.
- WEP: Enabled or disabled.
- Pre-Amble: Long or short.
- RSSI: Received signal strength indicator in dBm.
- SNR: Signal-to-noise ratio.

## **Monitor Rogue Alarm > Events**

Use **MONITOR/Alarms** and click an item under Failure Objects from the Select a command pulldown, select **Event History** to access this page.

Click an alarm square in the **Alarm Monitor** (lower left-hand side of the screen) click a list item under **Rogue MAC Addresses**, from the Select a command pulldown, select **Event History** to access this page.

This page allows you review information about system events.

Click the title of each column to reorder the listings:

- Severity: Color coded display of the severity of the event. Refer to Alarm Monitor.
- Rogue MAC Address: Click a list item to display information about the entry. Refer to <u>Monitor Alarm > Events > Rogue AP < MACaddress ></u>.
- Date/Time: Date and time of the alarm.
- Channel: Channel upon which the alarm occurred.
- SSID: Service Set Identifier being broadcast by the rogue access point radio.

## Monitor Alarm > Events > Rogue AP < MACaddress >

Use **MONITOR/Alarms** and click an item under Failure Object, click Event History, click **Rogue AP** address to access this page.

Click an alarm square in the **Alarm Monitor** (lower left-hand side of the screen) click a list item under **Rogue MAC Addresses**, from the Select a command pulldown, select **Event History**, click **Rogue AP address** to access this page.

Use MONITOR/Events, and click a list item under Failure Object to access this page.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Alcatel OmniAccess Switches or Appliances.

Table - General

Parameter	Description
Rogue MAC Address	Media Access Control of the rogue access point.
Rogue Type	Type of rogue access point, for example, Infrastructure AP or Ad-Hoc (peer-to-peer).
Owner	Name of person to which this alarm is assigned.
State	State of this radio relative to the network or Alcatel OmniAccess Switch or Appliance. Rogue access point radios appear as "Alert" when first scanned by the Alcatel OmniAccess Switch or Appliance, or as "Pending" when Alcatel Wireless Operating System identification is still underway.
Channel Number	Which channel the rogue access point is broadcasting on.
SSID	Service Set Identifier being broadcast by the rogue access point radio.
Containment Level	An AP which is being contained will either not be able to provide service at all, or will provide exceedingly slow service. There is a level associated with the containment activity which indicates how many OmniAccess APs to use in containing the threat. This service is not automatic at this time and must be initiated and halted by the administrator. Containment Type - 'Contained' if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise "unassigned."
Created	Month, day, year, hour minute, second, am or pm.
Severity	Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

### Table - General (Continued)

Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded. Refer to Alarm
	<u>Monitor</u> .

- Message: Displays descriptive information about the alarm.
- **Help:** Displays information about the alarm.

### **MONITOR/Events Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance events summary details. Use the selector area to access the respective events details. Making this selection from the menu bar displays the *Monitor Events* page.

### **Monitor Events**

Use **MONITOR/Events** to access this page.

This page displays event information.

The data area of this screen contains a table with the following columns:

Table - Events

Parameter	Description
Severity	Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.
Failure Object	Click the title to toggle between the name and the object in the Message column. Click a list item to display parameter details. Refer to <u>Monitor Alarm &gt; Events &gt; <device name=""> <macaddress></macaddress></device></u> .
Date/Time	When the event occurred. Click the title to toggle between ascending and descending order.
Message	Message explaining why the event occurred. Click the title to toggle between ascending and descending order (alphabetical).

If there are more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

### Left sidebar

- Severity (pulldown): (All Severities, Critical, Major, Minor, Warning, Clear, Info).
- Alarm Category: (All Types, AP, Switch, Security, Coverage, Rogue AP).
- Search (button).

### Monitor Alarm > Events > <device name> <MACaddress>

Use MONITOR/Events, and click a list item under Failure Object to access this page.

This page information for a specific event. It contains the following information:

#### Table - General

Parameter	Description
Failure Object	Click the title to toggle between the name and the object in the Message column. Click a list item to display parameter details. Refer to <u>Monitor Alarm &gt; Events &gt; <device name=""> <macaddress></macaddress></device></u> .
Owner	Owner of the event.
Category	Type of alarm, for example, Security
Created	When the event occurred.
Severity	Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

- Help: A short explanation of the event.
- Message: Message explaining why the event occurred. Click the title to toggle between ascending and descending order (alphabetical).

### **Monitor Link Test Results**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Users**, click **n clients**, click **User Name**, from the Select a Command pulldown, select **Link Test Results** to access this page.

When the link test is performed from the Client <cli>client name> page, results similar to those below, appear in a pop up window:

```
Link test to: 00.0c:41:15:1b:55

Link test Packets sent: 20

Link test Packets received: 20

Local Signal Strength: -56 dBm

Local Signal to Noise Ratio: 39 dBm
```

View the results and click **OK**.

# **MONITOR/Network Menu Bar Selection**

Use MONITOR/Network to access Monitor Network Summary.

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance and OmniAccess Radio summary details.

# **Monitor Network Summary**

Use MONITOR/Network to access this page.

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance and OmniAccess Radio summary details. Use the selector area to access the respective network details.

The following information appears on the Monitor/Network Menu Bar Selection:

- Switches: Displays the total number of Alcatel OmniAccess Switches and Appliances and the number that are unreachable.
- Coverage Areas

- Most Recent Critical Rogue APs
- <u>Top 5 APs</u>
- <u>Top 5 Coverage Holes</u>
- <u>Clients</u>
- <u>Left Sidebar</u>

# **Coverage Areas**

This table contains the following information:

Column	Description
Name	Displays a hierarchy of the coverage area in the form campus,building,outdoor area, andfloor. Refer to <u>Monitor Maps &gt; Campus</u> , <u>Monitor Maps &gt; Campus &gt; Building</u> , <u>Monitor Maps &gt; Campus &gt; coutdoor area &gt; Campus &gt; Building &gt; Floor</u> .
Total APs	Displays the total number of OmniAccess Radios detected.
a Radios	Displays the number of 802.11a OmniAccess Radios.
b/g Radios	Displays the number of 802.11b/g OmniAccess Radios.
OOS Radios	Displays the number of Out of Service Alcatel OmniAccess Wireless Access Points associated with this Alcatel OmniAccess Switch or Appliance.
Clients	Displays the number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.

# **Most Recent Critical Rogue APs**

This table contains the following information:

Column	Description
MAC Address	Media Access Control of the rogue access point. Click any MAC address in the list. Refer to <u>Monitor Alarms &gt; Rogue AP &lt; MACaddress &gt;</u> .
SSID	Service Set Identifier being broadcast by the rogue access point radio.
Channel	Which channel the rogue access point is broadcasting on.
Туре	Access point's RF type.
Date/Time	Date and Time of the rogue access point's detection.

# Top 5 APs

This table contains the following information:

Column	Description
AP Name	This is the name assigned to the OmniAccess AP. Click an OmniAccess AP Name to display <i>Monitor Access Points</i> > < <i>name</i> >.

Column	Description
Location	User-defined location map. Refer to <u>Monitor Maps &gt; Campus</u> .
a Clients	Number of 802.11a clients currently associated with the Alcatel OmniAccess Switch or Appliance.
b Clients	Number of 802.11b clients currently associated with the Alcatel OmniAccess Switch or Appliance.
g Clients	Number of 802.11g clients currently associated with the Alcatel OmniAccess Switch or Appliance.
Total	Total number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.

# **Top 5 Coverage Holes**

Coverage holes are areas where clients cannot receive a signal from the wireless network. When deploying wireless networks, there is a trade-off between the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations may receive marginal service. After launch, the OmniVista AirView Software identifies these coverage areas and reports them to the IT manager, allowing the IT manager to fill holes based on user demand.

This table contains the following information:

- Access Point: Number of coverage holes found per OmniAccess AP. If none were found, the message "No Coverage Holes Found" appears.
- Percent: Percentage of coverage are that cannot receive a signal.

### **Clients**

This graphs associated clients versus time.

# Left Sidebar

The left side bar for this screen contains the following:

- Search for Alcatel OmniAccess Switches and Appliances by (pulldown):
  - IP Addresses: Local network IP Address of the Alcatel OmniAccess Switch or Appliance <u>Management Interface</u>, described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - Switch Name: The user-defined name for the Alcatel OmniAccess Switch or Appliance.
  - Networks: Networks available.
- Select a Network (All Networks, x.x.x.x).
- Search button.

## **MONITOR/Maps Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance maps summary details. Use the selector area to access the respective network details. Making this selection from the menu bar displays the <u>Monitor Maps</u> page.

# **Monitor Maps**

## Use MONITOR/Maps to access this page.

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance map displays and details. Use this screen to create a campus (then building, then floors), or a building (then floors) upon which to place Access Points. Note that the campus map files can be anywhere in your file system, and that the map files are automatically backed up when ACS is backed up.

The following information appears on the Maps Page:

- Name: Click any Name in the list. Refer to <u>Monitor Maps > Campus</u>, <u>Monitor Maps > Campus > Building</u> or <u>Monitor Maps > Building</u>.
- Type: Indicates the type of map, that is, campus or building.
- Status: A colored icon indicating the status (green for Up, yellow for Warning, or red for Down).

#### Right Command pulldown

Select a command and click GO:

- New Campus.... Refer to <u>Configure Maps > New Campus</u>.
- New Building... For creation of a new building on an existing campus, refer to <u>Configure Campus</u>
   <u>New Building</u>. For creation of a new building without a campus, refer to <u>Configure Maps</u> > <u>New Building</u>.
- Properties -- Select and click GO. Refer to <u>Configure Maps > Properties</u>.
- GO (button).

#### Left sidebar

- Search for (pulldown): (All Maps, Campuses, Buildings, Floor Areas, Outdoor Areas, Access Points).
- Enter Name (text).
- **Search**: Make a selection from the pulldown, or enter a name and click.

# **Monitor Maps > Campus**

From <u>Monitor Network Summary</u>, click a Campus in the Coverage Areas Name column to access this page.

From *Monitor Maps*, click a Campus in the Name column to access this page.

Use **CONFIGURE/Switches** and click an list item under the **Location** column to access this page.

This page allows you to view a map of the campus. Double-click the map to enlarge it. Whether or not it is enlarged, the page shows the following item:

Show grid checkbox: Overlays a grid in feet of the campus map.

#### Select a command

- New Building: Select this command and click **GO** to add a new building with devices to the campus. Refer to <u>Configure Campus > New Building</u>.
- New Outdoor Area: Select this command and click **GO** to add a new outdoor area with devices to the campus. Refer to <u>Configure Campus > New Outdoor Area</u>.
- Edit Campus: Select this command and click **GO** to change an already existing campus. Refer to <u>Configure Maps > Edit Campus < name ></u>.

• Delete Campus: Select this command and click **GO** to delete a selected campus. When you do this, the following message appears: "Are you sure you want to delete this Campus and all its contents, if any? Also note that any APs contained by Campus or its containers will be moved to Unassigned State." Click **OK** or **Cancel**.

# Monitor Maps > Campus > Building

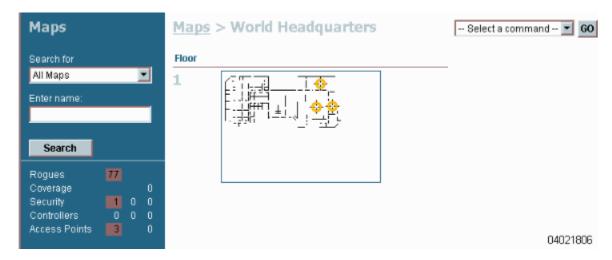
From <u>Monitor Network Summary</u>, click a --Building in the Coverage Areas Name column to access this page.

Use **MONITOR/Maps**, then click an item in the **Name** column, to access this page.

This page allows you to view a map of the selected campus building.

Note: The maps are designed to stack floors in a representational decreasing order. That is, from top to bottom in a building with three floors and two basements, you will see Floor 3, Floor 2, Floor 1, Basement 1 and Basement 2.

When you view maps that have already had APs added (using <u>Configure Add Access Points</u>), you will see AP icons similar to the following:



- Move your cursor over an icon to have ACS display the AP name.
- These icons are colored to indicate AP status: Green (both OmniAccess Radios are active, or one of them is up and the other is administratively disabled), Amber (one or both OmniAccess Radios are experiencing an interference, noise, coverage or load Profile Failure), or Red (both OmniAccess Radios have failed).

#### Select a command

Select a command and click GO.

- New Floor Area: This command allows you to add a new floor area. Refer to <u>Configure Building</u>
   New Floor.
- Edit Building: This commands allows you to edit an existing building. Refer to <u>Configure Maps > Edit Building > <name></u>.
- Delete Building: Select this command and click **GO** to delete a selected building. When you do this, the following message appears: "Are you sure you want to delete this building and all its contents, if any? Also note that any APs contained by building or its containers will be moved to Unassigned State." Click **OK** or **Cancel**.

**Single-click a map to enlarge it.** When enlarged, the page shows the following items. The pulldowns control the icon display. Refer to <u>Monitor Maps > Campus > Building > Floor</u>.

# Monitor Maps > Campus > Building > Floor

From <u>Monitor Network Summary</u>, click a Building Floor in the Coverage Areas Name column to access this page.

Use MONITOR/Access Points and click a list item under Location to access this page.

Use **MONITOR/Maps**, then click an item in the **Name** column, then double-click the floor map to access this page.

This page allows you to view a map of the selected campus building floor.

#### **AP Icons**

If any APs have been added, an icon of cross-hairs surrounded by a circle represent AP locations. The colors of the circles (refer to <u>Alarm Monitor</u>) indicate the alarm status of the OmniAccess Radio.

- Each AP contains two OmniAccess Radios.
  - When a single protocol is selected (that is, 802.11a or 802.11b/g) the entire icon represents this condition.
  - When both protocols are selected (that is, 802.11a and 802.11b/g), the top half of the circle represents the state of the 802.11a OmniAccess Radio and the bottom half of the circle represents the 802.11b/g OmniAccess Radio.
- Blinking AP icons indicate that an interference, noise, coverage or load Profile Failure Alarm is pending against the specific AP.
- Click the AP icon to review information about the AP performance. Refer to <u>Monitor Access</u>
   *Points* > < name > .
- If a OmniAccess Radio is disabled, a small "x" will appear on the portion of the icon circle representing the AP.

The following pulldowns control the icon display:

## Protocol pulldown

- 802.11a and 802.11b (the default display).
- 802.11a.
- 802.11b.

Depending upon which protocol you select, an overlay on the map displays the predicted coverage of the selected OmniAccess Radio. Refer to <u>Monitor Predicted Coverage (RSSI)</u>.

### Display pulldown

- Channels: Refer to <u>Monitor Channels on Floor Map</u>.
- Tx Power Level: Refer to <u>Monitor Tx Power Levels on Floor Map</u>.
- Coverage Holes: Refer to <u>Monitor Coverage Holes on Floor Map</u>.
- MAC Address: In the panel next to the AP icon on the map, displays the MAC address of the AP.
- Names: In the panel next to the AP icon on the map, displays the name of the AP.
- Users: Refer to <u>Monitor Users on Floor Map</u>.

# **RSSI Color Lookup**

Describes the color-keyed coverage area on the map.

#### Select a command

- Add Access Points: This allows you to add access points to the selected floor on the map display. Refer to <u>Configure Add Access Points</u>.
- Position APs: Allows you to position Access Points on the building floor plan. Refer to <u>Configure</u>
   *Position Access Points on Floor <floor name>*.
- Remove Access Points: This allows you to remove specified Access Points from the floor plan. Refer to *Configure Remove Access Points*.
- Edit Floor Area: This allows you to modify the parameters of the floor area. Refer to <u>Configure <building name > Edit Floor <floor name ></u>.
- Delete Floor Plan: This allows you to delete a specified floor.
- GO button.

#### Refresh pulldown

Refreshes the page display. Selections are: 5 sec, 10 sec, 15 sec, 30 sec, 1 min, 5 min (default).

#### Zoom pulldown

Determines the size of the map display, leaving the icon size unchanged. Selections are: 50%, 75%, 90%, 100%, 125%, 150%, 200%, 300%. Scroll bars appear when the enlarged map covers more than the space on the page.

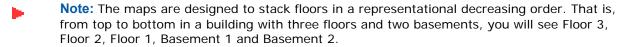
#### **Show Grid**

This check box allows you to place a grid over the map on the page.

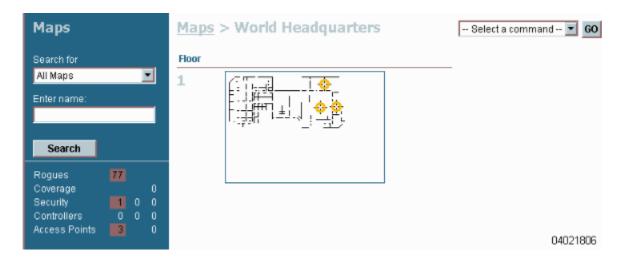
## **Monitor Maps > Building**

When you have created a building that is not part of a campus, from <u>Monitor Network Summary</u>, click a Building in the Coverage Areas Name column to access this page.

This page allows you to view a map of the selected building.



When you view maps that have already had APs added (using <u>Configure Add Access Points</u>), you will see AP icons similar to the following:



- Move your cursor over an icon to have ACS display the AP name.
- These icons are colored to indicate AP status: Green (both OmniAccess Radios are active, or one of them is up and the other is administratively disabled), Amber (one or both OmniAccess Radios are experiencing an interference, noise, coverage or load Profile Failure), or Red (both OmniAccess Radios have failed).

#### Select a command

Select a command and click GO.

- New Floor Area: This command allows you to add a new floor area. Refer to <u>Configure Building</u>
   New Floor.
- Edit Building: This commands allows you to edit an existing building. Refer to <u>Configure Maps > Edit Building > <name ></u>.
- Delete Building: Select this command and click **GO** to delete a selected building. When you do this, the following message appears: "Are you sure you want to delete this building and all its contents, if any? Also note that any APs contained by building or its containers will be moved to Unassigned State." Click **OK** or **Cancel**.

**Single-click a map to enlarge it.** When enlarged, the page shows the following items. The pulldowns control the icon display. Refer to *Monitor Maps > Campus > Building > Floor*.

## Monitor Maps > Building > Floor

From <u>Monitor Network Summary</u>, click a Building Floor in the Coverage Areas Name column to have ACS display <u>Monitor Maps > Building</u>, then click a floor plan map to access this page.

This page allows you to view a map of the selected building floor.

#### AP Icons

If any OmniAccess APs have been added, an icon of cross-hairs surrounded by a circle represent Omni-Access AP locations. The colors of the circles (refer to <u>Alarm Monitor</u>) indicate the alarm status of the OmniAccess Radio.

- Each OmniAccess AP contains two OmniAccess Radios.
  - When a single protocol is selected (that is, 802.11a or 802.11b/g) the entire icon represents this condition.

- When both protocols are selected (that is, 802.11a and 802.11b/g), the top half of the circle represents the state of the 802.11a OmniAccess Radio and the bottom half of the circle represents the 802.11b/g OmniAccess Radio.
- Blinking OmniAccess AP icons indicate that an interference, noise, coverage or load Profile Failure Alarm is pending against the specific OmniAccess AP.
- Click the OmniAccess AP icon to review information about the OmniAccess AP performance.
   Refer to Monitor Access Points > <name>.
- If a OmniAccess Radio is disabled, a small "x" will appear on the portion of the icon circle representing the OmniAccess AP.

The following pulldowns control the icon display:

### Protocol pulldown

- 802.11a and 802.11b (the default display).
- 802.11a.
- 802.11b.

Depending upon which protocol you select, an overlay on the map displays the predicted coverage of the selected OmniAccess Radio. Refer to *Monitor Predicted Coverage (RSSI)*.

## Display pulldown

- Channels: Refer to <u>Monitor Channels on Floor Map</u>.
- Tx Power Level: Refer to <u>Monitor Tx Power Levels on Floor Map</u>.
- Coverage Holes: Refer to <u>Monitor Coverage Holes on Floor Map</u>.
- MAC Address: In the panel next to the OmniAccess AP icon on the map, displays the MAC address of the OmniAccess AP.
- Names: In the panel next to the OmniAccess AP icon on the map, displays the name of the OmniAccess AP.
- Users: Refer to Monitor Users on Floor Map.

#### **RSSI Color Lookup**

Describes the color-keyed coverage area on the map.

### Select a command

- Add Access Points: This allows you to add access points to the selected floor on the map display. Refer to <u>Configure Add Access Points</u>.
- Position APs: Allows you to position Access Points on the building floor plan. Refer to <u>Configure Position Access Points on Floor <floor name></u>.
- Remove Access Points: This allows you to remove specified Access Points from the floor plan. Refer to *Configure Remove Access Points*.
- Edit Floor Area: This allows you to modify the parameters of the floor area. Refer to <u>Configure</u>
   <u>Souilding name</u> <u>Floor of the floor area.</u> Refer to <u>Configure</u>
- Delete Floor Plan: This allows you to delete a specified floor.
- GO button.

#### Refresh pulldown

Refreshes the page display. Selections are: 5 sec, 10 sec, 15 sec, 30 sec, 1 min, 5 min (default).

## Zoom pulldown

Determines the size of the map display, leaving the icon size unchanged. Selections are: 50%, 75%, 90%, 100%, 125%, 150%, 200%, 300%. Scroll bars appear when the enlarged map covers more than the space on the page.

#### **Show Grid**

This check box allows you to place a grid over the map on the page.

# Monitor Maps > Campus > <outdoor area>

From <u>Monitor Maps > Campus</u>, click the name of the outdoor area on the campus map to view the outdoor area graphic is displayed.

This page allows you to view a map of the selected campus outdoor area.

Select a command: Select a command and click GO.

- Add Access Points: Allows you to add access points to the outdoor area if any are available.
- Edit Outdoor Area: Refer to <u>Configure Campus > Edit Outdoor Area < name ></u>.
- Delete Outdoor Area: Deletes the selected outdoor area.

# Monitor Alarms > Rogue AP < MACaddress >

From Monitor Network Summary, click a roque access point MAC Address to access this page.

### Use MONITOR/Alarms and click an item under Failure Objects to access this page.

Click an alarm square in the **Alarm Monitor** (lower left-hand side of the screen) and click a list item under **Rogue MAC Addresses** to access this page.

This page allows you to view rogue access point radio information. Rogue access point radios are unauthorized access points detected by Alcatel OmniAccess Switch or Appliance.

Table - General

Parameter	Description
Rogue MAC Address	Media Access Control of the rogue access point.
Rogue Type	Type of rogue access point, for example AP.
Owner	Name of person to which this alarm is assigned.
Status	Configurable state of this radio relative to the network or Alcatel OmniAccess Switch or Appliance. Rogue access point radios will appear as "Alert" when first scanned by the Alcatel OmniAccess Switch or Appliance, or as "Pending" when Alcatel Wireless Operating System identification is still underway.
Channel Number	Which channel the rogue access point is broadcasting on.
SSID	Service Set Identifier being broadcast by the rogue access point radio.

Table - General (Continued)

Containment Level	This feature allows the administrator to target a rogue access point for containment. An AP which is being contained will either not be able to provide service at all, or will provide exceedingly slow service. There is a level associated with the containment activity which indicates how many OmniAccess APs to use in containing the threat. This service is not automatic at this time and must be initiated and halted by the administrator. Containment Type - 'Contained' if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise "unassigned".
Created	Month, day, year, hour minute, second, am or pm.
Modified	Month, day, year, hour minute, second, am or pm.
Severity	Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.

- Annotations: Use this text box to type notes about this rogue access point radio, then click Add.
- Message: Displays descriptive information about the alarm.
- Help: Displays information about the alarm.
- History: Displays alarm history.

#### Select a command

- Assign to me: Assigns this alarm to the user.
- Unassign: Unassigns this alarm from the user.
- Delete: Deletes the displayed alarm.
- Event History: Refer to <u>Monitor Rogue Alarm > Events</u>.
- Detecting APs: Refer to <u>Monitor Alarms > Roque AP <MACaddress> > Detecting APs</u>.
- Map (High resolution): For High resolution Heat Maps, you must have ACS Location (High-Resolution) Software (OV-ACSLOC). Low Resolution Heat Maps are enabled for ACS Basic (Low-Resolution) Software (OV-ACS-BASE).
- Trend: Refer to <u>Monitor Alarms > Roque AP <MACaddress>2</u>.
- Set State to "Unknown": Sets the alarm state as indicated.
- Set State to "Known-Internal": Sets the alarm state as indicated.
- Set State to "Know-External": Sets the alarm state as indicated.
- Level 1 Containment, Level 2 Containment, Level 3 Containment, Level 4 Containment: This feature allows the administrator to target a rogue access point for containment. An AP which is being contained will either not be able to provide service at all, or will provide exceedingly slow service. There is a level associated with the containment activity which indicates how many OmniAccess APs to use in containing the threat. Note that this service is not automatic at this time and must be initiated and halted by the administrator.

# Monitor Alarms > Rogue AP < MACaddress > 2

Use **MONITOR/Alarms** and click an item under Failure Object from the Select a command pulldown, select the **Trend** command to access this page.

Click an alarm square in the **Alarm Monitor** (lower left-hand side of the screen) click a list item under **Rogue MAC Addresses**, from the Select a command pulldown, select **Trend** to access this page.

This page allows you to view a line graph of RSSI in dBm against time for the APs.

### MONITOR/Switches Menu Bar Selection

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance summary details. Use the selector area to access the respective Alcatel OmniAccess Switch or Appliance details.

Making this selection from the menu bar displays <u>Monitor Switches > Search Results</u>.

### Monitor Switches > Search Results

Use MONITOR/Switches to access this page.

The data area of this screen contains a table with the following columns:

- IP Address: Local network IP Address of the Alcatel OmniAccess Switch or Appliance
   <u>Management Interface</u>, described in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Click an IP
   Address in the list. Refer to <u>Monitor Switches</u> > < <u>IPaddress</u> > Summary.
- Switch Name: Click the title to toggle from ascending to descending order.
- Location: The geographical location (such as a campus or building).
- Version: The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
- Status: (colored icon).

## Left sidebar

Search for Alcatel OmniAccess Switches and Appliances by (pulldown):

- IP Addresses: Local network IP Address of the Alcatel OmniAccess Switch or Appliance
   <u>Management Interface</u>, described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- Switch Name.
- Networks: Select a Network (All Networks, x.x.x.x).
- Search (button).

## Monitor Switches > < IPaddress > Summary

Use **MONITOR/Switches** and click one of the IP addresses under IP Address to access this page.

From *Monitor Access Points* > <*name* >, click **Registered Switch** to access this page.

Use **CONFIGURE/Access Points** and select a list item under **AP Name**, then click **Registered Switch** to access this page.

This page displays a summary of Alcatel OmniAccess Switch or Appliance parameters with a graphic displaying the actual Alcatel OmniAccess Switch or Appliance.

Click **Switches** in the page title to view a list of all Alcatel OmniAccess Switches and Appliances. Refer to *Monitor Switches > Search Results*.

Graphic of front of Alcatel OmniAccess Switch or Appliance with front-panel ports (click a port to go to  $\underline{Monitor\ Switches} > \underline{IPaddress} > \underline{Ports} > \underline{n}$  for information about that port).

Table - General

Parameter	Description
IP Address	Local network IP Address of the Alcatel OmniAccess Switch or Appliance <u>Management Interface</u> , described in the <u>Alcatel OmniAccess Wireless</u> <u>Product Guide</u> .
UP Time	Time in days, hours and minutes since the last reboot.
Name	User-defined name of the Alcatel OmniAccess Switch or Appliance.
Location	Physical location of the Alcatel OmniAccess Switch or Appliance.
Total Client Count	Total number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
Current LWAPP Transport Mode	Lightweight Access Point Protocol transport mode. Communications between Alcatel OmniAccess Switches or Appliances and access points. Selections are Layer 2 or Layer 3.

Table - Inventory

Parameter	Description
Software Version	The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
Description	Description of the inventory item, for example, Alcatel Switch.
Model No.	Specifies the Machine Model as defined by the Vital Product Data.
Serial No.	Unique Serial Number for this Alcatel OmniAccess Switch or Appliance.
Burned-in MAC Address	The burned-in Medium Access Control address for this Alcatel OmniAccess Switch or Appliance.
Maintenance Level	The Alcatel OmniAccess Switch or Appliance maintenance level, for example, 1.1.0.3.
GigE Card Present	Displays the presence or absence of the optional 1000Base-T/ 1000Base-SX GigE card.
Crypto Card Present	Displays the presence or absence of an optional Enhanced Security Module which enables IPSec security and which provides enhanced processing power.

**GIGE Port(s) Status**: Up or Down. Click to review the status of the port. Refer to  $\underline{Monitor\ Switches} > \underline{IPaddress} > \underline{Ports} > \underline{n}$ .

#### Table - Access Points

Parameter	Description
Access Points	Name of the Access Point. Click to access ( <u>Monitor Access Points &gt; <name></name></u> ).
MAC Address	Medium Access Control address for this AP.
Port	Alcatel OmniAccess Switch or Appliance port number of the client's associated access point.
Status	Status of the Access Point. Colored icon: Red (down) or Green (up).

# Sidebar Menu: Switch

- System
  - Summary: Displays the Switch Summary page (this page).
  - Spanning Tree Protocol: Refer to <u>Monitor Switches > <IPaddress> > Spanning Tree Protocol</u>.
  - CLI Sessions: Refer to *Monitor Switches > <IPaddress> > CLI Sessions*.
- WLANs: Refer to <u>Monitor WLAN</u>.
- Ports: Refer to <u>Configure <IPaddress> > Ports > <port#></u>.
- RADIUS
  - Authentication: Refer to <u>Monitor Switches > <IPaddress> > RADIUS Authentication Servers</u>.
  - Accounting: Refer to <u>Monitor Switches > <IPaddress> > RADIUS Accounting Servers</u>.
- Mobility
  - Mobility Stats: Refer to <u>Monitor Switches > <IPaddress> > Mobility Stats</u>.
- 802.11a
  - Parameters: Refer to <u>Monitor Switches > <IPaddress> > 802.11a Parameters</u>.
  - RRM Grouping: Refer to *Monitor Switches* > <*IPaddress* > \* 802.11a RRM Groups.
- 802.11b/g
  - Parameters: Refer to <u>Monitor Switches > <IPaddress> > Switch 802.11b/g</u>
    <u>Parameters</u>.
  - RRM Grouping; Refer to <u>Monitor Switches > <IPaddress> > 802.11b/g RRM Groups</u>.

### Monitor Switches > < IPaddress > Ports > n

Use **MONITOR/Switches,** click one of the IP addresses under **IP Address**, and click a port to access this page.

Use **MONITOR/Access Points** and click a list item under AP Name, click **Registered Switch**, then click a port to access this page.

Use **MONITOR/Clients** and click a list item under AP Name, then click **Registered Switch**, then click a port to access this page.

This page displays information about a specific physical port (n) on a selected Alcatel OmniAccess Switch or Appliance.

Table - Interface

Parameter	Description
Operational Status	Displays the operational status of the Alcatel OmniAccess Switch or Appliance: either UP or DOWN.
Unknown Protocol Packets	The number of packets of unknown type which were received from this server on this port.

Table - Traffic (Received/Transmitted)

Parameter	Description
Total Bytes	The total number of packets received.
Packets (64 Octets)	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets (65-127 Octets)	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (128-255 Octets)	128-255 Octets Packets: The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (256-511 Octets)	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (512-1023 Octets)	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets (1024-1518 Octets)	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Table - Packets (Received/Transmitted)

Parameter	Description
Total	Total number of packets received/transmitted.
Unicast Packets	The number of subnetwork-unicast packets delivered/sent to a higher-layer protocol.
Broadcast Packets	The total number of packets received/sent that were directed to the broadcast address.

Table - Packets (Received/Transmitted) (Continued)

Parameter	Description
Packets Discarded	Packets Discarded (Received/Transmitted): The number of inbound/ outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Errors in Packets	The total number of packets received that were with errors.

Table - Received Packets with MAC Errors

Parameter	Description
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10Base-5) and section 10.3.1.4 (10Base-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 and 150 ms.
Fragments/Undersize	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Table - Transmit Discards

Parameter	Description
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which transmission on a particular interface fails due to deferred transmissions.

Table - Transmit Discards (Continued)

Parameter	Description
Late Collisions	A count of frames for which transmission on a particular interface fails due to late collisions.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.

Table - Ether Stats

Parameter	Description
CRC Align Errors	The number of incoming packets with the Checksum (FCS) alignment error. This represents a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
Undersized Packets	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Oversize Packets	The total number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.
Ether Stats Collisions	The number of packets with collision errors.
SQE Test Errors	Signal Quality Error Test errors (i.e. Heartbeat) during transmission. This tests the important collision detection electronics of the transceiver, and lets the Ethernet interface in the computer know that the collision detection circuits and signal paths are working correctly. The errors indicate a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.

Table - Ether Stats (Continued)

Parameter	Description
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions property, the ExcessiveCollisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.
Carrier Sense Errors	The Carrier Sense detects the presence of a carrier. The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Too Long Frames	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLong status is returned by the MAC layer to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

# **Monitor Switches > <IPaddress> > Spanning Tree Protocol**

Use MONITOR/Switches and select System/Spanning Tree Protocol to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **System**, select **Spanning Tree Protocol** to access this page.

The Spanning Tree Protocol (STP) is a link management protocol. Alcatel implements the IEEE 802.1D standard for media access control bridges.

Using the spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

This page allows you to view the following Spanning Tree Algorithm parameters:

Table - General

Parameter	Description
Spanning Tree Specification	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations will return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version a new value will be defined.

# Table - General (Continued)

Parameter	Description
Spanning Tree Algorithm	Specifies if this Alcatel OmniAccess Switch or Appliance will participate in the spanning tree protocol. May be enabled or disabled by selecting the corresponding line on the pulldown entry field. The factory default is disabled.
Priority	The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535. The factory default is 32768.

# **Table - STP Statistics**

Parameter	Description
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Algorithm	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Maximum Age (centisec)	The value that all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (centisec)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Hold Time (centisec)	The minimum time period to elapse between the transmission of Configuration BPDUs through a given LAN Port: at most one Configuration BPDU shall be transmitted in any Hold Time period.

Table - STP Statistics (Continued)

Parameter	Description
Forward Delay (centisec)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. Valid values are 4 through 30 seconds. The factory default is 15.

## Monitor Switches > < IPaddress > > CLI Sessions

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **System**, select **CLI Sessions** to access this page.

Use **MONITOR/Clients,** click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **System**, select **CLI Sessions** to access this page.

This page provides a list of open Command Line Interface sessions. It details the following information:

Table - CLI Session Details

Parameter	Description
Session Index	Session identification.
User Name	Login user name.
Connection Type	Telnet or serial session.
IP Address	IP Address of the client computer system.
Session Time	Elapsed active session time.
Idle Time	Elapsed inactive session time.

## Monitor Switches > < IPaddress > > WLANs

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, click **WLANs**, then click a **WLAN ID** to access this page.

This page shows you to change the parameters for a specific WLAN.

Table - WLAN Parameters

Parameter	Description
WLAN ID	WLAN ID assigned by Alcatel Wireless Operating System.
SSID	WLAN broadcast SSID.
Security Policies	Summary of Security Policies for each WLAN definition.
Admin Status	Enable or Disable.

Table - WLAN Parameters (Continued)

Parameter	Description
No. of Clients	Clients currently associated with the WLAN

# Monitor Switches > < IPaddress > > Ports

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, click **Ports** to access this page.

This page displays port information.

Table - Ports

Parameter	Description
Port Number	The port number. Click an item in the list for details about this port. Refer to $\underline{\textit{Monitor Switches}} > \underline{\textit{IPaddress}} > \underline{\textit{Ports}} > \underline{\textit{n}}.$
Physical Mode	Displays the physical mode of all ports. Selections are:  • 100 Mbps Full Duplex  • 100 Mbps Half Duplex  • 10 Mbps Full Duplex  • 10 Mbps Half Duplex.
STP State	Displays the STP state of the port of either Forwarding or Disabled.
Admin Status	Displays the state of the port of either Enable or Disable.
Mirror Mode	Enabled or disabled. Mirror Mode is described in the <u>Alcatel OmniAccess</u> <u>Wireless Product Guide</u> .
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port.
Physical Status	Displays the actual port physical interface. Pulldown: Auto Negotiate, Half Duplex 10 Mbps, Full Duplex 10 Mbps, Full Duplex 100 Mbps, Full Duplex 1 Gbps.
Link Status	Red (failure), Yellow (alarm), Green (normal).

## Monitor Switches > <IPaddress> > RADIUS Authentication Servers

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **Radius**, select **Authentication** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **Radius**, select **Authentication** to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **Radius**, select **Authentication** to access this page.

This page displays RADIUS authentication server information and allows you to add or delete a RADIUS authentication server.

Table - RADIUS Authentication Servers

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the Alcatel OmniAccess Switch or Appliance. Refer to Configure RADIUS Authentication Server > Template < name >.
Server Address	IP Address of the RADIUS server.
Port	Alcatel OmniAccess Switch or Appliance port number for the interface protocols.
Admin Status	Whether the server is enabled or disabled.

# Table - Details

Parameter	Description
Round Trip Time (msec)	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Access Retransmissions	The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout, or retransmission.

Table - Details (Continued)

Parameter	Description
Client Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

# Monitor Switches > < IPaddress > > RADIUS Accounting Servers

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the RADIUS sidebar menu, select **Accounting** to access this page.

Use **MONITOR/Clients** and click a list item under AP Name, click **Registered Switch**, then from the RADIUS sidebar menu, select **Accounting** to access this page.

Use **MONITOR/Maps**, click an item in the **Name** column, click an AP icon, **click Switch**, then from the RADIUS sidebar menu, select **Accounting** to access this page.

Use **CONFIGURE/Access Points** and select a list item under **AP Name**, click **Registered Switch**, then from the RADIUS sidebar menu, select **Accounting** to access this page.

This page displays RADIUS accounting server information and statistics.

**Table - RADIUS Accounting Server** 

Parameter	Description
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the Alcatel OmniAccess Switch or Appliance. Refer to <a href="Configure RADIUS Accounting Server">Configure RADIUS Accounting Server</a> > <a href="Template &lt; name">Template &lt; name</a> .
Server Address	IP Address of the RADIUS server.
Port	Alcatel OmniAccess Switch or Appliance port.
Admin Status	Whether the server is enabled or disabled.

Table - Details

Parameter	Description
Round Trip Time (msec)	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Access Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.

Table - Details (Continued)

Parameter	Description
Access Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Client Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Client Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.

# **Monitor < IPaddress> > Local Authentication**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Local Authentication**, click a list item under **User Name** to access this page.

This page allows you to view local authentication parameters for a specific user.

- User Name: User defined identification.
- Category: Network Manager, Network User, Client MAC Address.
- Access Level: Read/Write, Read Only

# **Command Buttons**

- Save
- Audit

# Monitor Switches > < IPaddress > > Mobility Stats

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **Mobility**, select **Mobility Stats** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **Mobility**, select **Mobility Stats** to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **Mobility**, select **Mobility Stats** to access this page.

This page displays the statistics for Mobility Group events. The parameters and descriptions or each of these Statistics are listed in the following table:

Table - Global Mobility Statistics

Parameter	Description
Rx Errors	Generic protocol packet receive errors, such as packet too short or format incorrect.
Tx Errors	Generic protocol packet transmit errors, such as packet transmission fail.
Responses Retransmitted	The Mobility protocol uses UDP and it resends requests several times if it doesn't receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This is a count of the response resends.
Handoff Requests Received	Total number of handoff requests received, ignored or responded.
Handoff End Requests Received	Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.
State Transitions Disallowed	PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.

Table - Mobility Initiator Statistics

Parameter	Description
Handoff Requests Sent	Number of client clients that have associated with an Alcatel OmniAccess Switch or Appliance and have been 'announced' to the mobility group.
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.

Table - Mobility Initiator Statistics (Continued)

Parameter	Description
Handoff Denys Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. Handoff was received from another foreign and the new Alcatel OmniAccess Switch or Appliance is requesting the anchor to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.

Table - Mobility Responder Statistics

Parameter	Description
Handoff Requests Ignored	Number of handoff requests/client announces that were ignored. The Alcatel OmniAccess Switch or Appliance simply had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 sec).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the 'local' role.
Client Handoff as Foreign	Number of handoffs responses sent while in the 'foreign' role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client has moved from a foreign Alcatel OmniAccess Switch or Appliance to an Alcatel OmniAccess Switch or Appliance on the same subnet as the current anchor.

### Monitor Switches > < IPaddress > 802.11a Parameters

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **802.11a**, select **Parameters** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11a**, select **Parameters** to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under 802.11a, select **Parameters** to access this page.

This page displays 802.11a parameters:

**Table - MAC Operation Parameters** 

Parameter	Description
RTS Threshold	This attribute shall indicate the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size shall have the effect of turning off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero shall have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted.
Short Retry Limit	The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 4.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.
Max Rx Lifetime	The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

**Table - Station Configuration Parameters** 

Parameter	Description
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.

Table - Station Configuration Parameters (Continued)

Parameter	Description
CF Pollable	When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Table - Tx Power Parameter

Parameter	Description
Max Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

**Table - Physical Channel Parameters** 

Parameter	Description
T1 Threshold	The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.

Table - Multi-Domain Capability

Parameter	Description
First Channel Number	The value of the lowest channel number in the subband for the associated domain country string.
Number of Channels	The value of the total number of channels allowed in the subband for the associated domain country string.

# Monitor Switches > <IPaddress> > 802.11a RRM Groups

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **802.11a**, select **RRM Grouping** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11a**, select **RRM** Grouping to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11a**, select **RRM Grouping** to access this page.

This page displays 802.11a RRM groups parameters.

Table - 802.11a Grouping Control

Parameter	Description
Grouping Algorithm	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is on, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this Alcatel OmniAccess Switch or Appliance.
Is 802.11a Group Leader	Yes, this Alcatel OmniAccess Switch or Appliance is the group leader or No the Alcatel OmniAccess Switch or Appliance is not the group leader. This leader is automatically determined by the OmniVista AirView Software within the Alcatel Mobility Group as described in the Alcatel OmniAccess Wireless Product Guide.
Last Update Time (msec)	The elapsed time since the last group update in seconds. This is only valid if this Alcatel OmniAccess Switch or Appliance is a group leader.
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.

Table - Group Members

Parameter	Description
Peer MAC Address	MAC address of the peer.

Table - Group Members (Continued)

Parameter	Description
Peer IP Address	<ul> <li>N/A when the client is Local (has not roamed from its original subnet).</li> <li>Anchor IP Address (the IP Address of the original Alcatel Omni-Access Switch or Appliance) when the client is Foreign (has roamed to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> <li>Foreign IP Address (the IP Address of the original Alcatel OmniAccess Switch or Appliance) when the client is Anchor (has roamed back to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> </ul>

# **Monitor Switches > <IPaddress> > Switch 802.11b/g Parameters**

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **802.11b/g**, select **Parameters** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11b/g**, select **Parameters** to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11b/g**, select **Parameters** to access this page.

This page displays 802.11b/g parameters:

Table - MAC Operation Parameters

Parameter	Description
RTS Threshold	This attribute shall indicate the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size shall have the effect of turning off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero shall have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
Short Retry Limit	The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 4.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.

Table - MAC Operation Parameters (Continued)

Parameter	Description
Max Rx Lifetime	The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

**Table - Station Configuration Parameters** 

Parameter	Description
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that may be generated by the PCF. It is modified by MLME-START.request primitive.
CF Pollable	When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Table - Tx Power Parameter

Parameter	Description
Max Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

**Table - Physical Channel Parameters** 

Parameter	Description
ED Threshold	The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.

Table - Multi-Domain Capability

Parameter	Description
First Channel Number	The value of the lowest channel number in the subband for the associated domain country string.
Number of Channels	The value of the total number of channels allowed in the subband for the associated domain country string.

# Monitor Switches > <IPaddress> > 802.11b/g RRM Groups

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then from the Sidebar menu, under **802.11b/g**, select **RRM Grouping** to access this page.

Use **MONITOR/Access Points**, click a list item under AP Name, click **Registered Switch**, then from the Sidebar menu, under **802.11b/g**, select **RRM Grouping** to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click Registered **Switch**, then from the Sidebar menu, under **802.11b/g**, select **RRM Grouping** to access this page.

This page displays 802.11b/g RRM grouping parameters:

Table - 802.11b/g Grouping Control

Parameter	Description
Grouping Algorithm	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is on, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this Alcatel OmniAccess Switch or Appliance.
Is 802.11b/g Group Leader	Yes, this Alcatel OmniAccess Switch or Appliance is the group leader or No the Alcatel OmniAccess Switch or Appliance is not the group leader. This leader is automatically determined by the OmniVista AirView Software within the Alcatel Mobility Group as described in the Alcatel OmniAccess Wireless Product Guide.
Last Update Time (msec)	The elapsed time since the last group update in seconds. This is only valid if this Alcatel OmniAccess Switch or Appliance is a group leader.

Table - 802.11b/g Grouping Control (Continued)

Parameter	Description
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.

Table - Peer Group Members

Parameter	Description
Peer MAC Address	MAC address of the peer.
Peer IP Address	<ul> <li>N/A when the client is Local (has not roamed from its original subnet).</li> <li>Anchor IP Address (the IP Address of the original Alcatel Omni-Access Switch or Appliance) when the client is Foreign (has roamed to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> <li>Foreign IP Address (the IP Address of the original Alcatel OmniAccess Switch or Appliance) when the client is Anchor (has roamed back to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> </ul>

# Monitor < IPaddress > > Interface

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Interfaces** to access this page.

This page allows you to view existing interfaces and add new interfaces.

- Checkbox: Select the interface to delete before using the Select a command.
- Interface Name: User-defined name for this interface, for example, management, service-port, virtual.
- VLAN ID: VLAN Identifier between 0 and 4096.
- Interface Type: Static or Dynamic.
- IP Address: IP Address of the interface.

## Select a command

- Add Interface: Refer to <u>Configure < IPaddress > Add Interface</u>.
- Delete Dynamic Interface: Select an interface to be deleted, select this command and click GO.

## Monitor < IPaddress > Network Route

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and click **Network Route**, then click on a list item from **IP Address** column to access this page.

This page allows you to view a list of network routes, and contains the same information displayed on the <u>Configure < IPaddress > Network Route</u> for this Service Port.

- IP Address: IP Address of the route.
- Network Mask: Network Mask of the Route.
- Gateway IP Address: Gateway IP Address of the Route.

# Monitor < IPaddress > Mobility Group < name > > Group Members

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Mobility Groups** to access this page.

This page allows you to view, add or delete mobility group members.

- Checkbox: Use this to select a group member.
- Switch Name: User-defined Alcatel OmniAccess Switch or Appliance name.
- Member MAC Address: MAC address of the mobility group member.
- Member IP Address: IP Address of the mobility group member.

#### Select a command

- Add Group Members: Select this command and click GO. Refer to <u>Configure < IPaddress > Mobility Group < name ></u>.
- Delete Group Members: To delete a group member, select a check box, select this command, and click GO.

# **Monitor WLAN**

Use **CONFIGURE/Switches** and click **Switches/WLANs** to access this page.

This page allows you to view a summary of the wireless local access networks (WLANs) that you have configured on your network. From this page, you may add, delete or edit WLANs.

Table - WLANs

Parameter	Description
Checkbox	Use this checkbox to select a WLAN to delete.
WLAN ID	Identification number of the WLAN. Refer to <u>Monitor <ipaddress> &gt; WLANs &gt; <wlan id=""></wlan></ipaddress></u> .
SSID	Service Set Identifier being broadcast by the WLAN.
Security Policies	Security policies enabled on the WLAN.
Admin Status	Status of the WLAN is either enabled or disabled.

### Select a command pulldown

- Add WLAN: Refer to Configure <IPaddress> > WLAN Template > Add From Template.
- Delete WLAN: Select a WLAN to delete by clicking the check box in front of it, select this command and click GO.

# Monitor < IPaddress > WLANs > < WLAN ID>

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, click **WLANs**, then click a **WLAN ID** to access this page.

This page allows you to view and edit the parameters for a specific WLAN.

Table - General Policies

Parameter	Description
Radio Policy	Set the WLAN policy to apply to All = 802.11a/b/g, 802.11a only, 802.11b only, 802.11g only, 802.11b/g only, 802.11a/b only, or 802.11a/g only. All, 802.11a only, 802.11b/g only.
Admin Status	Set the status of the WLAN to either enabled or disabled.
Interface	Select from the available Interface Names. The Interfaces are created in <i>Configure <ipaddress> &gt; Add Interface</ipaddress></i> .
Session Timeout	Set the maximum time for a client session before requiring reauthorization.
Quality of Service (QoS)	Set QoS to: Gold (Highest); Silver (Mid-range); Bronze (Low). Services such as VoIP should be set to Gold while non-discriminating services such as text messaging can be set to Bronze.
Allow AAA Override	<ul> <li>Enable or disable AAA override for global WLAN parameters.</li> <li>When AAA Override is enabled, and a client has conflicting AAA and Alcatel OmniAccess Switch or Appliance WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the Alcatel Wireless Operating System will move clients from the default Alcatel WLAN VLAN to a VLAN returned by the AAA server and predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Alcatel Wireless Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)</li> <li>For instance, if the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the Alcatel Wireless Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</li> <li>When AAA Override is disabled, all client authentication defaults to the Alcatel OmniAccess Switch or Appliance authentication parameter settings, and authentication is only performed by the AAA server if the Alcatel OmniAccess Switch or Appliance WLAN do not contain any client-specific authentication parameters.</li> <li>The AAA override values may come from a RADIUS server, for example.</li> </ul>

Table - General Policies (Continued)

Parameter	Description
Disable Timeout	Enable or disable automatic disabling, and set the timeout in seconds for disabled client machines. Client machines are disabled by MAC address and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client. Set** checkbox, Timeout Value (secs) field.
DHCP Relay	<ul> <li>When selected, you can enter the IP Address of your DHCP server. This is a Required field for some WLAN configurations. There are three valid configurations and one invalid combination:</li> <li>DHCP Required and a valid DHCP Server IP Address: Requires all WLAN clients to obtain an IP Address from the DHCP Server.</li> <li>DHCP Not Required and a valid DHCP Server IP Address: Allows all WLAN clients to obtain an IP Address from the DHCP Server or use a static IP Address.</li> <li>DHCP Not Required and DHCP Server IP Address 0.0.0.0: Forces all WLAN clients to use a static IP Address. All DHCP requests are dropped.</li> <li>DHCP Required and DHCP Server IP Address 0.0.0.0 is not allowed.</li> </ul>

<sup>\*\*</sup> When Disable timeout is not set, it implies that a disabled client will remain so and will never timeout from the disabled state. It does not imply that the blackslisting feature will be disabled.

You can choose both Layer 2 and Layer 3 security policies from the drop down list under the Security Policies heading. The selected security policy options are at the bottom of the page with the appropriate parameters listed. The following table describes these parameters.

Table - Security Policies

Parameter	Description
Layer 2 Security	None, WPA, 802.1X, Static WEP, Cranite, MAC Filtering checkbox.
Layer 3 Security	None, IPSec, VPN Pass Through, Web Authentication* Checkbox.
* Alcatel OmniAccess Switch or Appliance must be rebooted for Web Authentication to take effect. Web Authentication cannot be used in combination with IPSec.	

## **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this WLAN.

## Monitor Client <client name>

Use **MONITOR/Maps**, click an item in the **Name** column, single-click the floor map, from the Display pulldown menu, select **Users**, click **n clients**, click **User Name** to access this page.

This page displays parameters for a client selected by name.

Table - Client-General

Parameter	Description
Client User Name	User-defined client user name.
Client IP Address	Client AP address.
Client MAC Address	Client MAC address.
Switch	Client Alcatel OmniAccess Switch or Appliance. Click to view Alcatel OmniAccess Switch or Appliance parameters. Refer to <u>Monitor Switches &gt; <ipaddress> Summary</ipaddress></u> .
Port	Port Alcatel OmniAccess Switch or Appliance to which the client is attached.
Client State	Client statE may be one of the following:  • idle (0) normal operation: no rejections of client association requests  • aaaPending (1) completing an aaa transaction  • authenticated (2) 802.11 authentication completed  • associated (3) 802.11 association completed  • powersave (4) client in powersave mode  • disassociated (5) 802.11 disassociation completed  • tobedeleted (6) to be deleted after disassociation  • probing (7) client not associated or authorized yet  • disabled (8) automatically disabled by Alcatel Wireless Operating  System for an operator-defined time
Authenticated	Yes or No.
SSID	Service Set Identifier being broadcast by the OmniAccess Radio.
Association Id	Client's AP association identification number.
Reason Code	The client reason code may be one of the following:  • no reason code (0) normal operation  • unspecified reason (1) client associated but no longer authorized  • previousAuthNotValid (2) client associated but not authorized  • deauthenticationLeaving (3) the OmniAccess AP went offline, deauthenticating the client  • disassociationDueToInactivity (4) client session timeout exceeded  • disassociationAPBusy (5) the OmniAccess AP is busy, performing load balancing, for example  • class2FrameFromNonAuthStation (6) client attempted to transfer data before it was authenticated  • class2FrameFromNonAssStation (7) client attempted to transfer data before it was associated  • disassociationStaHasLeft (8) Alcatel Wireless Operating System moved the client to another OmniAccess AP using non-aggressive load balancing  • staReqAssociationWithoutAuth (9) client not authorized yet, still attempting to associate with an Alcatel WLAN  • missingReasonCode (99) client momentarily in an unknown state

Table - Client-General (Continued)

Parameter	Description
Anchor Status	<ul> <li>Local when the client has not roamed from its original Alcatel Omni-Access Switch or Appliance, or when the client has roamed to another Alcatel OmniAccess Switch or Appliance on the same subnet.</li> <li>Remote when the client has roamed from its original Alcatel OmniAccess Switch or Appliance to another Alcatel OmniAccess Switch or Appliance on a different subnet.</li> <li>Anchor when the client has roamed back to its original Alcatel OmniAccess Switch or Appliance after roaming to another Alcatel OmniAccess Switch or Appliance on a different subnet.</li> </ul>
Anchor Address	<ul> <li>N/A when the client is Local (has not roamed from its original subnet)</li> <li>Anchor IP Address (the IP Address of the original Alcatel OmniAccess Switch or Appliance) when the client is Foreign (has roamed to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> <li>Foreign IP Address (the IP Address of the original Alcatel OmniAccess Switch or Appliance) when the client is Anchor (has roamed back to another Alcatel OmniAccess Switch or Appliance on a different subnet).</li> </ul>

# Table - AP Properties

Parameter	Description
AP Name	User-defined an OmniAccess AP name. Refer to <u>Monitor Access Points &gt; <name></name></u> .
AP Type	an OmniAccess AP's RF type.
AP MAC Address	AP MAC address.
Protocol	802.11a or 802.11b/g.

## Table - Client Statistics

Parameter	Description
Bytes received	Total number of bytes received by the Alcatel OmniAccess Switch or Appliance from the client.
Bytes sent	Total number of bytes sent to the client from the Alcatel OmniAccess Switch or Appliance.
Packets received	Total number of packets received by the Alcatel OmniAccess Switch or Appliance from the client.
Packets sent	Total number of packets sent to the client from the Alcatel OmniAccess Switch or Appliance.
Policy errors	Number of policy errors for the client.
RSSI	Receive signal strength indicator of the client RF session.

Table - Client Statistics (Continued)

Parameter	Description
SNR	Signal to noise ratio of the client RF session.

Select one of the following commands and click **GO**:

- Link Test: Select to perform a link test. Refer to <u>Monitor Link Test Results</u>.
- Disable: Select to disable this client. Refer to <u>Configure Black List Client</u> > < <u>MACaddress</u> >.
- Deauthenticate: Select to deauthenticate the client. The following question pops up: "Are you sure you want to disassociate this client?" Click **Ok** or **Cancel**.
- Recent Map (Low Resolution): For High resolution Heat Maps, you must have ACS Location (High-Resolution) Software (OV-ACSLOC). Low Resolution Heat Maps are enabled for ACS Basic (Low-Resolution) Software (OV-ACS-BASE).
- Present Map (Low Resolution): For High resolution Heat Maps, you must have ACS Location (High-Resolution) Software (OV-ACSLOC). Low Resolution Heat Maps are enabled for ACS Basic (Low-Resolution) Software (OV-ACS-BASE).
- Recent Map (High Resolution): For High resolution Heat Maps, you must have ACS Location (High-Resolution) Software (OV-ACSLOC). Low Resolution Heat Maps are enabled for ACS Basic (Low-Resolution) Software (OV-ACS-BASE).
- Present Map (High Resolution): For High resolution Heat Maps, you must have ACS Location (High-Resolution) Software (OV-ACSLOC). Low Resolution Heat Maps are enabled for ACS Basic (Low-Resolution) Software (OV-ACS-BASE).
- AP Association History: A listing of connection association or non-association of the selected AP.
   Only available for clients in a watch list.
- Add to Watch List: Select to add this Client to a Watch List. Refer to <u>Configure Clients > Add to</u> Watch List > < MAC address >.

## **Monitor Disabled Clients**

Use MONITOR/Clients and click Disabled Clients to access this page.

This page allows you to view disabled (blacklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or disabled, from further association attempts for an operator-defined timeout. After the disable timeout, the client is allowed to retry authentication until it associates or fails authentication and is disabled again.

Table - Disabled Clients

Parameter	Description
MAC Address	Disabled Client MAC addresses. Click a list item to get details about the disabled client. Refer to <u>Configure Disabled Clients &gt; Template <template name=""></template></u> .
Description	Description of disabled client.

- Add Disabled Client: Select and click GO. Refer to Configure Disabled Clients > New Template.
- Delete Disabled Clients: Select one or more clients to delete by clicking the check box(es), select this command and click GO.

### **Monitor Access Control List**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Security** and click **Access Control Lists** to access this page.

This page displays access control lists available for this Alcatel OmniAccess Switch or Appliance:

- Checkbox: Use the checkbox to select one or more ACLs.
- ACL Name: User-defined name of this template. Click an ACL item to view its parameters. Refer
  to <u>Monitor <IPaddress> > Access Control List > Iistname>.
  </u>

#### Select a command

- Add Access Control: Refer to <u>Configure <IPaddress> > Access Control List > Add from Template</u>.
- Delete Access Controls: Use the checkbox to select a user, select this command and click GO.

## **Monitor Access Control List Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Security/Access Control Lists** to access this page. This page displays information about access control lists.

This page allows you to view information about access control list templates available for Alcatel Omni-Access Switches or Appliances.

• ACL Name: User defined identification. Click a list item to display and modify parameters in this ACL. Refer to <u>Configure Access Control List > Template < name ></u>.

### Select a command

• Add Template: Refer to <u>Configure Access Control List > New Template</u>.

## Monitor < IPaddress > Access Control List > < listname >

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Security/Access Control Lists**, click a list item under **ACL Name** to access this page.

This page displays current access control list rules applied to this Access Control List.

- Checkbox: Check to select access control list rules to be deleted.
- Seq#: The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5. Note that if you add or change a Sequence number, Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
- Action: Permit, Deny.
- Source IP/Mask: Source IP Address and Mask.

- Destination IP/Mask: Destination IP Address and Mask.
- Protocol: Protocol to use for this ACL:
  - Any All protocols
  - TCP Transmission Control Protocol
  - UDP User Datagram Protocol
  - ICMP Internet Control Message Protocol
  - ESP IP Encapsulating Security Payload
  - AH Authentication Header
  - GRE Generic Routing Encapsulation
  - IP Internet Protocol
  - Eth Over IP Ethernet over Internet Protocol
  - Other Port OSPF Open Shortest Path First
  - Other Any other IANA protocol (http://www.iana.org/)
- If TCP or UDP is selected, Source Port: Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- Dest Port: Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- DSCP (Differentiated Services Code Point): Any, or 0 through 256.
- Direction: Any, Inbound (from client) or Outbound (to client).

- Add New Rule: Refer to Monitor <IPaddress> > Access Control List > stname>.
- Delete Rules

### **Command Buttons**

- Apply to Switches
- Delete
- Cancel

## Monitor < IPaddress > Certificate

Use **CONFIGURE/Switches**, navigate to <u>Configure < IPaddress > Switch General</u>, and select **Security/ID Certificate** to access this page.

This page lists the existing network ID Certificates by Certificate name. An ID Certificate can used by Web server operators to ensure secure server operation. Refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information about this and other feature descriptions.

### **Command Buttons**

- Add Certificate: Select this command and click **GO**. Refer to <u>Configure < IPaddress > Certificate Details</u>.
- Delete Certificates: To delete a certificate, select it, select this command and click GO.

# Monitor < IPaddress > > Trap Receivers

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control** and click **Trap Receivers** to access this page.

This page allows you to add or delete trap receivers:

Table - Trap Receivers-Configure

Parameter	Description
(Check box)	Check this box to indicate which trap receiver to delete.
Name	Refer to <u>Configure <ipaddress> &gt; Trap Receiver</ipaddress></u> to edit the Trap Receivers.
IP Address	Local network IP Address of the Alcatel OmniAccess Switch or Appliance as described in <u>Management Interface</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
Admin Status	Status must be enabled for the SNMP traps to be sent to the receiver. Enabled checkbox.

## Select a command

- **Add Receiver:** Allows you to add trap receivers. Select and click **GO**. Refer to <u>Configure < IPaddress> > Trap Receiver > Add From Template</u>.
- Delete Receivers: Select a receiver to delete from the list, select this command and click GO.

## MONITOR/Access Points Menu Bar Selection

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance access points (APs) summary details. Use the selector area to access the respective access point details.

Making this selection from the menu bar displays *Monitor Access Points > Search Results*.

## **Monitor Access Points > Search Results**

Use **MONITOR/Access Points**, click a list item under AP Name, click **Access Points** in the Page title to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **Access Points** in the Page title to access this page.

Use **MONITOR/Switches**, click one of the IP addresses under IP Address, click **Access Points**, click **Access Points** in the Page title to access this page.

This page allows you to view a summary of access point information for all known APs.

Table - MONITOR/Access Points--Search Results

Column	Options
(Selection check box)	Check or uncheck to select the AP.
AP Name	This is the name assigned to the OmniAccess AP. Click a list item. Refer to <u>Monitor Access Points &gt; <name></name></u> .

Table - MONITOR/Access Points--Search Results (Continued)

Column	Options
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click a list item. Refer to $\underline{Monitor\ Access\ Points} > < \underline{name} > < \underline{Radio}$ $\underline{Type} >$ .
Location	Click a list item to go to the location indicated on the list. Refer to <u>Monitor Maps &gt; Campus</u> .
Switch	Click a list item to display a graphic and information about the Alcatel OmniAccess Switch or Appliance. Refer to <u>Monitor Switches &gt; <ipaddress> Summary</ipaddress></u> .
Port	Alcatel OmniAccess Switch or Appliance port used for the associated access point.
Oper Status	Displays the operational status of the Alcatel device, either Up or Down.
Alarm Status	Colored icon. Refer to <u>Alarm Monitor</u> .

### Left sidebar

- Search for APs by (pulldown): (All APs, MAC Address, AP Name, Switch. All Foreign APs, Indoor Area, Outdoor Area).
- Select Radios (All Radios, 802.11a, 802.11b/g).
- Search (button).

Table - Generate Report for Selected APs Pulldown

Command	Results
Load	Generates a report with load information. Refer to <u>Monitor Access Points &gt; Load</u> .
Dynamic Power Control	Generates a report with Dynamic Power Control information. Refer to <u>Monitor Access Points &gt; Dynamic Power Control</u> .
Noise	Generates a report with Noise information. Refer to <u>Monitor Access Points</u> > <u>Noise</u> .
Interference	Generates a report with Interference information. Refer to <u>Monitor Access</u> <u>Points &gt; Interference</u> .
Coverage (RSSI)	Generates a report with Coverage (RSSI) information. Refer to <u>Monitor Access Points &gt; Coverage (RSSI)</u> .
Coverage (SNR)	Generates a report with Coverage (SNR) information. Refer to <u>Monitor Access Points &gt; Coverage (SNR)</u> .
Up Time	Time in days, hours and minutes since the last reboot. Generates a report with Up Time information. Refer to <u>Monitor Access Points &gt; Up Time</u> .

## Monitor Access Points > <name>

From Monitor Network Summary, click an AP Name under Top 5 APs to access this page.

Use MONITOR/Access Points and click a list item under AP Name to access this page.

Use **MONITOR/Clients** and click a list item under AP Name to access this page.

Use **MONITOR/Switches** and click one of the IP addresses under IP Address, then click **Access Points** to access this page.

This page allows you to view access point information for a single AP.

Click **Access Points** in the page title to view a list of all APs. Refer to <u>Monitor Access Points > Search Results</u>.

Table - General

Parameter	Description
AP Name	This is the user-assigned name of the OmniAccess AP.
AP MAC Address	Media Access Control of the OmniAccess AP.
AP IP Address	IP address of the OmniAccess AP.
Admin Status	Displays the administration state of the OmniAccess AP of either enabled or disabled.
Monitor Only Mode	Displays the OmniAccess AP Monitor mode (monitor for rogue access points without allowing clients to associate), local or OmniAccess AP 1200R.  Note: In order for Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) to operate correctly, this parameter must be set to OmniAccess AP 1200R.
Operational Status	The operational status of the OmniAccess AP comes up as either registered or not registered automatically by the Alcatel OmniAccess Switch or Appliance.
Registered Switch	The Alcatel OmniAccess Switch or Appliance to which the OmniAccess AP is registered. Click to display the parameters of the registered Alcatel OmniAccess Switch or Appliance. Refer to <u>Monitor Switches &gt; &lt; IPaddress &gt; Summary</u> .
Primary Switch	This is the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance SNMP name. The OmniAccess AP will attempt to associate with this Alcatel OmniAccess Switch or Appliance first for all network operations and in the event of a hardware reset.
Port Number	Port Number: The OmniAccess AP is connected to this Alcatel OmniAccess Switch or Appliance port.
Location	Customer-definable location name for the OmniAccess AP. Click to look at the actual location on a map. Refer to <u>Monitor Maps &gt; Campus &gt; Building &gt; Floor</u> or <u>Monitor Maps &gt; Building &gt; Floor</u> .
Statistics Timer	This counter sets the time in seconds that the OmniAccess AP sends its DOT11 statistics to the Alcatel OmniAccess Switch or Appliance.

### Table - AP Interfaces

Parameter	Description
AP Interfaces	This is the user-assigned name of the OmniAccess AP. Click a list item to view the parameters. Refer to $\underline{Monitor\ Access\ Points} > < \underline{name} > < \underline{Radio}$ $\underline{Type} >$ .
Admin Status	Displays the administration state of the OmniAccess AP of either enabled or disabled.
Op Status	Displays the operational status of the OmniAccess Radio: either UP or DOWN.
Alarm Status	Indicates any pending alarms. Refer to Alarm Monitor.

### Table - Version

Parameter	Description
Software	The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
Boot Version	Alcatel Wireless Operating System bootloader version number.

## **Table - Inventory Information**

Parameter	Description
AP Model	The Access Point model number.
AP Serial Number	Unique Serial Number for this Access Point.

## Monitor Access Points > <name> > <Radio Type>

From <u>Monitor Access Points > <name></u>, click 802.11a or 802.11b under AP Interfaces to access this page.

Use MONITOR/Access Points and click a list item under Radio to access this page.

Use **MONITOR/Maps**, then click an item in the **Name** column, then click an OmniAccess AP icon to access this page.

This page allows you to view access point information for a single 802.11a or 802.11b OmniAccess Radio.

The default is to show On Demand Statistics. Use the View pulldown menu to select a different view:

- Select On Demand Statistics and click GO to display On Demand Statistics.
- Select Operational Parameters and click GO to display <u>Operational Parameters</u>.
- Select 802.11 MAC Counters and click GO to display 802.11 MAC Counters.

## **On Demand Statistics**

From <u>Monitor Access Points > <name> > <Radio Type></u>, select On Demand Statistics and click **GO** to access this page.

This page allows you to view access point 802.11a or 802.11b OmniAccess Radio statistics for a single OmniAccess AP.

Table - General

Parameter	Description
AP Name	This is the name assigned to the OmniAccess AP. Click to view the OmniAccess AP parameters in <u>Configure Access Point &gt; OmniAccess AP &gt; <name>.</name></u>
AP MAC Address	Media Access Control of the OmniAccess AP.
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click a list item for details. Refer to <u>Configure Access Points &gt; OmniAccess AP &gt; <name> &gt; <math>802.11a</math></name></u> .
Admin Status	Administration state of the OmniAccess AP (Enable or Disabled).
Operational Status	Displays the operational status of the OmniAccess Radios (Up or Down).
Channel	The channel upon which the OmniAccess Radio is broadcasting.
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Switch	IP Address of Alcatel OmniAccess Switch or Appliance. Click to display <u>Monitor Switches &gt; <ipaddress> Summary</ipaddress></u> .
Port	(1 to 24) Port to which the OmniAccess AP is connected.
Location	Click to display the floor map showing the OmniAccess AP location. Refer to <u>Monitor Maps &gt; Campus &gt; Building &gt; Floor</u> .

### **Profile Information**

- Noise Profile: Notification sent when Noise Profile state changes between PASS and FAIL.
- Interference Profile: Notification sent when Interference Profile state changes between PASS and FAIL.
- Load Profile: Notification sent when Load Profile state changes between PASS and FAIL.
- Coverage Profile: Notification sent when Coverage Profile state changes between PASS and FAIL.

## Noise by Channel (dBm)

Graph showing channel and noise.

## Interference by Channel (dBm%)

Graph showing the percentage of interference per channel.

### **Load Statistics**

- RX Utilization: 802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
- TX Utilization: 802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
- Channel Utilization: 802.11a RF utilization threshold between 0 and 100 percent (Subcolumns for Actual and Threshold).
- Attached Client Count: The number of clients attached.

## **Client Distribution by Received Signal Strength Indicator**

Graph with % and RSSI.

## Client Distribution by Signal-to-Noise Ratio

Graph with % and SNR.

### **Rx Neighbors**

- MAC Address
- IP Address
- RSSI (dBm)

## View Pulldown

- Select On Demand Statistics and click GO to display On Demand Statistics.
- Select Operational Parameters and click GO to display Operational Parameters.
- Select 802.11 MAC Counters and click GO to display 802.11 MAC Counters.

## **Operational Parameters**

From  $\underline{Monitor\ Access\ Points} > < name > > < Radio\ Type >$ , select Operational Parameters and click **GO** to access this page.

This page allows you to view configuration information for a single 802.11a or 802.11b OmniAccess Radio.

Table - General

Parameter	Description
AP Name	This is the name assigned to the OmniAccess AP. Click to view the OmniAccess AP parameters in <u>Configure Access Point &gt; OmniAccess AP &gt; &lt; name &gt; .</u>
AP MAC Address	MAC address of the access point.
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g.
Admin Status	Whether the OmniAccess AP is enabled or disabled.

Table - General (Continued)

Parameter	Description
Operational Status	Displays the operational status of the OmniAccess Radios (Up or Down).
Channel	The channel the OmniAccess Radio is broadcasting on.
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Switch	IP Address of Alcatel OmniAccess Switch or Appliance. Click to display <i>Monitor Switches</i> > < <i>IPaddress</i> > <i>Summary</i> .
Port	Port to which the OmniAccess AP is connected.
Location	Refer to <u>Monitor Maps &gt; Campus &gt; Building &gt; Floor</u> .

**Table - Station Configuration Parameters** 

Parameter	Description
Configuration Type	Automatic or Custom.
Number of WLANs	1 (one) is the default.
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator may control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs.
CFP Max. Duration	The maximum duration of the CFP in TU that may be generated by the PCF.
BSSID	MAC address of the OmniAccess AP.
Beacon Period	The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
DTIM Period	The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
Country String	Identifies the country in which the station is operating. The first two octets of this string is the two character country code as described in <i>Alcatel OmniAccess Wireless System Supported Regulatory Domains</i> in the <i>Alcatel OmniAccess Wireless Product Guide</i> .

## **Physical Channel Parameters**

- Current Channel: Current operating frequency channel.
- Configuration: Locally customized or globally controlled.
- Current CCA Mode: CCA method in operation. Valid values are:
  - Energy detect only (edonly) = 01.
  - Carrier sense only (csonly) = 02.
  - Carrier sense and energy detect (edandcs) = 04.
  - Carrier sense with timer (cswithtimer) = 08.
  - High rate carrier sense and energy detect (hrcsanded)=16.
- ED/TI Threshold: The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.

### **Physical Antenna Parameters**

- Antenna Type: Internal or External.
- Diversity: Enabled via the internal antennas or via either Connector A or Connector B. (Enabled or Disabled).

Table - RF Recommendation Parameters

Parameter	Description
Channel	802.11a Low Band, Medium Band, and High Band; 802.11b/g. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide.
Tx Power Level	Zero (0) if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled.
RTS/CTS Threshold	Zero (0) if OmniVista AirView Software disabled, 1 - 5 if OmniVista AirView Software enabled. Refer to RTS Threshold in MAC Operation Parameters above.
Fragmentation Threshold	Zero (0) if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.
Antenna Pattern	Zero (0) if OmniVista AirView Software disabled, or as OmniVista AirView Software recommends.

Table - MAC Operation Parameters

Parameter	Description
Configuration Type	Automatic or Custom.

Table - MAC Operation Parameters (Continued)

Parameter	Description
RTS Threshold	This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed. An RTS/CTS handshake shall be performed at the beginning of any frame exchange sequence where the MPDU is of type Data or Management, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size shall have the effect of turning off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero shall have the effect of turning on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
Long Retry Limit	The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.
Short Retry Limit	The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.
Fragmentation Threshold	The current maximum size, in octets, of the MPDU that may be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.
Max Rx Lifetime	The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Table - Tx Power

Parameter	Description
# Supported Power Levels	Five or fewer power levels, depending on operator preference.

Table - Tx Power (Continued)

Parameter	Description
Tx Power Level x	Power Level (1, highest through 5, lowest) OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Tx power Configuration	Globally controlled or Customized for this OmniAccess AP (Custom or Global).
Current Tx Power Level	Displays the operating transmit power level from the transmit power table.

### View Pulldown

- Select On Demand Statistics and click GO to display On Demand Statistics.
- Select Operational Parameters and click GO to display Operational Parameters.
- Select 802.11 MAC Counters and click GO to display <u>802.11 MAC Counters</u>.

### 802.11 MAC Counters

From  $\underline{Monitor\ Access\ Points} > < name > > < Radio\ Type >$ , select 802.11 MAC Counters and click **GO** to access this page.

This page allows you to view 802.11 MAC Counter information for a single 802.11a or 802.11b Omni-Access Radio.

Table - General

Parameter	Description
AP Name	This is the name assigned to the OmniAccess AP. Click to view the OmniAccess AP parameters in <u>Configure Access Point &gt; OmniAccess AP &gt; &lt; name &gt; .</u>
AP MAC Address	MAC address of the access point.
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g.
Admin Status	Whether the OmniAccess AP is enabled or disabled.
Operational Status	Displays the operational status of the OmniAccess Radios (Up or Down).
Channel	The channel the OmniAccess Radio is broadcasting on.

Table - General (Continued)

Parameter	Description
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Switch	IP Address of Alcatel OmniAccess Switch or Appliance. Click to display <i>Monitor Switches &gt; <ipaddress> Summary</ipaddress></i> .
Port	Port to which the OmniAccess AP is connected.
Location	Refer to <u>Monitor Maps &gt; Campus &gt; Building &gt; Floor</u> .

Table - RF Counters

Parameter	Description
Tx Fragment Count	This counter shall be incremented for each successfully received MPDU of type Data or Management.
Multicast Tx Frame Count	This counter shall increment only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the OmniAccess AP, this implies having received an acknowledgment to all associated MPDUs.
Tx Failed Count	This counter shall increment when an MSDU is successfully transmitted after one or more retransmissions.
Retry Count	This counter shall increment when an MSDU is successfully transmitted after one or more retransmissions.
Multiple Retry Count	This counter shall increment when an MSDU is successfully transmitted after more than one retransmission.
Frame Duplicate Count	This counter shall increment when a frame is received that the Sequence Control field indicates is a duplicate.
RTS Success Count	This counter shall increment when a CTS is received in response to an RTS.
RTS Failure Count	This counter shall increment when a CTS is not received in response to an RTS.
ACK Failure Count	This counter shall increment when an ACK is not received when expected.
Rx Fragment Count	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Multicast Rx Framed Count	This counter shall increment when a MSDU is received with the multicast bit set in the destination MAC address.

Table - RF Counters (Continued)

Parameter	Description
FCS Error Count	This counter increments when an FCS error is detected in a received MPDU.
Tx Frame Count	This counter shall increment for each successfully transmitted MSDU.
WEP Undecryptable Count	This counter increments when a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the TA's MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

#### View Pulldown

- Select On Demand Statistics and click GO to display On Demand Statistics.
- Select Operational Parameters and click GO to display <u>Operational Parameters</u>.
- Select 802.11 MAC Counters and click GO to display 802.11 MAC Counters.

## **Monitor RADIUS Authentication Server**

Use **CONFIGURE/Templates** and from the Security sidebar menu, select **Security/Radius Auth Servers** to access this page.

This page allows you to view a summary of existing RADIUS authentication server templates, and add or delete a RADIUS authentication server template. Click any **Template Name** to go to the corresponding <u>Configure RADIUS Authentication Server > Template < name > to edit the template.</u>

Table - RADIUS Authentication Server

Parameter	Description
Template Name	Operator-defined names of RADIUS Accounting servers.
Server Address	IP Address of the RADIUS server (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port (read only).
Admin Status	Enabled or disabled (read only).
Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

#### Select a command

• Add Template: Refer to Configure RADIUS Authentication Server > New Template.

## **Monitor Local Authentication**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Security/Local Authentication** to access this page.

This page presents a summary of the existing local network templates for clients who are allowed to access a specific Alcatel WLAN. This is an administrative bypass of the RADIUS authentication process.

Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database will be granted access to network services if the RADIUS authentication fails or does not exist.

This page displays a table with the following columns:

- User Name: Click a list item. Refer to <u>Monitor Local Authentication > Template < name ></u> to view and apply the template.
- Category: Category of User, for example, Network Manager Network User.
- SSID: Service Set Identifier being broadcast by the OmniAccess Radio.
- Access Level: Read/Write or Read Only.

### Select a command

Add Template: Refer to <u>Configure Local Authentication > New Template</u>.

## **Monitor Local Authentication > Template <name>**

Use **CONFIGURE/Templates**, from the left sidebar menu, select **Security/Local Authentication**, then click a list item under **User Name** to access this page.

This page displays a table with the following columns:

- User Name: Login user name (Read only).
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Category: Category of User, for example, Network Manager Network User.
- Access Level: User privilege assignment can be Read Only or Read/Write.

### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## **MONITOR/Clients Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance clients summary details. Use the selector area to access the respective clients details.

Making this selection from the menu bar displays the *Monitor Clients Summary*.

## **Monitor Clients Summary**

Use MONITOR/Clients to access this page.

This page displays information about OmniAccess AP clients.

### **Client Watch Lists**

Click the column title to display all watch lists. Refer to <u>Monitor Watch Lists</u>.

- Name: The name of the client. Click a list item to display its parameters. Refer to <u>Monitor</u> <u>Watch Lists</u> > < <u>list name</u>>.
- Description: User-defined description of the watch list.
- Admin Status: Whether the AP is enabled or disabled.
- Expires On: Time the watch list expires.
- Clients: Number of clients on the watch list.

### **Most Recent Blacklisted Clients**

- User Name: User-defined user name.
- IP Address: IP Address of blacklisted client.
- MAC Address: MAC address of the blacklisted client.
- Blacklist Time: Time the client was blacklisted.

#### **Disabled Clients**

Refer to <u>Monitor Disabled Clients</u>.

### Top 5 APs

- AP Name: This is the name assigned to the OmniAccess AP. Click an item in the list to see the details of that OmniAccess AP. Refer to *Monitor Access Points* > <*name*>.
- Location: The name of the map were the client is located. Refer to <u>Monitor Maps > Campus > Building > Floor</u>.
- a Clients: Number of 802.11a clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- b Clients: Number of 802.11b clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- g Clients: Number of 802.11g clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Total: Total number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.

### Clients (Associated Clients vs. Time [Graph])

### Left sidebar

Search for clients by (pulldown):

- All Clients: All clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- All Blacklisted Clients: List of all clients who fail to authenticate three times when attempting to associate who are automatically blocked, or disabled, from further association attempts for an operator-defined timeout.
- IP Address: Local network IP Address of the Alcatel OmniAccess Switch or Appliance Distribution System Port, described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- User Name: User-defined client user name.
- MAC Address: Client MAC address.
- AP: Alcatel OmniAccess Wireless Access Points associated with this Alcatel OmniAccess Switch or Appliance.

- Switch: Alcatel OmniAccess Switch or Appliance to which the user is attached.
- Indoor Area: User defined name of the indoor location.
- Outdoor Area: User-defined name of the outdoor location.
- Search (button).

### **Monitor Watch Lists**

Use MONITOR/Clients and click the column title to access this page.

This page allows you to view existing watch lists.

- Checkbox: Select the desired watch list(s).
- Watch List Name: Click the desired watch list to display it. Refer to <u>Monitor Watch Lists</u> > < <u>list name</u>>.
- Description: Displays a description of the client watch list.
- Admin Status: Whether the watchlist is enabled or disabled.
- Expiries On: Displays the time the watch list expires.
- · Clients: Total clients being watched on this list.

### Select a command

- New Watch List: Allows you to specify a new watch list. Refer to <u>Configure Watch Lists > New Watch List</u>.
- Delete Watch List: Allows you to delete a watch list.

### Monitor Watch Lists > < list name>

Use **MONITOR/Clients** and click a list item under Name to access this page.

This page displays the watch lists by name.

Click "Watch Lists" in the title of the page to display a list of active watch lists. Refer to <u>Monitor Watch Lists</u>.

- Check box: Click the box to select a watch list to apply commands.
- User Name: Name of the watch list. Click to display its parameters.
- IP Address: IP Address of the watch list.
- MAC Address: MAC address of the watch list.
- Access Point: Click to display its parameters. Refer to <u>Monitor Access Points > <name></u>.
- Switch: Click to display its parameters. Refer to <u>Monitor Switches > <IPaddress> Summary</u>.
- Port: Alcatel OmniAccess Switch or Appliance port to which the client is attached.
- Status: Whether the client is associated or not associated with the OmniAccess AP.
- SSID: Service Set Identifier being broadcast by the OmniAccess Radio.
- Auth: Yes or No.
- Protocol: 802.11a or 802.11b/g.

- Edit Watch List: Allows you to change the parameters of a selected watch list. Select a watch list and click **GO**. Refer to *Configure Watch Lists > New Watch List*.
- Delete Watch List: Allows you to delete a selected watch list.
- Add Client by Username: Allows you to add a client to a watch list, using the username.
- Remove from Watch List: Allows you to remove a selected OmniAccess AP name from a watch list.

### **Command Buttons**

- **Apply to Switches:** Select this command and click Go. Refer to <u>Configure Watch List > < watch list name > > Apply to Switches</u>.
- **Remove from Switches:** Allows you to remove the watch list from the Alcatel OmniAccess Switch or Appliance. Refer to <u>Configure Watch List</u> > <<u>watch list name</u>> > <u>Remove From Switches</u>.

## **Monitor 802.11a Parameters**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11a/Parameters** to access this page.

This page displays 802.11a template policies:

Table - 802.11a Parameters

Parameter	Description
Policy Name	Click to go to <u>Configure 802.11a Parameters &gt; Template <name></name></u> .
Admin Status	Whether the OmniAccess Radio is enabled or disabled.
Channel Mode	Dynamic channel assignment has three modes:  • Automatic - The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Channel assignments are updated when the Assign Now button is clicked.  • OFF - No dynamic channel assignments occur and value are set to their global default.  Default is Automatic.
Power Mode	Dynamic transmit power assignment has three modes.  • Automatic - The transmit power will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Transmit power is updated when the Assign Now button is selected.  • Fixed - No dynamic transmit power assignments occur and value are set to their global default.  Default is Automatic.
Switches Applied to	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

Add Template: Select this command and click GO. Refer to <u>Configure 802.11a Parameters > New Template</u>.

### Monitor 802.11a RRM Thresholds

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11a/RRM Thresholds** to access this page.

This page allows you to view and edit existing 802.11a RRM Threshold templates, and add a new 802.11a RRM Threshold template.

Table - 802.11a RRM Thresholds

Parameter	Description
Template Name	User-defined name of the RRM template. Refer to <u>Configure 802.11a</u> <u>RRM Thresholds &gt; Template &lt; name &gt;</u> .
Interference Threshold	(0 to 100%) Foreign 802.11a interference threshold between 0 and 100 percent.
Noise Threshold	(-127 to 0 dBm) Foreign noise threshold between -127 and 0 dBm.
Max Clients	(1 to 75) Maximum number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
RF Utilization	802.11a RF utilization threshold between 0 and 100 percent.
No of Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this parameter is applied (read only).

### Select a command:

• Add Template: Refer to Configure 802.11a RRM Thresholds > New Template.

## **Monitor 802.11b/g Parameters**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11b/g/Parameters** to access this page.

This page displays 802.11b/g parameters:

Table - 802.11b/g Parameters

Parameter	Description
Policy Name	Refer to <u>Configure 802.11b/g Parameters &gt; Template <name></name></u> .
Admin Status	Whether the OmniAccess Radio is enabled or disabled.

Table - 802.11b/g Parameters (Continued)

Parameter	Description
Channel Mode	Dynamic channel assignment has three modes.  • Automatic - The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Channel assignments are updated when the Assign Now button is clicked.  • OFF - No dynamic channel assignments occur and value are set to their global default.  Default is Automatic.
Power Mode	Dynamic transmit power assignment has three modes.  • Automatic - The transmit power will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Transmit power is updated when the Assign Now button is selected.  • Fixed - No dynamic transmit power assignments occur and value are set to their global default.  Default is Automatic.
Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this parameter is applied.

Add Template: Refer to Configure 802.11b/q Parameters > Add Template < name >.

## **Monitor 802.11b/g RRM Thresholds Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Thresholds** to access this page.

This page allows you to view and add an 802.11b/g threshold template:

- Template Name: The user-defined template name. Refer to <u>Configure 802.11b/g RRM</u> <u>Thresholds > Template <name></u>.
- Interference Threshold (%): (0 to 100%) 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.
- Max Clients: Maximum number of 802.11b/g clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

### Select a command:

• Add Template: Refer to <u>Configure 802.11b/q RRM Thresholds > New Template</u>.

## Monitor 802.11b/g RRM Intervals Template

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Intervals** to access this page.

This page allows you to view 802.11b/g RRM intervals thresholds for a template:

- Template Name: User-defined name of this template. Click a list item. Refer to <u>Configure</u> 802.11b/g RRM Intervals > Template < name >.
- Signal Measurement Interval: The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
- Noise Measurement Interval: The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
- Load Measurement Interval: The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
- Coverage Measurement Interval: The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

### Select a command:

Add Template: Refer to Configure 802.11b/g RRM Intervals > New Template.

## Monitor Historically Known Rogue AP

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Known Rogues** to access this page.

Rogue access point radios are unauthorized access points detected by Alcatel OmniAccess Switch or Appliance.

This page allows you to view a table that includes Historically Known Roque APs:

- MAC Address: Media Access Control of the rogue access point. Click a name to have ACS display <u>Configure Historically Known Rogue AP > Add Rogue AP</u> to edit the rogue access point record.
- Status: State of this radio relative to the network or Alcatel OmniAccess Switch or Appliance. Rogue access point radios will appear as "Alert" when first scanned by the Alcatel OmniAccess Switch or Appliance, or as "Pending" when Alcatel Wireless Operating System identification is still underway.
- Comment: User text about this rogue access point.
- Suppress Alarm: Prevent the alarm from being displayed on the Alarm Monitor.

#### Select a command

- Add Rogue AP: Refer to <u>Configure Historically Known Rogue AP > Add Rogue AP</u>.
- Delete Roque APs: Select a roque access point, select this command, and click GO.

## **Monitor TFTP Server**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **TFTP Server** to access this page.

This page displays a list of TFTP Servers and allows you to add new ones or delete existing ones.

- Selection Checkbox.
- TFTP Server Name: This server is required for error-free Alcatel Wireless Operating System software updates. It must be able to access http://www.alcatel.com/. Refer to <u>Configure TFTP Server > TFTP Server < name > to edit a TFTP server definition.</u>

**Note:** The TFTP server cannot run on the same computer as the OmniVista Air Control System Software, because the ACS Software and the TFTP server use the same communication port. Click a list item to display the path to the server.

IP Address: Local network IP Address of the Alcatel OmniAccess Switch or Appliance
 *Management Interface*, described in the *Alcatel OmniAccess Wireless Product Guide*.

### Select a command

- Add TFTP Server: Select the command and click GO. Refer to <u>Configure TFTP Server > Add</u> TFTP Server.
- Delete TFTP Servers: Use the checkbox to select a server, select this command and click **GO** to delete a server.

## **Monitor Trap Receiver**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Trap Receiver** to access this page.

This page allows you to view trap receiver templates.

- Template Name: The name of the server where the traps are sent. Click on a list name. Refer to <u>Configure Trap Receiver > Template < name ></u> to edit a trap receiver template.
- IP Address: The IP Address of the server.
- Admin Status: Status must be enabled for the SNMP traps to be sent to the server.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

#### Select a command

• Add Template: Select this command and click **GO**. Refer to <u>Configure Trap Receiver > New Template</u>.

## **Monitor Trap Controls**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Trap Controls** to access this page.

This page allows you to view trap control template information.

- Template Name: User-defined name of this template. Click a list item to display <u>Configure Trap</u> <u>Controls > Template < name ></u> and edit a trap control template.
- Port Status: Port status, Enable or Disable.
- Rogue APs: Enable or Disable.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

Add Template: Select this command and click GO. Refer to <u>Configure Trap Controls > New Template</u>.

## **Monitor Telnet SSH Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Telnet SSH** to access this page.

This page allows you to view Telnet SSH template information.

- Template Name: Name of this SSH Template. Click a list item. Refer to <u>Configure Telnet SSH</u> <u>Configuration > Template < name ></u>.
- Sessions Timeout (min): This object indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions: Selectable from a pulldown menus for values of from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The factory default is 5.
- Allow New Telnet Sessions: Indicates that new Telnet sessions will not be allowed on the DS Port when set to no. The factory default value is no.
- Allow New SSH Session: Indicates that new Secure Shell Telnet sessions will not be allowed when set to no. The factory default value is yes.
  - **Note:** New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service (Management) port.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

### Select a command

• Add Template: Select this command and click **GO**. Refer to <u>Configure Telnet SSH Configuration</u> > <u>New Template</u>.

# **Monitor Syslog Configuration**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Syslog** to access this page.

This page allows you to view syslog configuration template information.

- Template Name: Name of this template. Click a list item. Refer to <u>Configure Syslog Configuration</u> > < <u>template name</u> > to edit a syslog configuration.
- Syslog Enabled: Enabled or Disabled.
- Syslog Host: Syslog host IP Address.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.

### Select a command

• Add Template: Select this command and click **GO**. Refer to <u>Configure Syslog Configuration > New Template</u>.

## **Monitor Access Points > Load**

Use **MONITOR/Access Points**, select one or more OmniAccess APs, from the **Generate a report for selected AP**, select **Load** to access this page.

Traffic Load is how much total bandwidth is used for transmitting and receiving traffic. This allows WLAN managers to track network growth and plan network growth ahead of client demand.

This page displays a table with load data.

Parameter	Description
AP Name	This is the name assigned to the OmniAccess AP. Refer to <u>Monitor Access Points &gt; <name></name></u> .
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Refer to <i>Monitor Access Points</i> > < <i>name</i> > > < <i>Radio Type</i> >.
Attached Client Count	(Subcolumns for Actual and Threshold) Number of clients attached.
Channel Utilization	802.11a RF utilization threshold between 0 and 100 percent. (Subcolumns for Actual and Threshold).
Receive Utilization	802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
Transmit Utilization	802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
Status	Status of the client connection.

# **Monitor Access Points > Dynamic Power Control**

Use **MONITOR/Access Points**, select one or more OmniAccess APs, then from the **Generate a report for selected AP**, select **Dynamic Power Control**.

This page displays dynamic control parameters for access points as follows:

- AP Name: This is the name assigned to the OmniAccess AP. Click an OmniAccess AP name on the list to access its parameters. Refer to <u>Monitor Access Points > <name></u>.
- Radio: Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click a
   OmniAccess Radio on the list to access its parameters. Refer to <u>Monitor Access Points >
   </ame> > < <u>Radio Type></u>.
  </u>
- Current Power Level: Displays the operating transmit power level from the transmit power table. OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
- Power Assignment Mode: Dynamic transmit power assignment has three modes:
  - Automatic The transmit power will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Transmit power is updated when the Assign Now button is selected.

- Fixed No dynamic transmit power assignments occur and value are set to their global default. Default is Automatic.
- Recommended Power Level

### Monitor Access Points > Noise

Use **MONITOR/Access Points**, select one or more OmniAccess APs, then from the **Generate a report for selected AP**, select **Noise**.

This page displays a bar graph of noise (RSSI in dBm) for each channel.

## **Monitor Access Points > Interference**

Use **MONITOR/Access Points**, select one or more OmniAccess APs, then from the **Generate a report for selected AP**, select **Interference**.

This page displays a bar graph of interference (RSSI in dBm) for each channel:

- High interference 40 to 0 dBm.
- Marginal interference -100 to -40 dBm.
- Low interference -140 to -100 dBm.

## **Monitor Access Points > Coverage (RSSI)**

Use MONITOR/Access Points, select one or more OmniAccess APs, then from the Generate a report for selected AP, select Coverage (RSSI).

This page displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

## Monitor Access Points > Coverage (SNR)

Use **MONITOR/Access Points**, select one or more OmniAccess APs, then from the **Generate a report for selected AP**, select **Coverage (SNR)**.

This page displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

## **Monitor Access Points > Up Time**

Use **MONITOR/Access Points**, select one or more OmniAccess APs, then from the **Generate a report for selected AP**, select **Up Time**.

Up Time is Time in days, hours and minutes since the last reboot.

This page displays a line graph of access point up time graphed against time.

If you select more than one AP, the following message appears: Please select only one AP for the Up Time Report.

## Monitor < IPaddress > Audit Reports

Use **CONFIGURE/Switches** and under Select a command, select **View Audit Reports** to access this page.

This page displays an audit report for the selected Alcatel OmniAccess Switch or Appliance.

Device Name: The IP address of the selected Alcatel OmniAccess Switch or Appliance.

- Time of Audit.
- Device Name.
- Synchronization Status.

Delete Audit Reports: Select a report using the check box, select this command and click GO.

# Monitor < IPaddress > Audit Report

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Configuration Commands** pulldown, select **Audit Config** to access this page.

Use **CONFIGURE/Switches** and under **Select a command**, select **View Audit Reports**, click **Report ID** to access this page.

This page displays a specific selected audit report with the following information:

- Device Name
- Time of Audit
- Report ID
- Synchronization Status
- Object Name
- Attribute
- Value in ACS
- Value in Device

Note: Shared keys and passwords are not audited.

# **Adding Maps, Devices and Templates**

You can add Alcatel OmniAccess Wireless System Campus, Building, Floor, and Outdoor Area Maps, and place OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points, and add Third-Party APs from the following:

- <u>Configure Maps > New Campus</u>
- Configure Campus > New Building
- Configure Campus > New Outdoor Area
- Configure Maps > New Building
- <u>Configure Maps > Properties</u>
- <u>Configure Building > New Floor</u>
- <u>Configure Building > New Floor 2</u>
- <u>Configure <building name> Edit Floor <floor name></u>
- CONFIGURE/Switches Menu Bar Selection
- Configure All Switches
- Configure Add Switch
- <u>Configure <IPaddress> > Add Interface</u>
- <u>Configure <IPaddress> > Add Network Route</u>
- <u>Configure <IPaddress> > Mobility Group <name></u>
- <u>Configure <IPaddress> > Mobility Group Member</u>
- Configure <IPaddress> > WLAN Template > Add From Template
- Configure WLAN Template
- <u>Configure WLAN > New Template</u>
- Configure <IPaddress> > Local Auth. > Add from Template
- Configure Access Control List > New Template
- Configure Access Control List > Add Template Rule <name>
- Configure Access Control > Add Template < name >
- Configure <IPaddress> > Access Control List > stname>
- Configure <IPaddress> > Access Control List > Add from Template
- Configure < IPaddress > Certificate Details
- <u>Configure <IPaddress> > Web Auth Certificate</u>
- Configure <IPaddress> > Download Web Auth Certificate to Switch
- Configure < IPaddress > Roque Policy Setup
- Configure < IPaddress > OmniAccess AP
- Configure <IPaddress> > Connected Third Party AP
- <u>Configure < IPaddress > Connected Third Party AP > Add New</u>
- Configure <IPaddress> > Trap Receiver > Add From Template
- CONFIGURE/Access Points Menu Bar Selection

- Configure Add Access Points
- <u>Configure Position Access Points on Floor <floor name></u>
- Configure Access Points > OmniAccess AP > <name> > 802.11a
- Configure Access Points > OmniAccess AP > <name> > 802.11b
- Configure <IPaddress> > OmniAccess AP > <name> > 802.11a > WLANs Overridden
- Configure Remove Access Points
- Configure Add Foreign AP
- Configure Disabled Clients
- <u>Configure Black List Client > <MACaddress></u>
- Configure Clients > Add to Watch List > <MAC address>
- Configure Watch Lists > New Watch List
- <u>Configure Watch Lists > Edit > <name></u>
- Configure Watch List > <watch list name> > Apply to Switches
- Configure Watch List > <watch list name> > Remove From Switches
- <u>Configure Historically Known Rogue AP > Add Rogue AP</u>
- <u>Configure TFTP Server > Add TFTP Server</u>
- <u>Configure Software Version > Add</u>
- CONFIGURE/Templates Menu Bar Selection
- Configure RADIUS Authentication Server > New Template
- <u>Configure <IPaddress> > RADIUS Auth. Server > Add From Template</u>
- <u>Configure RADIUS Authentication Server</u>
- Configure <IPaddress> > RADIUS Authentication Server
- <u>Configure RADIUS Accounting Server > New Template</u>
- Configure <IPaddress> > RADIUS Accounting Server > Add From Template
- Configure Local Authentication > New Template
- Configure Disabled Clients > New Template
- Configure <IPaddress> > Disabled Clients > Add From Template
- Configure 802.11a Parameters > New Template
- Configure 802.11a RRM Thresholds > New Template
- Configure 802.11a RRM Intervals > New Template
- Configure 802.11b/g Parameters > Add Template < name >
- <u>Configure 802.11b/g RRM Thresholds > New Template</u>
- Configure 802.11b/g RRM Intervals > New Template
- Configure Trap Receiver > New Template
- <u>Configure Trap Controls > New Template</u>
- Configure Telnet SSH Configuration > New Template

• <u>Configure Syslog Configuration > New Template</u>

## **Configure Maps > New Campus**

Use **MONITOR/Maps** to have ACS display <u>Monitor Maps</u>, then select **New Campus** from the command pulldown and click **GO**.

This page allows you to define the parameters for a new campus:

- Campus Name: User-defined, top-level location name.
- Contact: User-defined contact name.
- Image File Name: Name of the file containing the map of the campus. Use the **Browse** button
  to find the file.
- Maintain Aspect Ratio checkbox: Select this checkbox to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Dimensions (feet):
  - Horizontal span: Horizontal measurements (left to right) of the campus as it appears on the page.
  - Vertical span: Vertical measurements (up and down) of the campus as it appears on the page.

**Note:** To change the troubleshooting mode (refer to <u>Configure Maps > Properties</u>), select Monitor > Maps and select the command Properties from the pulldown.

**Note:** To change the unit of measurement (feet or meters), select Monitor > Maps and select the command Properties from the pulldown.

#### **Command Buttons**

- OK
- Cancel

## **Configure Campus > New Building**

From Monitor Maps > Campus, select **New Building** from the command pulldown and click **GO**.

This page allows you to create a new building with devices on an existing campus. This page consists of the following areas:

### **Campus and Building Graphic**

There is a blue rectangle in the upper right hand corner, superimposed on the map of the campus.

- Using the mouse, drag this rectangle to the desired building location.
- Use <CTRL>-Left Click on the blue rectangle to resize it.

### **Building Identification Information**

- Building Name: The user-defined name of the building.
- Contact: User-defined contact name.
- Number of Floors: The number of floors contained in the new building.
- Number of Basements: The number of basements contained in the new building.

- Dimensions (feet):
  - Horizontal: Horizontal measurements (left to right) of the floor as it appears on the page.
  - Vertical: Vertical measurements (up and down) of the floor as it appears on the page.

### **Command Buttons**

- Place: Fixes the changes on the display.
- Save: Saves the changes in the database. To edit the building, refer to <u>Monitor Maps > Campus</u>
   > Building.
- Cancel: Cancels the operation.

### Sidebar: Maps

- Search for All Maps, Campuses, Buildings, Floor Areas, Outdoor Areas, Access Points.
- Enter Name: User-defined name of the map displayed.
- Search Button.

## **Configure Campus > New Outdoor Area**

From <u>Monitor Maps > Campus</u>, select **New Outdoor Area** from the select a command pulldown and click **GO**.

This page allows you to add a new outdoor area to a campus for AP placement.

## **Outdoor Area Graphic**

There is a blue rectangle in the upper right hand corner, superimposed on the map of the campus.

- Using the mouse, drag this rectangle to the desired outdoor area location.
- Use <CTRL>-Left Click on the blue rectangle to resize it.

#### **Outdoor Area Identification Information**

- Name: The user-defined name of the new outdoor area.
- Contact: The user-defined contact name.
- Image File: Name of the file containing the outdoor area map. Use the Browse button to find the file.
- Horizontal Position: Shows position.
- Vertical Position: Shows position.

**Note:** To change the unit of measurement (feet or meters), select Monitor>Maps and select the command Properties from the pulldown.

- Horizontal Span: Enter and click place to change size of blue rectangle cursor.
- Vertical Span: Enter and click place to change size of blue rectangle cursor.

## **Command Buttons**

- **Place:** Fixes the changes on the display.
- Save: Saves the changes in the database. Once saved, the name of the new outdoor area
  appears on the campus map. To edit the outdoor area, refer to <u>Monitor Maps > Campus >
  <outdoor area ></u>.

Cancel: Cancels the operation.

## **Map Area Display**

Use the blue rectangle to position the outdoor area.

## **Configure Maps > New Building**

When there is no campus to create, but only a building, Use **MONITOR/Maps** to have ACS display *Monitor Maps*, then select **New Building** from the command pulldown and click **GO**.

This page allows you to add a new building without having an existing campus. This page contains the following:

- Building Name: Enter the user-defined name of the new building.
- Contact: Enter the user-defined contact name for this building.
- Number of Floors: Enter the number of floors for this building.
- Number of Basements: Enter the number of basements for this building.
- Dimensions (feet):
  - Horizontal Span: Enter the horizontal length of the building as it appears on the page (left to right).
  - Vertical Span: Enter the vertical length of the building as it appears on the page (up and down).

### **Command Buttons**

- OK
- Cancel

## **Configure Maps > Properties**

Use **MONITOR/Maps** to have ACS display *Monitor Maps*, then select **Properties** from the command pulldown and click **GO**.

This page allows you to select Map Properties.

• Troubleshooting Mode: When enabled, this mode provides a printable report of data about OmniAccess APs and their locations on the maps.

## **Command Buttons**

- OK
- Cancel

# **Configure Building > New Floor**

Use **MONITOR/Maps**, then click an item in the **Name** column, then from the Select a command pulldown, select **New Floor Area** to access this page.

This page allows you to set the parameters for a new floor in an existing building. This page contains the following:

- Floor Name: User-defined floor name.
- Contact: User-defined contact name.

- Floor: Number of the floor.
- Floor Height (feet): Enter the ceiling height of the floor.
- Import FPE File: Check this box and use the **Browse** button that appears to find a .FPE graphic.
- Image File: Name of the file containing the floor map. Use the **Browse** button to find the file. If you have imported a .FPE file, also add a .GIF or .JPG rendering of the .FPE file.

### **Command Buttons**

- **Next:** Click to continue with the new floor process. Refer to <u>Configure Building > New Floor 2</u>.
- Cancel

## **Configure Building > New Floor 2**

Use **MONITOR/Maps**, click an item in the **Name** column, from the Select a command pulldown, select **New Floor Area**, and then click the **Next** command button to access this page.

This page allows you to continue specifying the parameters for a new floor. It contains the following parameters:

- Floor Name: User-defined floor name.
- Contact: User-defined contact name.
- Floor: Number of the floor.
- Floor Height (feet): Enter the ceiling height of the floor.
- FPE File Name: Read only, set in last screen.
- Image File Name: Read only, set in last screen.
- Maintain Aspect Ratio: Select this checkbox to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Dimension (feet): For floorplan maps entered without .FPE components, enter the Horizontal Span (left to right on the map) and the Vertical Span (up and down on the map) and click **Place** to make the changes to the blue rectangle on the grid. For floorplan maps entered with .FPE components, these dimensions are specified in the .FPE file, and cannot be changed.
- Coordinates of top left corner (feet): For floorplan maps entered without .FPE components, these are the coordinates of the horizontal position and vertical position of the top left corner of the blue rectangle. For floorplan maps entered with .FPE components, these dimensions are specified in the .FPE file, and cannot be changed.
- Position (feet): Using the mouse, move the blue rectangle to the desired location on the grid.
  - **Note:** To change the troubleshooting mode (refer to *Configure Maps > Properties*), select Monitor > Maps and select the command Properties from the pulldown.
  - **Note:** To change the unit of measurement (feet or meters), select Monitor > Maps and select the command Properties from the pulldown.
- Resizing non-FPE graphics: Hold down the <CTRL> key, left-click and drag the corner of the image. Note that this does not work for FPE images, as the size of the image is defined in the FPE file.

## **Command Buttons**

Place: Fixes the changes on the display.

- Save: Saves the changes in the database.
- Cancel: Cancels the operation.

## Configure <building name> Edit Floor <floor name>

Use **MONITOR/Maps**, click an item in the **Name** column, single-click the floor map, from the Select a command pulldown menu, select **Edit Floor Area** to access this page.

This page allows you to edit a specific floor on a map:

- Floor Name: The user-defined name of the floor.
- Contact: The name of the person responsible for the design of this floor.
- Floor: The number of the floor.
- Floor Height (feet): The ceiling height of the selected floor.
- Image File: Displays the path of the floor graphic, or two graphics, if a .FPE file was imported for this floor. To change the image, use the **Browse** button.
- Maintain Aspect Ratio: Select this checkbox to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Dimension (feet): Enter the Horizontal Span (the distance from left to right on the map display)
  and the Vertical Span (the distance up and down on the map display) and click **Place** to make
  the changes take place on the grid.
- Position (feet): Using the mouse, move the blue rectangle to the desired location.
  - **Note:** To change the unit of measurement (feet or meters), select Monitor>Maps and select the command Properties from the pulldown.
- Resizing non-FPE graphics: Hold down the <CTRL> key, left-click and drag the corner of the image. Note that this does not work for FPE images, as the size of the image is defined in the FPE file.

### **Command Buttons**

- Place: Fixes the changes on the display.
- **Save:** Saves the changes in the database.
- **Cancel:** Cancels the operation.

### **CONFIGURE/Switches Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance summary details. Use the selector area to access and configure the respective Alcatel OmniAccess Switch or Appliance details. Making this selection displays <u>Configure All Switches</u>.

## **Configure All Switches**

Use **CONFIGURE/Switches** to access this page.

This page allows you to view a summary of all Alcatel OmniAccess Switches and Appliances in the ACS database. It also allows you to add Alcatel OmniAccess Switches and Appliances, remove and reboot selected Alcatel OmniAccess Switches and Appliances, download software from ACS to selected Alcatel OmniAccess Switches and Appliances, save the current configuration to nonvolatile (Flash) memory on

selected Alcatel OmniAccess Switches and Appliances, and view audit reports for selected Alcatel OmniAccess Switches and Appliances.

The data area of this page contains a table with the following columns:

- (checkbox): Click to select the Alcatel OmniAccess Switch or Appliance.
- IP Address: Local network IP Address of the Alcatel OmniAccess Switch or Appliance <u>Management Interface</u>, described in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Click the title to sort the list items. Click a list item to display parameters for that IP Address. Refer to <u>Configure <IPaddress> > Switch General</u>.
- Switch Name: Click to sort. Name of the of the Alcatel OmniAccess Switch or Appliance.
- Location: Indicates the location of the Alcatel OmniAccess Switch or Appliance. Click the list item to reveal a map showing the location of the device. Refer to <u>Monitor Maps > Campus</u>.
- Version: The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
- Status: A colored dot indicating Up (green), Minor Alarm (yellow) or Critical Alarm (red).

### Select a command pulldown

- Add Switch: Adds an Alcatel OmniAccess Switch or Appliance. Refer to <u>Configure Add Switch</u>.
- Remove Switches: Select an Alcatel OmniAccess Switch or Appliance by clicking the checkbox, select this command and click **GO**.
- Reboot Switches: Select an Alcatel OmniAccess Switch or Appliance by clicking the checkbox, select this command and click GO.
- Download Software: Select an Alcatel OmniAccess Switch or Appliance by clicking the checkbox, select this command and click GO. Refer to <u>Download Software</u>.
- Save Config to Flash: Save the current configuration to flash memory.
- View Audit Reports: Refer to <u>Monitor <IPaddress> > Audit Reports</u>.
- GO button.

#### Left sidebar

Search for Alcatel OmniAccess Switches and Appliances by (pulldown):

- Networks.
- IP Address.
- Switch Name.
- Select a Network (All Networks, x.x.x.x).
- Search (button).

# **Configure Add Switch**

Use **CONFIGURE/Switches** and under **Select a command**, select **Add Switch** to access this page.

This page allows you to add an Alcatel OmniAccess Switch or Appliance:

• **IP Address:** Enter the IP Address of the new Alcatel OmniAccess Switch or Appliance. This is an IP Address from which this device will accept SNMP packets with the associated community. The requesting entity's IP Address is ANDed with the Subnet Mask before being compared to the IP Address.

- Note: If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP Addresses.
  - **Network Mask:** Enter the network mask of the new Alcatel OmniAccess Switch or Appliance. The default value is 0.0.0.0.

Table - SNMP Read/Write

Parameter	Description
Version	SNMP Version: v1, v2c, or v3.
Retries	Attempt to discover Alcatel OmniAccess Switch or Appliance this many times.
Timeout (seconds)	Client Session timeout. Sets the maximum amount of time allowed a client before it is forced to reauthenticate.
Community	Public or Private.

- OK
- Cancel

# Configure < IPaddress > > Add Interface

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Interfaces**, from the Select a Command pulldown, select **Add Interface** to access this page.

This page allows you to add an interface description.

- Interface Name: User-defined name for this interface, for example, management, service-port, virtual, and "VLAN n'.
- Interface Address:
  - IP Address: IP Address of the interface.
  - Netmask: Netmask of the interface
  - VLAN ID: 1 through 4096, or Untagged.
  - Gateway: Gateway address of the interface.
- Interface Address:
  - Port Number: Interface port number.
- DHCP Information:
  - Primary DHCP Server: IP Address of the primary DHCP server.
  - Secondary DHCP Server: IP Address of the secondary DHCP server.
- Access Control List:
  - ACL Name: User-defined name of the access control list.

### **Command Buttons**

Save

Cancel

# Configure < IPaddress > > Add Network Route

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and click **Network Route**, then from the Select a command pulldown, select **Add Network Route** and click **GO** to access this page.

This page allows you to add a route to the Alcatel OmniAccess Switch or Appliance Service (Management) port. This route allows you to direct all Service port traffic to the designated management IP address.

- IP Address
- Network Mask
- Gateway IP Address

#### **Command Buttons**

- Save
- Cancel

# Configure < IPaddress > Mobility Group < name >

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Mobility Groups**, from the Select a command pulldown, select **Add Group Members** to access this page.

This page allows you to define a mobility group member from a list of existing Alcatel OmniAccess Switches or Appliances.

- Switch Name. Check to add to the Mobility Group.
- Member MAC Address: MAC address of the mobility group member.
- Member IP Address: IP Address of the mobility group member.

To manually add members, use the **click here** link. Refer to <u>Configure < IPaddress > Mobility Group Member</u>.

### **Command Buttons**

- Save
- Cancel

# **Configure <IPaddress> > Mobility Group Member**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Mobility Groups**, from the Select a command pulldown, select **Add Group Members**, click on the "click here" link to access this page.

This page allows you to define a mobility group member.

- Member MAC Address: MAC address of the mobility group member.
- Member IP Address: IP Address of the mobility group member.

### **Command Buttons**

Save

### Cancel

# **Configure <IPaddress> > WLAN Template > Add From Template**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, click **WLANs**, from the Select a command pulldown, select **Add WLAN** to access this page.

This page allows you to add information from an existing WLAN template.

• **Select a template to create from**: Use the pulldown to select an already existing template name.

Note: You can also create a New Template. Refer to Configure WLAN > New Template.

- Command Buttons:
  - Create: Click to create.Cancel: Click to cancel.
- SSID: Name of the WLAN.
- Template Name: User-defined name of the template.
- WLAN for 3rd Party APIs Checkbox: The third-party AP WLAN can only be configured with 802.1X encryption as described in <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Drop down configurable 802.1X parameters are not available for this WLAN.

### Table - General Policies

Parameter	Description
Radio Policy	Set the WLAN policy to apply to All = 802.11a/b/g, 802.11a only, 802.11b only, 802.11g only, 802.11b/g only, 802.11a/b only, or 802.11a/g only. All, 802.11a only, 802.11b/g only.
Admin Status	Check the box to set the status of the WLAN to enabled.
Session Timeout	Set the maximum time for a client session before requiring reauthorization.
Quality of Service (QoS)	Set QoS to: Gold (Highest); Silver (Mid-range); Bronze (Low). Services such as VoIP should be set to Gold while non-discriminating services such as text messaging can be set to Bronze.

Table - General Policies (Continued)

Parameter	Description
Allow AAA Override	Enable or disable AAA override for global WLAN parameters.  • When AAA Override is enabled, and a client has conflicting AAA and Alcatel OmniAccess Switch or Appliance WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the Alcatel Wireless Operating System will move clients from the default Alcatel WLAN VLAN to a VLAN returned by the AAA server and predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Alcatel Wireless Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)  For instance, if the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the Alcatel Wireless Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.  • When AAA Override is disabled, all client authentication defaults to the Alcatel OmniAccess Switch or Appliance authentication parameter settings, and authentication is only performed by the AAA server if the Alcatel OmniAccess Switch or Appliance WLAN do not contain any client-specific authentication parameters.  The AAA override values may come from a RADIUS server, for example.
Disable Timeout	Enable or disable automatic disabling, and set the timeout in seconds for disabled client machines. Client machines are disabled by MAC address and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client. Set (see Note) checkbox, Timeout Value (secs) field.
DHCP Server	<ul> <li>When selected, you can enter the IP Address of your DHCP server. This is a Required field for some WLAN configurations. There are three valid configurations and one invalid combination:</li> <li>DHCP Required and a valid DHCP Server IP Address: Requires all WLAN clients to obtain an IP Address from the DHCP Server.</li> <li>DHCP Not Required and a valid DHCP Server IP Address: Allows all WLAN clients to obtain an IP Address from the DHCP Server or use a static IP Address.</li> <li>DHCP Not Required and DHCP Server IP Address 0.0.0.0: Forces all WLAN clients to use a static IP Address. All DHCP requests are dropped.</li> <li>DHCP Required and DHCP Server IP Address 0.0.0.0 is not allowed.</li> </ul>
DHCP Addr Assignment	Required checkbox.

timeout from the disabled state. It does not imply that the blackslisting feature will be disabled.

You can choose both Layer 2 and Layer 3 security policies from the drop down list under the Security Policies heading. The selected security policy options are at the bottom of the page with the appropriate parameters listed. The following table describes these parameters.

Note: The values in the other tables on this page change depending upon the security policies selected.

Table - Security Policies

Parameter	Description
Layer 2 Security	None, WPA, 802.1X, Static WEP, Cranite MAC Filtering checkbox.
Layer 3 Security	None, IPSec, VPN Pass Through, Web Authentication (Note) Checkbox.

**Note:** Alcatel OmniAccess Switch or Appliance must be rebooted for Web Authentication to take effect. Web Authenticating cannot be used in combination with IPSec.

Table - 802.1X Parameters

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Radio Button	Active when there is more than one type of encryption available.
Туре	WEP, TKIP-MIC.
Key Size	40 bits, 104 bits, 128 bits.
Key Index	1 through 4.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.
Key Format	ASCII or HEX.

**Note:** The values in these fields and the fields themselves change depending upon the security policies selected.

**Table - WPA Parameters** 

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Туре	Active when there is more than one type of encryption available.
Key Size	TKIP-MIC.
Preshared Key Mode	Enable checkbox.

**IPSec Pass through:** Available only when VPN Pass through is selected for Layer 3 Security. Displays the IP Address of the VPN Gateway Address.

 Table - IPSec Parameters (Available only when IPSec is selected under Layer 3 Security)

Parameter	Description
IPSec Authentication	None, HMAC-MD5, HMAC-SHA1.
IPSec Encryption	DES3, None, AES-CBC, DES.
IKE Authentication	Displays a radio button for selection of Type (Certificate, Pre-Shared Key, XAuth Pre-Shared Key) and Key (Note).
IKE Phase1	Aggressive, Main.
Lifetime (seconds)	Timeout in seconds.
IKE Diffle Hellman Group	Group 1 (768 bits), Group 2 (1024 bits), Group 3 (1536 bits).

**Note:** When you select XAuth Pre Shared Key, the key must be at least eight bytes to interoperate with Cisco clients. Other tested clients function with a key of less than eight bytes.

# **Configure WLAN Template**

Use **CONFIGURE/Templates** to access this page.

Templates allow you to set parameters that you can then apply to multiple devices without having re-enter the common information, such as SSID or Security policies.



**Note:** Template information can be overridden on individual devices.

This page displays a summary of WLAN templates and their parameters, and allows you to edit and add Templates.

Templates allow you to set parameters that you can then apply to multiple devices without having re-enter the common information, such as SSID or Security policies.

- Template Name: User-defined name of this template. Click the name to display parameters for this template. Refer to <u>Configure WLAN Template > Template < name ></u> to edit an existing template.
- SSID: Name of the WLAN.
- Security Policies: None, 802.1X.
- Admin Status: Enable or Disable.
- Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances this template is currently applied to.

### Select a command

Add Template: Refer to <u>Configure WLAN > New Template</u>.

## Left sidebar (Templates)

Click the arrow or on title to display menu choices.

- WLAN: This page.
- Security: Click to reveal/hide the menu selections:

- Radius Auth Servers: Refer to Monitor RADIUS Authentication Server.
- Radius Acct Servers: Refer to Configure RADIUS Accounting Server.
- Local Authentication: Refer to <u>Configure < IPaddress > CA Certification</u>.
- Disabled Clients: Refer to Configure Disabled Clients.
- Access Control Lists: Refer to Monitor Access Control List.
- 802.11a: Click to reveal/hide the menu selections:
  - Parameters: Refer to *Monitor 802.11a Parameters*.
  - RRM Thresholds: Refer to <u>Monitor 802.11a RRM Thresholds</u>.
  - RRM Intervals: Refer to <u>Configure 802.11a RRM Intervals > New Template</u>.
- 802.11b/g: Click to reveal/hide the menu selections:
  - Parameters: Refer to <u>Monitor 802.11b/g Parameters</u>.
  - RRM Thresholds: Refer to Monitor 802.11b/g RRM Thresholds Template.
  - RRM Intervals: Refer to Monitor 802.11b/g RRM Intervals Template.
- Known Rogues: Refer to <u>Monitor Historically Known Rogue AP</u>.
- TFTP Servers: Refer to Monitor TFTP Server.
- Control: Click to reveal/hide the menu selections:
  - Trap Receivers: Refer to <u>Monitor Trap Receiver</u>.
  - Trap Control: Refer to *Monitor Trap Controls*.
  - Telnet SSH: Refer to <u>Monitor Telnet SSH Template</u>.
  - Syslog: Log of system events. Refer to *Monitor Syslog Configuration*.

### **Configure WLAN > New Template**

Use **CONFIGURE/Templates** and from the **Select a command** pulldown, select **Add Template** to access this page.

This page allows you to create a new WLAN template.

- SSID: Name of the WLAN.
- Template Name: User-defined name of the template.
- WLAN for 3rd Party APIs Checkbox: The third-party AP WLAN can only be configured with 802.1X encryption as described in <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Drop down configurable 802.1X parameters are not available for this WLAN.

Table - General Policies

Parameter	Description
Radio Policy	Set the WLAN policy to apply to All = 802.11a/b/g, 802.11a only, 802.11b only, 802.11g only, 802.11b/g only, 802.11a/b only, or 802.11a/g only. All, 802.11a only, 802.11b/g only.
Admin Status	Check the box to set the status of the WLAN to enabled.
Session Timeout	Set the maximum time for a client session before requiring reauthorization.

Table - General Policies (Continued)

Parameter	Description
Quality of Service (QoS)	Set QoS to: Gold (Highest); Silver (Mid-range); Bronze (Low). Services such as VoIP should be set to Gold while non-discriminating services such as text messaging can be set to Bronze.
Allow AAA Override	<ul> <li>Enable or disable AAA override for global WLAN parameters.</li> <li>When AAA Override is enabled, and a client has conflicting AAA and Alcatel OmniAccess Switch or Appliance WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the Alcatel Wireless Operating System will move clients from the default Alcatel WLAN VLAN to a VLAN returned by the AAA server and predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Alcatel Wireless Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)</li> <li>For instance, if the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the Alcatel Wireless Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</li> <li>When AAA Override is disabled, all client authentication defaults to the Alcatel OmniAccess Switch or Appliance authentication parameter settings, and authentication is only performed by the AAA server if the Alcatel OmniAccess Switch or Appliance WLAN do not contain any client-specific authentication parameters.</li> <li>The AAA override values may come from a RADIUS server, for example.</li> </ul>
Disable Timeout	Enable or disable automatic disabling, and set the timeout in seconds for disabled client machines. Client machines are disabled by MAC address and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client., Set** checkbox, Timeout Value (secs) field.
DHCP Relay	<ul> <li>When selected, you can enter the IP Address of your DHCP server. This is a Required field for some WLAN configurations. There are three valid configurations and one invalid combination:</li> <li>DHCP Required and a valid DHCP Server IP Address: Requires all WLAN clients to obtain an IP Address from the DHCP Server.</li> <li>DHCP Not Required and a valid DHCP Server IP Address: Allows all WLAN clients to obtain an IP Address from the DHCP Server or use a static IP Address.</li> <li>DHCP Not Required and DHCP Server IP Address 0.0.0.0: Forces all WLAN clients to use a static IP Address. All DHCP requests are dropped.</li> <li>DHCP Required and DHCP Server IP Address 0.0.0.0 is not allowed.</li> </ul>

**Note:** When Disable timeout is not set, it implies that a disabled client will remain so and will never timeout from the disabled state. It does not imply that the blackslisting feature will be disabled.

You can choose both Layer 2 and Layer 3 security policies from the drop down list under the Security Policies heading. The selected security policy options are at the bottom of the page with the appropriate parameters listed. The following table describes these parameters.

**Note:** The values in the other tables on this page change depending upon the security policies selected.

Table - Security Policies

Parameter	Description
Layer 2 Security	Selections are: None, WPA, 802.1X, Static WEP, Cranite, MAC Filtering checkbox.
Layer 3 Security	None, IPSec, VPN Pass Through, Web Authentication (Note) Checkbox.

**Note:** Alcatel OmniAccess Switch or Appliance must be rebooted for Web Authentication to take effect. Web Authenticating cannot be used in combination with IPSec.

Table - 802.1X Parameters

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Radio Button	Active when there is more than one type of encryption available.
Туре	WEP, TKIP-MIC.
Key Size	40 bits, 104 bits, 128 bits.
Key Index	1 through 4.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.
Key Format	ASCII or HEX.

**Note:** The values in these fields and the fields themselves change depending upon the security policies selected.

Table - WPA Parameters

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Туре	Active when there is more than one type of encryption available.
Key Size	TKIP-MIC.

Table - WPA Parameters (Continued)

Parameter	Description
Preshared Key Mode	Enable checkbox.

IPSec Pass through: Available only when VPN Pass through is selected for Layer 3 Security. Displays the IP Address of the VPN Gateway Address.

Table - IPSec Parameters (Available only when IPSec is selected under Layer 3 Security)

Parameter	Description
IPSec Authentication	None, HMAC-MD5, HMAC-SHA1.
IPSec Encryption	DES3, None, AES-CBC, DES.
IKE Authentication	Displays a radio button for selection of Type (Certificate, Pre-Shared Key, XAuth Pre-Shared Key) and Key (Note).
IKE Phase1	Aggressive, Main.
Lifetime (seconds)	IKE timeout in seconds.
IKE Diffle Hellman Group	Group 1 (768 bits), Group 2 (1024 bits), Group 3 (1536 bits).

Note: When you select XAuth Pre Shared Key, the key must be at least eight bytes to interoperate with Cisco clients. Other tested clients function with a key of less than eight bytes.

### **Command Buttons**

The buttons displayed depend upon the selection made under security policies.

- Save
- Cancel

### **Configure <IPaddress> > Local Auth. > Add from Template**

Use CONFIGURE/Switches and click an IP address under the IP Address column, on the left sidebar menu, select Security and click Local Authentication, from the Select a command pulldown, select Add Local User to access this page.

This page allows you to add information from a template for local authentication.

**Select a template to create from** (pulldown list of available templates).

- Create
- Cancel

To create a New Template for Local Authentication click here to get redirected to template creation page. Refer to Configure Local Authentication > New Template.

- User Name: User defined identification.
- Number of Switches applied to.
- Category: Network Manager, Network User, Client MAC Address.
- Access Level: ReadWrite, Read Only.

# **Configure Access Control List > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Access Control Lists**, under the Select a command pulldown, select **Add Template**, click **GO** to access this page.

This page allows you to add a new access control list template name.

Add a new Access Control List Template Name.

### **Command Buttons**

- **Save:** Add the new ACL name to the ACS database and go to the <u>Monitor Access Control List Template</u>.
- Cancel

# Configure Access Control List > Add Template Rule <name>

Use **CONFIGURE/Templates**, from the left sidebar menu under **Security**, select **Access Control Lists**, click an **ACL Name** and then select **Add New Rule** to access this page.

This page displays current access control template information for a specific ACL, and allows you to add a new rule to an ACL Template for an Alcatel OmniAccess Switch or Appliance.

The rules are listed in the following order:

- Sequence: The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5. Note that if you add or change a Sequence number, Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
- Source: Source IP Mask.
- Destination: Destination IP Mask.
- Protocol: Protocol to use for this ACL:
  - Any All protocols
  - TCP Transmission Control Protocol
  - UDP User Datagram Protocol
  - ICMP Internet Control Message Protocol
  - ESP IP Encapsulating Security Payload
  - AH Authentication Header
  - GRE Generic Routing Encapsulation
  - IP Internet Protocol
  - Eth Over IP Ethernet over Internet Protocol
  - OSPF Open Shortest Path First
  - Other Any other IANA protocol (http://www.iana.org/)
- If TCP or UDP Protocol is selected, Source Port: Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.

- Dest Port: Destination port. If TCP or UDP Protocol is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- DSCP (Differentiated Services Code Point): Any, IP Address.
- Direction: Any, Inbound (from client) or Outbound (to client).
- Action: Permit, Deny.

- Save
- Cancel

## Configure Access Control > Add Template <name>

Use **CONFIGURE/Templates**, on the left sidebar menu, select **Security** and click **Access Control Lists**, click a list item under **ACL Name** to access this page.

This page displays access control template information:

Table - General

Parameter	Description
Template Name	User-defined name of this template.
Sequence	The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5. Note that if you add or change a Sequence number, Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IP Address and Netmask.
Destination	Any or IP Address and Netmask.
Protocol	Protocol to use for this ACL: Any protocol TCP - Transmission Control Protocol UDP - User Datagram Protocol ICMP - Internet Control Message Protocol ESP - IP Encapsulating Security Payload AH - Authentication Header GRE - Generic Routing Encapsulation IP - Internet Protocol Eth Over IP - Ethernet over Internet Protocol OSPF - Open Shortest Path First Other - Any other IANA protocol (http://www.iana.org/)
Src Port	Source port, HTTP, 80.

### Table - General (Continued)

Parameter	Description
Dst Port	Destination port, HTTP, 80.
Direction	Inbound, Outbound.
Action	Permit, Deny.
Delete	(check box).

### Select a command

- Add New Rule: Refer to <u>Configure <IPaddress> > Access Control List > Istname>.
  </u>
- Delete Rules

### **Command Buttons**

- Apply to Switches
- Delete
- Cancel

# Configure < IPaddress > Access Control List > < listname >

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Access Control Lists**, click an **ACL Name**, and from the Select a command pulldown, select **Add New Rule** to access this page.

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Security/Access Control Lists**, click a list item under **ACL Name**, from the Select a command pulldown, select **Add New Rule** to access this page.

This page allows you to add a new rule for an access control list for an Alcatel OmniAccess Switch or Appliance.

- Sequence: The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5. Note that if you add or change a Sequence number, Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.
- Source: Any or IP Address and Netmask.
- Destination: Any or IP Address and Netmask.
- Protocol: Protocol to use for this ACL:
  - Any All protocols
  - TCP Transmission Control Protocol
  - UDP User Datagram Protocol
  - ICMP Internet Control Message Protocol
  - ESP IP Encapsulating Security Payload
  - AH Authentication Header

- GRE Generic Routing Encapsulation
- IP Internet Protocol
- Eth Over IP Ethernet over Internet Protocol
- OSPF Open Shortest Path First
- Other Any other IANA protocol (http://www.iana.org/)
- If TCP or UDP Protocol is selected, Source Port: Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- Dest Port: Destination port. If TCP or UDP Protocol is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- DSCP: Differentiated Services Code Point. Any, IP Address.
- Direction: Any, Inbound, Outbound.
- Action: Permit, Deny.

- Save
- Cancel

# Configure < IPaddress > Access Control List > Add from Template

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Access Control Lists**, under the Select a command pulldown, select **Add Access Control**, click **GO** to access this page.

This page allows you to add information from a template to an access control list.

**Select a template to create from** (pulldown list of available templates).

- Create
- Cancel

To create a New Template for Access Control List **click here** to get redirected to template creation page. Refer to <u>Configure Access Control List > New Template</u>.

Access Control List Name: The name of currently-applied access control list(s).

## **Configure < IPaddress> > Certificate Details**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **ID Certificate** and use the Command Button **Add Certificate** to access this page.

This page allows you to add network ID certificates.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

Name: Name of the certificate.

- Password: Password for the certificate.
- Use the **Browse** button to find the certificate so that it can be imported.
- To set a certificate, paste the certificate in the box.

- Save
- Cancel

# **Configure < IPaddress> > Web Auth Certificate**

Use CONFIGURE/Switches and select Security/Web Auth Certificate to access this page.

This page allows you to download a web authorization certificate or regenerate the internally-generated web auth certificate.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

 Download Web Auth Certificate: Takes you to <u>Configure < IPaddress> > Download Web Auth</u> Certificate to Switch.

#### **Command Buttons**

• **Regenerate Cert:** Regenerate the internally-generated web auth certificate.

# Configure < IPaddress > Download Web Auth Certificate to Switch

From the <u>Configure <IPaddress> > Web Auth Certificate</u> page, click Download Web Auth Certificate to access this page.

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Upload/Download Commands** pulldown, select **Download WEB Auth Cert** to access this page.

This page allows you to download a web authorization certificate.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance to receive the certificate.
- Status: Status of the certificate, for example, not initiated.

#### **TFTP Servers**

- Server Name: Use the Pulldown to select Default Server or New. When you select New, type in the IP Address.
- Server Address: IP Address of the server.
- Path: Path to the certificate.
- File Name: File name of the certificate.
- Password: Password to access the certificate.

- OK
- Cancel

# Configure < IPaddress > Rogue Policy Setup

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Rogue Policy** to access this page.

This page allows you to set up policies for rogue access points.

- Rogue Location Discovery Protocol: Enable, Disable
- Automatically contain rogues on my network: Enable, Disable
- Expiration for Rogue AP Entries Timeouts (seconds)

#### **Command Buttons**

- Save
- Audit

# Configure < IPaddress > OmniAccess AP

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Access Points** and click **OmniAccess APs** to access this page.

This page displays information about OmniAccess APs:

Table - OmniAccess AP

Parameter	Description
Name	Customer definable name of the OmniAccess AP. Refer to <u>Configure</u> <u>Access Point &gt; OmniAccess AP &gt; <name></name></u> .
MAC Address	Media Access Control of the OmniAccess AP.
Admin Status	Administration state of the OmniAccess AP is either enabled or disabled.
AP Mode	Indicates the state of the OmniAccess AP Monitor mode (monitor for rogue access points without allowing clients to associate): either local, OmniAccess AP 1200R or Monitor.  Note: In order for Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) to operate correctly, this parameter must be set to OmniAccess AP 1200R.
Software Version	Displays the Software version, for example, 1.3.25.5.
Primary Switch Name	This is the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance SNMP name. The OmniAccess AP will attempt to associate with this Alcatel OmniAccess Switch or Appliance first for all network operations and in the event of a hardware reset (Note).

Table - OmniAccess AP (Continued)

Parameter	Description
-----------	-------------

**Note:** After the OmniAccess AP is reset, it will attempt to connect with its Primary Alcatel OmniAccess Switch or Appliance as configured on this page. If the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance is not available, it will search for the Master Alcatel OmniAccess Switch or Appliance, and finally the least loaded Alcatel OmniAccess Switch or Appliance on the network.

# Configure < IPaddress > > Connected Third Party AP

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Access Points** and click **Third Party APs** to access this page.

This page lists the Cisco 1200, Cisco 350 and ORINOCO 2000 Access Points directly connected to your 4012 or 4024 OmniAccess Wireless Switch:

Table - Connected Third Party AP

Parameter	Description
Checkbox	Use the checkbox to select one or more third party APs.
IP Address	Third party AP IP Address. Blank if obtaining IP Address from a DHCP server. Click to edit <u>Configure &lt; IPaddress &gt; Connected Third Party AP &gt; New</u> .
MAC Address	Third party AP MAC address.
802.1X Required	Checkbox indicating whether 802.1X is enabled or disabled.
Switch Port Number	Alcatel OmniAccess Switch or Appliance interface port.

### Select a command

Make a selection and click GO:

- Add Third Party AP: Refer to Configure < IPaddress> > Connected Third Party AP > Add New.
- Delete Third Party AP: Check the AP to be deleted, select this command and click GO.

# Configure < IPaddress > Connected Third Party AP > Add New

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Access Points** and click **Third Party APs**, then from the Select a command pulldown, select **Add Third Party AP** to access this page.

This page allows you to a new connected third party AP:

- IP Address: IP Address of the third party AP.
- MAC Address: MAC Address of the third party AP.
- Switch Port Number: Alcatel OmniAccess Switch or Appliance port number of the third party AP.
- 802.11x Required: Click the box to require 802.11x.
- Mirror Mode: Disable or enable.

- Save
- Cancel

# **Configure <IPaddress> > Trap Receiver > Add From Template**

Use CONFIGURE/Switches, click an IP address under the IP Address column, on the left sidebar menu, select Control and click Trap Receivers, from the Select a command pulldown, select Add **Receivers** to access this page.

Select a template to create from IP Address: IP Address pulldown.

### **Command Buttons**

- Create
- Cancel

To create a New Template for 'Trap Receiver' click here to get redirected to template creation page;

- Template Name: User-defined template name.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this information is applied.
- IP Address: IP Address.
- Admin Status: Whether the AP is enabled or disabled.

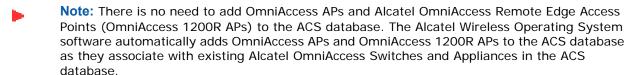
## **CONFIGURE/Access Points Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Wireless Access Point summary details. Use the selector area to access and configure the respective access points details. Making this selection from the menu bar displays Configure All Access Points.

# **Configure All Access Points**

Use **CONFIGURE/Access Points** to access this page.

This page allows you to view a summary of all OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs) in the ACS database. It also allows you to add Third-Party APs, and remove selected OmniAccess APs and OmniAccess 1200R APs.



The data area of this page contains a table with the following columns:

- Selection Checkbox
- AP Name: This is the name assigned to the OmniAccess AP. Click a list item for details about the AP. Refer to Configure Access Point > OmniAccess AP > < name >.
- Radio: Protocol of the OmniAccess Radio is either 802.11a, 802.11b or 802.11g. Click a list item for details about the OmniAccess Radio. Refer to Monitor Access Points > <name> > <Radio Type>.
- Location: Unassigned or location on a map of the location of the AP.

- Switch: IP Address of the Alcatel OmniAccess Switch or Appliance to which this AP is attached.
- Port: The OmniAccess AP is connected to this Alcatel OmniAccess Switch or Appliance port.
- Oper Status: Displays the operational status of the Alcatel device, either Up or Down.
- Alarm Status: A colored dot indicating Up (green), Alarm (yellow) or Down (red).

### Select a command pulldown

- To add a foreign AP, select the command Add Foreign AP and click **GO. Refer to** <u>Configure Add Foreign AP.</u>
- To remove an AP, select the command Remove APs and Click GO.

#### Left sidebar

- Search for APs by (pulldown): (All APs, MAC Address, AP Name, Switch. All Foreign APs, Indoor Area, Outdoor Area).
- Select Radio Type (All Radios, 802.11a, 802.11b/g).
- Search (button).

# Configure < IPaddress > OmniAccess AP > < name > > 802.11x > Perf. Profile

Use **MONITOR/Access Points**, click a list item under Radio, then click **Radio**, then click the phrase "To view/edit Performance Profile parameters for this AP interface, click here." to access this page.

Use **MONITOR/Maps**, click an item in the **Name** column, click an AP icon, then click **Radio**, then click the phrase "To view/edit Performance Profile parameters for this AP interface, click here." to access this page.

Use **MONITOR/Clients**, click a list item under AP Name, click **AP Interfaces**, then click **Radio**, then click the phrase "To view/edit Performance Profile parameters for this AP interface, click here." to access this page.

This page details the performance profile of the selected OmniAccess Radio. The profile parameters are detailed in the following table and should be enabled for global control:

Table - 802.11 Performance Parameters

Parameter	Description
Interface Type	Displays the 802.11a or 802.11b/g OmniAccess Radio type.
AP Name	Displays the customer definable name of the OmniAccess AP.
AP ID	Displays the OmniAccess AP identification number.
Profile Parameters Globally Controlled	<b>Note:</b> You cannot change the following parameters if the Profile Parameters Globally Controlled checkbox is selected.
Interference Thres (%)	Foreign 802.11a or 802.11b/g interference threshold between 0 and 100 percent.
Noise (-127 to 0 dBm)	Noise threshold between -127 and 0 dBm.
RF Utilization (%)	802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

Table - 802.11 Performance Parameters (Continued)

Parameter	Description
Throughput Thres. (bps)	802.11a or 802.11b/g throughput threshold between 1 Kbps and 1000 Kbps.
Max Clients (1 to 75)	Client threshold between 1 and 75 clients.
Min Failed Clients (#)	Client minimum exception level (1 to 75).
Min SNR Level	Minimum signal to noise ratio allowed.
Min Failed Clients (%)	Client threshold between 1 to 100%.

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

# **Configure Add Access Points**

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor or outdoor area map, from the Select a command pulldown menu, select **Add Access Points** to access this page.

This page allows you to add unassigned access points to an Outdoor Area or Floor Map.

When Access Points are physically installed, they are detected as unassigned. Only in this state can they be added to maps. If there are no unassigned OmniAccess APs, the following message appears when you use this command:

There are no more unassigned APs. ALL APs have been added to Areas. To assign APs to this area, first remove those APs from their respective areas.

When there are unassigned APs, they appear on this page with a checkbox. To add an OmniAccess AP to the map, click the checkbox, and select **OK**.

### **Command Buttons**

- OK
- Cancel

## Configure Position Access Points on Floor <floor name>

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Select a command pulldown menu, select **Position APs** to access this page.

This page allows you to position Access Points on the selected floor map. The map in gray displays the associated APs with information about the AP in the panel next to it.

- Select an AP: This pulldown allows you to select any one of the APs on the floor plan. When selected, its icon turns blue and can be repositioned by dragging it with the mouse.
- Horiz: Displays the horizontal span position (left to right) of the selected AP on the floor.
- Vert: Displays the Vertical span position (up and down) of the selected AP on the floor.

**Note:** To change the unit of measurement (feet or meters), select Monitor>Maps and select the command Properties from the pulldown.

• Antenna Angle: Indicates the placement of the AP internal antenna in respect to the floor map. Selections are: 0, 45, 90, 135, 180, 225, 270, 360 degrees.

### **Command Buttons**

- Place AP: Fixes the position of the AP on the display and updates the display of its coordinates.
- **Save:** Saves the placed AP position in the database.
- Cancel: Cancels the operation.

# Configure Access Points > OmniAccess AP > <name> > 802.11a

Use **CONFIGURE/Access Points** and select an 802.11a item under **Radio** to access this page.

This page displays parameters of the selected OmniAccess AP 802.11a OmniAccess Radio:

### Table - General

Parameter	Description
AP Name	The customer definable name of the OmniAccess AP.
Admin Status	Check to box to indicate the administration state of the OmniAccess AP as enabled.
Site Config ID	Site identification number.

### Table - Antenna

Parameter	Description
Antenna Mode	Omni, Sector A, Sector B.
Antenna Type	Internal or external antennas

### Table - RF Channel Assignment

Parameter	Description
Current Channel	Channel number of the OmniAccess AP.
Assignment Method	Channels may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally Check a circle for Global or Custom (when checked, from the pulldown menu, select one of the following: 36, 40, 44, 48, 52, 56, 60, 64, 149, 159, 157, 161.

Table - Tx Power Level Assignment

Parameter	Description
Current Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note: The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Assignment Method	Channels may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally using the custom option. Check a circle for Global or Custom (then use the pulldown menu with 1 through 5).  Note: The assignment method should normally be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the channel number as determined by the OmniVista AirView Software.

### Table - WLAN Override

Parameter	Description
WLAN Override	Enable, Disable. When you enable WLAN Override, Alcatel Wireless Operating System displays a table showing all current Alcatel WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a OmniAccess Radio.

### **Performance Profile**

"To view/edit Performance Profile parameters for this AP interface, click here." Refer to <u>Configure < IPaddress</u> > OmniAccess AP > < name > > 802.11x > Perf. Profile.

### **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

# Configure Access Points > OmniAccess AP > <name> > 802.11b

Use CONFIGURE/Access Points and select an 802.11b item under Radio to access this page.

This page allows you to edit parameters of the selected 802.11b OmniAccess Radio:

### Table - General

Parameter	Description
AP Name	The customer definable name of the OmniAccess AP.

# Table - General (Continued)

Parameter	Description
Admin Status	Check to box to indicate the administration state of the OmniAccess AP as enabled.
Site Config ID	Site identification number.

## Table - Antenna

Parameter	Description
Antenna Type	Internal or external antennas, Omni, Sector A, Sector B.
Antenna Diversity	Diversity enabled or external antennas identified by connectors. Enabled, Connector A, Connector B.

# Table - RF Channel Assignment

Parameter	Description
Current Channel	Channel number of the OmniAccess AP.
Assignment Method	Channels may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally Check a circle for Global or Custom (when checked, from the pulldown menu, select one of the following: 36, 40, 44, 48, 52, 56, 60, 64, 149, 159, 157, 161.

**Table -** Tx Power Level Assignment

Parameter	Description
Current Tx Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power).  Note: The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis. Refer to Alcatel OmniAccess Wireless System Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.
Assignment Method	Channels may be set either globally by the Alcatel OmniAccess Switch or Appliance or locally using the custom option. Check a circle for Global or Custom (then use the pulldown menu with 1 through 5).  Note: The assignment method should normally be left at the global setting. This allows the Alcatel OmniAccess Switch or Appliance to dynamically change the channel number as determined by the OmniVista AirView Software.

### Table - WLAN Override

Parameter	Description
WLAN Override	Enable, Disable for this OmniAccess AP. When you enable WLAN Override, Alcatel Wireless Operating System displays a table showing all current Alcatel WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this OmniAccess AP 802.11b/g OmniAccess Radio.
	802.11b/g OmniAccess Radio.

"To view WLAN Override entries for this AP Interface, click here." Refer to <u>Configure < IPaddress > OmniAccess AP > < name > > 802.11a > WLANS Overridden</u>.

#### **Performance Profile**

### **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

# Config < IPaddr > OmniAccess AP > < name > > 802.11a > WLANs Overridden

Use **MONITOR/Maps**, click an item in the **Name** column, click an AP icon, then click **Radio**, then click the phrase "To view WLAN Override entries for this AP Interface, click here." to access this page.

Use **CONFIGURE/Access Points** and select a list item under **Radio**, then click the phrase "To view WLAN Override entries for this AP Interface, click here." to access this page.

This page allows you to override WLANs.

- Checkbox: Use this box to select.
- WLAN Override Id: Use this checkbox to enable or disable WLAN Override for this 802.11a
   OmniAccess Radio.

**Note:** When you enable WLAN Override, Alcatel Wireless Operating System displays a table showing all current Alcatel WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a OmniAccess Radio.

WLANSsId: Name of the WLAN.

### **Command Buttons**

- Save
- Cancel

## **Configure Remove Access Points**

Use **MONITOR/Maps**, click an item in the **Name** column, left-click the floor map, from the Select a command pulldown menu, select **Remove Access Points** and click **GO** to access this page.

This page allows you to remove access points from Floor Area <floor area name>.

Check the boxes of the APs to be removed and click **OK**. To cancel, click **Cancel**.

# **Configure Add Foreign AP**

Use **CONFIGURE/Access Points** and select **Add Foreign AP** from the Select a command pulldown to access this page.

This page allows you to add a foreign AP:

• **IP Address:** An IP Address from which this device will accept SNMP packets with the associated community. The requesting entity's IP Address is ANDed with the Subnet Mask before being compared to the IP Address.

**Note:** If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP Addresses. The default value is 0.0.0.0.

• **Network Mask:** A mask to be ANDed with the requesting entity's IP Address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP Address.

For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP Addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.

Table - SNMP Read/Write

Parameter	Description
Version	SNMP Version: v1, or v2.
Retries	Maximum number of times each read/write operation can be attempted.
Timeout (seconds)	The amount of time allowed for each read/write operation.
Community	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.

### **Command Buttons**

- OK
- Reset
- Cancel

# **Configure Disabled Clients**

Use **CONFIGURE/Templates**, on the left sidebar menu, select **Security** and click **Disabled Clients** to access this page.

This page shows disabled (blacklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or disabled, from further association attempts for an operator-defined timeout. After the disable timeout, the client is allowed to retry authentication until it associates or fails authentication and is disabled again.

### Table - Disabled Clients

Parameter	Description
MAC Address	Disabled Client MAC addresses. Click a list item to get details about the disabled client. Refer to <u>Configure Disabled Clients &gt; Template</u> < <u>MACaddress&gt;</u> to edit the template and apply it to Alcatel OmniAccess Switches and Appliances.
Description	Description of disabled client.

### Select a command

Add Template: Select this command and click GO. Refer to <u>Configure Disabled Clients > New Template</u>.

# Configure Black List Client > <MACaddress>

Use **MONITOR/Maps**, click an item in the **Name** column, single-click the floor map, from the Display pulldown menu, select **Users**, click **n clients**, click **User Name**, from the Select a Command pulldown select **Disable** to access this page.

When this page appears, enter a description of this client and click **OK** to add it to the Watch List (refer to *Monitor Watch Lists*) or click **Cancel** to view the current Watch List.

# Configure Clients > Add to Watch List > <MAC address>

Use **MONITOR/Maps**, click an item in the **Name** column, double-click the floor map, from the Display pulldown menu, select **Users**, click **n clients**, under the Select a Command pulldown, select **Add to Watch List** to access this page.

This page allows you to add a client to a watch list by MAC address.

From the "Select Watch List to Add Client for" list, select a watch list and click **OK** or **Cancel**.

When you do this, a page showing the current available watch lists appears. Refer to <u>Monitor Watch</u> Lists.

## **Configure Watch Lists > New Watch List**

Use MONITOR/Clients, click the column title, click an item in the Watch List Name, from the Select a command pulldown, select New Watch List to access this page.

This page allows you to define new watch list parameters:

- Watch List Name: Change the watch list name as desired.
- Description: Change the description of the watch list as desired.
- Admin Status: Whether the watchlist is enabled or disabled (Pulldown).
- Expiration (in hours): Type the expiration in hours of the watch list.

### **Command Buttons**

- OK
- Cancel

# Configure Watch Lists > Edit > <name>

Use **MONITOR/Clients**, click the column title, click an item in the Watch List Name, from the Select a command pulldown, select **New Watch List**, and then select **Edit Watch List** to access this page.

This page allows you to edit watch list parameters:

- Watch List Name: Change the watch list name as desired.
- Description: Change the description of the watch list as desired.
- Admin Status: Whether the watchlist is enabled or disabled (Pulldown).
- Expiration (in hours): Type the expiration in hours of the watch list.

#### **Command Buttons**

- OK
- Cancel

# Configure Watch List > <watch list name> > Apply to Switches

Use **MONITOR/Clients** and click a list item under Name, use the **Apply to Switches** command button to access this page.

Use **MONITOR/Clients** and click the column title, click an item in the Client Watch List, use the **Apply to Switches** command button to access this page.

This page allows you to apply a specific watch list to selected Alcatel OmniAccess Switches and Appliances:

- Checkbox: Use this box to select items.
- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance.
- Switch Name: User-defined Alcatel OmniAccess Switch or Appliance name.
- Sync Status: Alcatel OmniAccess Switch or Appliance synchronous status, for example, Out of Sync.

### **Command Buttons**

- OK
- Cancel

# Configure Watch List > <watch list name> > Remove From Switches

Use **MONITOR/Clients** and click the column title, click an item in the Watch List Name, use the **Remove from Switches** command button to access this page.

This page allows you to remove a specific watch list from selected Alcatel OmniAccess Switches and Appliances:

- Checkbox: Use this box to select items.
- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance.
- Switch Name: User-defined Alcatel OmniAccess Switch or Appliance name.
- Sync Status: Alcatel OmniAccess Switch or Appliance synchronous status, for example, Out of Sync.

- OK
- Cancel

# Configure Historically Known Rogue AP > Add Rogue AP

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Known Rogue APs**, from the Select a command pulldown, select **Add Rogue AP** to access this page.

This page allows you to add a Historically Known Roque AP to the ACS database:

- MAC address: IP Address of the rogue access point (read only).
- Status: Type of rogue access point, Internal, External.
- Comment: Short user-determined comment.
- Suppress Alarms checkbox: Check to suppress alarms from this rogue access point.

### **Command Buttons**

- Save
- Cancel

## **Configure TFTP Server > Add TFTP Server**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **TFTP Server**, then from the Select a command pulldown, select **Add TFTP Server** to access this page.

This page allows you to add a TFTP server.

- TFTP Server Name: User-defined name of the TFTP server.
- IP Address: IP Address of the TFTP server.

### **Command Buttons**

- Save
- Cancel

## **Configure Software Version > Add**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **TFTP Server**, click a list item under **TFTP Server**, from the Select a command pulldown, select **Add Version** to access this page.

This page allows you to add a software version.

- Version Id: Alcatel Wireless Operating System software version number.
- Path: The complete directory path on the server (default = /), showing the location of the software
- Filename: The name of the file containing the software.

### **Command Button**

- Save
- Cancel

# **CONFIGURE/Templates Menu Bar Selection**

This menu bar selection provides access to the Alcatel OmniAccess Switch or Appliance templates summary details. Use the selector area to access and configure the respective templates details.

Making this selection from the menu bar displays Configure WLAN Template.

# **Configure RADIUS Authentication Server > New Template**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Auth Servers**, from the Select a command pulldown, select **Add Auth Server**, click **Create** to access this page.

This page allows you to create a template for RADIUS authentication server information.

#### General

- Template Name: Name of the RADIUS accounting server.
- Server Address: IP Address of the RADIUS server.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Port Number: Port number for the interface protocols.
- Shared Secret: RADIUS server login Shared Secret (text field).
- Confirm Shared: Confirmation of Shared Secret (text field).
- Admin Status: The state of the server, enabled or disabled (checkbox).

### **Command Buttons**

- Save
- Cancel

# Configure < IPaddress > > RADIUS Auth. Server > Add From Template

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Auth Servers**, from the Select a command pulldown, select **Add Auth Server** to access this page.

This page allows you to apply information from a RADIUS authentication server template.

**Select a template to create from** (pulldown list of available templates).

- Create button
- Cancel button

Refer to Configure RADIUS Authentication Server > New Template.

#### Table - General

Parameter	Description
Template Name	Operator-defined name of RADIUS authentication server template.
Server Address	IP Address of the RADIUS server (read only).

Table - General (Continued)

Parameter	Description
No of Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port number for the interface protocols (read only).
Shared Secret	RADIUS server login Shared Secret (text field).
Confirm Shared Secret	Confirmation of Shared Secret (text field).
Admin Status	Whether the interface is Enabled or Disabled (checkbox).

- Save
- Cancel

# **Configure RADIUS Authentication Server**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Security** and click **RADIUS Auth Servers** to access this page.

This page allows you to view existing RADIUS authentication servers, and add or delete a RADIUS accounting server to the Alcatel OmniAccess Switch or Appliance. Click the **Server Index** link to go to the <u>Configure < IPaddress> > RADIUS Authentication Server</u>.

Table - RADIUS Authentication Server

Parameter	Description
Checkbox	Use to select a Server Index to delete.
Server Index	Access priority number for this RADIUS server (read only).
Server Address	IP Address of the RADIUS server (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port (read only).
Admin Status	Enabled or disabled (checkbox).

### Select a command

- Add Auth Server: Refer to <u>Configure <IPaddress> > RADIUS Auth. Server > Add From</u> Template.
- **Delete Auth Server:** Select a server to be deleted, select this command and click **GO** to delete the server from the database.

# **Configure <IPaddress> > RADIUS Authentication Server**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Security**, click **RADIUS Auth Servers**, then click on a list item under **Server Index** to access this page.

This page allows you to change an existing RADIUS authentication server shared secret and/or administrative status.

Table - RADIUS Authentication Server

Parameter	Description
Server Index	Access priority number for the RADIUS server (read only).
Server Address	IP Address of the RADIUS server (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port (read only).
Shared Secret	RADIUS server login Shared Secret (text field).
Confirm Shared Secret	Confirmation of Shared Secret (text field).
Admin Status	Enabled or disabled (checkbox).

#### Select a command

- Save
- Audit: Discover the current status stored on the Alcatel OmniAccess Switch or Appliance.

# **Configure RADIUS Accounting Server > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Security**, select **Radius Acct Servers**, from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to create a new template for RADIUS accounting server information.

### General

- Template Name: Name of the RADIUS accounting server.
- Server Address: IP Address of the RADIUS server.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Port Number: Port number for the interface protocols.
- Shared Secret: RADIUS server login Shared Secret (text field).
- Confirm Shared: Confirmation of Shared Secret (text field).
- Admin Status The state of the server, enabled or disabled (checkbox).

### **Command Buttons**

- Save
- Cancel

# **Configure RADIUS Accounting Server**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Security/Radius Acct Servers** to access this page.

This page allows you to view existing RADIUS accounting servers, and add or delete a RADIUS accounting server to the Alcatel OmniAccess Switch or Appliance. Click the **Server Index** link to go to the <u>Configure RADIUS Accounting Server > Template < name > to edit the template.</u>

Table - RADIUS Accounting Server

Parameter	Description
Checkbox	Use to select a Server Index to delete.
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and Alcatel OmniAccess Switch or Appliance polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the Alcatel OmniAccess Switch or Appliance.
Server Address	IP Address of the RADIUS server.
Port Number	Alcatel OmniAccess Switch or Appliance port.
Admin Status	Enabled or disabled.

### Select a command

• Add Template: Refer to Configure RADIUS Accounting Server > New Template.

# **Configure < IPaddress> > RADIUS Accounting Server > Add From Template**

Use **CONFIGURE/Templates**, select an **IP Address**, from the left sidebar menu, under **Security**, select **RADIUS Acct Servers**, and select the **Add Acct Server** command to access this page.

This page allows you to add information from an existing RADIUS accounting server template.

• Select a Template to Create From: Pick one from the existing Templates.

Table - General

Parameter	Description
Template Name	Operator-defined names of RADIUS Accounting servers. Click on a list item. Refer to <u>Configure RADIUS Accounting Server &gt; Template &lt; name &gt;</u> .
Server Address	IP Address of the RADIUS server (read only).
No. of Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port (read only).
Shared Secret, Confirm Shared Secret	The Shared Secret that acts as a password to the RADIUS accounting server.
Admin Status	Enabled or disabled (read only).

### Select a command

Create

### Cancel

# **Configure Local Authentication > New Template**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **Security/Local Authentication**, from the Select a command pulldown, select **Add Template**.

This page allows you to add a new local authentication template. Add the following information:

- User Name: User defined identification.
- Number of Switches applied to (read only).
- Category: Network Manager, Network User, Client MAC Address.
- Password.
- Confirm Password.
- Access Level: ReadWrite, Read Only.

#### **Command Buttons**

- Save
- Cancel

### **Configure Disabled Clients > New Template**

Use **MONITOR/Clients** and click Disabled Clients, under the Select a command pulldown, select **Add Template** to access this page.

This page allows you to create a new template for disabled (blacklisted) clients.

### General

- MAC Address: MAC address of the disabled client.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Description: User-defined text description.

### **Command Buttons**

- **Save** to save the Disabled Client Template to the ACS database and have ACS display <u>Configure Disabled Clients > Template < template name ></u>.
- Cancel

# **Configure < IPaddress> > Disabled Clients > Add From Template**

Use **CONFIGURE/Switches**, click **Security/Disabled Clients**, select **Add Disabled Client** and **GO** to access this page.

This page allows you to disable (blacklist) clients from a disable template.

- Select a Template to create from: Done on <u>Configure Disabled Clients > New Template</u>.
- If not done yet, To create a New Template for Disabled Clients **click here** to get redirected to template creation (*Configure Disabled Clients > New Template*) page.

#### General

- MAC Address: MAC address of the disabled client.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Description: User-defined text description.
- To create a New Template for Disabled Clients **click here** to get redirected to template creation page. Refer to Configure Local Authentication > New Template.

### **Command Buttons**

- Create
- Cancel

### **Configure 802.11a Parameters > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11a**, select **Parameters**, then select **Add Template** to access this page.

This page allows you to add a new template for a 802.11a parameters.

### General

- Policy Name: Security policy in force.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Admin Status: Whether the OmniAccess Radio is enabled or disabled (Enable checkbox).
- Beacon Period: The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.

### 802.11a Power Status

- Dynamic Assignment: Dynamic transmit power assignment has three modes:
  - Automatic The transmit power will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Transmit power is updated when the Assign Now button is selected.
  - Fixed No dynamic transmit power assignments occur and value are set to their global default. Default is Automatic.
- Tx Level OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

### 802.11a Channel Status

- Assignment Mode: Dynamic channel assignment has three modes:
  - Automatic The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Channel assignments are updated when desired.
  - OFF No dynamic channel assignments occur and value are set to their global default.

Default is Automatic.

- Avoid Foreign AP Interference: Checkbox, enabled or disabled.
- Avoid OmniAccess AP Load: Checkbox, enabled or disabled.
- Avoid non 802.11a Noise: Checkbox, enabled or disabled.
- Signal Strength Contribution: Checkbox, enabled or disabled.

### **Data Rates**

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. 6, 9, 12, 18, 24, 36, 48, 54 Mbps For each rate, a pulldown selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

#### **Command Buttons**

- Save
- Cancel

# **Configure 802.11a RRM Thresholds > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11a**, select **RRM Thresholds**, under select a command, choose **Add Template**.

This page allows you to add a new template for 802.11a RRM Threshold parameters:

#### General

- Template Name: User-defined name of this RRM template.
- No of Switches Applied To (read only): Number of Alcatel OmniAccess Switches and Appliances
  to which this parameter is applied (read only).

#### **Coverage Thresholds**

- Min Failed Clients (%): Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min Failed Clients (#): Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min SNR Level (dB): Minimum signal to noise ratio allowed.

### **Load Thresholds**

- Max Clients: Maximum number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

### **Other Thresholds**

- Interference Threshold (%): 802.11a or 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.

- Save
- Cancel

### **Configure 802.11a RRM Intervals > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11a/RRM Intervals**, under select a command, choose **Add Template** to access this page.

This page allows you to add a new 802.11a RRM Intervals template:

- Template Name: User-defined name of this template.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Signal Measurement Interval: The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
- Noise Measurement Interval: The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
- Load Measurement Interval: The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
- Coverage Measurement Interval: The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

- Save
- Cancel

## Configure 802.11b/g Parameters > Add Template <name>

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **Parameters**, click a list item under **Policy Name**, from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to add an 802.11b/g parameters template.

#### General

- Policy Name: Security policy in force.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Admin Status: Whether the OmniAccess Radio is enabled or disabled (Enable checkbox).
- 802.11g Support: Enabled checkbox
- Beacon Period: The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
- Short Preamble: Enabled checkbox.

#### 802.11b/g Power Status

Dynamic Assignment: Dynamic transmit power assignment has three modes:

- Automatic The transmit power will be periodically updated for all OmniAccess APs that permit this operation.
- On Demand Transmit power is updated when the Assign Now button is selected.
- Fixed No dynamic transmit power assignments occur and value are set to their global default. Default is Automatic.
- Tx Level OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

#### 802.11b/g Channel Status

- Assignment Mode: Dynamic channel assignment has three modes:
  - Automatic The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Channel assignments are updated when desired.
  - OFF No dynamic channel assignments occur and value are set to their global default.

Default is Automatic.

- Avoid Foreign AP Interference: Checkbox, enabled or disabled.
- Avoid OmniAccess AP Load: Checkbox, enabled or disabled.
- Avoid non 802.11a Noise: Checkbox, enabled or disabled.
- Signal Strength Contribution: Checkbox, enabled or disabled.

#### **Data Rates**

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. 6, 9, 12, 18, 24, 36, 48, 54 Mbps For each rate, a pulldown selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## **Configure 802.11b/g RRM Thresholds > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Thresholds**, then select **Add Template** to access this page.

This page allows you to add a new 802.11b/g RRM thresholds template:

#### General

- Template Name: User-defined name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

#### **Coverage Thresholds**

- Min Failed Clients (%): Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min Failed Clients (#): Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min SNR Level (dB): Minimum Signal to noise ratio of the client RF session.

#### **Load Thresholds**

- Max Clients: Maximum Number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

### **Other Thresholds**

- Interference Threshold (%): (0 to 100%) 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

- Save
- Cancel

### **Configure 802.11b/g Thresholds > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Thresholds**, from the Select a command pulldown, choose **Add Template** to access this page.

This page displays 802.11b/g thresholds for a specified template:

### General

- Template Name: User-defined name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

## **Coverage Thresholds**

- Min Failed Clients (%): Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min Failed Clients (#): Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min SNR Level (dB): Minimum Signal to noise ratio of the client RF session.

### **Load Thresholds**

 Max Clients: Maximum Number of clients currently associated with the Alcatel OmniAccess Switch or Appliance. RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

#### Other Thresholds

- Interference Threshold (%): (0 to 100%) 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

- Save
- Cancel

### Configure 802.11b/g RRM Intervals > New Template

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Intervals**, from the Select a command pulldown choose **Add Template** to access this page.

This page allows you to add a new 802.11b/g RRM intervals template:

- Template Name: User-defined name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.
- Signal Measurement Interval: The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
- Noise Measurement Interval: The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
- Load Measurement Interval: The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
- Coverage Measurement Interval: The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

- Save
- Cancel

### **Configure Trap Receiver > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Trap Receiver**, then from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to create a new trap receiver template.

Table - New Trap Receiver Template

Parameter	Description
Template Name	User-defined name of this new template.
No of Switches Applied to	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
IP Address	The IP Address of the server.

Table - New Trap Receiver Template (Continued)

Parameter	Description
Admin Status	Status must be enabled for the SNMP traps to be sent to the receiver. Enabled checkbox.

- Save
- Cancel

## **Configure Trap Controls > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Trap Controls**, then from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to add a new trap control template:

- Template Name: Type in the name of the new template.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

Check the boxes as desired.

Table - Miscellaneous Traps

Trap Name	Description
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated.
Port Status	Port changes status from up or down.
Multiple Users	Two users login with the same login ID.
Spanning Tree	Spanning Tree traps. Refer to the STP specifications for descriptions of individual parameters.
Rogue AP	Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
Switch Config Save	Notification sent when the configuration is modified.

Table - Client Related Traps

Trap Name	Description
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.

Table - Client Related Traps (Continued)

Trap Name	Description
802.11 Auth Failure	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
802.11 Association Failure	The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
Disabled	The associate failure notification is sent when a client is disabled.

## Table - OmniAccess AP Traps

Trap Name	Description
AP Register	Notification sent when OmniAccess AP associates or disassociates with the Alcatel OmniAccess Switch or Appliance.
AP Interface Up/Down	Notification sent when OmniAccess AP interface (802.11a or 802.11b/g) status goes up or down.

## Table - Auto RF Profile Traps

Trap Name	Description
Load Exceeded	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Exceeded	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Exceeded	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Unsatisfactory	Notification sent when Coverage Profile state changes between PASS and FAIL.

## Table - Auto RF Update Traps

Trap Name	Description
Channel Change	Notification sent when OmniAccess AP's dynamic channel algorithm is updated.
Tx Power Change	Notification sent when OmniAccess AP's dynamic transmit power algorithm is updated.
Antenna Change	Notification sent when OmniAccess AP's dynamic antenna algorithm is updated.

### Table - AAA Traps

Trap Name	Description
User Auth Failure	This trap is to inform that a client RADIUS Authentication failure has occurred.
RADIUS Servers No Response	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

Table - IP Security Traps

Trap Name	Description
ESP Auth Failure	IPSec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPSec packets with invalid sequence numbers were found in an inbound ESP SA.
ESP Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
IKE Neg Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
Suite Neg Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.

### **Command Buttons**

- Save
- Cancel

## **Configure Telnet SSH Configuration > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Telnet SSH**, from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to add a new Telnet SSH configuration template.

Table - New SSH Configuration Template

Parameter	Description
Template Name	User-defined name of this new template.
No of Switches Applied to	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

**Table -** New SSH Configuration Template (Continued)

Parameter	Description
Session Timeout (min)	Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
Maximum Sessions	Selectable from a pulldown menus for values of from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The factory default is 5.  Note: New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service (Management) port.
Allow New Telnet Session	Indicates that new Telnet sessions will not be allowed on the DS Port when set to no. The factory default value is no.  Note: New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service (Management).
Allow New SSH Session	Indicates that new Secure Shell Telnet sessions will not be allowed when set to no. The factory default value is yes.

- Save
- Cancel

## **Configure Syslog Configuration > New Template**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Syslog**, from the Select a command pulldown, select **Add Template** to access this page.

This page allows you to specify syslog configuration template information.

**Table - New Syslog Configuration Template** 

Parameter	Description
Template Name	User-defined name of this new template.
No of Switches Applied to	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
Syslog Enabled	Use the checkbox to enable the syslog.

### **Command Buttons**

- Save
- Cancel

# **Editing Templates, Maps and Devices**

You can add Alcatel OmniAccess Wireless System Campus, Building, Floor, and Outdoor Area Maps, and place OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points, and add Third-Party APs from the following:

- <u>Configure WLAN Template > Template < name ></u>
- <u>Configure RADIUS Authentication Server > Template < name > </u>
- <u>Configure RADIUS Accounting Server > Template < name > </u>
- Configure <IPaddress> > RADIUS Accounting Server
- <u>Configure Disabled Clients > Template <MACaddress></u>
- Configure Template > <template name> > Apply to Switches
- <u>Configure 802.11a Parameters > Template < name > </u>
- Configure 802.11a RRM Thresholds > Template <name>
- <u>Configure 802.11a RRM Intervals > Template < name ></u>
- <u>Configure 802.11b/g Parameters > Template < name > </u>
- Configure 802.11b/g RRM Thresholds > Template < name >
- <u>Configure 802.11b/g RRM Intervals > Template < name > </u>
- Configure Trap Receiver > Template < name >
- <u>Configure Trap Controls > Template <name></u>
- Configure Telnet SSH Configuration > Template <name>
- Configure Syslog Configuration > <template name>
- Configure Maps > Edit Campus <name>
- Configure Campus > Edit Outdoor Area <name>
- <u>Configure <campus name> > Edit Building <building name></u>
- Configure Maps > Edit Building > <name>
- Configure Access Point > OmniAccess AP > <name>
- Configure < IPaddress > Connected Third Party AP > New
- Configure <IPaddress> > Switch General
- Configure <IPaddress> > Networking Setups
- Configure <IPaddress> > Interface
- <u>Configure <IPaddress> > Network Route</u>
- Configure <IPaddress>> Switch STP Properties
- Configure Local Authentication
- <u>Configure Disabled Clients > Template <template name></u>
- Configure < IPaddress > Disabled Clients
- Configure Access Control List > Template <name>
- <u>Configure <IPaddress> > CA Certification</u>
- Configure <IPaddress> > Switch 802.11

- <u>Configure <IPaddress> > 802.11a Parameters</u>
- <u>Configure <IPaddress> > 802.11a RRM Thresholds</u>
- Configure <IPaddress> > 802.11a RRM Intervals
- Configure < IPaddress > 802.11a Grouping Control
- <u>Configure <IPaddress> > 802.11b/g Parameters</u>
- Configure <IPaddress> > 802.11b/g RRM Thresholds
- Configure <IPaddress> > 802.11b/g RRM Intervals
- <u>Configure <IPaddress> > 802.11b/g RRM Grouping Control</u>
- <u>Configure <IPaddress> > Ports</u>
- <u>Configure <IPaddress> > Ports > <port#></u>
- <u>Configure <IPaddress> > Ports > <#></u>
- <u>Configure <IPaddress> > Trap Receiver</u>
- <u>Configure <IPaddress> > Trap Controls</u>
- <u>Configure <IPaddress> > Telnet SSH Configuration</u>
- Configure <IPaddress> > Syslog Configuration
- <u>Configure <IPaddress> > WEB Admin</u>
- <u>Configure <IPaddress> > Download Web Admin Certificate</u>

## Configure Historically Known Rogue AP > Rogue AP < MACaddress >

Use **CONFIGURE/Templates** and from the left sidebar menu, select **Known Rogue APs**, click a **MAC Address** entry to access this page.

This page allows you to add a Historically Known Rogue AP to the ACS database:

- MAC address: IP Address of the rogue access point (read only).
- Status: Type of rogue access point, Internal, External.
- Comment: Short user-determined comment.
- Suppress Alarms checkbox: Check to suppress alarms from this rogue access point.

#### **Command Buttons**

- Save
- Cancel

### Configure WLAN Template > Template < name>

Use **CONFIGURE/Templates** and select a list item from the **Template Name** column to access this page.

This page allows you to display and edit selected WLAN template information for a specific template. To define a WLAN template, refer to <u>Configure WLAN > New Template</u>.

- SSID: Name of the WLAN.
- Template Name: User-defined name of the template.

• WLAN for 3rd Party APIs Checkbox: The third-party AP WLAN can only be configured with 802.1X encryption as described in <u>Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Drop down configurable 802.1X parameters are not available for this WLAN.

Table - General Policies

Parameter	Description
Radio Policy	Set the WLAN policy to apply to All = 802.11a/b/g, 802.11a only, 802.11b only, 802.11g only, 802.11b/g only, 802.11a/b only, or 802.11a/g only. All, 802.11a only, 802.11b/g only.
Admin Status	Check to box to set the status of the WLAN to enabled.
Session Timeout	Set the maximum time for a client session before requiring reauthorization.
Quality of Service (QoS)	Set QoS to: Gold (Highest); Silver (Mid-range); Bronze (Low). Services such as VoIP should be set to Gold while non-discriminating services such as text messaging can be set to Bronze.
Allow AAA Override	<ul> <li>Enable or disable AAA override for global WLAN parameters.</li> <li>When AAA Override is enabled, and a client has conflicting AAA and Alcatel OmniAccess Switch or Appliance WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the Alcatel Wireless Operating System will move clients from the default Alcatel WLAN VLAN to a VLAN returned by the AAA server and predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the Alcatel Wireless Operating System will also use QoS and ACL provided by the AAA server, as long as they are predefined in the Alcatel OmniAccess Switch or Appliance Interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.)</li> <li>For instance, if the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the Alcatel Wireless Operating System redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</li> <li>When AAA Override is disabled, all client authentication defaults to the Alcatel OmniAccess Switch or Appliance authentication parameter settings, and authentication is only performed by the AAA server if the Alcatel OmniAccess Switch or Appliance WLAN do not contain any client-specific authentication parameters.</li> <li>The AAA override values may come from a RADIUS server, for example.</li> </ul>
Blacklist Timeout	Enable or disable automatic disabling, and set the timeout in seconds for disabled client machines. Client machines are disabled by MAC address and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client., Set (Note) checkbox, Timeout Value (secs) field.

Table - General Policies (Continued)

Parameter	Description
DHCP Server	<ul> <li>When selected, you can enter the IP Address of your DHCP server. This is a Required field for some WLAN configurations. There are three valid configurations and one invalid combination:</li> <li>DHCP Required and a valid DHCP Server IP Address: Requires all WLAN clients to obtain an IP Address from the DHCP Server.</li> <li>DHCP Not Required and a valid DHCP Server IP Address: Allows all WLAN clients to obtain an IP Address from the DHCP Server or use a static IP Address.</li> <li>DHCP Not Required and DHCP Server IP Address 0.0.0.0: Forces all WLAN clients to use a static IP Address. All DHCP requests are dropped.</li> <li>DHCP Required and DHCP Server IP Address 0.0.0.0 is not allowed.</li> </ul>
DHCP Addr. Assignment	Required checkbox
Nieder Mil	ut is mat set it impulses that a dischlad alient will remain as and will resum

**Note:** When session timeout is not set, it implies that a disabled client will remain so and will never timeout from the disabled state. It does not imply that the blackslisting feature will be disabled.

You can choose both Layer 2 and Layer 3 security policies from the drop down list under the Security Policies heading. The selected security policy options are at the bottom of the page with the appropriate parameters listed. The following tables describe these parameters.

**Note:** The values in the other tables on this page change depending upon the security policies selected.

Table - Security Policies

Parameter	Description
Layer 2 Security	None, WPA, 802.1X, Static WEP, Cranite, MAC Filtering checkbox.
Layer 3 Security	None, IPSec, VPN Pass Through, Web Authentication (Note) Checkbox.

**Note:** Alcatel OmniAccess Switch or Appliance must be rebooted for Web Authentication to take effect. Web Authenticating cannot be used in combination with IPSec.

Table - Layer 2 Security Policies

Parameter	Description
None	No Layer 2 security selected.
WPA	Wi-Fi Protected Access 802.11 data encryption types: • TKIP-MIC, or • WEP: 40/64, 104/128, and 128/152 bit key sizes.
802.1X	WEP 802.1X data encryption type (Note 3):  • 40/64 bit key  • 104/128 bit key  • 128/152 bit key.

Table - Layer 2 Security Policies (Continued)

Parameter	Description
Static WEP	Static WEP encryption parameters:  • Key sizes: 40/64, 104/128 and 128/152 bit key sizes.  • Key Index: 1 to 4 (Note 1).  • Enter encryption key.  • Select encryption key format in ASCII or HEX.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite WirelessWall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Alcatel OmniAccess Wireless System (Note 2).
Fortress	The Fortress passthrough is a Layer 2 security feature that is FIPS 40-2 compliant.
MAC Filtering	Select to filter clients by MAC address.

**Note 1:** One unique WEP Key Index can be applied to each WLAN. As there are only four WEP Key Indexes, only four WLANs can be configured for Static WEP Layer 2 encryption.

**Note 2:** When Cranite is selected as the Layer 2 security policy, no Layer 3 security policies are allowed.

**Note 3:** The third-party AP WLAN (17) can only be configured with 802.1X encryption as described in *Third-Party Access Points* in the *Alcatel OmniAccess Wireless Product Guide*. Drop down configurable 802.1X parameters are not available for this WLAN.

Table - 802.1X Parameters

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Radio Button	Active when there is more than one type of encryption available.
Туре	WEP, TKIP-MIC.
Key Size	40 bits, 104 bits, 128 bits.
Key Index	1 through 4. One unique WEP Key Index can be applied to each WLAN. As there are only four WEP Key Indexes, only four WLANs can be configured for Static WEP Layer 2 encryption.
Encryption Key	Encryption Key.
Key Format	ASCII or HEX.
<b>11</b> 4 =	

**Note:** The values in these fields and the fields themselves change depending upon the security policies selected.

Layer 3 security is available via VPN Pass Through or IPSec. Check software availability and client hardware compatibility before implementing IPSec. Layer 3 IPSec parameters are described in the following table.

**Table - WPA Parameters** 

Parameter	Description
802.11 Data Encryption	Displays the current Key of the security selected in the Security Policies area.
Туре	Active when there is more than one type of encryption available.
Key Size	TKIP-MIC.
Preshared Key Mode	Enable checkbox.

**VPN Pass through:** Available only when VPN Pass through is selected for Layer 3 Security. Displays the IP Address of the VPN Gateway Address.

 Table - IPSec Parameters (Available only when IPSec is selected under Layer 3 Security)

Parameter	Description
IPSec Authentication	None, HMAC-MD5, HMAC-SHA1.
IPSec Encryption	DES3, None, AES-CBC, DES.
IKE Authentication	Displays a radio button for selection of Type (Certificate, Pre-Shared Key, XAuth Pre-Shared Key) and Key (Note).
IKE Phase1	Aggressive, Main.
Lifetime (seconds)	Timeout in seconds.
IKE Diffle Hellman Group	Group 1 (768 bits), Group 2 (1024 bits), Group 3 (1536 bits).

**Note:** When you select XAuth Pre Shared Key, the key must be at least eight bytes to interoperate with Cisco clients. Other tested clients function with a key of less than eight bytes.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure RADIUS Authentication Server > Template <name>

Use **CONFIGURE/Templates**, from the left sidebar menu, under **Security**, select **Radius Auth Server**, then click **Template Name** to access this page.

This page allows you to edit RADIUS authentication server information and apply this information to Alcatel OmniAccess Switches and Appliances.

### Table - General

Parameter	Description
Template Name	Operator-defined RADIUS authentication server name.
Server Address	IP Address of RADIUS authentication server (read only).
No of Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
Port Number	Port number for the interface protocols (read only).
Shared Secret	RADIUS server login Shared Secret (text field).
Confirm Shared Secret	Confirmation of Shared Secret (text field).
Admin Status	The state of the server, enabled or disabled (checkbox).

### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure RADIUS Accounting Server > Template <name>

Use  ${f CONFIGURE/Templates}$ , from the left sidebar menu, select  ${f Security/Radius\ Acct\ Server}$ , then click  ${f Template\ Name}$  to access this page.

This page allows you to edit RADIUS accounting server information and apply this information to Alcatel OmniAccess Switches and Appliances.

Table - General

Parameter	Description
Template Name	Operator-defined RADIUS accounting server name.
Server Address	IP Address of RADIUS accounting server (read only).
No of Switches Applied To	Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
Port Number	Port number for the interface protocols (read only).
Shared Secret	RADIUS server login Shared Secret (text field).
Confirm Shared Secret	Confirmation of Shared Secret (text field).
Admin Status	The state of the server, enabled or disabled (checkbox).

#### **Command Buttons**

Save

- Apply to Switches
- Delete
- Cancel

## Configure < IPaddress > RADIUS Accounting Server

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Security/RADIUS Acct Servers**, then click on a list item under **Server Index** to access this page.

This page allows you to edit an existing RADIUS accounting server shared secret and/or administrative status.

Table - RADIUS Accounting Server

Parameter	Description
Server Index	Access priority number for the RADIUS server (read only).
Server Address	IP Address of the RADIUS server (read only).
Port Number	Alcatel OmniAccess Switch or Appliance port (read only).
Shared Secret	RADIUS server login Shared Secret (text field).
Confirm Shared Secret	Confirmation of Shared Secret (text field).
Admin Status	Enabled or disabled (checkbox).

#### Select a command

- Save
- Audit: Discover the current status stored on the Alcatel OmniAccess Switch or Appliance.

## Configure Disabled Clients > Template <MACaddress>

Use MONITOR/Clients and click Disabled Clients, select Add Template to access this page.

This page allows you to edit, apply or delete an existing template Description for disabled (blacklisted) clients.

### General

- MAC Address: MAC address of the disabled client (read only).
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Description: User-defined text description.

#### **Command Buttons**

- Save to save the Disabled Client Template to the ACS database.
- Apply to Switches to have ACS display <u>Configure Template > <template name> > Apply to Switches</u>.
- Delete

#### Cancel

## **Configure Template > <template name> > Apply to Switches**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Syslog**, click a list item under **Template Name**, click **Apply to Switches** to access this page.

Use **MONITOR/Clients** and click **Disabled Clients**, click a list item under MAC Address, click the **Apply to Switches** command button to access this page.

Use **CONFIGURE/Switches**, click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Disabled Clients**, click a list item under MAC Address, click the **Apply to Switches** command button to access this page.

This page allows you to apply a template to Alcatel OmniAccess Switches and Appliances.

- Checkbox: Check this to indicate which Alcatel OmniAccess Switch or Appliance to apply the template to.
- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance.
- Switch Name: User-defined Alcatel OmniAccess Switch or Appliance name.

#### **Command Buttons**

- OK
- Cancel

## Configure 802.11a Parameters > Template <name>

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11a/Parameters**, then click **Policy Name** to access this page.

This page allows you to edit 802.11a parameters for a selected template.

### General

- Policy Name.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Admin Status: Whether the AP is enabled or disabled (Checkbox).
- Beacon Period: The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.

#### 802.11a Power Status

- Dynamic Assignment: Dynamic transmit power assignment has three modes:
  - Automatic The transmit power will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Transmit power is updated when the Assign Now button is selected.
  - Fixed No dynamic transmit power assignments occur and value are set to their global default. Default is Automatic.
- Tx Level: OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System</u>

Supported Regulatory Domains in the Alcatel OmniAccess Wireless Product Guide for the maximum Transmit Power Levels for each country.

#### 802.11a Channel Status

- Assignment Mode: Dynamic channel assignment has three modes:
  - Automatic The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Channel assignments are updated when desired.
  - OFF No dynamic channel assignments occur and value are set to their global default.

Default is Automatic.

- Avoid Foreign AP Interference: Checkbox, enabled or disabled.
- Avoid OmniAccess AP Load: Checkbox, enabled or disabled.
- Avoid non 802.11a Noise: Checkbox, enabled or disabled.
- Signal Strength Contribution: Checkbox, enabled or disabled.

#### **Data Rates**

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. 6, 9, 12, 18, 24, 36, 48, 54 Mbps For each rate, a pulldown selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

### **Command Buttons**

- Save
- **Apply to Switches**
- **Delete**
- Cancel

## Configure 802.11a RRM Thresholds > Template <name>

Use CONFIGURE/Templates and from the left sidebar menu, under 802.11a, select RRM Thresholds, then click **Template Name** to access this page.

This page allows you to edit 802.11a RRM Threshold parameters for a specified template:

#### General

- Template Name: User-defined name of this RRM template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this parameter is applied (read only).

### **Coverage Thresholds**

- Min Failed Clients (%): Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min Failed Clients (#): Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.

Min SNR Level (dB): Minimum signal to noise ratio allowed.

#### **Load Thresholds**

- Max Clients: Maximum number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

#### **Other Thresholds**

- Interference Threshold (%): 802.11a or 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure 802.11a RRM Intervals > Template <name>

Use **CONFIGURE/Templates** and from the left sidebar menu, select **802.11a/RRM Intervals,** and then click a Template Name to access this page.

This page allows you to edit an 802.11a RRM Intervals template:

- Template Name: User-defined name of this template.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Signal Measurement Interval: The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
- Noise Measurement Interval: The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
- Load Measurement Interval: The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
- Coverage Measurement Interval: The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure 802.11b/g Parameters > Template <name>

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **Parameters**, then click **Policy Name** to access this page.

This page allows you to edit 802.11b/g template parameters:

#### General

- Policy Name.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Admin Status: Whether the AP is enabled or disabled (Enabled checkbox).
- 802.11b/g Support: Enabled checkbox.
- Beacon Period: The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
- Short Preamble: If this parameter indicates that Short Preamble is Disabled (box is unchecked), this Alcatel OmniAccess Switch or Appliance is already optimized for SpectraLink NetLink Telephones; if desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### 802.11a Power Status

- Dynamic Assignment: Dynamic transmit power assignment has three modes:
  - Automatic The transmit power will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Transmit power is updated when the Assign Now button is selected.
  - Fixed No dynamic transmit power assignments occur and value are set to their global default.

Default is Automatic.

• Tx Level: OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.

## 802.11b/g Channel Status

- Assignment Mode: Dynamic channel assignment has three modes:
  - Automatic The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.
  - On Demand Channel assignments are updated when desired.
  - OFF No dynamic channel assignments occur and value are set to their global default.

Default is Automatic.

- Avoid Foreign AP Interference: Checkbox, enabled or disabled.
- Avoid OmniAccess AP Load: Checkbox, enabled or disabled.
- Avoid non 801.11 Noise: Checkbox, enabled or disabled.
- Signal Strength Contribution: Checkbox, enabled or disabled.

### Data Rates

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also

supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. 1, 2, 5, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps For each rate, a pulldown selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure 802.11b/g RRM Thresholds > Template <name>

Use **CONFIGURE/Templates** and from the left sidebar menu, under **802.11b/g**, select **RRM Thresholds**, then click **Template Name** to access this page.

This page allows you to edit an 802.11b/g threshold template:

### General

- Template Name: User-defined name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

#### **Coverage Thresholds**

- Min Failed Clients (%): Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min Failed Clients (#): Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- Min SNR Level (dB): Minimum Signal to noise ratio of the client RF session.

#### **Load Thresholds**

- Max Clients: Maximum Number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
- RF Utilization (%): 802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.

#### **Other Thresholds**

- Interference Threshold (%): (0 to 100%) 802.11b/g interference threshold between 0 and 100 percent.
- Noise Threshold (dBm): Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## Configure 802.11b/g RRM Intervals > Template <name>

Use CONFIGURE/Templates and from the left sidebar menu, under 802.11b/g, select RRM Intervals, then click **Template Name** to access this page.

This page allows you to edit an 802.11b/g RRM intervals template.

- Template Name: User-defined name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied.
- Signal Measurement Interval: The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
- Noise Measurement Interval: The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
- Load Measurement Interval: The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
- Coverage Measurement Interval: The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

- Save
- **Apply to Switches**
- **Delete**
- Cancel

## **Configure Trap Receiver > Template <name>**

Use CONFIGURE/Templates, from the left sidebar menu, under Control, select Trap Receiver, click a list item under **Template Name** to access this page.

This page allows you to edit a trap receiver template.

- Template Name: The name of the server where the traps are sent.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- IP Address: The IP Address of the server.
- Admin Status: Status must be enabled for the SNMP traps to be sent to the server.

#### **Command Buttons**

- Save
- **Apply to Switches**
- Delete
- Cancel

### **Configure Trap Controls > Template <name>**

Use CONFIGURE/Templates and from the left sidebar menu, under Control, select Trap Controls, click a list item under **Template Name** to access this page.

This page allows you to edit SNMP trap controls for a specified template.

- Template Name: User-defined name of this template.
- No of Switches Applied to: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).

Check the boxes as desired.

Table - Miscellaneous Traps

Trap Name	Description
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated.
Port Status	Port changes status from up or down.
Multiple Users	Two users login with the same login ID.
Spanning Tree	Spanning Tree traps. Refer to the STP specifications for descriptions of individual parameters.
Rogue AP	Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
Switch Config Save	Notification sent when the configuration is modified.

Table - Client Related Traps

Trap Name	Description
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.
802.11 Auth Failure	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
802.11 Association Failure	The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
Disabled	The associate failure notification is sent when a client is disabled.

Table - OmniAccess AP Traps

Trap Name	Description
AP Register	Notification sent when OmniAccess AP associates or disassociates with the Alcatel OmniAccess Switch or Appliance.
AP Interface Up/Down	Notification sent when OmniAccess AP interface (802.11a or 802.11b/g) status goes up or down.

Table - Auto RF Profile Traps

Trap Name	Description
Load Exceeded	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Exceeded	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Exceeded	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Unsatisfactory	Notification sent when Coverage Profile state changes between PASS and FAIL.

## **Table -** Auto RF Update Traps

Trap Name	Description
Channel Change	Notification sent when OmniAccess AP's dynamic channel algorithm is updated.
Tx Power Change	Notification sent when OmniAccess AP's dynamic transmit power algorithm is updated.
Antenna Change	Notification sent when OmniAccess AP's dynamic antenna algorithm is updated.

## Table - AAA Traps

Trap Name	Description
User Auth Failure	This trap is to inform that a client RADIUS authentication failure has occurred.
RADIUS Servers No Response	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

## Table - IP Security Traps

Trap Name	Description
ESP Auth Failure	IPSec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPSec packets with invalid sequence numbers were found in an inbound ESP SA.
ESP Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.

Table - IP Security Traps (Continued)

Trap Name	Description
IKE Neg Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
Suite Neg Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.

#### 802.11 Security Traps

WEP Key Description

#### **Command Buttons**

- Save
- Apply to Switches
- Delete
- Cancel

## **Configure Telnet SSH Configuration > Template <name>**

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Telnet SSH**, then click **Template Name** to access this page.

This page allows you to edit SSH configuration information for a selected template.

- Template Name: Name of this template.
- No of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Session Timeout (minutes): This object indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions: Selectable from a pulldown menus for values of from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The factory default is 5.
- Allow New Telnet Session: Indicates that new Telnet sessions will not be allowed on the DS Port when set to no. The factory default value is no.
- Note: New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service (Management) port.
  - Allow New SSH Session: Indicates that new Secure Shell Telnet sessions will not be allowed when set to no. The factory default value is yes.

### **Command Buttons**

- Save
- Apply to Switches

- Delete
- Cancel

## Configure Syslog Configuration > <template name>

Use **CONFIGURE/Templates** and from the left sidebar menu, under **Control**, select **Syslog**, click a list item under **Template Name** to access this page.

This page allows you to edit and apply a syslog configuration to Alcatel OmniAccess Switches and Appliances.

#### General

- Template Name: Name of the template.
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Syslog Enabled: Check the box to enable.

### **Command Buttons**

- Save
- Apply to Switches: Refer to Configure Template > < template name > > Apply to Switches.
- Delete
- Cancel

## Configure Maps > Edit Campus <name>

From Monitor Maps > Campus, select Edit Campus from the select a command pulldown and click GO.

This page provides the opportunity to edit an existing campus. This page consists of two areas:

### **Campus Identification Information**

- Campus Name: User-definable name for the campus.
- Contact: User-defined contact name.
- Image File: Name of the file containing the campus map. Use the **Browse** button to find the file.
- Maintain Aspect Ration: Select this checkbox to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Dimensions (feet):
  - Horizontal: Horizontal measurements (left to right) of the campus as it appears on the page.
  - Vertical: Vertical measurements (up and down) of the campus as it appears on the page.

#### **Command Buttons**

- OK
- Cancel

### **Campus and Building Graphic**

The graphic of the current campus.

#### Sidebar: Maps

- Search for All Maps, Campuses, Buildings, Floor Areas, Outdoor Areas, Access Points.
- Enter Name: User-defined map name.
- Search Button.

## Configure Campus > Edit Outdoor Area <name>

From Monitor Maps > Campus > <outdoor area>, select Edit Outdoor Area to access this page.

This page allows you to edit an existing outdoor area.

- Name: The user-defined name of the new outdoor area.
- Contact: The user-defined contact name.
- Image File: Name of the file containing the outdoor area map. Use the **Browse** button to find the file.
- Horizontal Position: Shows position.
- Vertical Position: Shows position.

**Note:** To change the unit of measurement (feet or meters), select Monitor>Maps and select the command Properties from the pulldown.

- Horizontal Span: Enter and click place to change size of blue rectangle cursor.
- Vertical Span: Enter and click place to change size of blue rectangle cursor.

#### **Command Buttons**

- Place: Fixes the changes on the display.
- **Save:** Saves the changes in the database. Once saved, the name of the new outdoor area appears on the campus map. To edit the outdoor area, refer to Edit Outdoor Area.
- Cancel: Cancels the operation.

#### Map Area Display

Use the blue rectangle to position the outdoor area.

### Configure <campus name> > Edit Building <building name>

Use **MONITOR/Maps**, then click an item in the **Name** column, then from the Select a command pulldown, select **Edit Building** to access this page.

This page allows you to edit an existing building on an existing campus.

## **Building Identification Information**

- Building Name: The user-defined name of the building.
- Contact: User-defined contact name.
- Number of Floors: The number of floors contained in the building.
- Basements: The number of basements contained in the building.
- Dimensions (feet):

- Horizontal: Horizontal measurements (left to right) of the floor as it appears on the page.
- Vertical: Vertical measurements (up and down) of the floor as it appears on the page.

- Place: Fixes the changes on the display.
- Save: Saves the changes in the database.
- Cancel: Cancels the operation.

#### **Campus and Building Graphic**

- To move the blue rectangle on the map, drag the blue rectangle to a desired new location on the campus.
- To size the blue rectangle, press the Ctrl Key and drag the corner of the rectangle to the desired size.

#### Sidebar: Maps

- Search for All Maps, Campuses, Buildings, Floor Areas, Outdoor Areas, Access Points.
- Enter Name:
- Search Button

## Configure Maps > Edit Building > <name>

Use **MONITOR/Maps**, click an item in the **Name** column, from the Select a command pulldown, select **Edit Building** to access this page.

This page allows you to edit a selected building:

- Building Name: User-defined name of the building.
- Contact: User-defined contact name.
- Number of Floors: Enter the desired number of floors in the building.
- Number of Basements: Enter the desired number of basements in the building.
- Dimensions (feet):
  - Horizontal: Horizontal measurements (left to right) of the floor as it appears on the page.
  - Vertical: Vertical measurements (up and down) of the floor as it appears on the page.

### **Command Buttons**

- OK
- Cancel

## Configure Access Point > OmniAccess AP > <name>

Use CONFIGURE/Access Points and select a list item under AP Name to access this page.

This page contains configuration information about specific APs:

Table - General

Parameter	Description
Name	Set the customer definable name of the OmniAccess AP.
MAC Address	Media Access Control of the OmniAccess AP.
Admin Status	Check the box to indicate the administration state of the OmniAccess AP as enabled.
AP Mode	Status of the OmniAccess AP Monitor mode (Monitor, Local, or Remote).
Registered Switch	The Alcatel OmniAccess Switch or Appliance to which this AP is attached. Click a list item. Click the IP Address to view Alcatel OmniAccess Switch or Appliance configuration. Refer to <u>Monitor Switches &gt; <ipaddress> Summary</ipaddress></u> .
Primary Switch Name	This is the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance SNMP name. The OmniAccess AP will attempt to associate with this Alcatel OmniAccess Switch or Appliance first for all network operations and in the event of a hardware reset (Note).
Location	Customer-definable location name for the OmniAccess AP.
Stats Collection Period (secs)	This counter sets the time in seconds that the OmniAccess AP sends its DOT11 statistics to the Alcatel OmniAccess Switch or Appliance.
Mirror Mode	Disable or Enable.

**Note:** After the OmniAccess AP is reset, it will attempt to connect with its Primary Alcatel OmniAccess Switch or Appliance as configured on this page. If the OmniAccess AP's Primary Alcatel OmniAccess Switch or Appliance is not available, it will search for the Master Alcatel OmniAccess Switch or Appliance and finally the least loaded Alcatel OmniAccess Switch or Appliance on the network.

Table - Version

Parameter	Description
Software Version	Displays the Software version, for example, 2.0.113.3.
Boot Version	Displays the Boot ROM versions for example, 11.20.0.

**Table - Inventory Information** 

Parameter	Description
Model	Displays the OmniAccess AP Model and Serial Number. For example (Part Number TBD).

Table - Inventory Information (Continued)

Parameter	Description
Serial Number	Displays the OmniAccess AP Serial Number, for example, 01012203-10057105-01182.

Save: Save the current settings.

Audit: Discover the present status of this AP.

Table - Radio Interfaces

Parameter	Description
Protocol	802.11a, or 802.11b/g. Click an item in the list. Refer to <u>Configure <ipaddress> &gt; OmniAccess AP &gt; <name> &gt; 802.11x &gt; Perf. Profile</name></ipaddress></u> .
Previous Channel Number	Enable last channel number.
Channel Number	Channel number.
Power Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Antenna Mode	Not applicable, Sector A, Sector B, or OMNI (Sector A and Sector B).
Antenna Diversity	For Internal antennas, Enable diversity, or select Side A for the front (door) antenna, or select Side B for the rear antenna.  For External antennas, Enable diversity, or select Right for the Right (Connector B) antenna, or select Left for the Left (Connector A) antenna.
Antenna Type	Internal, External.
Number of WLANs	Number of WLANs.

#### **Hardware Reset**

Click **Reset Ap Now** to perform a hardware reset on this AP.

### **Set to Factory Defaults**

Click Clear Config to clear configuration on this AP and reset it to factory defaults.

## Configure < IPaddress > Connected Third Party AP > New

From the <u>Configure <IPaddress> > Connected Third Party AP</u> page, click an IP Address to access this page.

This page allows you to edit a connected third party AP for Mirror Mode:

- IP Address: IP Address of the third party AP (read only).
- MAC Address: MAC Address of the third party AP (read only).
- Switch Port Number: Alcatel OmniAccess Switch or Appliance port number of the third party AP (read only).
- 802.11x Required: Click the box to require 802.11x (read only).
- Mirror Mode: Disable or enable.

- Save
- Audit
- Cancel

## **Configure < IPaddress> > Switch General**

Use **CONFIGURE/Switches** and click an IP address under the **IP Address** column to access this page.

This page allows you to edit information for a selected Alcatel OmniAccess Switch or Appliance.

Table - Switch General Parameters

Parameter	Description
IP Address	Local network IP Address of the Alcatel OmniAccess Switch or Appliance as described in <u>Management Interface</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
Software Version	The Alcatel Wireless Operating System release.version.dot.maintenance number of the code currently running on the Alcatel OmniAccess Switch or Appliance.
Name	User-defined Alcatel OmniAccess Switch or Appliance name.
Location	Map location of the Alcatel OmniAccess Switch or Appliance.
Refresh on Save Config Trap	Check to use refresh on the trap.
Restore on Cold Start Trap	Check to use refresh on the trap.
Backup Automatically	Check to backup automatically. (see TFTP Server below)
Save Before Backup	Checkbox appears when Backup Automatically is checked.
Backup Frequency	Daily or weekly. Appears when Backup Automatically is checked.
Most Recent Backup	Indicates the most recent backup
TFTP Server	This appears only when Backup Automatically is checked. It displays the current TFTP server.
Trap Destination Port	Number of the trap destination port

Table - SNMP Parameters for Read Operations

Parameter	Range
Version	v1, v2, v3.
Retries	Number of retries allowed.
Timeout (seconds)	User-defined timeout interval.
Community	Public or Private
The following fields appear when you select v3 in the Version field:	
User Name	User defined name.
Auth. Type	HMAC-MD5, HMAC-SHA
Auth Password	Authentication password
Privacy Type	DES, None
Privacy Password	Privacy password

Table - SNMP Parameters for Write Operations

Parameter	Range
Version	v1, v2, v3.
Retries	Number of retries allowed.
Timeout (seconds)	User-defined timeout interval.
Community	Public or Private
The following fields appear when you select v3 in the Version field:	
User Name	User defined name.
Auth. Type	HMAC-MD5, HMAC-SHA
Auth Password	Authentication password
Privacy Type	DES, None
Privacy Password	Privacy password

- OK
- Reset
- Cancel

### **Sidebar Switches Menus**

• System: Click the menu title to reveal menu selections.

- General: The current page. This page displays general information.
- Commands: Refer to *Configure <IPaddress> > Switch Commands*.
- Networking: Refer to <u>Configure < IPaddress > Networking Setups</u>.
- Interfaces: Refer to <u>Monitor <IPaddress> > Interface</u>.
- Network Route: Refer to Configure < IPaddress> > Network Route.
- Spanning Tree Protocol: Refer to Configure < IPaddress >> Switch STP Properties.
- Mobility Groups: Refer to <u>Monitor <IPaddress> > Mobility Group <name> > Group Members</u>.
- WLANs Refer to Monitor WLAN.
- Security: Click the menu title to reveal menu selections.
  - RADIUS Auth Servers: Refer to Configure RADIUS Authentication Server.
  - RADIUS Acct Servers: Refer to Configure RADIUS Accounting Server.
  - Local Authentication: Refer to <u>Configure < IPaddress > CA Certification</u>.
  - Disabled Clients: Refer to <u>Monitor Disabled Clients</u>.
  - Access Control Lists: Refer to Monitor Access Control List.
  - CA Certificate: This page contains the current CA certificate information. If you choose
    to add an operator-generated or purchased CA Certificate, paste the new CA certificate
    ASCII text into the Certificate box and click **Save**. Use **Browse** to find the certificate
    location.
  - ID Certificate: Refer to *Monitor <IPaddress> > Certificate*.
  - Web Auth. Certificate: Use this page to view the current Web Authentication certificate type, download an SSL certificate, or regenerate a new locally- generated Web Auth certificate.

**Note:** The Alcatel Wireless Operating System automatically generates a fully-functional Web Authentication certificate as it is loaded onto your Alcatel OmniAccess Switch or Appliance. This means that you do not have to do anything to use certificates with Layer 3 Web Auth.

- Rogue Policy: Refer to <u>Configure < IPaddress > Rogue Policy Setup</u>.
- Access Points: Click the menu title to reveal menu selections.
  - OmniAccess AP: Refer to Configure < IPaddress > OmniAccess AP.
  - Third Party APs: Refer to <u>Configure <IPaddress> > Connected Third Party AP</u>.
- 802.11: Refer to Configure < IPaddress > Switch 802.11.
- 802.11a: Click the menu title to reveal menu selections.
  - Parameters: Refer to <u>Configure <IPaddress> > 802.11a Parameters</u>.
  - RRM Thresholds: Refer to <u>Configure <IPaddress> > 802.11a RRM Thresholds</u>.
  - RRM Intervals: Refer to <u>Configure <IPaddress> > 802.11a RRM Intervals</u>.
  - RRM Radio Grouping: Refer to Configure < IPaddress >> 802.11a Grouping Control.
- 802.11b/g: Click the menu title to reveal menu selections.
  - 802.11b/g Parameters: Refer to <u>Configure <IPaddress> > 802.11b/g Parameters</u>.
  - RRM Thresholds: Refer to Configure < IPaddress > 802.11b/q RRM Thresholds.
  - RRM Intervals: Refer to Configure < IPaddress > 802.11b/q RRM Intervals.

- RRM Radio Grouping: Refer to <u>Configure <IPaddress> > 802.11b/g RRM Grouping</u> <u>Control</u>.
- Ports: Refer to <u>Configure < IPaddress > Ports</u>.
- Control: Click the menu title to reveal menu selections.
  - Trap Receivers: Refer to <u>Monitor <IPaddress> > Trap Receivers</u>.
  - Trap Control: Refer to <u>Configure <IPaddress> > Trap Controls</u>.
  - Telnet SSH: Refer to <u>Configure <IPaddress> > Telnet SSH Configuration</u>.
  - Syslog: Refer to <u>Configure <IPaddress> > Syslog Configuration</u>.
  - WEB Admin: Refer to *Configure <IPaddress> > WEB Admin*.

## **Configure <IPaddress> > Networking Setups**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and **Networking** to access this page.

This page displays networking setup information.

Table - General

Parameter	Description
802.3x Flow Control Mode	Enable or Disable.
LWAPP Transport Mode	Lightweight Access Point Protocol transport mode. Communications between Alcatel OmniAccess Switch or Appliance and access points. Selections are Layer2 or Layer3.
Current LWAPP Operating Mode	Layer 2 or Layer 3.
Ethernet Multicast Support	Enable or disable multicast support.
Aggressive Load Balancing	Enable or disable aggressive load balance algorithm.
Peer to Peer Blocking Mode	Enable or Disable
Over Air Provision Ap Mode	Enable or Disable
Master Switch Mode	When there is a Master Alcatel OmniAccess Switch or Appliance enabled, all newly-added OmniAccess APs with no Primary Alcatel OmniAccess Switch or Appliance assigned associate with the Master Alcatel OmniAccess Switch or Appliance on the same subnet. This allows the operator to verify the OmniAccess AP configuration and assign a Primary Alcatel OmniAccess Switch or Appliance to the OmniAccess AP. Selections are: Enable, Disable.
Wireless Management	Enables or disables access to the Alcatel OmniAccess Switch or Appliance management interface from a wireless client. The default setting is disabled.
Watch List Feature	Enable or Disable.

### Table - General (Continued)

Parameter	Description
User Idle Timeout	Set time out for idle clients in seconds. The factory default is 300. When timeout expires, client loses authentication, briefly disassociates from the OmniAccess AP, reassociates, and re authenticates.
ARP Timeout	Timeout in seconds for the Address Resolution Protocol. The factory default is 300.

#### **Command Buttons**

- Save
- Audit

## Configure < IPaddress > > Interface

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and click **Interfaces**, from the Interface Name column, select the Interface you wish to edit.

This page allows you to edit an interface description.

- Interface Name: User-defined name for this interface, for example, management, service-port, virtual (read only).
- MAC Address: Burned-in MAC address of the Management Interface.
- Interface Address:
  - IP Address: IP Address of the interface.
  - Netmask: Netmask of the interface
  - VLAN ID: 1 through 16, 17 for third-party AP WLAN (only for 4012 and 4024 Alcatel OmniAccess Wireless Switches in Direct-Connect Mode). Refer to <u>Third-Party Access Points Third-Party Access Points</u> in the <u>Alcatel OmniAccess Wireless Product</u>
     GuideAlcatel OmniAccess Wireless Product Guide.
  - Gateway: Gateway address of the interface.
- Interface Address:
  - Port Number: Interface port number.
- DHCP Information:
  - Primary DHCP Server: IP Address of the primary DHCP server.
  - Secondary DHCP Server: IP Address of the secondary DHCP server.
- Access Control List:
  - ACL Name: User-defined name of the access control list.

#### **Command Buttons**

- Save
- Audit
- Cancel

## Configure < IPaddress > Network Route

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and click **Network Route** to access this page.

This page displays a list of network routes and allows you to edit a network route to an Alcatel Omni-Access Switch or Appliance Service (Management) port. If desired, click an IP Address link to go to the *Monitor <IPaddress> > Network Route*.

- Checkbox: Used to select network routes to be deleted.
- IP Address: IP Address of the route.
- Network Mask: Network Mask of the Route.
- Gateway IP Address: Gateway IP Address of the Route.

#### Select a command pulldown

- **Add Network Route:** Select this command and click **GO**. Refer to <u>Configure <IPaddress> > Add Network Route</u>.
- **Delete Network Route:** Select a route from the list, select this command and click **GO** to delete the selected route.

## Configure < IPaddress > Switch STP Properties

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and click **Spanning Tree Protocol** to access this page.

The Spanning Tree Protocol (STP) is a link management protocol. Alcatel implements the IEEE 802.1D standard for media access control bridges.

Using the spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

This page allows you to modify STP parameters as follows.

Table - General

Parameter	Description
Protocol Spec	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations will return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version a new value will be defined.
Admin Status	Checkbox
Priority	The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value may be specified as a number between 0 and 65535. The factory default is 32768.

Table - General (Continued)

Parameter	Description
Maximum Age (centisec)	The value that all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (centisec)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Forward Delay (centisec)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent may return a badValue error if a set is attempted to a value which is not a whole number of seconds. Valid values are 4 through 30 seconds. The factory default is 15.

#### **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

## **Configure Local Authentication**

Use **CONFIGURE/Switches** and on the left sidebar menu, select **Security** and click **Local Authentication** to access this page.

This page allows you to set local authentication parameters for this Alcatel OmniAccess Switch or Appliance.

- Checkbox: Use this checkbox to select a user.
- User Name: User defined identification. Click a list item to display parameters about this user. Refer to <u>Monitor <IPaddress> > Local Authentication</u>.
- Category: Network Manager, Network User, Client MAC Address.
- WLAN ID: Identification number of the WLAN. Refer to <u>Monitor <IPaddress> > WLANs > <WLAN ID></u>.
- Access Level: Read/Write, Read Only

#### Select a command:

- Add Local User: Refer to <u>Configure <IPaddress> > Local Auth. > Add from Template</u>.
- Delete Local Users: Use the checkbox to select a user, select this command and click GO.

## Configure Disabled Clients > Template <template name>

Use **MONITOR/Clients** and click **Disabled Clients**, click a list item under **MAC Address** to access this page.

Use **CONFIGURE/Switches**, click an IP address under the IP Address column, on the left sidebar menu, select **Security** and click **Disabled Clients**, click a list item under **MAC Address** to access this page.

This page allows you to edit and apply disabled (blacklisted) client template information.

#### General

- MAC Address: MAC address of the disabled client (read only).
- No. of Switches Applied To: Number of Alcatel OmniAccess Switches and Appliances to which this template is applied (read only).
- Description: User-defined text description.

#### **Command Buttons**

- Save
- Apply to Switches: Refer to Configure Template > <template name> > Apply to Switches.
- Delete
- Cancel

## **Configure <IPaddress> > Disabled Clients**

Use **CONFIGURE/Switches**, click **Security/Disabled Clients**, select a **MAC Address** to access this page.

This page allows you to edit a disabled (blacklist) client Description.

- MAC Address: MAC address of the disabled client (read only).
- Description: User-defined text description.

#### **Command Buttons**

- Save
- Audit

## Configure Access Control List > Template <name>

Use **CONFIGURE/Templates**, from the left sidebar menu under **Security**, select **Access Control Lists**, click on a list item under **ACL Name** to access this page.

This page allows you to view current access control template information about a specific ACL, and allows you to add new rules, delete rules, and/or apply the ACL Template to an Alcatel OmniAccess Switch or Appliance.

The rules are listed in the following order:

• Seq#: The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5. Note that if you add or change a Sequence number, Alcatel Wireless Operating System adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change

number 7 to 5, Alcatel Wireless Operating System automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.

- Action: Permit, Deny.
- Source IP/Mask: Source IP Mask.
- Destination IP/Mask: Destination IP Mask.
- Protocol: Protocol to use for this ACL:
  - Any All protocols
  - TCP Transmission Control Protocol
  - UDP User Datagram Protocol
  - ICMP Internet Control Message Protocol
  - ESP IP Encapsulating Security Payload
  - AH Authentication Header
  - GRE Generic Routing Encapsulation
  - IP Internet Protocol
  - Eth Over IP Ethernet over Internet Protocol
  - OSPF Open Shortest Path First
  - Other Any other IANA protocol (http://www.iana.org/)
- If TCP or UDP Protocol is selected, Source Port: Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- Dest Port: Destination port. If TCP or UDP Protocol is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- DSCP (Differentiated Services Code Point): Any, IP Address.
- Direction: Any, Inbound (from client) or Outbound (to client).

#### Select a command

- Add New Rule: Refer to Configure Access Control List > Add Template Rule < name >.
- Delete Rules

#### **Command Buttons**

- Apply to Switches: Refer to <u>Configure Template > <template name> > Apply to Switches</u>.
- Delete
- Cancel

#### **Configure <IPaddress> > CA Certification**

Use **CONFIGURE/Switches** and on the left sidebar menu, select **Security/CA Certificate** to access this page.

This page allows you to view, import and local authentication parameters for this Alcatel OmniAccess Switch or Appliance.



**CAUTION:** Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

- Import a Certificate from a File: Use **Browse** to select a CA certificate file.
- Or select Paste and then paste the contents of a CA certificate file in the large window.

#### **Command Buttons**

- Save
- Audit

## Configure < IPaddress > Switch 802.11

Use **CONFIGURE/Switches** and select **802.11** to access this page.

This page allows you to edit information about an 802.11 Alcatel OmniAccess Switch or Appliance:

#### Table - Country

Parameter	Description
Country	Countries and the protocols allowed. Refer to <u>Alcatel</u> <u>OmniAccess Wireless System Supported Regulatory Domains</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u> .

#### Table - Timers

Parameter	Description
Authentication Response Timeout	Configures 802.11 authentication response timeout in seconds.
Rogue AP Flush Interval	Expiration timeout in seconds for rogue access points.

#### Table - RF Mobility Group

Parameter	Description
RF Mobility Group	Operator-defined Mobility Group Name. Refer to the <u>Alcatel Mobility Group</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u> .
Broadcast SSID Support	Service Set Identifier being broadcast by the OmniAccess Radio, selections are Enabled, Disabled.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

# **Configure <IPaddress> > 802.11a Parameters**

Use **CONFIGURE/Switches** and select **802.11a/Parameters** to access this page.

This page allows you to edit 802.11a parameters for an 802.11a OmniAccess Radio with a specific IP Address:

## Table - General

Parameter	Description
Admin Status	Displays the interface status either enabled or disabled.
Beacon Period	The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
Template Applied	User-defined name of the template currently applied.

## Table - 802.11a Band Status

Parameter	Description
Low Band	Read only Enable or Disable.
Medium Band	Read only Enable or Disable.
High Band	Read only Enable of Disable.

## Table - 802.11a Power Status

Parameter	Description
Dynamic Assignment	Dynamic transmit power assignment has three modes.  • Automatic - The transmit power will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Transmit power is updated when the Assign Now button is selected.  • Fixed - No dynamic transmit power assignments occur and value are set to their global default.  Default is Automatic.
Current Tx Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Control Interval (sec)	The period of time used by the ACS power algorithm to check the OmniAccess Radio power levels for adjustment, for example, 600 seconds.

Table - 802.11a Channel Status

Parameter	Description
Assignment Mode	<ul> <li>Dynamic channel assignment has three modes.</li> <li>Automatic - The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.</li> <li>On Demand - Channel assignments are updated when the user determines.</li> <li>OFF - No dynamic channel assignments occur and value are set to their global default.</li> <li>Default is Automatic.</li> </ul>
Update Interval (sec)	Interval in seconds to update the channel.
Avoid Foreign AP Interference	Checkbox, enabled or disabled.
Avoid OmniAccess AP Load	Checkbox, enabled or disabled.
Avoid non 802.11 Noise	Checkbox, enabled or disabled.
Signal Strength Contribution	Checkbox, enabled or disabled.

#### **Data Rates**

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. Pulldown selection of Mandatory or Supported for each of the following: 6, 9, 12, 18, 24, 35, 48, and 54 Mbps. Each data rate can also be set to Disabled to match Client settings.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## Configure < IPaddress > > 802.11a RRM Thresholds

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11a/RRM Thresholds** to access this page.

This page allows you to edit 802.11a RRM threshold information.

**Template Applied:** User-defined template name currently applied.

Table - Coverage Thresholds

Parameter	Description
Min Failed Clients (%)	Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
Min Failed Clients (#)	Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.

Table - Coverage Thresholds (Continued)

Parameter	Description
Min SNR Level (dB)	Minimum signal to noise ratio allowed.

#### Table - Load Thresholds

Parameter	Description
Max Clients	(1 to 75) Maximum number of clients currently associated with the Alcatel OmniAccess Switch or Appliance.
RF Utilization (%)	802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.
Throughput Threshold (bps)	Between 1000 and 10000000 bytes per second.

## Table - Other Thresholds

Parameter	Description
Interference Thres (%)	(0 to 100%) Foreign 802.11a interference threshold between 0 and 100 percent.
Noise Threshold (dBm)	Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

# **Configure <IPaddress> > 802.11a RRM Intervals**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11a/RRM Intervals** to access this page.

This page allows you to specify 802.11a RRM interval parameters:

Table - 802.11a RRM Intervals

Parameter	Description
Template Applies	User-defined template name currently applied.
Signal Measurement Interval	The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
Noise Measurement Interval	The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
Load Measurement Interval	The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.

Table - 802.11a RRM Intervals (Continued)

Parameter	Description
Coverage Measurement Interval	The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## **Configure <IPaddress> > 802.11a Grouping Control**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11a** and click **RRM Radio Grouping** to access this page.

This page allows you to specify 802.11a grouping control parameters:

Table - 802.11a Grouping Control

Parameter	Description
Grouping Algorithm	Dynamic grouping has two modes: off and automatic. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is automatic, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Update Interval (sesc)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## Configure < IPaddress > > 802.11b/g Parameters

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11b/g** and click **Parameters** to access this page.

This page allows you to specify 802.11b/g parameters:

Table - General

Parameter	Description
Admin Status	Use this checkbox to enable the OmniAccess Radio.

## Table - General (Continued)

Parameter	Description
802.11g Support	Enabled checkbox.
Beacon Period	The rate at which the SSID is broadcast by the OmniAccess AP, from 100 to 600 milliseconds.
Short Preamble	Enabled checkbox.
Template Applied	The user-defined template which applies.

Table - 802.11b/g Power Status

Parameter	Description
Dynamic Assignment	Dynamic transmit power assignment has three modes.  • Automatic - The transmit power will be periodically updated for all OmniAccess APs that permit this operation.  • On Demand - Transmit power is updated when the Assign Now button is selected.  • Fixed - No dynamic transmit power assignments occur and value are set to their global default.  Default is Automatic.
Current Tx Level	OmniAccess AP transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and 5 = 6.25% power). Note that the power levels and available channels are regulated on a country by country basis. Refer to <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for the maximum Transmit Power Levels for each country.
Control Interval (secs)	The period of time used by the ACS power algorithm to check the OmniAccess Radio power levels for adjustment, for example, 600 seconds.

Table - 802.11b/g Channel Status

Parameter	Description
Assignment Mode	<ul> <li>Assignment Mode: Dynamic channel assignment has three modes.</li> <li>Automatic - The channel assignment will be periodically updated for all OmniAccess APs that permit this operation.</li> <li>On Demand - Channel assignments are updated when desired.</li> <li>OFF - No dynamic channel assignments occur and value are set to their global default.</li> <li>Default is Automatic.</li> </ul>
Update Interval (sec)	Checkbox, enabled or disabled.
Avoid Foreign AP Interference	Checkbox, enabled or disabled.

Table - 802.11b/g Channel Status (Continued)

Parameter	Description
Avoid OmniAccess AP Load	Checkbox, enabled or disabled.
Avoid non 802.11 Noise	Checkbox, enabled or disabled.
Signal Strength Contribution	Checkbox, enabled or disabled.

#### **Data Rates**

The data rates set are negotiated between the client and the Alcatel OmniAccess Switch or Appliance. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the Alcatel OmniAccess Switch or Appliance, any associated client that also supports that same rate may communicate with the Alcatel OmniAccess Wireless Access Point using that rate. But it is not required that a client be able to use all the rates marked Supported in order to associate. Pulldown menu selections of Mandatory or Supported for each of the following: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. Each data rate can also be set to Disabled to match Client settings.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## Configure < IPaddress > > 802.11b/g RRM Thresholds

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11b/g** and click **RRM Thresholds** to access this page.

This page allows you to specify 802.11b/g RRM threshold parameters.

**Template Applied:** Specifies the template to apply.

**Table -** Coverage Thresholds

Parameter	Description
Min Failed Clients (%)	Minimum percentage of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
Min Failed Clients (#)	Minimum number of failed clients currently associated with the Alcatel OmniAccess Switch or Appliance.
Min SNR Level (dB)	Minimum signal to noise ratio allowed.

Table - Load Thresholds

Parameter	Description
Min Clients	Minimum number of clients allowed.
RF Utilization	802.11a or 802.11b/g RF utilization threshold between 0 and 100 percent.
Min SNR Level (dB)	Minimum signal to noise ratio allowed.

Table - Other Thresholds

Parameter	Description
Interference Thres (%)	(0 to 100%) Foreign 802.11a interference threshold between 0 and 100 percent.
Noise Thres (dB)	Noise threshold between -127 and 0 dBm.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## Configure < IPaddress > > 802.11b/g RRM Intervals

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11b/g** and click **RRM Intervals** to access this page.

This page allows you to specify 802.11b/g RRM intervals parameters:

Table - 802.11b/g RRM Intervals

Parameter	Description
Template Applied	The user-defined name of the template currently applied.
Signal Measurement Interval	The interval (in seconds) for strength measurements at each OmniAccess AP. Default is 300 seconds.
Noise Measurement Interval	The interval (in seconds) for noise and interference measurements at each OmniAccess AP. Default is 300 seconds.
Load Measurement Interval	The interval (in seconds) for load measurements at each OmniAccess AP. Default is 300 seconds.
Coverage Measurement Interval	The interval (in seconds) for coverage measurements at each OmniAccess AP. Default is 300 seconds.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

# Configure < IPaddress > > 802.11b/g RRM Grouping Control

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **802.11b/g** and click **RRM Radio Grouping** to access this page.

This page allows you to specify 802.11b/g RRM grouping control parameters.

Table - 802.11b/g RRM Intervals

Parameter	Description
Grouping Algorithm	Dynamic grouping has two modes: automatic and off. When the grouping is off, no dynamic grouping occurs. Each Alcatel OmniAccess Switch or Appliance optimizes only its own OmniAccess AP's parameters. When grouping is automatic, the Alcatel OmniAccess Switch or Appliance forms groups and elects leaders to perform better dynamic parameter optimization.
Group Update Interval Time (sec)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.

#### **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

# **Configure < IPaddress> > Ports**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, click **Ports** to access this page.

This page displays port information.

Table - Ports

Parameter	Description
Port Number	The port number. Click an item in the list for details about this port. Refer to $\underline{Monitor\ Switches} > <\underline{IPaddress} > >\underline{Ports} >\underline{n}$ .
Physical Mode	Displays the physical mode of all ports. Selections are:  • 100 Mbps Full Duplex  • 100 Mbps Half Duplex  • 10 Mbps Full Duplex  • 10 Mbps Half Duplex.
Admin Status	Displays the state of the port of either Enable or Disable.
Mirror Mode	Enable or disable
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port.
Link Traps	indicates that the port should send or not send a trap when link status changes. The factory default is enabled. Enable or Disable
Power Over Ethernet	Indicates if the connecting device is equipped to receive power via the Ethernet cable and if so provides -48 VDC per 802.3af.

## Table - Ports (Continued)

Parameter	Description
General Config	Refer to <u>Configure <ipaddress> &gt; Ports &gt; <port#></port#></ipaddress></u> .
STP Config	Refer to <u>Configure <ipaddress> &gt; Ports &gt; &lt;#&gt;</ipaddress></u> .

## Configure < IPaddress > > Ports > < port#>

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, click **Ports**, then click **General Config** to access this page.

This page allows you to edit port parameters:

Table - Ports

Parameter	Description
Port Number	Port number on the Alcatel OmniAccess Switch or Appliance.
Admin Status	Displays the state of the port of Enable or Disable.
Physical Status	Displays the actual port physical interface. Pulldown: Auto Negotiate, Half Duplex 10 Mbps, Full Duplex 10 Mbps, Full Duplex 100 Mbps, Full Duplex 1 Gbps.
STP Mode	<ul> <li>State of the Spanning Tree Protocol Administrative Mode associated with the port. The possible values are:</li> <li>802.1D - all ports participate in the spanning tree and will go through all of the spanning tree states when the link state transitions from Down to Up.</li> <li>Off - spanning tree is disabled for all ports.</li> <li>Fast - all ports participate in the spanning tree and will be put in the forwarding state when the link state transitions from Down to Up faster than when STP Mode is 802.1D. In this state, the Forwarding Delay timer is ignored on Link Up.</li> </ul>
Power Over Ethernet	Displays status of Power over Ethernet functionality. Pulldown: Enable or Disable.
Link Traps	Indicates if the port is set to send a trap when link status changes. Pulldown: Enable or Disable.
Mirror Mode	Disable or enable.

#### **Command Buttons**

- Save: Save the current settings.
- Audit: Discover the present status of this AP.

## Configure < IPaddress > > Ports > < #>

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, click **Ports**, click **STP Config** to access this page.

This page allows you to edit the Spanning Tree Protocol for the specified port.

- Port Number (read only)
- Priority
- Path Cost

#### **Command Buttons:**

Save: Save the current settings.

Audit: Discover the present status.

## **Configure < IPaddress> > Trap Receiver**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control/Trap Receivers**, then click a **Name** to access this page.

This page allows you to edit the trap receiver admin status:

Table - Trap Receiver Details

Parameter	Description
Name	Trap receiver name (read only).
IP Address	Local network IP Address of the Alcatel OmniAccess Switch or Appliance as described in <u>Management Interface</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> (read only).
Admin Status	Status must be enabled for the SNMP traps to be sent to the receiver. Enabled checkbox.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## **Configure <IPaddress> > Trap Controls**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control/Trap Control** to access this page.

This page allows you to select which traps logs should be captured. Select the applicable logs and select **Save**.

Table - Miscellaneous Traps

Trap Name	Description
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated.
Port Status	Port changes status from up or down.
Multiple Users	Two users login with the same login ID.
Spanning Tree	Spanning Tree traps. Refer to the STP specifications for descriptions of individual parameters.

Table - Miscellaneous Traps (Continued)

Trap Name	Description
Rogue AP	Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
Switch Config Save	Notification sent when the configuration is modified.

## Table - Client Related Traps

Trap Name	Description
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.
802.11 Auth Failure	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
802.11 Association Failure	The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
Blacklisting	The associate failure notification is sent when a client is disabled.

## Table - OmniAccess AP Traps

Trap Name	Description
AP Register	Notification sent when OmniAccess AP associates or disassociates with the Alcatel OmniAccess Switch or Appliance.
AP Interface Up/Down	Notification sent when OmniAccess AP interface (802.11a or 802.11b/g) status goes up or down.

## Table - Auto RF Profile Traps

Trap Name	Description
Load Profile	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Exceeded	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Exceeded	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Unsatisfactory	Notification sent when Coverage Profile state changes between PASS and FAIL.

## Table - Auto RF Update Traps

Trap Name	Description
Channel Change	Notification sent when OmniAccess AP's dynamic channel algorithm is updated.
Tx Power Change	Notification sent when OmniAccess AP's dynamic transmit power algorithm is updated.
Antenna Change	Notification sent when OmniAccess AP's dynamic antenna algorithm is updated.

## Table - AAA Traps

Trap Name	Description
User Auth Failure	This trap is to inform that a client RADIUS authentication failure has occurred.
RADIUS Server No Response	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

## Table - IP Security Traps

Trap Name	Description
ESP Auth Failure	IPSec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPSec packets with invalid sequence numbers were found in an inbound ESP SA.
ESP Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
IKE Neg Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
Suite Neg Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.

## 802.11 Security Traps

• WEP key Decrypt Error: Static WEP key authentication.

#### **Command Buttons**

Save: Save the current settings.

Audit: Discover the present status of this AP.

## **Configure <IPaddress> > Telnet SSH Configuration**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control** and click **Telnet SSH** to access this page.

Use this page to modify Telnet accessibility to the Alcatel OmniAccess Switch or Appliance:

- Template Name: Name of this template.
- **Session Timeout (minutes)**: This object indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
- **Maximum Sessions**: Selectable from a pulldown menus for values of from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The factory default is 5.
- **Allow New Sessions**: Indicates that new Telnet sessions will not be allowed on the DS Port when set to no. The factory default value is no.
- Note: New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service (Management) port.
  - Allow New SSH Sessions: Indicates that new Secure Shell Telnet sessions will not be allowed
    when set to no. The factory default value is yes.

#### **Command Buttons**

- Save: Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Audit: Discover the present status of this AP.

## **Configure < IPaddress> > Syslog Configuration**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control** and click **Syslog** to access this page.

This page allows you to display and enable an Alcatel OmniAccess Switch or Appliance log:

- Template Name: User-defined name of this template.
- Syslog Enabled: checkbox.

#### **Command Buttons**

- **Save:** Data is sent to the Alcatel OmniAccess Switch or Appliance and made to take effect, but not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- Audit: Discover the present status of this AP.

## Configure < IPaddress > > WEB Admin

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **Control** and click **WEB Admin** to access this page.

This page displays Web administration information:

• **WEB Mode:** This is the http Web interface which is accessible using a login and password. If you disable Web Mode, you will need Secure Web Mode enabled, or will need to use the CLI or OmniVista Air Control System interface to configure the Alcatel OmniAccess Switch or

Appliance. If you disable Web Mode and Secure Web Mode, and will need to use the CLI interface to configure the Alcatel OmniAccess Switch or Appliance (Enable or Disable).

- Secure WEB Mode: This is the https Secure Shell (SSL) interface accessible using secure certificate authentication (configured below). If you disable Secure Web Mode, you will need Web Mode enabled or will need to use the CLI or OmniVista Air Control System interface to configure the Alcatel OmniAccess Switch or Appliance (Enable or Disable).
- Certificate Type: The type of certificate used to authenticate the server and encrypt data transmissions between server and browser, for example, CA or ID Certificate.
- Download WEB Certificate: Click this phrase to download a WEB certificate. Refer to Configure < IPaddress> > Download Web Admin Certificate.

#### **Command Buttons**

- Save
- Audit: Discover the present status of this AP.
- **Regenerate Certificate:** Regenerate the internally-generated WEB certificate.

## **Configure < IPaddress> > Download Web Admin Certificate**

Use CONFIGURE/Switches and click an IP address under the IP Address column, on the left sidebar menu, select System and Commands and from the Upload/Download Commands pulldown, select **Download WEB Admin Cert** to access this page.

This page allows you to download a web administration certificate.



CAUTION: Each certificate has a variable-length embedded RSA Key. The RSA key can be from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), MAKE SURE the RSA key embedded in the certificate is AT LEAST 768 Bits.

- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance to receive the certificate.
- Status: Status of the certificate, for example, not initiated.

#### **TFTP Servers**

- Server Name: Use the Pulldown to select Default Server or New. When you select New, type in the IP Address.
- Server Address: IP Address of the server.
- Maximum Retries: Maximum number of times each download operation can be attempted.
- Timeout (seconds): The amount of time allowed for each download operation.
- Path: Path to the certificate.
- File Name: File name of the certificate.
- Password: Password to access the certificate.

#### **Command Buttons**

- OK
- Cancel

# Configure TFTP Server > TFTP Server < name >

Use **CONFIGURE/Templates** and from the left sidebar menu, select **TFTP Servers**, then click a list item under **TFTP Server Name** to access this page.

This page allows you to edit the IP address for an existing TFTP server record.

- TFTP Server Name: User-defined TFTP server name (read only).
- IP Address: IP Address of the TFTP server.
- Command Buttons:
  - Save
  - Cancel
- Software Version on this Server:
  - Version Id: Alcatel Wireless Operating System software version number.
  - Path: The complete directory path on the server (default = /), showing the location of the software.
  - Filename: The name of the file containing the software.

#### Select a command

- Add Version: Select this command and click GO. Refer to <u>Configure Software Version > Add</u>.
- Delete Version: Select an item on the list, select this command and click GO.

# **Operating Devices**

You can operate Alcatel OmniAccess Wireless Switches, OmniAccess Wireless Appliances, OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points using the following:

- Configure <IPaddress> > Switch Commands
- Restore to Factory Default Command
- <IPaddress> > Refresh Config
- <IPaddress> > Restore Config
- < IPaddress> > Set Time
- Upload File Command
- <u>Download Configuration Command</u>
- Download Software to Switch
- <u>Download Sof</u>tware
- Configure <IPaddress> > Download Web Auth Certificate to Switch
- <u>Configure <IPaddress> > Download Web Admin Certificate</u>

## **Configure < IPaddress> > Switch Commands**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, then on the left sidebar menu, select **System** and then **Commands** to access this page.

This page allows you to edit important Alcatel OmniAccess Switch or Appliance functions.

Administrative Commands: Select a command from the pulldown and click GO.

- Save Config To Flash: Data is saved to the Alcatel OmniAccess Switch or Appliance in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the Alcatel OmniAccess Switch or Appliance is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot: This command allows you to confirm the restart of your Alcatel OmniAccess Switch or Appliance after saving your configuration changes. All system connections will be lost so you will need to open a new session and log back into the Alcatel OmniAccess Switch or Appliance. You will be prompted for confirmation.
- Reset To Factory Default: Refer to <u>Restore to Factory Default Command</u>.
- Ping From Switch: Send a Ping to a network element. This pop-up window allows the you to tell the Alcatel OmniAccess Switch or Appliance to send a Ping request to a specified IP Address. This is useful for determining if there is connectivity between the Alcatel OmniAccess Switch or Appliance and a particular IP station. Once you click **OK**, three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it will show No Reply Received from IP xxx.xxx.xxx.xxx, otherwise shows Reply received from IP xxx.xxx.xxx.xxx.xxx (send count = 3, receive count = n).

Configuration Commands: Select a command from the pulldown and click GO.

- Audit Config: Refer to <u>Monitor <IPaddress> > Audit Report</u>.
- Refresh Config from Switch: Refer to <<u>IPaddress> > Refresh Config</u>.
- Restore Config to Switch: Refer to <<u>IPaddress</u>> > <u>Restore Config</u>.
- Set System Time: Refer to <<u>IPaddress> > Set Time</u>.

**Upload/Download Commands:** Select a command from the pulldown and click **GO**.

- Upload File from Switch: Refer to *Upload File Command*.
- Download Config.: Refer to <u>Download Configuration Command</u>.
- Download Software: Refer to <u>Download Software to Switch</u>.
- Download Web Auth. Cert: Refer to <u>Configure < IPaddress > Download Web Auth Certificate to Switch.</u>
- Download Web Admin Cert.: <u>Configure < IPaddress > Download Web Admin Certificate</u>.

**RRM Commands:** Select a command from the pulldown and click **GO**.

- RRM 802.11a Reset: Resets Remote Radio Management for 802.11a OmniAccess Radios.
- RRM 802.11b/g Reset: Resets Remote Radio Management for 802.11b/g OmniAccess Radios.
- 802.11a Channel Update: Updates OmniAccess AP's dynamic channel algorithm for 802.11a
   OmniAccess Radios
- 802.11b/g Channel Update: Updates OmniAccess AP's dynamic channel algorithm for 802.11b/g OmniAccess Radios.
- 802.11a Power Update: Updates OmniAccess AP's dynamic transmit power algorithm for 802.11a OmniAccess Radios.
- 802.11b/g Power Update: Updates OmniAccess AP's dynamic transmit power algorithm for 802.11b/g OmniAccess Radios.

## **Restore to Factory Default Command**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Administrative Commands** pulldown, select **Reset to Factory Default** to access this page.

This command allows you to reset the Alcatel OmniAccess Switch or Appliance configuration to the factory default. This will overwrite all applied and saved configuration parameters! You will be prompted for confirmation to reinitialize your Alcatel OmniAccess Switch or Appliance.

All configuration data files are deleted, and upon reboot, the Alcatel OmniAccess Switch or Appliance is restored to its original unconfigured state. This will remove all IP configuration, and you will need a serial connection to restore its base configuration.

**Note:** After confirming configuration removal, you must reboot the Alcatel OmniAccess Switch or Appliance and select the "Reboot Without Saving" option.



**CAUTION:** Have a serial session available to complete the <u>Startup Wizard</u> as described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### <IPaddress> > Refresh Config

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Configuration Commands** pulldown, select **Refresh Config from Switch** to access this page.

This page allows you refresh the configuration from the Switch to the ACS database. It contains the following:

#### **Command Buttons**

Leave Extra: Leave parameter values that may not still be valid.

- Remove Extra: Remove parameter values that are no longer valid
- Cancel

#### <IPaddress> > Restore Config

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Configuration Commands** pulldown, select **Restore Config from Switch** to access this page.

This page allows you to restore the configuration from the ACS database to the Alcatel OmniAccess Switch or Appliance. It contains the following:

#### **Command Buttons**

- OK
- Cancel

#### < IPaddress > Set Time

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Configuration Commands** pulldown, select **Set System Time** to access this page.

Use this command to set the current time and date on the Alcatel OmniAccess Switch or Appliance.

Current Time: Shows the time currently being used by the system.

#### **Date**

- Month: Select the month from the pulldown.
- Day: Select the day from the pulldown.
- Year: Select the year from the pulldown.

#### Time

- Hour: Select the hour from the pulldown.
- Minutes: Type in the minutes.
- Seconds: Type in the seconds.

#### **Command Buttons**

- Save
- Cancel

## **Upload File Command**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Upload/Download Commands** pulldown, select **Upload File from Switch** to access this page.

Use this command to upload files from your Alcatel OmniAccess Switch or Appliance to a local TFTP (trivial file transfer protocol) server. You can upload the following files:

- Configuration file
- Error log

- System Trace
- Trap Log
- Crash file

Enter the IP Address of the TFTP server, the directory path on the server (default = /), and a name for the file you have selected for upload.

**Note:** The TFTP server cannot run on the same computer as the OmniVista Air Control System Software, because the ACS Software and the TFTP server use the same communication port.

When you click Upload, the selected file will be uploaded to your TFTP server and named what you entered in the File Name field.

## **Download Configuration Command**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Upload/Download Commands** pulldown, select **Download Config** to access this page.

Use this command to download and install a configuration file to your Alcatel OmniAccess Switch or Appliance from a local TFTP (trivial file transfer protocol) server.

**Note:** The TFTP server cannot run on the same computer as the OmniVista Air Control System Software, because the ACS Software and the TFTP server use the same communication port.

- Select Code to download and automatically install new Alcatel OmniAccess Switch or Appliance
  Alcatel Wireless Operating System software. This process will take at least three minutes and
  will overwrite your existing code and configuration. You will need to reboot the Alcatel
  OmniAccess Switch or Appliance after the new Alcatel Wireless Operating System software is
  installed.
- Select Configuration to download a backup configuration file to the Alcatel OmniAccess Switch or Appliance.
- Configure the IP Address of the TFTP server, the directory path on the server (default = /), and the name of the file to be transferred.
- Cancel

## **Download Software to Switch**

Use **CONFIGURE/Switches** and click an IP address under the IP Address column, on the left sidebar menu, select **System** and **Commands** and from the **Upload/Download Commands** pulldown, select **Download Software** to access this page.

Use this command to download and install new Alcatel OmniAccess Switch or Appliance Alcatel Wireless Operating System software to your Alcatel OmniAccess Switch or Appliance from a local TFTP (trivial file transfer protocol) server.

**Note:** The TFTP server cannot run on the same computer as the OmniVista Air Control System Software, because the ACS Software and the TFTP server use the same communication port.

- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance to receive the software.
- Current Software Version: The software version currently running on the Alcatel OmniAccess Switch or Appliance.
- Status: Status of the software, for example, Not Initiated.

#### **TFTP Servers**

- Server IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance to receive the software.
- Maximum Retries: Maximum number of unsuccessful attempts before the download is abandoned.
- Timeout: Maximum number of seconds before the download is abandoned.
- Path: File location of the software.
- File Name: File name of the software.

#### **Command Buttons**

- OK
- Cancel

#### **Download Software**

Use **CONFIGURE/Switches** and under **Select a command**, select **Download Software** to access this page.

This page allows you download a specific version of ACS Software.

- IP Address: IP Address of the Alcatel OmniAccess Switch or Appliance to receive the software.
- Current Software Version: The software version currently running on the Alcatel OmniAccess Switch or Appliance.
- Status: Status of the software, for example, Not Initiated.
- TFTP Servers:
  - Server Name: The user-defined server name.
  - Server Address: The IP Address of the server.
- Software Version:
  - Version Id: The software version identifier.
  - Path: File location of the software.
  - File Name: File name of the software.

#### **Command Buttons**

- OK
- Cancel

Notes:

# Alcatel OmniAccess Wireless Access Point Deployment Guide

System Release 2.0

This Guide is intended for VARs, OEM distributors, and IT managers to determine how many Alcatel OmniAccess Wireless Access Points (OmniAccess APs) are needed for a deployment, and where the OmniAccess APs should be placed.

The following general steps will guide you through the planning and deployment steps for an Alcatel wireless network:

- <u>Deployment Overview</u>
- Step 1: Determining Deployment Requirements
  - <u>Assumptions</u>
  - <u>Coverage Area Requirements</u>
  - Building Type
  - <u>Building Homogeneity</u>
  - Average Client Throughput
  - <u>Voice over IP Requirements</u>
- <u>Step 2: Determining Deployment Strategy</u>
- Step 3: Optional Minimal Site Survey
- Step 4. OmniAccess AP Placement Guidelines
- Deploy the OmniAccess APs -- <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point</u>
  <u>Quick Installation Guide</u> or <u>External-Antenna Alcatel OmniAccess Wireless Access Point Quick</u>
  <u>Installation Guide</u>

# **Deployment Overview**

The Alcatel wireless network provides features and tools that simplify wireless network deployment, allowing IT departments to deploy wireless networks with existing resources, and allowing system integrators to design and deploy wireless networks with greater predictability.

The Alcatel OmniVista AirView Software part of the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System) detects coverage holes and interference, and automatically determines transmit power level and transmit channels for each OmniAccess AP, which allows the Alcatel OmniAccess Wireless System to be deployed without a site survey when the building RF characteristics are well known.

The Alcatel OmniAccess Wireless System features that simplify the deployment process include:

- Internal dual-band antennas that provide the performance of external antennas without requiring external antennas and RF cables.
- Standards-based 802.3af Power over Ethernet (PoE) that allows the OmniAccess APs to be powered over unused pairs in the Ethernet cable.
- The Alcatel Site Survey Tool, which is optimized for the Alcatel OmniAccess Wireless System infrastructure.
- External power supply option allows the OmniAccess APs to be easily moved during the site survey to verify RF building characteristics.
- The Dynamic Transmit Power algorithm automatically lowers OmniAccess AP transmit power to minimize overlap between adjacent 802.11a or 802.11b/g OmniAccess Radio coverage areas, and automatically increases power to fill coverage holes if a nearby OmniAccess AP fails.
- Real-time coverage hole detection and client performance monitoring provides the IT manager with real-time visibility into coverage holes based on client traffic.
- Automatic interference detection detects interference from microwave ovens, Bluetooth devices, and other APs, and automatically changes the assigned OmniAccess AP channel to avoid the interference.

This guide reviews the step-by-step process for deploying Alcatel OmniAccess Wireless Access Points.

# **Step 1: Determining Deployment Requirements**

There are a few important deployment criteria to consider when deploying a wireless network:

- Assumptions
- Protocol Requirements
- Coverage Area Requirements
- Building Type
- Building Homogeneity
- Average Client Throughput
- Voice over IP Requirements
- Note: Most enterprise installations are initially designed and deployed for coverage. If there is a large installed base of wireless clients, capacity must also be considered.

## **Assumptions**

The guidelines in this document are based on the following conditions and assumptions:

- Client Data Terminal Transmit (Tx) Power: >=15 dBm.
- Client Data Terminal Antenna Gain: >=0 dBi.
- Capacity: up to 15 Data client Terminals or up to 14 VoIP clients per OmniAccess AP.
- Handover Times: 37 milliseconds or less for Layer 2 (same- Alcatel OmniAccess Switch or Appliance) handovers, 48 milliseconds or less for Layer 3 (inter-Alcatel OmniAccess Switch and Appliance and inter-subnet) handovers.
- Quality of Service: Assigned on a per-WLAN basis. VoIP clients with Gold QoS take precedence (90+% of bandwidth) over clients with Silver or Bronze QoS.
- Note: These assumptions are typical for available 802.11 client Data Terminals and typical cubicle density.

## **Protocol Requirements**

One of the critical decisions in deploying a wireless LAN is what protocols and bands it will support. The following table shows the options and the pros and cons of each.

Protocol/Band	Pros	Cons
802.11a/b/g	Highest capacity option (three 802.11b/g channels and thirteen 802.11a channels)  Highest performance option (54 Mbps for both 802.11g and 802.11a)  Rogue access point detection for both 2.4 GHz 802.11b/g and 5.0 GHz 802.11a bands	Small increase in the Alcatel OmniAccess Wireless Access Point cost

Protocol/Band	Pros	Cons
802.11 b/g only	Supports legacy clients  Lowest cost Alcatel OmniAccess Wireless Access Point	802.11g performance is limited in the presence of 802.11b users  Limited capacity  Does not support 802.11a clients
802.11a only	High performance High Capacity	Does not support 802.11b/g clients

#### **Coverage Area Requirements**

Customers typically want seamless full RF coverage or partial RF coverage in conference rooms, lunch rooms, etc.

- Full or partial coverage.
- What percentage of coverage holes is acceptable? (0 10%)

Coverage holes are areas where clients cannot receive a signal from the wireless network. When deploying wireless networks, there is a tradeoff between the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations may receive marginal service. After launch, the Alcatel OmniVista AirView Software will identify these coverage areas and report them to the IT manager, allowing the IT manager to fill holes based on user demand.

#### **Building Type**

Identifying the building type and its RF characteristics is critical in determining how many OmniAccess Radios will be needed. The following table shows three basic building types that are common in the enterprise market. If the building does not fall into one of these categories then some amount of professional service may be needed.

Building Type	Description			
Typical Office Space	This is the most common enterprise building. This type of building consists large open cubicle areas with walled offices and conference rooms.			
Drywall Office Space	This type of building consists of mostly offices with dry wall characteristics.			
Brick/Concrete Walled Office Space	This type of building consists of concrete or brick walls for both exterior and for interior office space. Old buildings found on college campuses are good examples of this type of building.			
Other	There are some buildings such as sports arenas and stock exchanges that do not fit into one of the typical categories. These buildings typically require some special consideration or professional service.			

#### **Building Homogeneity**

Is the floor-to-floor and/or building-to-building floor plan layout similar? (Yes or No)

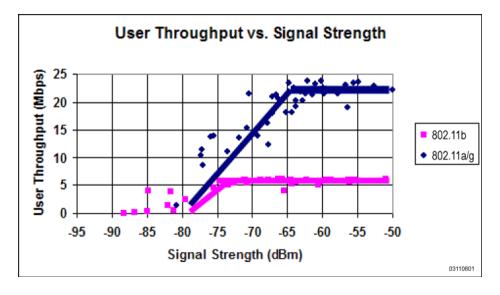
If the building does not have similar RF characteristics throughout the coverage area, the coverage area needs to be divided into areas with similar characteristics and the design process repeated for each area.

## **Average Client Throughput**

What is desired average user throughput? (1 Mbps to 18 Mbps)

Average client throughput is related to 802.11 protocol and signal strength, and thus OmniAccess AP density. In terms of protocol, 802.11b can support an average user throughput of up to 6 Mbps and 802.11a and 802.11g can support a typical average user throughput of up to 20 Mbps with reasonable OmniAccess AP densities. Generally, the stronger the signal, the higher the client throughput. However, as shown in the figure below, there is a point above which a stronger signal does not increase client throughput. For 802.11b networks, this point is typically -75 dBm, above which average client throughput is 5 to 6.5 Mbps regardless of increase in signal strength. For 802.11a networks, this point is typically between -50 dBm and -60 dBm, above which average client throughput is 24 to 30 Mbps regardless of increase in signal strength. Note that for 802.11a, the range over which the average client throughput improves is between -80 dBm and -50 dBm.





The following figures show the relationship between average client performance and OmniAccess AP density for 802.11a and 802.11b clients. The typical OmniAccess AP density for most enterprise buildings deployed for full coverage is between 2500 and 7000 square feet per OmniAccess AP.

Figure - Average 802.11a Client Throughput versus OmniAccess AP Density for Typical Office Spaces

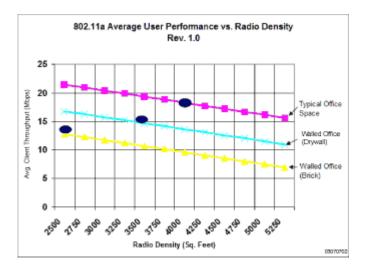
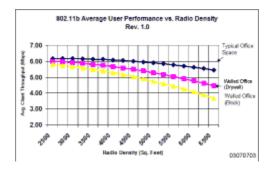


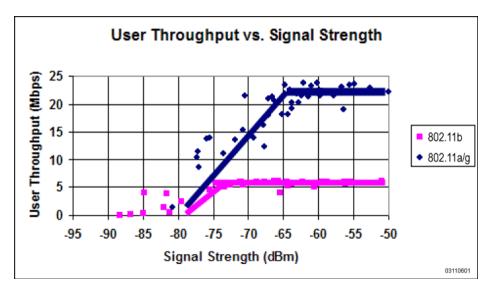
Figure - Average 802.11b Client Throughput versus OmniAccess AP Density for Typical Office Spaces



The following table provides a summary of OmniAccess Radio Coverage as a function of building type and average user performance requirements:

Coverage Area	Area = Z <sup>2</sup> (square ft.)	R (ft.)	Z (ft.)
	2500	35	50
	3000	39	55
	3500	42	59
	4000	45	63
	4500	47	67
	5000	50	71
	5500	52	72
\	6000	55	57
	6500	57	81
	7000	59	84
03082901	7500	61	87
	8000	63	89

Figure - Average Client Throughput versus Signal Strength



Building Type	Measure-		Average User Throughput		
	ment (Note 1)	1 Mbps	5 Mbps	12 Mbps (Note 2)	18 Mbps (Note 2)
Typical Office	A (ft. <sup>2</sup> )	7000	6000	5000	4000
	R (ft.)	59	55	50	45
	Z (ft.)	84	77	71	63
	S (dBm)	-85	-75	-70	-65
Drywall Office Space	A (ft. <sup>2</sup> )	5000	4000	3500	3000
	R (ft.)	50	45	42	39
	Z (ft.)	71	63	59	55
	S (dBm)	-85	-75	-70	-65
Brick Wall Office Space	A (ft. <sup>2</sup> )	4000	3500	3000	N/A
	R (ft.)	45	42	39	-
	Z (ft.)	63	59	55	-
	S (dBm)	-85	-75	-70	-
Hospital	A (ft. <sup>2</sup> )	5000	4000	3500	3000
	R (ft.)	50	45	42	39
	Z (ft.)	71	63	59	55
	S (dBm)	-85	-75	-70	-65
Warehouse/ Manufacturing	A (ft. <sup>2</sup> )	7000	6000	5000	4000
	R (ft.)	59	55	50	45
	Z (ft.)	84	77	71	63
	S (dBm)	-85	-75	-70	-65

**Note 1:** S is the minimum signal strength over 95% of the coverage area.

Note 2: Requires 802.11a.

#### **Voice over IP Requirements**

When deploying 802.11 wireless LANs to support Voice over IP (VoIP) telephones, such as SpectraLink NetLink Telephones, a few special considerations are needed in the deployment process. When deploying an 802.11b voice system, seamless full coverage with an average user throughput of 5 Mbps or more should be used. Areas such as stairways, bathrooms, cafeterias and outside areas may require special consideration and additional access points. These are areas that are not typically critical for data users but are critical coverage areas for voice users who want seamless coverage.

# **Step 2: Determining Deployment Strategy**

Depending on the customer and the deployment requirements determined in <u>Step 1: Determining</u> <u>Deployment Requirements</u>, there are three strategies for designing and deploying an Alcatel wireless network. The following table provides guidelines for which one is appropriate.

Deployment Option	Deployment Requirements
Professional Site Survey	<ul> <li>This option should be considered when:</li> <li>Deployments require full coverage with 0% coverage holes.</li> <li>The RF characteristics of the building vary throughout the coverage area.</li> <li>The building type is not typical or does not fit into one of the standard configurations (e.g. Arena, Convention Center, Stock Exchange).</li> <li>The cost or logistics of running Ethernet cables is prohibitive.</li> </ul>
RF Prediction with Optional Site Survey	<ul> <li>This option should be considered when:</li> <li>The RF characteristics of the building vary throughout the coverage area.</li> <li>The building type is not typical (e.g. Arena, Convention Center, Stock Exchange).</li> <li>A Professional Site Survey is too costly, and a graphical coverage plot is desired before deployment.</li> </ul>
Basic Guidelines with Optional Site Survey	This option is adequate for 80% to 90% of deployments, and is suitable when:  • The RF Characteristics are homogenous throughout the coverage area.  • The building type can be easily classified.

#### **Professional Site Survey**

Generally, the professional site survey involves temporarily placing one or more OmniAccess APs and then measuring the resulting coverage(s). Based on the results of these measurements, OmniAccess APs are relocated and/or reoriented to achieve complete coverage of the target space without unnecessary coverage overlap or coverage holes between OmniAccess APs. This approach is appropriate given the following deployment requirements:

- Full Coverage with 0% coverage holes
- The RF characteristics of the building vary throughout the coverage area
- The building type is not typical (e.g. Arena, Convention Center, Stock Exchange)

During the Professional Site Survey, one or two APs are placed at or near one end of a building. Their coverage is measured and the APs are relocated and reoriented as necessary to ensure that this end of the building is completely covered. When measurements confirm that this is true, a second or third AP is added so its coverage area somewhat overlaps the coverage area of the first AP(s). (Generally, 10 to 15 percent coverage overlap is considered appropriate.) Its coverage is measured to ensure that its overlap with the first AP(s) is appropriate and to determine the coverage in the rest of the building. This process continues, adding a third or fourth AP and so on. This process continues until all areas of the building are covered.

The professional site survey allows the designer to provide full seamless coverage; however, the OmniVista AirView Software ensures that the channel assignments and transmit power levels are optimized for the Alcatel OmniAccess Wireless System coverage area, freeing the site survey professional from having to fine-tune these variables.

Other variables designers may include static transmit power level, geometric pattern used for AP placement, and the antenna type (omnidirectional, wide beam directional, or narrow-beam directional). Some designers like to have the flexibility to select antenna types most suited to specific buildings.

Designers may differ in the criteria they use to determine coverage area. Some prefer to use signal strength (RSSI), some prefer signal-to-noise ratio (SNR), and others prefer to use some indication of throughput, such as packet retry rate. These measurements are normally made using site survey software provided by a wireless LAN manufacturer, running on a PC or PDA. They may also be made using one of the handheld measurement tools currently available, such as Air Magnet or Berkeley Varitronics. The measurement tools are usually selected based on their ability to measure the desired variable, RSSI, SNR, or packet retry rates.

#### **RF Prediction with Optional Site Survey**

RF prediction consists of importing the floor plans of the coverage area into a Computer Aided Design system in which a user can place access points, draw in the walls of the building and assign RF characteristics to the walls. Depending on the confidence level of the estimates made for the building RF characteristics and the cost of filling in potential coverage holes after deployment, an optional site survey may be appropriate to verify assumptions. This approach is appropriate given the following deployment requirements:

- Full Coverage with 2 to 10% coverage holes
- The RF characteristics of the building vary throughout the coverage area
- The building type is not typical (e.g. Arena, Convention Center, Stock Exchange)

#### **Basic Guidelines with Optional Site Survey**

The Basic Guideline approach is based on empirical data from existing wireless deployments and is adequate for most deployments. This approach is based on most enterprise buildings having common RF characteristics, and that only a part of the building needs to be characterized to verify the access point coverage for the entire building. This approach leverages the algorithms built into the Alcatel OmniVista AirView Software that ensure that the overlap between APs is minimized and that coverage holes are detected and eliminated before clients find them.

When deploying 802.11 wireless LANs to support Voice over IP (VoIP) telephones, such as SpectraLink NetLink Telephones, a few special considerations are needed in the deployment process. When deploying an 802.11 voice system, full coverage with an average user throughput of 5 Mbps or more should be used. Areas such as stairways, bathrooms, cafeterias and outside areas may require special consideration and access points. These are areas that are not typically critical for data users but are critical coverage areas for voice users who want seamless coverage.

Refer to the Sample Basic Guidelines Process for an example of the Basic Guidelines approach.

# **Sample Basic Guidelines Process**

Here is an example of the Basic Guidelines Process:

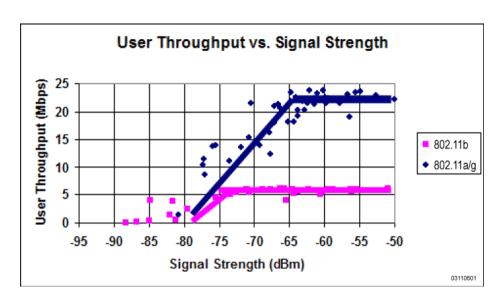
- Step A: Determine Radius and Z Factor
- Step B. Determine How Many APs are Needed
- Step C. Optional Minimal Site Survey
- Step D. Place Access Points

#### **Step A: Determine Radius and Z Factor**

In this step you determine the coverage area of an OmniAccess Radio based on the building type and desired average user performance using the table below. The Z factor represents the length of a square that corresponds to the coverage area of the access point.

Coverage Area	Area = Z <sup>2</sup> (square ft.)	R (ft.)	Z (ft.)
	2500	35	50
	3000	39	55
	3500	42	59
	4000	45	63
$\left(\begin{array}{c c} & & \\ & & \\ & & \\ \end{array}\right)$	4500	47	67
	5000	50	71
	5500	52	72
	6000	55	57
\	6500	57	81
	7000	59	84
03082901	7500	61	87
	8000	63	89

The following graph displays actual measurements, and shows the relationship between actual user throughput and corresponding signal strength.



The following table includes building types, and shows the coverage area measurements for various average user throughputs.

Building Type	Measure- ment (Note 1)	Average User Throughput				
		1 Mbps	5 Mbps	12 Mbps (Note 2)	18 Mbps (Note 2)	
Typical Office	A (ft. <sup>2</sup> )	7000	6000	5000	4000	
	R (ft.)	59	55	50	45	
	Z (ft.)	84	77	71	63	
	S (dBm)	-85	-75	-70	-65	
Drywall Office Space	A (ft. <sup>2</sup> )	5000	4000	3500	3000	
	R (ft.)	50	45	42	39	
	Z (ft.)	71	63	59	55	
	S (dBm)	-85	-75	-70	-65	
Brick Wall Office Space	A (ft. <sup>2</sup> )	4000	3500	3000	N/A	
	R (ft.)	45	42	39	-	
	Z (ft.)	63	59	55	-	
	S (dBm)	-85	-75	-70	-	

Building Type	Measure- ment (Note 1)	Average User Throughput				
		1 Mbps	5 Mbps	12 Mbps (Note 2)	18 Mbps (Note 2)	
Hospital	A (ft. <sup>2</sup> )	5000	4000	3500	3000	
	R (ft.)	50	45	42	39	
	Z (ft.)	71	63	59	55	
	S (dBm)	-85	-75	-70	-65	
Warehouse/ Manufacturing	A (ft. <sup>2</sup> )	7000	6000	5000	4000	
	R (ft.)	59	55	50	45	
	Z (ft.)	84	77	71	63	
	S (dBm)	-85	-75	-70	-65	

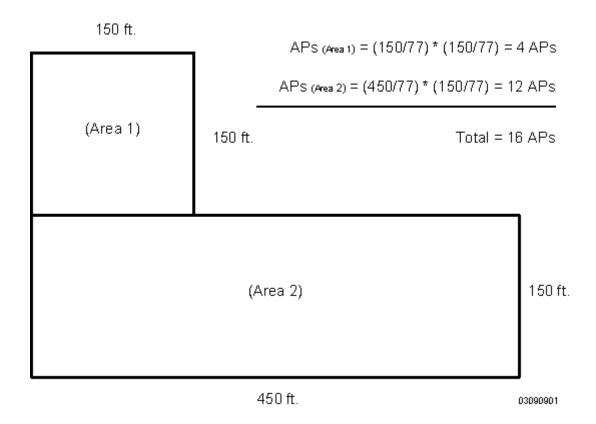
**Note 1:** S is the minimum signal strength over 95% of the coverage area.

Note 2: Requires 802.11a.

## Step B. Determine How Many APs are Needed

In this step you define the coverage area for each floor in the building and divide it into rectangles and calculate how many APs are needed by dividing the area of each rectangle by the Z factor squared.

This example is for a typical office building with a desired average user throughput of 5 Mbps.

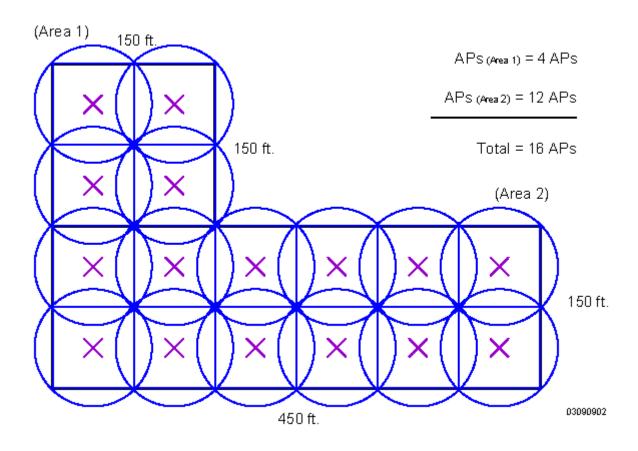


## **Step C. Optional Minimal Site Survey**

If the building type estimate needs to be verified, a quick minimal site survey can be done to verify the signal strength of the access point for the coverage radius. For example, for a typical office building with a desired average user performance of 12 Mbps a signal strength of -75 dBm or better is needed and the site survey will be used to verify that the -75 dBm coverage radius of an OmniAccess AP is 50 feet. Review the "Optional Minimal Site Survey" section of this document for how to perform a site survey using an OmniAccess AP.

### **Step D. Place Access Points**

The final step is to determine the installation location of the access point. First, using the radius or Z factor found in Step A, distribute the circles or squares evenly across the rectangles found in Step B. Note that the large "X" in the middle of each coverage area indicates the approximate location of the OmniAccess APs. Also notice that the Z factor between the centers of each OmniAccess AP location is the same as the OmniAccess AP squares when the squares are directly adjacent to each other, as shown in this figure.



## **Step 3: Optional Minimal Site Survey**

If the <u>Building Type</u> or RF characteristics assumptions are in doubt, complete this step to verify those assumptions.

The minimal site survey consists of the following:

- Collecting Tools and Materials
- Selecting OmniAccess AP Locations
- Enabling Site Survey Mode
- Preparing Optional OmniAccess AP Tripod Test Assemblies
- Positioning an OmniAccess AP at Each Planned Location
- Verifying RF Coverage Using the Alcatel Site Survey Tool

### **Collecting Tools and Materials**

Before you start a site survey, you must collect some items:

- Maps or building plans of the areas to be covered, with a feet or meters scale included.
- Duct Tape and Cable Ties.
- T-10 Security Torx screwdriver.
- A PC with a crossover CAT-5 or higher Ethernet cable capable of establishing a Telnet session with each OmniAccess AP.
- The Site Survey Tool, consisting of a laptop computer equipped with 802.11a and 802.11b/g transceivers and the signal strength monitoring and recording software, such as the <u>Alcatel Site Survey Tool</u>.
- Between one and five OmniAccess APs with power supplies:
  - OmniAccess APs.
  - Available Power Sources:
    - \* Recommended factory-orderable 110 VAC-to-48 VDC power supplies.
    - \* Optional Ethernet Power Injectors: Single RJ-45, 300 mA 48 VDC output, (MILAN Model MIL-L1611, or equivalent). Refer to <u>Preparing Optional OmniAccess AP Tripod Test Assemblies</u> for more information.
- Recommended temporary stands, such as photographer's telescoping lighting stands, that can be raised to ceiling height. Refer to <u>Preparing Optional OmniAccess AP Tripod Test Assemblies</u> for more information.
  - Optionally, you can temporarily position the OmniAccess APs at or near ceiling height using ladders and/or tall bookcases, but they do not offer the portability of the OmniAccess AP tripod test assemblies.

### **Selecting OmniAccess AP Locations**

Using the OmniAccess Radio density estimate from <u>Step 1: Determining Deployment Requirements</u> and the guidelines for placing OmniAccess APs described in <u>Step 4. OmniAccess AP Placement Guidelines</u>, determine the location for three to five OmniAccess APs in a typical test coverage area.

### **Enabling Site Survey Mode**

When the OmniAccess AP is in Site Survey mode, it broadcasts its SSID beacon on a manually-selected channel. Perform the following to enable Site Survey mode:

## Setting Up an ESD Workspace

You need an Electrostatic Discharge (ESD) workspace to complete this installation. Because the 802.11 OmniAccess Radio Cards are very sensitive to electrostatic discharge, you can destroy them by not following ESD procedures.



**CAUTION:** DO NOT attempt to open the OmniAccess APs if you do not have an ESD work-place, or you may destroy the OmniAccess AP circuitry, and will void your warranty.

### Configuring the OmniAccess AP for Site Survey Mode

Use the T-10 Security Torx screwdriver to open the door on the front of each OmniAccess AP.

Figure - OmniAccess AP Door and Screw Locations



03031802

• Enable the Site Survey function by placing the factory-supplied jumper across both of the Site Survey header pins on the OmniAccess AP motherboard as shown in the following figure.

Figure - 802.11 Site Survey Jumper in the OmniAccess AP







B. Site Survey Jumper Installed 03031810

Put the door back on the OmniAccess AP case, and use one of the door screws to temporarily hold the door closed while you apply power to the OmniAccess AP.



WARNING: When you power up the OmniAccess AP by connecting it directly or indirectly to an active Alcatel OmniAccess Wireless Switch or Appliance, it begins radiating as soon as it associates with the Alcatel OmniAccess Wireless Switch or Appliance and has completed its startup cycle. Make sure the OmniAccess AP is located at least 20 cm (8 in.) from any bystanders, including yourself, before you apply power to it and allow it to associate with an Alcatel OmniAccess Switch or Appliance. Refer to the FCC Statements for OmniAccess APs section in the Alcatel OmniAccess Wireless Product Guide for more information.

- Power up the OmniAccess AP:
  - When the OmniAccess AP is to be powered over the CAT-5 Ethernet cable, make sure the OmniAccess AP Power LED lights when you connect the OmniAccess AP cable to the PoE equipment (an OmniAccess Wireless Switch or other switch, power injector, or power hub).
  - When the OmniAccess AP is to be powered by an external power supply, plug the power supply plug into the power jack on the side of the OmniAccess AP.
- Wait until the OmniAccess AP has gone though its startup cycle, and is flashing the green Power LED and either or both of the yellow/amber 2.4 GHz and/or 5 GHz LEDs.
- Connect the Ethernet cable from the configuration PC to the OmniAccess AP Ethernet port.
- Telnet to the OmniAccess AP using IP Address 192.168.1.1, and use the following commands to configure the OmniAccess AP: -> cli

AP login: [RETURN] Password: [RETURN]

```
Atheros Access Point Rev 2.3.0.70
       wlan0 ->
Verify that the OmniAccess AP interface defaults to modify 802.11a parameters:
       wlan0 -> get wirelessmode
       Wireless LAN Mode: 802.11a
Verify that the 802.11a OmniAccess Radio is set to a different channel than its nearest APs:
       wlan0 -> get channel
       Radio Frequency: 5320 MHz (IEEE 64)
       wlan0 -> set channel 60
       Radio Frequency: 5300 MHz (IEEE 60)
If necessary, change the 802.11a OmniAccess Radio SSID:
       wlan0 -> get ssid
       SSID: Aire
       wlan0 -> set ssid aire
       SSID: aire
Change the OmniAccess AP interface to modify 802.11b/g parameters:
       wlan0 ->
       wlan0 -> config wlan 1
       wlan: 1
       wlan1 -> get wirelessmode
       Wireless LAN Mode: 802.11b
Verify that the 802.11b/g OmniAccess Radio is set to a different channel than its nearest APs:
       wlan1 -> get channel
       Radio Frequency: 2412 MHz (IEEE 1)
       wlan1 -> set channel 6
       Radio Frequency: 2437 MHz (IEEE 6)
If necessary, change the 802.11b/g OmniAccess Radio SSID:
       wlan1 -> get ssid
       SSID: Aire
       wlan1 -> set ssid aire
       SSID: aire
       wlan1 ->
Reboot the OmniAccess AP to have the parameter changes take effect:
       wlan1 -> reboot
If necessary, change the OmniAccess AP interface to modify 802.11a parameters:
       wlan1 -> config wlan 0
       wlan: 0
```



**WARNING:** When you power up the OmniAccess AP and configure it for site survey mode, it begins radiating as soon as it has completed its startup cycle. Make sure the OmniAccess AP is located at least 20 cm (8 in.) from any bystanders, including yourself, before you apply power to it and configure it for site survey mode. Refer to the <u>FCC Statements for OmniAccess APs</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information.

• Continue with Verifying RF Coverage Using the Alcatel Site Survey Tool.

### **Preparing Optional OmniAccess AP Tripod Test Assemblies**

wlan0 -> get wirelessmode
Wireless LAN Mode: 802.11a

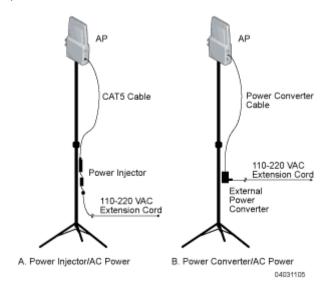
Note that you do not need to use the optional OmniAccess AP tripod test assemblies described in this section--you can tape or cable tie the OmniAccess APs to the ceiling, or place them on tall cabinets or ladders. However, if you must move them from their original positions, having them mounted on the tripod test assembly stands makes it easier to relocate them.



**WARNING:** You only need AC extension cords if you have enough 110 VAC convenience outlets within easy reach of all potential OmniAccess AP mounting locations. If you do use AC power cords, make sure you use duct tape to avoid creating trip hazards with the extension cords.

- Contact Alcatel Internetworking, Inc. for the OmniAccess AP mounting brackets and recommended telescoping stand screws.
- Use duct tape and/or cable ties to assemble the telescoping stands, OmniAccess APs, CAT-5 Ethernet cables, Ethernet power injectors, power inverter, external power supply, battery packs, and/or extension cords as shown in the following figure.
- Note: Make sure you support the CAT-5 and power cables to remove harmful stress on the OmniAccess AP connectors.

Figure - OmniAccess AP Tripod Test Assemblies



Continue with <u>Positioning an OmniAccess AP at Each Planned Location</u>.

## Positioning an OmniAccess AP at Each Planned Location

This section assumes that you have determined the OmniAccess AP locations as described in <u>Omni-Access AP Placement</u>.

Refer to <u>Preparing Optional OmniAccess AP Tripod Test Assemblies</u> for instructions on how to power the OmniAccess APs at each planned location.



**WARNING:** If you are using AC extension cords, make sure you use duct tape to avoid creating trip hazards.

- Using the floor plans and/or maps from <u>Step 4. OmniAccess AP Placement Guidelines</u>, place the OmniAccess AP assemblies at or near the indicated locations.
- If any power is being applied to the OmniAccess AP, remove the power now.

### **Verifying RF Coverage Using the Alcatel Site Survey Tool**

- Follow the manufacturer's instructions supplied with the Alcatel Site Survey Tool to collect signal strength information from the coverage area being tested.
- If necessary, reposition the OmniAccess AP(s) in the coverage area and repeat the previous steps until you have verified coverage, and then continue.
- As shown in the <u>802.11 Site Survey Jumper in the OmniAccess AP</u> figure, inside each OmniAccess AP, store the included Site Survey jumper on one, but not both, of the Site Survey Mode pins to disable site survey mode.



Note: OmniAccess APs cannot provide network access while in the site survey mode.



**WARNING:** DO NOT connect the OmniAccess AP to the network while the OmniAccess AP is in site survey mode. Doing this prevents all OmniAccess APs in site survey mode from responding to IP pings to the site survey IP Address.

Use the T-10 Security Torx screwdriver to close the door on the front of each OmniAccess AP.

## Step 4. OmniAccess AP Placement Guidelines

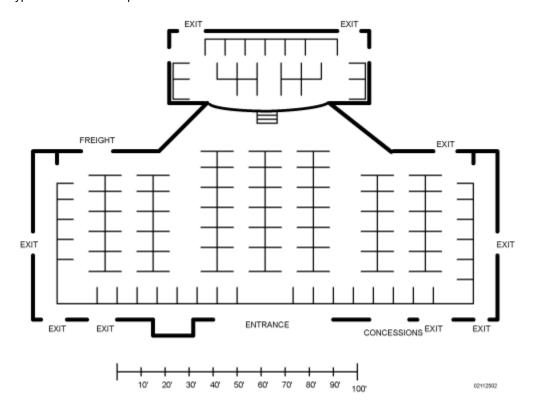
This step describes where and how OmniAccess APs should be placed. You must know certain information to select OmniAccess AP locations:

- Collecting Maps or Building Floor Plans
- Noting Any Deployment Constraints
- Access Point Placement Guidelines
- OmniAccess AP Placement

### **Collecting Maps or Building Floor Plans**

Collect maps or building plans of the areas to be covered, with a feet or meters scale included.

Figure - Typical Floor Plan -- Open Auditorium with Cubicles



### **Noting Any Deployment Constraints**

- If the OmniAccess APs are to use existing wiring, note these locations on the map.
- If there are locations where OmniAccess APs cannot be placed, note these locations on the map.

### **Access Point Placement Guidelines**

- Position the OmniAccess APs above obstructions.
- Position the OmniAccess APs vertically near the ceiling in the center of each coverage area, if possible.

Position OmniAccess APs in locations where users are expected to be. For example, large rooms
are typically a better location for OmniAccess APs than a hallway.

#### **OmniAccess AP Placement**

Place OmniAccess APs on the floor plan using the <u>Noting Any Deployment Constraints</u> and <u>Access Point Placement Guidelines</u> sections such that coverage circles are touching or slightly overlapping as illustrated in the following example.

#### For instance:

- The open auditorium (a Warehouse/Manufacturing Building Type) shown in the <u>Collecting Maps</u> or <u>Building Floor Plans</u> section is approximately 20,000 square feet.
- As described in the <u>Voice over IP Requirements</u> section, a typical SpectraLink NetLink Telephone requires approximately 6 Mbps 802.11b throughput, resulting in a minimum A = 5,000 square foot coverage area per OmniAccess AP for an open area.
- Dividing 20,000 square feet by A = 5,000 square feet per OmniAccess AP results in at least four OmniAccess APs required for the auditorium.
- Using the guidelines in <u>Step 1: Determining Deployment Requirements</u>, an A = 5,000 square foot coverage area results in an R = 50-foot coverage circle radius, or Z = 71-foot coverage square.
- On your floor plan map, arrange four 50-foot radius coverage circles so they overlap, as shown in the following figure.
- Note: The OmniAccess AP coverage areas should overlap approximately 10% to 15% to minimize the number of coverage holes.
  - Note the large "X" in the middle of each circular OmniAccess AP coverage area--those are the indicated locations of the associated OmniAccess APs.

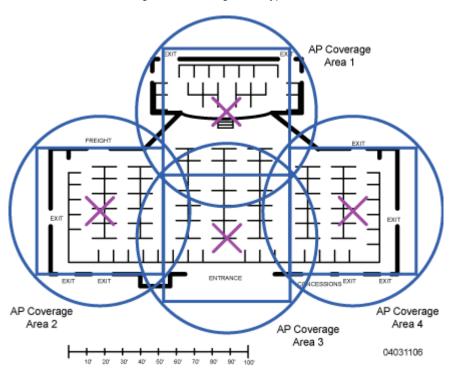
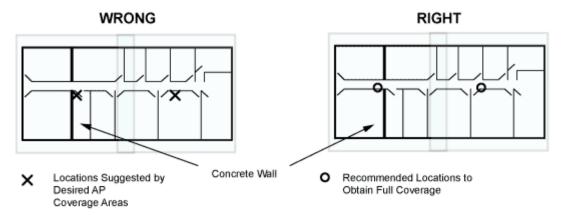


Figure - 802.11a OmniAccess AP Coverage Areas Arranged on Typical Warehouse Floor Plan

• See the following figure for a description of what to do if there are any large metal obstructions where you plan to install OmniAccess APs.

Figure - What to do about Metal RF Barriers in a Planned OmniAccess AP Location



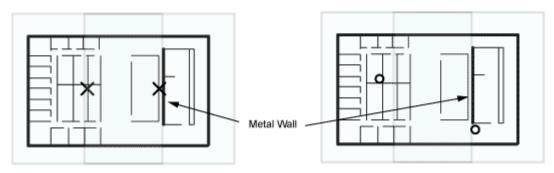
**Notes:** Both Locations moved up to mount in hallways, Left Location moved to other side of wall to provide coverage on left side of wall, and Right Location moved slightly left to provide better coverage to overlap area. Also note that the coverage areas remain where they were for coverage testing.

### A. I Have a Large Concrete Wall in the Middle of One Coverage Area



**Notes:** Upper Location moved to hallway at comer of plenum, Left Location moved next to plenum, Right Location moved to hallway, and Left Location moved to hallway to provide better coverage to overlap areas. Also note that the coverage areas remain where they were for coverage testing.

### B. I Have Large HVAC Plenums Next to Planned Locations



Notes: Right Location moved slightly to the right of one end of the Metal Wall in a hallway, and Left Location moved up and to the left to provide better coverage to overlap area.

Also note that the coverage areas remain where they were for coverage testing.

C. I Have a Large Metal Wall Next to a Planned Location

04031107

- When you are installing OmniAccess APs using the <u>RF Prediction with Optional Site Survey</u> or <u>Basic Guidelines with Optional Site Survey</u> method:
  - Complete <u>Step 3: Optional Minimal Site Survey</u> for the optional minimal site survey, or
  - Use the <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation</u>
    <u>Guide</u> or <u>External-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation</u>
    <u>Guide</u> to install the OmniAccess APs without a minimal site survey.

## Step 5: Where to Go from Here

You have successfully planned and tested the OmniAccess AP RF coverage in your target area, and have determined where the OmniAccess APs are to be located.

Continue with <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> or <u>External-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide</u> for final installation instructions, continue with the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u> after the OmniAccess APs have been installed, and refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information on using the Alcatel OmniAccess Wireless System.

Notes:

## Internal-Antenna OmniAccess AP Quick Installation Guide

System Release 2.0

This Guide contains several sections allowing you to install an OAW-1200BG or OAW-1200ABG Alcatel OmniAccess Wireless Access Point. These models contain internal 802.11a and 802.11b/g antennas and no connectors for optional external antennas.

If you are installing an OAW-1200BGE or OAW-1200ABGE Alcatel OmniAccess Wireless Access Point or an OAW-1200ABGR Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R) with internal 802.11a and 802.11b/g antennas and connectors for optional external 802.11a and 802.11b/g antennas, please refer to the *External-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide*.

- Overview
- Step 1: Collecting Required Tools and Supplies
- <u>Step 2: Configuring the OmniAccess AP Before Installation</u>
- <u>Step 3: Preparing Mounting Locations</u>
- Step 4: Mounting the OmniAccess APs
- <u>Step 5: Returning MAC Information</u>
- <u>Planning Notes</u>
- FCC Statements for OmniAccess APs

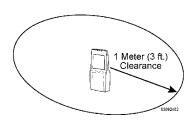
### **ATTENTION!**

While Alcatel OmniAccess Wireless Access Points have been engineered for easy installation, there are some guidelines that are very important to the end users:

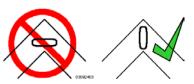
- PLACE Alcatel OmniAccess Wireless Access Points NO MORE THAN 140 FEET APART FROM EACH OTHER. Placing OmniAccess APs further apart almost always results in poor coverage.
- DO NOT MOUNT OmniAccess APs OUTSIDE BUILDINGS.
- DO NOT MOUNT OmniAccess APS ON BUILDING PERIMETER WALLS UNLESS THE OPERATOR WANTS TO PROVIDE COVERAGE OUTSIDE THE BUILDING.
- MAKE SURE that plenum-mounted OmniAccess APs are powered using Power Over Ethernet (POE) to comply with safety regulations.
- MAKE SURE THAT THE Alcatel OmniAccess Wireless Access
  Points ARE INSTALLED VERTICALLY. Alcatel OmniAccess
  Wireless Access Points ARE DESIGNED TO BE INSTALLED
  VERTICALLY, either standing up in a plenum or hanging from a
  ceiling, to create the largest coverage area per OmniAccess AP.
  Hanging the OmniAccess AP from the ceiling provides the best
  RF coverage.



DO NOT MOUNT Alcatel OmniAccess Wireless Access Point ANTENNAS WITHIN ONE METER (3 FT.) OF ANY METAL OBSTRUCTIONS. THE RF WAVES FROM Alcatel OmniAccess Wireless Access Points ARE BLOCKED AND/OR REFLECTED BY METAL OBJECTS, such as metal HVAC ducts, conduit, pipes, bookcases, elevator shafts, stairwells, and metal walls. REFER TO THE <u>Alcatel OmniAccess Wireless Access Point Deployment Guide</u> BEFORE MOUNTING OmniAccess APS NEAR METAL OBSTRUCTIONS.



 WHEN MOUNTING OmniAccess APS IN THE CORNER OF A RIGHT-ANGLE HALLWAY INTERSECTION, MOUNT THE OmniAccess AP AT A 45-DEGREE ANGLE TO THE TWO HALLWAYS. The OmniAccess AP internal antennas are not omnidirectional, and will cover a larger area if mounted this way.



## **Overview**

This guide is designed to provide you with the information needed to mount Alcatel OmniAccess Wireless Access Points (OmniAccess APs). OmniAccess APs are part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System), and require no manual configuration after they are mounted.

This document assumes that a site survey has been performed as described in the <u>Alcatel OmniAccess Wireless Access Point Deployment Guide</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>, that OmniAccess AP locations and mounting options have been selected, and that you have one OmniAccess AP per indicated location.

After the site survey is done, you should have a map indicating the following:

- AP locations.
- AP mounting options: in the middle of a ceiling/hallway, in the ceiling plenum, projecting away from the wall, or flat against the wall.
- AP power options: power supplied by the AC-to-DC power supply orderable from the factory, or Power over Ethernet (PoE) from the OmniAccess Wireless Switch, another network device, or a PoE injector/hub (usually located in a wiring closet).
- Note: Plenum-mounted OmniAccess APs and OmniAccess 1200R APs MUST BE powered using Power Over Ethernet (POE) to comply with safety regulations.

If you do not have a map, make one so you can record the MAC addresses from each location and return them to the to the person who is planning or managing this wireless network.

Refer to the following sections to install the OmniAccess APs.

**Note:** When mounting OmniAccess APs, make sure to maintain a 20 cm (8 in.) separation between the OmniAccess APs and bystanders to comply with FCC RF exposure regulations. Refer to the <u>FCC Statements for OmniAccess APs</u> section for more information.

For more details about OmniAccess AP installations, refer to the <u>Planning Notes</u> section at the end of this document.

## **Step 1: Collecting Required Tools and Supplies**

- One OmniAccess AP per location.
- OmniAccess AP Mounting Kits, factory-supplied with each OmniAccess AP.
- Optional OmniAccess AP Mounting Kits, factory-orderable.
- Optional external AC-to-DC power supplies, factory-orderable.
- Map showing OmniAccess AP locations, and mounting and power options.
- Screwdrivers, drills, and ladder.
- An assortment of sheet metal and drywall screws and toggle bolts.
- CAT-5 (or higher) cables to connect the OmniAccess AP locations and the OmniAccess Wireless Switch or other network device.
- Optional Kensington MicroSaver Security Cable to secure each OmniAccess AP.

Continue with Step 2: Configuring the OmniAccess AP Before Installation.

# **Step 2: Configuring the OmniAccess AP Before Installation**

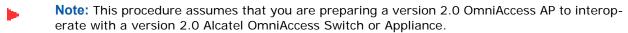
The following procedures are designed to make sure that your OmniAccess AP physical installation goes smoothly and that initial operation is as expected. If you are unable to prepare your OmniAccess AP for deployment, this Step also describes RMA (Return Material Authorization) procedures.

- Note: Perform the following procedure on each OmniAccess AP BEFORE deploying the Omni-Access AP in its final location.
  - <u>Preparing a Version 2.0 OmniAccess AP</u> for Installation in a Version 2.0 Alcatel OmniAccess Wireless System

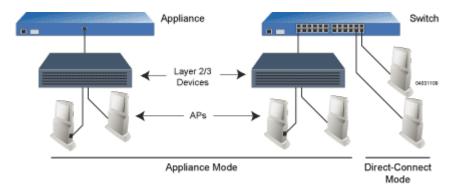
If you are unable to perform this procedure, refer to the <u>RMA Procedures</u> section in the <u>Alcatel Omni-Access Wireless Product Guide</u>.

## Preparing a Version 2.0 OmniAccess AP

If your OmniAccess AP has Alcatel Wireless Operating System 2.0 or a later version loaded on it, continue with this procedure.



### **Configuration Setup**



### Does My AP Qualify for this Procedure?

• If your 2.0 or later version later OmniAccess AP(s) cannot be configured for any other reason using the following procedure, refer to RMA Procedures later in this document.

### **Configuration Steps for an OmniAccess AP**

- Configure the Alcatel OmniAccess Switch or Appliance in LWAPP Layer 3 Mode and make sure its DS Port is connected to the network. Use CLI, Web Browser and/or ACS procedures as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u> and the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - Make sure AP ports are available (either <u>Direct-Connect Mode</u> through the Switch physical ports, or in <u>Appliance Mode</u> through the Alcatel OmniAccess Switch or Appliance Management/AP-Manager Interface).
  - Set the Alcatel OmniAccess Switch or Appliance as the Master, so new OmniAccess APs always associate with it.
  - Refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for other settings.

- 2. Take the AP out of the box and plug it into the front panel of the Master Switch (<u>Direct-Connect Mode</u>), or through the same subnet that Alcatel OmniAccess Switch or Appliance is on (<u>Appliance Mode</u>).
- 3. Apply power to the AP:
  - Use 802.3af-compatible Power Over Ethernet (PoE) from the Alcatel OmniAccess Switch
    or Appliance or from an orderable inline power injector. If you do not have PoE
    available, use an orderable external AC-to-48 VDC Power Supply plugged into the side
    of the AP.
  - After powering up the AP, the RED Alarm LED comes on for a short period (about 15-20 seconds) and then all the LEDs blink sequentially back and forth, indicating that the AP is trying to find an Alcatel OmniAccess Switch or Appliance to connect to. This can continue for up to five minutes. If the AP remains in this mode for more than five minutes, the AP is unable to find the Master Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance and make sure the AP and the Alcatel OmniAccess Switch or Appliance are on the same subnet.
  - If the power light does not come on, check the power (it can be powered either with Power over Ethernet or a from an orderable AP External Power Supply.
  - Make sure that a DHCP server is configured in the Alcatel OmniAccess Switch or Appliance for both the Management Interface and AP-Manager Interface using the CLI, Web Browser, or ACS interface, and that the DHCP server is operating correctly.
  - Once the AP finds the Alcatel OmniAccess Switch or Appliance, it attempts to download
    the new Alcatel Wireless Operating System code if the AP code version differs from the
    Alcatel OmniAccess Switch or Appliance code version. While this is happening, the LEDs
    on the top of the AP blink on and off together.
- 4. Once the Alcatel Wireless Operating System code download is successful, the AP reboots. The GREEN LED turns on and the two YELLOW/AMBER/ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled in the Alcatel Omni-Access Switch or Appliance, the corresponding YELLOW/AMBER/ORANGE LED remains off.
  - Note that the Red LED can light for a short period (10-20 seconds) when the AP reboots. If the RED LED comes on AND STAYS ON for more than a minute, disconnect the AP and call Alcatel Technical Support.
  - From the CLI, Web Browser or ACS interface, configure the AP with its Primary Alcatel OmniAccess Switch or Appliance name as described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - If required, use the CLI, Web Browser or ACS interface to customize the AP-specific 802.11a, 802.11b and 802.11g network settings. Once again, the two YELLOW/AMBER/ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled, the corresponding YELLOW/AMBER/ORANGE LED remains off
- 5. If everything works (the GREEN LED is on and the RED LED is off), disconnect the AP and take it to its final destination and install it as described in this document. If your OmniAccess AP fails this visual test, refer to RMA Procedures in the <u>Alcatel OmniAccess Wireless Product Guide</u> to return your OmniAccess APs.

- Note: When you are installing a Layer 3 OmniAccess AP on a different subnet than the Alcatel OmniAccess Switch or Appliance, MAKE SURE that a DHCP server is available on the subnet where you will be installing the AP, and that the subnet has a route back to the Alcatel OmniAccess Switch or Appliance. Also make sure that the route back to the Alcatel OmniAccess Wireless Switch or Appliance has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure the route back to the Primary Alcatel OmniAccess Switch or Appliance allows IP packet fragments. Finally, make sure that if address translation is used, that the AP and the Alcatel OmniAccess Switch or Appliance have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)
  - 6. When you have installed and powered up the AP in its final destination, verify that the LEDs are in the same state they were in at the end of Step 4. If no LEDs are on, the AP is most likely not receiving power. If the LEDs all the LEDs blink sequentially back and forth for more than five minutes, the AP is unable to find its Primary Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance, and make sure the AP and the Alcatel OmniAccess Switch or Appliance are either on the same subnet or that the AP has a route back to its Primary Alcatel OmniAccess Switch or Appliance. Also, if the OmniAccess AP is not on the same subnet as the Alcatel OmniAccess Switch or Appliance, make sure there is a DHCP server on the same subnet as the OmniAccess AP.

After you have prepared all OmniAccess APs, reconfigure the Alcatel OmniAccess Switch or Appliance so it is not the Master. A Master Alcatel OmniAccess Switch or Appliance should only be used for configuring OmniAccess APs and not in a working network.

After completing <u>Step 2: Configuring the OmniAccess AP Before Installation</u> for all OmniAccess APs and OmniAccess 1200R APs, continue with <u>Step 3: Preparing Mounting Locations</u>.

# **Step 3: Preparing Mounting Locations**

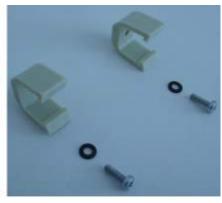
On your map, you should have the OmniAccess AP locations, mounting options, and power options.

- Find the required mounting locations.
- Use the ceiling-mount base to mark the wall or ceiling locations for sheet metal, drywall, or other screws. Make sure you leave enough space around the OmniAccess AP and base to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.

Figure - Factory-Supplied Mounting Options



A. Ceiling-Mount Base



B. Hanging-Ceiling Clips

- Alternatively, attach the hanging ceiling clips to the OmniAccess AP. Make sure you leave enough space around the OmniAccess AP to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.
- Alternatively, use the optional mounting bases and/or brackets to mark the wall or ceiling locations for sheet metal, drywall, or other screws. Make sure you leave enough space around the OmniAccess AP and brackets to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.

Figure - Factory-Orderable Mounting Brackets





A. Projection-Mount Bracket

B. Flush-Mount Bracket 03120303

- If necessary, drill holes for the various cables where they can be mostly hidden from casual view. When you are mounting the OmniAccess AP using an optional separately-orderable projection-mount L-bracket (the one with two long legs), the cables can be routed through the 5/8-inch (15.9 mm) holes in the bracket.
- Route the CAT-5, optional power supply, optional external antenna cable(s), and optional Kensington MicroSaver Security cables to where they can plug into the OmniAccess AP. Make sure to leave about 6 inches (15 cm) of slack in the cables for future modifications.
- Attach the brackets to the wall or ceiling, or install screws for ceiling-mount base:
  - Where you are going to use the projection-mount or flush-mount bracket, use customer-supplied sheet metal, drywall, or other screws to attach the bracket to the ceiling or wall.
  - Where you are going to use the ceiling-mount base, install customer-supplied sheet metal, drywall, or other screws with 1/4 inch (6.35 mm) or smaller heads protruding from the ceiling about 0.1 inch (2.5 mm).

You are now ready to install the OmniAccess APs. Continue with Step 4: Mounting the OmniAccess APs.

# **Step 4: Mounting the OmniAccess APs**

Using the supplied or optional separately-orderable OmniAccess AP mounting kits, mount each Omni-Access AP in its indicated location, oriented as shown on the map. Note that you can mount the OmniAccess APs in the ceiling plenum or below the ceiling, but the OmniAccess APs perform best when mounted below the ceiling.

Note that the Alcatel OmniAccess Wireless System supports Antenna Sectorization, which can be used to increase the number of clients and/or client throughput in a given air space. Installers can mount two OmniAccess APs back-to-back and the Alcatel OmniAccess Wireless System operator can disable the second antenna in both OmniAccess APs to create a 360-degree coverage area with two sectors.

The OmniAccess APs can be mounted in one of three configurations:

- Ceiling Mount Base
- Ceiling-Mount Clips
- Projection Wall Mount
- Flush Wall Mount

## **Ceiling Mount Base**

When you are mounting the OmniAccess AP in the middle of a ceiling (flat sides toward the room or hallway), use the ceiling-mount base to mount the OmniAccess AP as shown in the following figure and as described below:

Figure - Assembling the OmniAccess AP and Ceiling-Mount Base



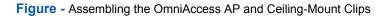
Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.

- Attach the ceiling-mount base to the bottom of the OmniAccess AP using the factory-supplied machine screws and washers.
- Position the ceiling-mount base so its keyhole slots are partly on the drywall, sheet metal, or other screw heads installed in *Step 3: Preparing Mounting Locations*.
- Note: If the screws do not securely hold the ceiling-mount base, remove the OmniAccess AP and adjust the screws until they hold the ceiling-mount base securely.
- Attach the cables to the sides of the OmniAccess AP.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/802.11a LEDs lit), the OmniAccess AP is broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.
- Slide the ceiling-mount base onto the drywall, sheet metal, or other screw heads until it snugs into place.

You have installed the OmniAccess AP. Repeat <u>Step 4: Mounting the OmniAccess APs</u> for each OmniAccess AP location, and then continue with <u>Step 5: Returning MAC Information</u>.

## **Ceiling-Mount Clips**

When you are mounting the OmniAccess AP on the extruded aluminium rails of a hanging ceiling, use the ceiling-mount clips to mount the OmniAccess AP as shown in the following figure and as described below:





- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- Attach the ceiling-mount clips to the bottom of the OmniAccess AP using the factory-supplied machine screws and washers.
- Snap the ceiling-mount clips onto a hanging ceiling rail.





- Attach the cables to the sides of the OmniAccess AP.
- Note: Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP is broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with <u>Step 5: Returning MAC Information</u>.

### **Projection Wall Mount**

When you are mounting the OmniAccess AP out from a wall (flat sides along the wall or hallway), use an optional factory-orderable projection-mount L-bracket.

- Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the OmniAccess AP. Make sure the spring washers have their convex (high center sections) pointing toward the screw heads.
- Note: The OmniAccess AP threaded holes have precision-depth threads. Do not overtighten the screws, or the bracket will not fit under the screw heads.

Figure - Assembling the Mounting Screws and Spring Washers to the OmniAccess AP





A. Screws and Spring Washers

B. Completed Assembly

04022105

- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- You have already attached the projection-mount L-bracket to the wall in <u>Step 3: Preparing</u> Mounting Locations.
- Slide the screws into the keyhole slots on the mounting bracket as shown in the following
- Note: If the screws do not securely hold the bracket, remove the OmniAccess AP and adjust the screws until they securely hold the bracket.

Figure - Assembling the OmniAccess AP to the Projection-Mount Bracket



Attach the cables to the sides of the OmniAccess AP.

- Note: Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP begins broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with Step 5: Returning MAC Information.

### **Flush Wall Mount**

When you are mounting the OmniAccess AP against a wall (flat side toward the inside of the building), use an optional separately-orderable flush-mount bracket.

- Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the OmniAccess AP. Make sure the spring washers have their convex (high center sections) pointing toward the screw heads.
- Note: The OmniAccess AP threaded holes have precision-depth threads. Do not overtighten the screws, or the bracket will not fit under the screw heads.

Figure - Assembling the Mounting Screws and Spring Washers to the OmniAccess AP







B. Completed Assembly

- 04022105
- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- You have already attached the flush-mount bracket to the wall in *Step 3: Preparing Mounting* Locations.
- Slide the screws into the keyhole slots on the mounting bracket as shown in the following figure.
- Note: Make sure the side of the OmniAccess AP with the door is facing away from the wall. This ensures that the correct antenna is facing the building, and makes future upgrades easier.
- Note: If the screws do not securely hold the bracket, remove the OmniAccess AP and adjust the screws until they securely hold the bracket.

Figure - Assembling the OmniAccess AP to the Flush-Mount Bracket



- Attach the cables to the sides of the OmniAccess AP.
- Note: Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP begins broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with <u>Step 5: Returning MAC Information</u>.

## **Step 5: Returning MAC Information**

When you have completed the installations as outlined in <u>Step 4: Mounting the OmniAccess APs</u>, return the MAC addresses and their locations on the maps or floor plans to the network planner or manager. The OmniVista Air Control System Software (ACS Software) operators will use the MAC address and location information to create maps for precise wireless Alcatel Wireless Operating System management.

Also return any unused mounting kit hardware and external power supplies to the network planner or manager for use in future deployments.



**Note:** Please remind the Network Planner or Manager that now is a good time to register the OmniAccess APs at <a href="http://www.alcatel.com/">http://www.alcatel.com/</a>.

## **Planning Notes**

#### **About Cables**

- You will run one CAT-5 Ethernet cable from the OmniAccess AP to the OmniAccess Wireless Switch, another network device, or a PoE injector/hub.
  - When the OmniAccess AP will be mounted below the ceiling using the ceiling mount or wall mount brackets, you may have to drill a hole into the ceiling plenum to run the CAT-5 cable to the wiring closet. When the CAT-5 cable cannot be run through the ceiling plenum, find another path to route the cable from the OmniAccess AP to the wiring closet.
  - When the OmniAccess AP will be mounted above the ceiling using the ceiling mount or wall mount brackets, run the CAT-5 cable to the wiring closet through the ceiling plenum. When the CAT-5 cable cannot be run through the ceiling plenum, find another path to route the cable from the OmniAccess AP to the wiring closet.
- When you are powering the OmniAccess AP from AC power, route the power supply cable from the AC convenience outlet to the OmniAccess AP. Make sure you secure the AC power plug so it will be difficult for people to pull on the power cord or unplug the power supply from the AC power outlet.
- When you are powering the OmniAccess AP from a PoE source (OmniAccess Wireless Switch, another network device, or a PoE injector/hub), you do not need to route a separate power cable to the OmniAccess AP, because the OmniAccess AP will receive its power across the CAT-5 Ethernet cable. Return the power supply to the wireless network planner/manager.

#### **About External Antennas**

- The OAW-1200BG and OAW-1200ABG OmniAccess APs are designed to be used exclusively with the internal high-gain antennas, and have no provisions for external antennas.
- Note: As described in the External-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide, the OAW-1200BG, and OAW-1200ABG OmniAccess APs and OAW-1200ABGR OmniAccess 1200R APs have jacks for external antennas.

### **About Mounting Options**

- Note: Because the OmniAccess AP internal antennas have been designed to reduce inter-floor interference, it is strongly recommended that you mount the OmniAccess AP standing or hanging straight up or down.
- Note: You can mount the OmniAccess APs in the ceiling plenum or below the ceiling using the ceiling mount base or wall mount brackets, but the OmniAccess APs perform best when mounted below the ceiling.
- Note: Plenum-mounted OmniAccess APs and OmniAccess 1200R APs MUST BE powered using Power Over Ethernet (POE) to comply with safety regulations.
  - When you are mounting the OmniAccess AP in the middle of a ceiling, hallway, or ceiling
    plenum, you will typically use the color-coordinated ceiling-mount base to stabilize the
    OmniAccess AP after it is mounted. Use the mounting base to mark the sheet metal, drywall, or
    other screw locations.
    - The mounting base attaches to the bottom of the OmniAccess AP with two supplied screws, and then the assembly slides and locks onto two sheet metal, drywall, or other screws.
  - When you are mounting the OmniAccess AP out from a wall (flat sides along the room or hallway), use the projection-mount L-bracket supplied with the OmniAccess AP. Use the L-bracket to mark the sheet metal, drywall, or other screw locations.

When you are mounting the OmniAccess AP against a wall (flat Side A toward the inside of the building), use the flush-mount bracket supplied with the OmniAccess AP. The flush-mount L-bracket is the one with one long and one short leg. Use the L-bracket to mark the sheet metal, drywall, or other screw locations.

## **About Physical Security**

Regardless of mounting, the OmniAccess AP can be secured with a Kensington MicroSaver Security Cable. If required, use any MicroSaver Security Cable to attach either side of your OmniAccess AP to a solid beam, pipe, or support.

### FCC Statements for OmniAccess APs

This section includes the following FCC statements for the OmniAccess AP:

- Class A Statement
- RF Radiation Hazard Warning
- Non-Modification Statement
- Deployment Statement

#### Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

## **RF Radiation Hazard Warning**

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location such that the antenna of the device will be greater than 20 cm (8 in.) from all persons. Using higher gain antennas and types of antennas not covered under the FCC certification of this product is not allowed.

Installers of the radio and end users of the Alcatel OmniAccess Wireless Enterprise Platform must adhere to the installation instructions provided in this manual.

### **Non-Modification Statement**

Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Unauthorized antennas, modifications, or attachments could damage the badge and could violate FCC regulations and void the user's authority to operate the equipment.



Note: Refer to the Alcatel OmniAccess Wireless System Release Notes for 802.11a external antenna information. Contact Alcatel Internetworking, Inc. for a list of FCC-approved 802.11a and 802.11b/g external antennas.

### **Deployment Statement**

This product is certified for indoor deployment only. Do not install or use this product outdoors.

Notes:

3/17/04 Notes 90-100831-300 Rev 1Alcatel OmniAccess Wireless Access Point Quick Installation Guide 20

## External-Antenna OmniAccess AP Quick Installation Guide

System Release 2.0

This Guide contains several sections allowing you to install an OAW-1200BGE or OAW-1200ABGE Alcatel OmniAccess Wireless Access Point or an OAW-1200ABGR Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R). These models contain internal 802.11a and 802.11b/g antennas and connectors for optional external 802.11a and 802.11b/g antennas.

If you are installing an OAW-1200BG or OAW-1200ABG Alcatel OmniAccess Wireless Access Point with internal 802.11a and 802.11b/g antennas and no connectors for optional external antennas, please refer to the *Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick Installation Guide*.

- Overview
- Step 1: Collecting Required Tools and Supplies
- Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation
- Step 3: Preparing Mounting Locations
- Step 4: Mounting the OmniAccess APs
- Step 5: Returning MAC Information
- <u>Planning Notes</u>
- FCC Statements for OmniAccess APs

## **ATTENTION!**

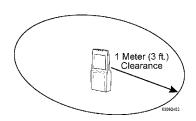
While Alcatel OmniAccess Wireless Access Points have been engineered for easy installation, there are some guidelines that are very important to the end users:

- PLACE Alcatel OmniAccess Wireless Access Points NO MORE THAN 140 FEET APART FROM EACH OTHER. Placing OmniAccess APs further apart almost always results in poor coverage.
- DO NOT MOUNT OmniAccess APs OUTSIDE BUILDINGS.
- DO NOT MOUNT OmniAccess APS ON BUILDING PERIMETER WALLS UNLESS THE OPERATOR WANTS TO PROVIDE COVERAGE OUTSIDE THE BUILDING.
- MAKE SURE that plenum-mounted OmniAccess APs and OmniAccess 1200R APs are powered using Power Over Ethernet (POE) to comply with safety regulations.
- MAKE SURE THAT THE Alcatel OmniAccess Wireless Access
   Points ARE INSTALLED VERTICALLY. Alcatel OmniAccess
   Wireless Access Points ARE DESIGNED TO BE INSTALLED
   VERTICALLY, either standing up in a plenum or hanging from a ceiling, to create the largest coverage area per OmniAccess AP.
   Hanging the OmniAccess AP from the ceiling provides the best RF coverage.

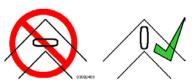




DO NOT MOUNT Alcatel OmniAccess Wireless Access Point ANTENNAS WITHIN ONE METER (3 FT.) OF ANY METAL OBSTRUCTIONS. THE RF WAVES FROM Alcatel OmniAccess Wireless Access Points ARE BLOCKED AND/OR REFLECTED BY METAL OBJECTS, such as metal HVAC ducts, conduit, pipes, bookcases, elevator shafts, stairwells, and metal walls. REFER TO THE <u>Alcatel OmniAccess Wireless Access Point Deployment Guide</u> BEFORE MOUNTING OmniAccess APS NEAR METAL OBSTRUCTIONS.



 WHEN MOUNTING OmniAccess APS IN THE CORNER OF A RIGHT-ANGLE HALLWAY INTERSECTION, MOUNT THE OmniAccess AP AT A 45-DEGREE ANGLE TO THE TWO HALLWAYS. The OmniAccess AP internal antennas are not omnidirectional, and will cover a larger area if mounted this way.



## **Overview**

This guide is designed to provide you with the information needed to mount OAW-1200BGE and OAW-1200ABGE Alcatel OmniAccess Wireless Access Points and OAW-1200ABGR Alcatel OmniAccess Remote Edge Access Points (OmniAccess 1200R APs). OmniAccess APs and OmniAccess 1200R APs are part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System), and require no manual configuration after they are mounted.

This document assumes that a site survey has been performed as described in the <u>Alcatel OmniAccess Wireless Access Point Deployment Guide</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>, that OmniAccess AP and OmniAccess AP 1200R locations and mounting options have been selected, and that you have one OmniAccess AP or OmniAccess AP 1200R per indicated location.

After the site survey is done, you should have a map indicating the following:

- AP and OmniAccess AP 1200R locations.
- AP and OmniAccess AP 1200R mounting options: in the middle of a ceiling/hallway, in the ceiling plenum, projecting away from the wall, or flat against the wall.
- AP and OmniAccess AP 1200R power options: power supplied by the AC-to-DC power supply orderable from the factory, or Power over Ethernet (PoE) from the OmniAccess Wireless Switch, another network device, or a PoE injector/hub (usually located in a wiring closet).
- Note: Plenum-mounted OmniAccess APs and OmniAccess 1200R APs MUST BE powered using Power Over Ethernet (POE) to comply with safety regulations.

If you do not have a map, make one so you can record the MAC addresses from each location and return them to the to the person who is planning or managing this wireless network.

Refer to the following sections to install the OmniAccess APs.

Note: When mounting OmniAccess APs and OmniAccess 1200R APs, make sure to maintain a 20 cm (8 in.) separation between the OmniAccess APs or OmniAccess 1200R APs and bystanders to comply with FCC RF exposure regulations. Refer to the <u>FCC Statements for OmniAccess APs</u> section for more information.

For more details about OmniAccess AP and OmniAccess AP 1200R installations, refer to the <u>Planning Notes</u> section at the end of this document.

# **Step 1: Collecting Required Tools and Supplies**

- One OmniAccess AP or OmniAccess AP 1200R per location.
- OmniAccess AP and OmniAccess AP 1200R Mounting Kits, factory-supplied with each OmniAccess AP.
- Optional OmniAccess AP and OmniAccess AP 1200R Mounting Kits, factory-orderable.
- Optional external AC-to-DC power supplies, factory-orderable.
- Optional external 802.11b/g antennas.
- Note: Refer to the Alcatel OmniAccess Wireless System Release Notes for 802.11a external antenna information. Contact Alcatel Internetworking, Inc. for a list of approved 802.11a and 802.11b/g external antennas.
  - Map showing OmniAccess AP and OmniAccess AP 1200R locations, and mounting and power options.
  - Screwdrivers, drills, and ladder.
  - An assortment of sheet metal and drywall screws and toggle bolts.
  - CAT-5 (or higher) cables to connect the OmniAccess AP and OmniAccess AP 1200R locations and the OmniAccess Wireless Switch or other network device.
  - Optional Kensington MicroSaver Security Cable to secure each OmniAccess AP and OmniAccess AP 1200R.

Continue with Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation.

# Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation

The following procedures are designed to make sure that your OmniAccess AP physical installation goes smoothly and that initial operation is as expected. If you are unable to prepare your OmniAccess AP for deployment, this Step also describes RMA (Return Material Authorization) procedures.

- Note: Perform the following procedure on each OmniAccess AP or OmniAccess AP 1200R BEFORE deploying the OmniAccess AP or OmniAccess AP 1200R in its final location.
  - <u>Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R</u> or <u>Alternate Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R</u> for installation in a Version 2.0 Alcatel OmniAccess Wireless System

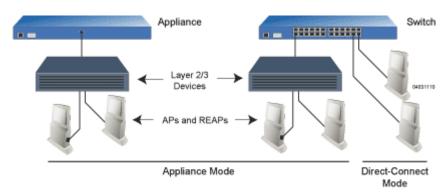
If you are unable to perform this procedure, refer to the <u>RMA Procedures</u> section in the <u>Alcatel Omni-Access Wireless Product Guide</u>.

## Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R

If your OmniAccess AP has Alcatel Wireless Operating System 2.0 or a later version (which includes all OmniAccess 1200R APs) loaded on it, continue with this procedure.

Note: This procedure assumes that you are preparing a version 2.0 OmniAccess AP or OmniAccess AP 1200R to interoperate with a version 2.0 Alcatel OmniAccess Switch or Appliance.

#### **Configuration Setup**



## Does My AP Qualify for this Procedure?

• If your 2.0 or later version later OmniAccess AP(s) or OmniAccess AP 1200R(s) cannot be configured for any reason using the following procedure, refer to <u>RMA Procedures</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

#### Configuration Steps for an OmniAccess AP or OmniAccess AP 1200R

- Configure the Alcatel OmniAccess Switch or Appliance in LWAPP Layer 3 Mode and make sure its DS Port is connected to the network. Use CLI, Web Browser and/or ACS procedures as described in the <u>Alcatel OmniAccess Switch and Appliance Quick Installation Guide</u> and the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- Note: When you are installing a OmniAccess AP 1200R or an OmniAccess AP, a DHCP server must be accessible by the OmniAccess AP 1200R or an OmniAccess AP.

- Make sure AP ports are available (either <u>Direct-Connect Mode</u> through the Switch physical ports, or in <u>Appliance Mode</u> through the Alcatel OmniAccess Switch or Appliance Management/AP-Manager Interface).
- Set the Alcatel OmniAccess Switch or Appliance as the Master, so new OmniAccess APs always associate with it.
- Refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for other settings.
- 2. Take the AP or OmniAccess AP 1200R out of the box and plug it into the front panel of the Master Switch (<u>Direct-Connect Mode</u>), or through the same subnet that Alcatel OmniAccess Switch or Appliance is on (<u>Appliance Mode</u>).
- 3. Apply power to the AP:
  - Use 802.3af-compatible Power Over Ethernet (PoE) from the Alcatel OmniAccess Switch or Appliance or from an orderable inline power injector. If you do not have PoE available, use an orderable external AC-to-48 VDC Power Supply plugged into the side of the AP.
  - After powering up the AP, the RED Alarm LED comes on for a short period (about 15-20 seconds) and then all the LEDs blink sequentially back and forth, indicating that the AP is trying to find an Alcatel OmniAccess Switch or Appliance to connect to. This can continue for up to five minutes. If the AP remains in this mode for more than five minutes, the AP is unable to find the Master Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance and make sure the AP and the Alcatel OmniAccess Switch or Appliance are on the same subnet.
  - If the power light does not come on, check the power (it can be powered either with Power over Ethernet or a from an orderable AP External Power Supply.
  - Make sure that a DHCP server is configured in the Alcatel OmniAccess Switch or Appliance for both the Management Interface and AP-Manager Interface using the CLI, Web Browser, or ACS interface, and that the DHCP server is operating correctly.
  - Once the AP finds the Alcatel OmniAccess Switch or Appliance, it attempts to download
    the new Alcatel Wireless Operating System code if the AP code version differs from the
    Alcatel OmniAccess Switch or Appliance code version. While this is happening, the LEDs
    on the top of the AP blink on and off together.
- 4. Once the Alcatel Wireless Operating System code download is successful, the AP reboots. The GREEN LED turns on and the two YELLOW/AMBER/ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled in the Alcatel Omni-Access Switch or Appliance, the corresponding YELLOW/AMBER/ORANGE LED remains off.
  - Note that the Red LED can light for a short period (10-20 seconds) when the AP reboots. If the RED LED comes on AND STAYS ON for more than a minute, disconnect the AP and call Alcatel Technical Support.
  - From the CLI, Web Browser or ACS interface, configure the AP with its Primary Alcatel OmniAccess Switch or Appliance name as described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - If required, use the CLI, Web Browser or ACS interface to customize the AP-specific 802.11a, 802.11b and 802.11g network settings. Once again, the two YELLOW/AMBER/ ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled, the corresponding YELLOW/AMBER/ORANGE LED remains off.
- 5. If everything works (the GREEN LED is on and the RED LED is off), disconnect the AP and take it to its final destination and install it as described in this document. If your OmniAccess AP fails

this visual test, refer to <u>RMA Procedures</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> to return your OmniAccess APs.

- Note: When you are installing a OmniAccess AP 1200R or a Layer 3 OmniAccess AP on a different subnet than the Alcatel OmniAccess Switch or Appliance, MAKE SURE that a DHCP server is available on the subnet where you will be installing the AP or OmniAccess AP 1200R, and that the subnet has a route back to the Alcatel OmniAccess Switch or Appliance. Also make sure that the route back to the Alcatel OmniAccess Wireless Switch or Appliance has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure the route back to the Primary Alcatel OmniAccess Switch or Appliance allows IP packet fragments. Finally, make sure that if address translation is used, that the AP and the Alcatel OmniAccess Switch or Appliance have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)
- 6. When you have installed and powered up the AP or OmniAccess AP 1200R in its final destination, verify that the LEDs are in the same state they were in at the end of Step 4. If no LEDs are on, the AP or OmniAccess AP 1200R is most likely not receiving power. If all the LEDs blink sequentially back and forth for more than five minutes, the AP is unable to find its Primary Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance are either on the same subnet or that the AP has a route back to its Primary Alcatel OmniAccess Switch or Appliance. Note that the OmniAccess 1200R APs at each remote location must be on the same subnet to allow client roaming. Also, if the OmniAccess AP or OmniAccess AP 1200R is not on the same subnet as the Alcatel OmniAccess Switch or Appliance, make sure there is a DHCP server on the same subnet as the OmniAccess AP or OmniAccess AP 1200R.

After you have prepared all OmniAccess APs, reconfigure the Alcatel OmniAccess Switch or Appliance so it is not the Master. A Master Alcatel OmniAccess Switch or Appliance should only be used for configuring OmniAccess APs and not in a working network.

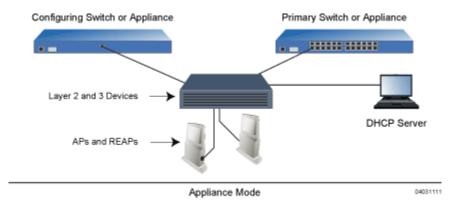
After completing <u>Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation</u> for all OmniAccess APs and OmniAccess 1200R APs, continue with <u>Step 3: Preparing Mounting Locations</u>.

## Alternate Preparing a Version 2.0 OmniAccess AP or OmniAccess AP 1200R

If your OmniAccess AP has Alcatel Wireless Operating System 2.0 or a later version (which includes all OmniAccess 1200R APs) loaded on it, you may choose to use this procedure.

Note: This procedure assumes that you are preparing a version 2.0 OmniAccess AP or OmniAccess AP 1200R to interoperate with a version 2.0 Alcatel OmniAccess Switch or Appliance. It also assumes that your Alcatel OmniAccess Switch or Appliance is already operating in LWAPP Layer 3 Mode. It also assumes that you are using the Internet Software Consortium (ISC) DHCP Server V3.0pl1. Finally, it assumes that if you have deployed multiple Alcatel OmniAccess Switches and Appliances, that the Alcatel OmniAccess Switch or Appliance you use to initialize the OmniAccess AP is in an Alcatel Mobility Group with the Primary Alcatel OmniAccess Switch or Appliance you want to assign to the new OmniAccess AP or OmniAccess AP 1200R.

## **Configuration Setup**



## Does My AP Qualify for this Procedure?

• If your 2.0 or later version later OmniAccess AP(s) or OmniAccess AP 1200R(s) cannot be configured for any reason using the following procedure, refer to <u>RMA Procedures</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## Configuration Steps for an OmniAccess AP or OmniAccess AP 1200R

 Configure the Internet Software Consortium (ISC) V3.0pl1 DHCP Server to provide the vendor-specific Option 43 using the following entries:

```
option controller code 43 = text;
option controller "<Switch IP Address>";
```

in which <switch IP Address> is the IP address of the Alcatel OmniAccess Switch or Appliance you are going to use to prepare the OmniAccess AP or OmniAccess AP 1200R, or which can be a comma-delimited string of Alcatel OmniAccess Switch or Appliance IP addresses.

(These commands direct all unconfigured OmniAccess APs and OmniAccess 1200R APs discovery messages to the configuring Alcatel OmniAccess Switch or Appliance.)

- 2. Make sure the configuring Alcatel OmniAccess Switch or Appliance is in **LWAPP Layer 3 Mode**, that if the configuring Alcatel OmniAccess Switch or Appliance is in the same mobility group as the planned *Primary Alcatel OmniAccess Switch or Appliance*, and that the configuring Alcatel OmniAccess Switch or Appliance's DS Port is connected to the network. Use CLI, Web Browser and/or ACS procedures as described in the *Alcatel OmniAccess Switch and Appliance Quick Installation Guide* and the *Alcatel OmniAccess Wireless Product Guide*.
- Also make sure that the DHCP server is configured in the Alcatel OmniAccess Switch or Appliance for both the Management Interface and AP-Manager Interface using the CLI, Web Browser, or ACS user interface.
- Note: When you are installing a OmniAccess AP 1200R or an OmniAccess AP, a DHCP server must be accessible by the OmniAccess AP 1200R or an OmniAccess AP.
  - 4. Take the AP or OmniAccess AP 1200R out of the box and plug it into the network so that it can request an IP address from the DHCP server.
  - 5. Apply power to the AP:
    - Use 802.3af-compatible Power Over Ethernet (PoE) from the Alcatel OmniAccess Switch
      or Appliance or from an orderable inline power injector. If you do not have PoE
      available, use an orderable external AC-to-48 VDC Power Supply plugged into the side
      of the AP.

- After powering up the AP, the RED Alarm LED comes on for a short period (about 15-20 seconds) and then all the LEDs blink sequentially back and forth, indicating that the AP is trying to find an Alcatel OmniAccess Switch or Appliance to connect to. This can continue for up to five minutes. If the AP remains in this mode for more than five minutes, the AP is unable to find the Master Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance and make sure the AP and the Alcatel OmniAccess Switch or Appliance are on the same subnet.
- If the power light does not come on, check the power (it can be powered either with Power over Ethernet or a from an orderable AP External Power Supply.
- 6. The AP or OmniAccess AP 1200R requests an IP address from the DHCP server, and the DHCP server returns an IP address for the AP or OmniAccess AP 1200R, and also returns the <switch IP Address> of the configuring Alcatel OmniAccess Switch or Appliance.
  - Once the AP or OmniAccess AP 1200R finds the configuring Alcatel OmniAccess Switch or Appliance, it attempts to download the new Alcatel Wireless Operating System code if the AP code version differs from the configuring Alcatel OmniAccess Switch or Appliance code version. While this is happening, the LEDs on the top of the AP or OmniAccess AP 1200R blink on and off together.
- 7. Once the Alcatel Wireless Operating System code download is successful, the AP or OmniAccess AP 1200R reboots. The GREEN LED turns on and the two YELLOW/AMBER/ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled in the configuring Alcatel OmniAccess Switch or Appliance, the corresponding YELLOW/AMBER/ORANGE LED remains off.
  - Note that the Red LED can light for a short period (10-20 seconds) when the AP or OmniAccess AP 1200R reboots. If the RED LED comes on AND STAYS ON for more than a minute, disconnect the AP or OmniAccess AP 1200R and call Alcatel Technical Support.
  - From the CLI, Web Browser or ACS interface, configure the AP with its Primary Alcatel OmniAccess Switch or Appliance name (which can be the name of the configuring Alcatel OmniAccess Switch or Appliance) as described in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - If required, use the CLI, Web Browser or ACS interface to customize the AP- or OmniAccess AP 1200R-specific 802.11a, 802.11b and 802.11g network settings. Once again, the two YELLOW/AMBER/ORANGE LEDs indicate the states of the 802.11a and 802.11b/g networks. If any part of the network is disabled, the corresponding YELLOW/AMBER/ORANGE LED remains off.
- 8. If everything works (the GREEN LED is on and the RED LED is off), reboot the AP or OmniAccess AP 1200R and install it as described in this document. If your OmniAccess AP or OmniAccess AP 1200R fails this visual test, refer to <u>RMA Procedures</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> to return your OmniAccess APs.
- Note: When you are installing a OmniAccess AP 1200R or a Layer 3 OmniAccess AP on a different subnet than the Alcatel OmniAccess Switch or Appliance, MAKE SURE that a DHCP server is available on the subnet where you will be installing the AP or OmniAccess AP 1200R, and that the subnet has a route back to the Primary Alcatel OmniAccess Switch or Appliance. Also make sure that the route back to the Alcatel OmniAccess Wireless Switch or Appliance has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure the route back to the Primary Alcatel OmniAccess Switch or Appliance allows IP packet fragments. Finally, make sure that if address translation is used, that the AP and the Alcatel OmniAccess Switch or Appliance have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

9. When you have installed and powered up the AP or OmniAccess AP 1200R in its final destination, verify that the LEDs are in the same state they were in at the end of Step 7. If no LEDs are on, the AP or OmniAccess AP 1200R is most likely not receiving power. If all the LEDs blink sequentially back and forth for more than five minutes, the AP is unable to find its Primary Alcatel OmniAccess Switch or Appliance. Check the connection between the AP and the Alcatel OmniAccess Switch or Appliance are either on the same subnet or that the AP has a route back to its Primary Alcatel OmniAccess Switch or Appliance. Note that the OmniAccess 1200R APs at each remote location must be on the same subnet to allow client roaming. Also, if the OmniAccess AP or OmniAccess AP 1200R is not on the same subnet as the Alcatel OmniAccess Switch or Appliance, make sure that a DHCP server is accessible on the same subnet as the OmniAccess AP or OmniAccess AP 1200R.

After completing <u>Step 2: Configuring the OmniAccess AP or OmniAccess AP 1200R Before Installation</u> for all OmniAccess APs and OmniAccess 1200R APs, continue with <u>Step 3: Preparing Mounting Locations</u>.

# **Step 3: Preparing Mounting Locations**

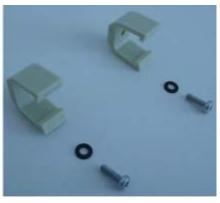
On your map, you should have the OmniAccess AP locations, mounting options, and power options.

- Find the required mounting locations.
- Use the ceiling-mount base to mark the wall or ceiling locations for sheet metal, drywall, or other screws. Make sure you leave enough space around the OmniAccess AP and base to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.

Figure - Factory-Supplied Mounting Options



A. Ceiling-Mount Base



B. Hanging-Ceiling Clips

- Alternatively, attach the hanging ceiling clips to the OmniAccess AP. Make sure you leave enough space around the OmniAccess AP to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.
- Alternatively, use the optional mounting bases and/or brackets to mark the wall or ceiling locations for sheet metal, drywall, or other screws. Make sure you leave enough space around the OmniAccess AP and brackets to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver Security Cable into the sides of the OmniAccess AP.

Figure - Factory-Orderable Mounting Brackets





A. Projection-Mount Bracket

B. Flush-Mount Bracket 03120303

- If necessary, drill holes for the various cables where they can be mostly hidden from casual view. When you are mounting the OmniAccess AP using an optional separately-orderable projection-mount L-bracket (the one with two long legs), the cables can be routed through the 5/8-inch (15.9 mm) holes in the bracket.
- Route the CAT-5, optional power supply, optional external antenna cable(s), and optional Kensington MicroSaver Security cables to where they can plug into the OmniAccess AP. Make sure to leave about 6 inches (15 cm) of slack in the cables for future modifications.
- Attach the brackets to the wall or ceiling, or install screws for ceiling-mount base:
  - Where you are going to use the projection-mount or flush-mount bracket, use customer-supplied sheet metal, drywall, or other screws to attach the bracket to the ceiling or wall.
  - Where you are going to use the ceiling-mount base, install customer-supplied sheet metal, drywall, or other screws with 1/4 inch (6.35 mm) or smaller heads protruding from the ceiling about 0.1 inch (2.5 mm).

You are now ready to install the OmniAccess APs. Continue with Step 4: Mounting the OmniAccess APs.

# **Step 4: Mounting the OmniAccess APs**

Using the supplied or optional separately-orderable OmniAccess AP mounting kits, mount each Omni-Access AP in its indicated location, oriented as shown on the map. Note that you can mount the OmniAccess APs in the ceiling plenum or below the ceiling, but the OmniAccess APs perform best when mounted below the ceiling.

Note that the Alcatel OmniAccess Wireless System supports Antenna Sectorization, which can be used to increase the number of clients and/or client throughput in a given air space. Installers can mount two OmniAccess APs back-to-back and the Alcatel OmniAccess Wireless System operator can disable the second antenna in both OmniAccess APs to create a 360-degree coverage area with two sectors.

The OmniAccess APs can be mounted in one of three configurations:

- Ceiling Mount Base
- <u>Ceiling-Mount Clips</u>
- Projection Wall Mount
- Flush Wall Mount

## **Ceiling Mount Base**

When you are mounting the OmniAccess AP in the middle of a ceiling (flat sides toward the room or hallway), use the ceiling-mount base to mount the OmniAccess AP as shown in the following figure and as described below:



Figure - Assembling the OmniAccess AP and Ceiling-Mount Base

03032002

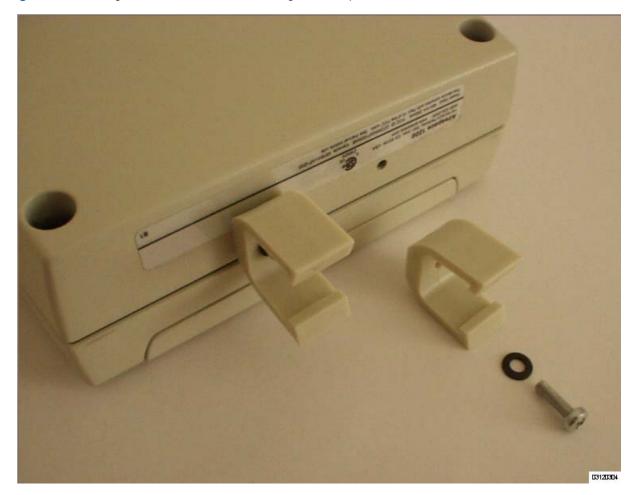
- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- Attach the ceiling-mount base to the bottom of the OmniAccess AP using the factory-supplied machine screws and washers.
- Position the ceiling-mount base so its keyhole slots are partly on the drywall, sheet metal, or other screw heads installed in Step 3: Preparing Mounting Locations.
- Note: If the screws do not securely hold the ceiling-mount base, remove the OmniAccess AP and adjust the screws until they hold the ceiling-mount base securely.
- Attach the cables to the sides of the OmniAccess AP.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP is broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.
  - Slide the ceiling-mount base onto the drywall, sheet metal, or other screw heads until it snugs into place.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with Step 5: Returning MAC Information.

## **Ceiling-Mount Clips**

When you are mounting the OmniAccess AP on the extruded aluminium rails of a hanging ceiling, use the ceiling-mount clips to mount the OmniAccess AP as shown in the following figure and as described below:

Figure - Assembling the OmniAccess AP and Ceiling-Mount Clips



- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- Attach the ceiling-mount clips to the bottom of the OmniAccess AP using the factory-supplied machine screws and washers.
- Snap the ceiling-mount clips onto a hanging ceiling rail.





- Attach the cables to the sides of the OmniAccess AP.
- **Note:** Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP is broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with Step 5: Returning MAC Information.

## **Projection Wall Mount**

When you are mounting the OmniAccess AP out from a wall (flat sides along the wall or hallway), use an optional separately-orderable factory-orderable projection-mount L-bracket.

- Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the OmniAccess AP. Make sure the spring washers have their convex (high center sections) pointing toward the screw heads.
- Note: The OmniAccess AP threaded holes have precision-depth threads. Do not overtighten the screws, or the bracket will not fit under the screw heads.

Figure - Assembling the Mounting Screws and Spring Washers to the OmniAccess AP



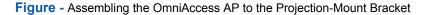


A. Screws and Spring Washers

B. Completed Assembly

04022105

- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- You have already attached the projection-mount L-bracket to the wall in <u>Step 3: Preparing</u> Mounting Locations.
- Slide the screws into the keyhole slots on the mounting bracket as shown in the following
- Note: If the screws do not securely hold the bracket, remove the OmniAccess AP and adjust the screws until they securely hold the bracket.





03032004

- Attach the cables to the sides of the OmniAccess AP.
- Note: Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP begins broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with Step 5: Returning MAC Information.

#### **Flush Wall Mount**

When you are mounting the OmniAccess AP against a wall (flat side toward the inside of the building), use an optional separately-orderable factory-orderable flush-mount bracket.

- Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the OmniAccess AP. Make sure the spring washers have their convex (high center sections) pointing toward the screw heads.
- Note: The OmniAccess AP threaded holes have precision-depth threads. Do not overtighten the screws, or the bracket will not fit under the screw heads.

Figure - Assembling the Mounting Screws and Spring Washers to the OmniAccess AP



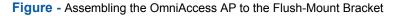


A. Screws and Spring Washers

B. Completed Assembly

04022105

- Copy the MAC address(es) from the label(s) on the OmniAccess AP onto the corresponding location on the map. MAC addresses have the format 000B85xxxxxx.
- You have already attached the flush-mount bracket to the wall in <u>Step 3: Preparing Mounting</u> Locations.
- Slide the screws into the keyhole slots on the mounting bracket as shown in the following
- Note: Make sure the side of the OmniAccess AP with the door is facing away from the wall. This ensures that the correct antenna is facing the building, and makes future upgrades
- Note: If the screws do not securely hold the bracket, remove the OmniAccess AP and adjust the screws until they securely hold the bracket.





03032005

- Attach the cables to the sides of the OmniAccess AP.
- **Note:** Make sure the cables are routed away from the OmniAccess AP antennas.
- Note: When the OmniAccess AP is powered up and is associated with an Alcatel OmniAccess Wireless Switch or Appliance (Green/Power and Yellow/802.11b/g and/or Yellow or Amber/ 802.11a LEDs lit), the OmniAccess AP begins broadcasting its beacon signal(s). When this happens, complete the installation as quickly as possible to remove yourself from within 8 inches (20 cm) of the OmniAccess AP to comply with FCC RF radiation exposure guidelines.

You have installed the OmniAccess AP. Repeat Step 4: Mounting the OmniAccess APs for each Omni-Access AP location, and then continue with Step 5: Returning MAC Information.

# **Step 5: Returning MAC Information**

When you have completed the installations as outlined in <u>Step 4: Mounting the OmniAccess APs</u>, return the MAC addresses and their locations on the maps or floor plans to the network planner or manager. The OmniVista Air Control System Software (ACS Software) operators will use the MAC address and location information to create maps for precise wireless Alcatel Wireless Operating System management.

Also return any unused mounting kit hardware and external power supplies to the network planner or manager for use in future deployments.



**Note:** Please remind the Network Planner or Manager that now is a good time to register the OmniAccess APs at <a href="http://www.alcatel.com/">http://www.alcatel.com/</a>.

# **Planning Notes**

#### **About Cables**

- You will run one CAT-5 Ethernet cable from the OmniAccess AP to the OmniAccess Wireless Switch, another network device, or a PoE injector/hub.
  - When the OmniAccess AP will be mounted below the ceiling using the ceiling mount or wall mount brackets, you may have to drill a hole into the ceiling plenum to run the CAT-5 cable to the wiring closet. When the CAT-5 cable cannot be run through the ceiling plenum, find another path to route the cable from the OmniAccess AP to the wiring closet.
  - When the OmniAccess AP will be mounted above the ceiling using the ceiling mount or wall mount brackets, run the CAT-5 cable to the wiring closet through the ceiling plenum. When the CAT-5 cable cannot be run through the ceiling plenum, find another path to route the cable from the OmniAccess AP to the wiring closet.
- When you are powering the OmniAccess AP from AC power, route the power supply cable from the AC convenience outlet to the OmniAccess AP. Make sure you secure the AC power plug so it will be difficult for people to pull on the power cord or unplug the power supply from the AC power outlet.
- When you are powering the OmniAccess AP from a PoE source (OmniAccess Wireless Switch, another network device, or a PoE injector/hub), you do not need to route a separate power cable to the OmniAccess AP, because the OmniAccess AP will receive its power across the CAT-5 Ethernet cable. Return the power supply to the wireless network planner/manager.

#### **About External Antennas**

- Refer to the <u>OmniAccess AP External and Internal Antennas</u> section in the <u>Alcatel OmniAccess</u> Wireless Product Guide for an overview of the external 802.11a and 802.11b/g external antennas available for use with the OmniAccess APs.
- Note: As described in the <u>Internal-Antenna Alcatel OmniAccess Wireless Access Point Quick</u> Installation Guide, the OAW-1200BG and OAW-1200ABG OmniAccess APs are designed to be used exclusively with the internal high-gain antennas, and have no jacks for external
- Note: Refer to the Alcatel OmniAccess Wireless System Release Notes for 802.11a external antenna information. Contact Alcatel Internetworking, Inc. for a list of FCC-approved 802.11a and 802.11b/g external antennas.
  - When you are attaching external antennas to the (Part Number TBD), OAW-1200BGE, or OAW-1200ABGE OmniAccess AP, use cables with female reverse-TNC connectors to connect antennas to the ports on the side of the OmniAccess AP. See the following figure for antenna port markings.

Figure - OmniAccess AP External Antenna Port Markings



A. 2.4 GHz/802.11b Left External Antenna Port



B. 5 GHz/802.11a and 2.4 GHz/802.11b Right External Antenna Ports

## **About Mounting Options**

- Note: Because the OmniAccess AP internal antennas have been designed to reduce inter-floor interference, it is strongly recommended that you mount the OmniAccess AP standing or hanging straight up or down.
- Note: You can mount the OmniAccess APs in the ceiling plenum or below the ceiling using the ceiling mount base or wall mount brackets, but the OmniAccess APs perform best when mounted below the ceiling.
- Note: Plenum-mounted OmniAccess APs and OmniAccess 1200R APs MUST BE powered using Power Over Ethernet (POE) to comply with safety regulations.
- When you are mounting the OmniAccess AP in the middle of a ceiling, hallway, or ceiling plenum, you will typically use the color-coordinated ceiling-mount base to stabilize the OmniAccess AP after it is mounted. Use the mounting base to mark the sheet metal, drywall, or other screw locations.

The mounting base attaches to the bottom of the OmniAccess AP with two supplied screws, and then the assembly slides and locks onto two sheet metal, drywall, or other screws.

- When you are mounting the OmniAccess AP out from a wall (flat sides along the room or hallway), use the projection-mount L-bracket supplied with the OmniAccess AP. Use the L-bracket to mark the sheet metal, drywall, or other screw locations.
- When you are mounting the OmniAccess AP against a wall (flat Side A toward the inside of the building), use the flush-mount bracket supplied with the OmniAccess AP. The flush-mount L-bracket is the one with one long and one short leg. Use the L-bracket to mark the sheet metal, drywall, or other screw locations.

## **About Physical Security**

Regardless of mounting, the OmniAccess AP can be secured with a Kensington MicroSaver Security Cable. If required, use any MicroSaver Security Cable to attach either side of your OmniAccess AP to a solid beam, pipe, or support.

#### FCC Statements for OmniAccess APs

This section includes the following FCC statements for the OmniAccess AP:

- Class A Statement
- RF Radiation Hazard Warning
- Non-Modification Statement
- Deployment Statement

#### **Class A Statement**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

#### **RF Radiation Hazard Warning**

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location such that the antenna of the device will be greater than 20 cm (8 in.) from all persons. Using higher gain antennas and types of antennas not covered under the FCC certification of this product is not allowed.

Installers of the radio and end users of the Alcatel OmniAccess Wireless Enterprise Platform must adhere to the installation instructions provided in this manual.

#### **Non-Modification Statement**

Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Unauthorized antennas, modifications, or attachments could damage the badge and could violate FCC regulations and void the user's authority to operate the equipment.

## **Deployment Statement**

This product is certified for indoor deployment only. Do not install or use this product outdoors.

# Alcatel OmniAccess Switch and Appliance Quick Installation Guide

System Release 2.0

This Guide contains several sections allowing you to install an Alcatel OmniAccess Wireless Switch or Appliance:

- Overview
- <u>Step 1: Collecting Required Tools and Information</u>
- Step 2: Determining a Location
- Step 3: Installing the Chassis
- Step 4: Connecting and Using the CLI Console
- Step 5: Performing Power On Self Test
- Step 6: Using the Startup Wizard
- Step 7: Logging In
- Step 8: Connecting the Network (Distribution System)
- Step 9: Connecting the Service Port Interfaces
- Step 10: Connecting Access Points
- Step 11: Where to Go from Here

## FCC Statements for Alcatel OmniAccess Switches and Appliances

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Model 4012 and 4024 PoE Alcatel OmniAccess Wireless Switches are only intended for installation in Environment A (same-building deployment) as defined in IEEE 802.3af. All interconnected equipment must be contained within the same building including the interconnected equipment's associated LAN connections.

## **Overview**

This guide is designed to provide you with the information needed to install Alcatel OmniAccess Wireless Switches and Appliances. Model 4012 and 4024 Alcatel OmniAccess Wireless Switches and Model 4102 OmniAccess Wireless Appliances are part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System).

This document assumes that the 802.11 topology has been determined as described in the <u>Direct-Connect Mode</u>, <u>Appliance Mode</u> and <u>Hybrid Mode</u> sections in the <u>Alcatel OmniAccess Wireless Product Guide</u>. Because the <u>OmniVista AirView Software</u> feature automatically detects and configures the Alcatel OmniAccess Wireless Access Points (OmniAccess APs) as they appear on network, it is not necessary to have any OmniAccess APs on the network to install and configure an Alcatel OmniAccess Switches and Appliances.

The Alcatel OmniAccess Switch or Appliance is a slim  $9 \times 5.5 \times 1.5$  in. (22.9 x 14.0 x 3.8 cm) chassis that can be rack, desktop, or shelf mounted. As shown in the following figures, the Alcatel OmniAccess Switch or Appliance is shipped with 19 inch (48.26 cm) EIA rack-mount ears and four rubber desktop/shelf mounting feet.

The following figure shows the 4024 OmniAccess Wireless Switch. The 4012 OmniAccess Wireless Switch is similar, except that it has 12 front-panel 10/100Base-T jacks instead of 24.

Figure - 4024 OmniAccess Wireless Switch



The following figure shows the 4102 OmniAccess Wireless Appliance, which has two front-panel 1000Base-SX connectors.

Figure - 4102 OmniAccess Wireless Appliance



The following figure shows the Alcatel OmniAccess Switch and Appliance network topology and network connections:

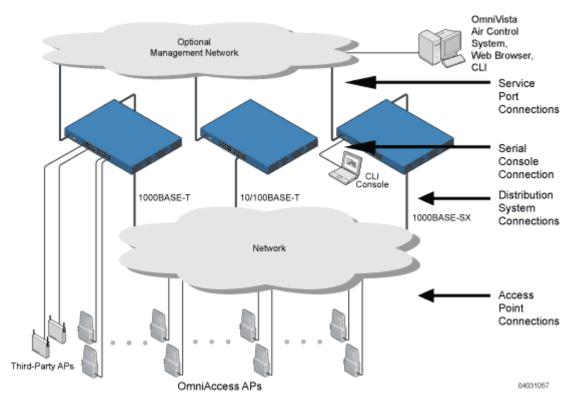
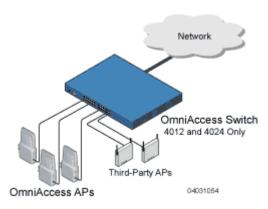


Figure - Typical Alcatel OmniAccess Wireless Switch and Appliance Topology and Network Connections

The 4012 and 4024 Alcatel OmniAccess Wireless Switches can be operated in <u>Direct-Connect Mode</u>, <u>Appliance Mode</u>, or in <u>Hybrid Mode</u>. In Direct-Connect Mode, the OmniAccess Wireless Switch is directly connected to up to 24 (Model 4024) or up to 12 (Model 4012) OmniAccess APs and/or third-party APs over CAT-5 or higher Ethernet cabling. The benefit of this mode is that the OmniAccess Wireless Switch can provide <u>Power Over Ethernet</u>. The following figure shows the OmniAccess Wireless Switch in Direct-Connect Mode.

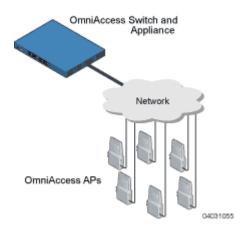
Figure - OmniAccess Wireless Switch Direct-Connect Mode



All 4012 and 4024 Alcatel OmniAccess Wireless Switches and 4102 OmniAccess Wireless Appliances can be operated in <u>Appliance Mode</u>. (The 4012 and 4024 Alcatel OmniAccess Wireless Switches can also be operated in <u>Direct-Connect Mode</u> or <u>Hybrid Mode</u>.) In Appliance Mode, the Alcatel OmniAccess Switch

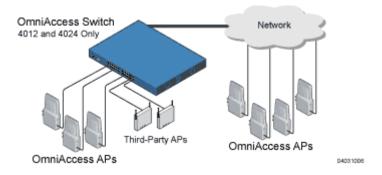
or Appliance communicates indirectly with up to 36 (Model 4102), up to 24 (Model 4024) or up to 12 (Model 4012) associated OmniAccess APs (and/or third-party APs for 4012 or 4024 Alcatel OmniAccess Wireless Switches) through the network. The following figure shows an OmniAccess Wireless Appliance or OmniAccess Wireless Switch in Appliance Mode.

Figure - Alcatel OmniAccess Wireless Switch or Appliance Deployed in Appliance Mode



The 4012 and 4024 Alcatel OmniAccess Wireless Switches can be operated in <u>Hybrid Mode</u>, <u>Appliance Mode</u> or <u>Direct-Connect Mode</u>. In Hybrid Mode, the OmniAccess Wireless Switch communicates directly and indirectly with up to 24 (Model 4024) or up to 12 (Model 4012) associated OmniAccess APs and/or third-party APs over Ethernet cabling, and with associated OmniAccess APs through the network. The following figure shows the OmniAccess Wireless Switch in Hybrid Mode.

Figure - OmniAccess Wireless Switch Deployed in Hybrid Mode



Continue with the following steps to install, configure, and use the Alcatel OmniAccess Switch or Appliance:

- <u>Step 1: Collecting Required Tools and Information</u>
- Step 2: Determining a Location
- Step 3: Installing the Chassis
- Step 4: Connecting and Using the CLI Console
- Step 5: Performing Power On Self Test
- Step 6: Using the Startup Wizard
- <u>Step 7: Logging In</u>

- Step 8: Connecting the Network (Distribution System)
- <u>Step 9: Connecting the Service Port Interfaces</u>
- Step 10: Connecting Access Points
- <u>Step 11: Where to Go from Here</u>

## **Step 1: Collecting Required Tools and Information**

#### **Hardware Installation**

- Alcatel OmniAccess Wireless Switch or Appliance (ships with factory-supplied power cord and mounting hardware).
- Network, Alcatel Wireless Operating System Service network, and Access Point cables, as required.

#### **CLI Console**

- VT-100 terminal emulator on CLI Console laptop or palmtop.
- Null modem serial cable to connect CLI Console and Alcatel OmniAccess Switch or Appliance DB-9 Console port.

#### **Local TFTP Server**

- Required for error-free Alcatel Wireless Operating System software updates. Must be able to access <a href="http://www.alcatel.com/">http://www.alcatel.com/</a>.
- **Note:** The TFTP server cannot run on the same computer as the <u>OmniVista Air Control System Software</u>, because the ACS Software and the TFTP server use the same communication port.

## **Initial System Configuration Information**

- Obtain the following initial configuration parameters from the wireless LAN/network planner:
  - System (Alcatel OmniAccess Switch or Appliance) name.
  - Administrative user name and password. (Default Administrative user name and password are admin and admin, respectively.)
- Note: The <u>Service-Port Interface</u> and <u>Management Interface</u> MUST be on different subnets.
  - <u>Service-Port Interface</u> IP Address configuration protocol (none or DHCP). (Refer to the third figure in the <u>Overview</u> for the Service port location.)
  - If Service port configuration protocol = none, Service Port (front-panel Service port) IP Address and Service Port netmask.
  - <u>Management Interface</u> (DS Port, or Network Interface Port) IP Address. (Refer to the third figure in the <u>Overview</u> for the Distribution System port locations.)
  - Management Interface netmask.
  - Management Interface default router IP address.
  - VLAN identifier, if the Management Interface is assigned to a VLAN, or '0' for an untagged VLAN.
  - Distribution System Physical Port number:
    - \* 4012: 1 12 for front panel or 13 for GigE port
    - \* 4024: 1 -24 for front panel or 25 for GigE port
    - \* 4102: 1 or 2 for the front panel GigE port
  - Enter the IP address of the default DHCP Server that will supply IP Addresses to clients, the Alcatel OmniAccess Switch or Appliance Management Interface, and optionally to the Service Port Interface.
  - Enter the LWAPP Transport Mode, LAYER2 or LAYER3 (refer to <u>Layer 2 and Layer 3</u> <u>Operation</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>).
  - Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.

- Alcatel Mobility Group (RF Group) Name, if required.
- 802.11 Network Name (SSID) for WLAN 1. This is the default SSID that the OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points, or OmniAccess 1200R APs, broadcast when they associate with the Alcatel OmniAccess Switch or Appliance.
- Whether or not to allow Static IP Addresses for clients.
  - \* Yes = more convenient, but lower security (session can be hijacked), clients can supply their own IP Address, better for devices that cannot use DHCP.
  - \* No = less convenient, higher security, clients must DHCP for an IP Address, works well for Windows XP devices.
- When you are configuring a RADIUS server, the server IP address, communication port, and Secret.
- Country Code for this installation. Refer to <u>Configuring the Alcatel OmniAccess Switch</u> <u>or Appliance</u> and <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- Enable or disable the 802.11b network.
- Enable or disable the 802.11a network.
- Enable or disable the 802.11g network.
- Enable or disable *OmniVista AirView Software* (Auto-RF).

Continue with Step 2: Determining a Location.

## **Step 2: Determining a Location**

The compact Alcatel OmniAccess Wireless Switch or Appliance can be installed almost anywhere, but security and reliability concerns can be addressed by installing the Alcatel OmniAccess Switch or Appliance in a secure equipment room or wiring closet.

For maximum reliability, mount the Alcatel OmniAccess Switch or Appliance using the following constraints:

- Make sure you can reach the Alcatel OmniAccess Switch or Appliance and all cables.
- Make sure that water or excessive moisture cannot get into the Alcatel OmniAccess Switch or Appliance.
- Ensure that airflow through the Alcatel OmniAccess Switch or Appliance is not obstructed.
   Leave at least 4 inches clear on both sides of the Alcatel OmniAccess Switch or Appliance chassis
- Verify that the ambient temperature remains between 0 to 40° C (32 to 104° F).
- When a OmniAccess Wireless Switch is to be used in Direct-Connect Mode, make sure it is within 100 m (328 ft.) of the associated OmniAccess APs and third-party APs.
- When the Alcatel OmniAccess Switch or Appliance is to be used in the Appliance Mode, make sure it is within 100 m (328 ft.) to any equipment connected to the 10/100Base-T ports.
- Whether an OmniAccess Wireless Switch is in Direct-Connect Mode or Appliance Mode, make sure it is within 100 m (328 ft.) of equipment connected to the optional 1000Base-T port.
- Whether an Alcatel OmniAccess Switch or Appliance is in Direct-Connect Mode or Appliance Mode, make sure it is within one of the following distances of equipment connected to the optional 1000Base-SX port:
  - 220 m (722 ft.) when using 160 MHz-km rated 62.5/125 µm multimode fiber.
  - 275 m (902 ft.) when using 200 MHz-km rated 62.5/125  $\mu$ m multimode fiber.
  - 400 m (1312 ft.) when using 400 MHz-km rated 50/125 μm multimode fiber.
  - 500 m (1641 ft.) when using 500 MHz-km rated 50/125 μm multimode fiber.



**CAUTION:** DO NOT look at the Fiber Optic connector or cable ends when the transmit laser is activated. You can permanently damage your eyes by looking at the fiber-optic laser beam.

• Ensure that the power cord can reach a 110 or 220 VAC grounded convenience outlet.

Continue with Step 3: Installing the Chassis.

# **Step 3: Installing the Chassis**

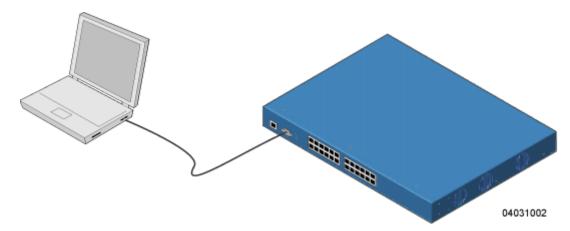
The Alcatel OmniAccess Wireless Switch or Appliance is shipped with rack-mounting ears attached, and the desktop/shelf mounting rubber feet in a separate bag. Mount the Alcatel OmniAccess Switch or Appliance as follows:

- When you are mounting the Alcatel OmniAccess Switch or Appliance on a desktop or shelf, adhere the rubber feet to the bottom of the chassis, and place the chassis on any secure horizontal surface. Note that you may also remove the rack mounting ears from the Alcatel OmniAccess Switch or Appliance, if desired.
- When you are mounting the Alcatel OmniAccess Switch or Appliance in an EIA-standard rack, attach the ears to the equipment rack using the factory-supplied screws. Note that you can remove the rubber feet from the bottom of the Alcatel OmniAccess Switch or Appliance, if desired.

You have installed the Alcatel OmniAccess Switch or Appliance chassis. Continue with <u>Step 4:</u> <u>Connecting and Using the CLI Console</u>.

# **Step 4: Connecting and Using the CLI Console**

For initial system configuration, Alcatel recommends that you use the Command Line Interface Console. As shown in the following figure, the CLI Console connects to the Alcatel OmniAccess Wireless Switch or Appliance front-panel Console port.



Note: You can also use OmniVista Air Control System Software to configure the Alcatel Omni-Access Switch or Appliance, but the ACS Software computer may not be as portable as the CLI Console.

Do the following to connect the CLI Console to the Alcatel OmniAccess Switch or Appliance:

- Use a null-modem serial cable to connect the CLI Console to the Alcatel OmniAccess Switch or Appliance Console port.
  - Note that the Alcatel OmniAccess Switch or Appliance end of the cable is female DB-9. The other end should be whatever plugs into your VT-100 terminal emulator (usually a laptop or palmtop computer).
- Make sure the VT-100 terminal emulator (HyperTerminal, ProComm, minicom, tip, or other) is configured for the following parameters:
  - 9600 baud
  - 8 data bits
  - no flow control
  - 1 stop bit
  - no parity
- Continue with Step 5: Performing Power On Self Test.

# **Step 5: Performing Power On Self Test**

When you plug an Alcatel OmniAccess Wireless Switch or Appliance into an AC power source, the bootup script initializes the system, verifies the hardware configuration, loads its microcode into memory, verifies its Alcatel Wireless Operating System software load, and initializes itself with its stored configurations. Do the following to perform POST and Alcatel Wireless Operating System software initialization:

- Note: This procedure assumes that you have connected the CLI Console to the Alcatel Omni-Access Switch or Appliance as described in <a href="Step 4">Step 4: Connecting and Using the CLI Console</a>.
  - Plug an AC power cord into the rear of the Alcatel OmniAccess Switch or Appliance, and connect the other end to a grounded 95 to 260 VAC 50/60 Hz convenience outlet.
    - Note that Alcatel supplies a North-American standard power cord; if you need a different country-specific cord, make sure the Alcatel OmniAccess Switch or Appliance end of the cord conforms with the IEC 320 standard.
- Note: If you wish to run a previous version of the Alcatel OmniAccess Switch or Appliance code, press the <ESC> key immediately after the Model and S/N line. This will take you to the Bootloader Boot Options Menu.
  - Monitor the Alcatel OmniAccess Switch or Appliance bootup using the CLI Screen:
    - The Bootup script displays Alcatel Wireless Operating System software initialization (code download and POST verification) and basic configuration as shown in the following sample Bootup display:

Press <ESC> now for additional boot options...

(If desired, press <ESC> now to display the Bootloader Boot Options Menu.)

Boot Options

00

Please choose an option from below:

- 1. Run active image (version 2.0.113.3)
- 2. Run backup image (version 2.0.112.0)
- 3. Manually perform system upgrade
- 4. Clear Configuration

Please enter your choice:

(Enter 1 to run the current Alcatel OmniAccess Switch or Appliance Code, enter 2 to run the previous Alcatel OmniAccess Switch or Appliance Code, enter 4 to run the current Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and clear the Alcatel OmniAccess Switch or Appliance Code and C

#### ance configuration to factory defaults. Do not enter 3 unless directed to do so by Alcatel **Technical Support.)**

```
BOOT Uncompressing RTOS Image ... OK
Loading Code at f0100000 ...
Relocating Code to 0785e000, end 07fa649e ... OK
Detecting hardware . .
```

(This may take a long time. Do not reboot the Alcatel OmniAccess Switch or Appliance at this time.)

(The rest of this process takes two to three minutes. Do not reboot the Alcatel OmniAccess Switch or Appliance until you receive the user login prompt.)

```
Software Copyright 2004 Airespace, Inc. All rights reserved.
AWOS Version 2.0.90.3
Checking for new bootloader: Upgrading... ok
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting ARP Services: ok
Starting System Services: ok
Starting Fast Path Hardware Acceleration: ok
Starting Switching Services: ok
Starting QOS Services: ok
Starting Network Interfaces: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting LWAPP: ok
Starting Crypto Accelerator: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Mobility Management: ok
Starting Authentication Engine: ok
Starting Broadcast Services: ok
Starting Power Over Ethernet Services: ok
Starting Logging Services: ok
Starting Management Services:
Web Server: ok
CLI: ok
Secure Web: Web Authentication Certificate not found (error).
Enter User Name (or 'Recover-Config' to reset configuration to factory defaults)
```

#### User:

- If this is the first time an Alcatel OmniAccess Switch or Appliance has been powered up with a factory Alcatel Wireless Operating System software load, or if you enter 'Recover-Config' in the User: prompt, the bootup script runs the Startup Wizard, which prompts you for basic configuration inputs.
- If this is the second or later time you have powered up an Alcatel OmniAccess Switch or Appliance, the bootup script prompts you for a login and password, or enter 'Recover-Config' to reset the Alcatel OmniAccess Switch or Appliance configuration to factory defaults.

In either of the last two cases, the Alcatel OmniAccess Switch or Appliance has passed the POST test.

Continue with <u>Step 6: Using the Startup Wizard</u>.

#### Step 6: Using the Startup Wizard

- The first time you power up the Alcatel OmniAccess Wireless Switch or Appliance with a new factory Alcatel Wireless Operating System software load, use the <u>Startup Wizard</u> to do the following:
- **Note:** Use the information you collected in <u>Step 1: Collecting Required Tools and Information</u> for this Step.
  - Enter the System (Alcatel OmniAccess Switch or Appliance) Name, up to 32 printable ASCII characters.
  - Enter the Administrative User Name and Password, each up to 24 printable ASCII characters. The default Administrative User login and password are admin and admin, respectively.
- **Note:** The <u>Service-Port Interface</u> and <u>Management Interface</u> must be on different subnets.
  - Enter the <u>Service-Port Interface</u> IP configuration protocol (none, or DHCP). If you do not want to use the Service port or if you want to assign a static IP Address to the Service port, enter none.

If you entered **none**, enter <u>Service-Port Interface</u> IP Address and netmask on the next two lines. If you do not want to use the Service port, enter **0.0.0.0** for the IP Address and netmask.

- Enter the Management Interface (refer to <u>Management Interface</u> in the <u>Alcatel</u> <u>OmniAccess Wireless Product Guide</u>) IP Address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier, or '0' for untagged).
- Network Interface (Distribution System) Physical Port number:
  - \* 4012: 1 12 for front panel or 13 for GigE port
  - \* 4024: 1 24 for front panel or 25 for GigE port
  - \* 4102: 1 or 2 for the front panel GigE port
- Enter the IP address of the default DHCP Server that will supply IP Addresses to clients, the Alcatel OmniAccess Switch or Appliance Management Interface, and optionally to the Service Port Interface.
- Enter the LWAPP Transport Mode, LAYER2 or LAYER3 (refer to <u>Layer 2 and Layer 3</u> <u>Operation</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>).
- Enter the Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Enter the <u>Alcatel Mobility Group</u> (RF Group) Name.
- Enter the WLAN 1 SSID, or Network Name. This is the default SSID that the OmniAccess APs and Alcatel OmniAccess Remote Edge Access Points, or OmniAccess 1200R APs, broadcast when they associate with the Alcatel OmniAccess Switch or Appliance.
- Allow or disallow Static IP Addresses for clients. (Yes = clients can supply their own IP Address. No = clients must request an IP Address from a DHCP server.)
- If you are configuring a RADIUS Server now, enter YES, and the RADIUS Server IP Address, communication port, and Secret. Otherwise, enter NO.
- Enter the Country Code for this installation. Type 'help' to list the supported countries, and refer to <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> and <u>Alcatel OmniAccess Wireless System Supported Regulatory Domains</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

- Independently enable and/or disable the 802.11b, 802.11a, and 802.11g OmniAccess AP networks.
- Enable or disable the *OmniVista AirView Software* (Auto RF).

The Alcatel OmniAccess Switch or Appliance saves your configuration, reboots with your changes, and prompts you to log in or enter 'Recover-Config' to repeat this Step.

#### Step 7: Logging In

- Enter a valid login and password to enter the CLI.
- **Note:** The login and password functions are case sensitive. The default Administrative User login and password are admin and admin, respectively.

User:

Password:

The CLI displays the root level system prompt:

>

The system prompt can be any alphanumeric string, up to 31 characters. You can change it using the **config prompt** command. Because this is a user-defined variable, it is omitted from the rest of this documentation.

- The CLI automatically logs you out without saving any changes after five minutes of inactivity. This automatic logout can be set from 0 (never log out) to 160 minutes using the config serial timeout command.
- Refer to the <u>Navigating the CLI</u> and <u>Logging Out of the CLI</u> sections in the <u>Alcatel OmniAccess</u> <u>Wireless Product Guide</u> for more information.

You have logged into the Alcatel OmniAccess Switch or Appliance. Continue with <u>Step 8: Connecting the Network (Distribution System)</u>.

#### **Step 8: Connecting the Network (Distribution System)**

See the following figure for up to three possible connections from the network (Distribution System) to the Alcatel OmniAccess Wireless Switch or Appliance.

- For the 4012 and 4024 OmniAccess Wireless Switch, the three connections are:
  - 1000Base-T (GigE, rear panel, RJ-45 physical port, unshielded twisted pair UTP cable)
  - 10/100Base-T (Ethernet, front panel, RJ-45 physical port, UTP cable)
  - 1000Base-SX (GigE, rear panel, LC physical port, multi-mode fiber optic cable)

For the 4102 OmniAccess Wireless Appliance, the connections are:

• Two (4102) 1000Base-SX (GigE, front panel, LC physical port, multi-mode fiber optic cable)

Depending on the Distribution System physical port to be assigned in <u>Configuring Alcatel OmniAccess Switch and Appliance Interfaces</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>, use Ethernet CAT-5 or higher Ethernet cables or LC compatible fiber optic cable to connect the network equipment to the Alcatel OmniAccess Switch or Appliance.

Figure - External Equipment Connections to the 4012 and 4024 Alcatel OmniAccess Wireless Switches

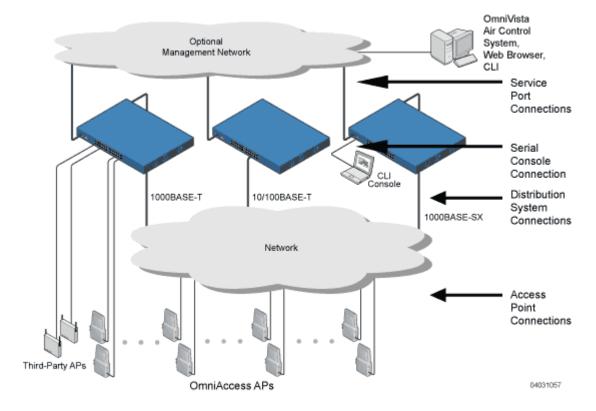
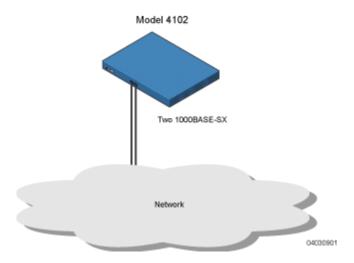


Figure - Physical Network Connections to the 4102 OmniAccess Wireless Appliance



Continue with <u>Step 9: Connecting the Service Port Interfaces</u>.

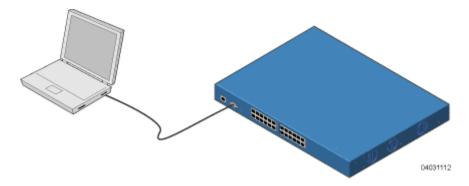
#### **Step 9: Connecting the Service Port Interfaces**

After connecting the network (Distribution System) to the Alcatel OmniAccess Wireless Switch or Appliance as described in <u>Step 8: Connecting the Network (Distribution System)</u>, you can make Alcatel Wireless Operating System OmniVista Air Control System Software, Web Browser, or CLI Console (management interface) connections to the Alcatel OmniAccess Switch or Appliance in one of two ways.

- You can connect any of the OmniVista Air Control System Software, Web Browser, or CLI Console directly to the secure front-panel Service Port.
- You can connect any or all of the OmniVista Air Control System Software, Web Browser, or CLI Console through a dedicated Management Network directly to the front-panel Service port.

Use the following figures to connect the OmniVista Air Control System Software, Web Browser, and/or CLI Console to the Alcatel OmniAccess Switch or Appliance.

• For a front-panel OmniVista Air Control System Software, Web Browser, or CLI Console connection, use Ethernet CAT-5 or higher Ethernet cables to connect the OmniVista Air Control System Software (ACS Software) Server, Web Browser interface, or another CLI Console to the dedicated front-panel Service port.



• For a front-panel OmniVista Air Control System Software, Web Browser, or CLI Console connection, use Ethernet CAT-5 or higher Ethernet cables to connect the Management Network to the front-panel Service Port.

Use the appropriate cables to connect the OmniVista Air Control System Software, Web Browser, or CLI Console to the management network.



Continue with Step 10: Connecting Access Points.

#### **Step 10: Connecting Access Points**

After you have installed and configured the Alcatel OmniAccess Wireless Switch or Appliance, use Ethernet CAT-5 or higher Ethernet cables to connect the OmniAccess APs either to the Alcatel Omni-Access Switch or Appliance front panel 10/100Base-T Ethernet ports or to the network (Distribution System) as shown in the following figures.

Note: As soon as the Alcatel OmniAccess Switch or Appliance is activated, it starts listening for OmniAccess APs and third-party APs on all front-panel Ethernet ports. As it detects APs, it records their MAC addresses in its database. The OmniVista AirView Software function then automatically configures the OmniAccess APs to start transmitting and start allowing clients to connect through the Alcatel OmniAccess Wireless System.

Figure - OmniAccess APs and Third-Party APs Connected to the 4012 and 4024 OmniAccess Wireless Switch Front Panel (Direct-Connect Mode)

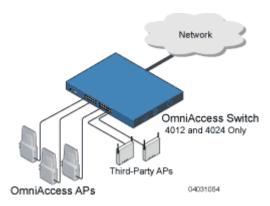
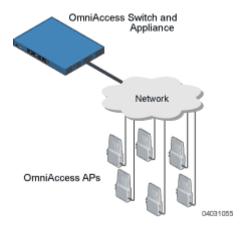


Figure - OmniAccess APs Connected to a 4012, 4024 and 4102 Alcatel OmniAccess Wireless Switch or Appliance Through the Network (Appliance Mode)



Note: The 4012 and 4024 Alcatel OmniAccess Wireless Switches can operate in Direct-Connect Mode and Appliance Mode at the same time. This Hybrid Mode allows a single OmniAccess Wireless Switch to control local and remote OmniAccess APs and third-party APs using the same WLAN(s).

Continue with Step 11: Where to Go from Here.

#### Step 11: Where to Go from Here

You have completely installed the Alcatel OmniAccess Wireless Switch or Appliance hardware.

- Refer to the Alcatel Internetworking, Inc. corporate website at <a href="http://www.alcatel.com/">http://www.alcatel.com/</a> to register your Alcatel OmniAccess Switch or Appliance.
- Refer to the <u>Configuring the Alcatel OmniAccess Switch or Appliance</u> in the <u>Alcatel OmniAccess</u> Wireless Product Guide for more information on configuring the Alcatel OmniAccess Switch or Appliance.
- Refer to the <u>Alcatel OmniAccess Wireless Product Guide</u> for more information on configuring operating, maintaining and troubleshooting the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System).

Notes:

#### **Enhanced Security Module Quick Installation Guide**

System Release 2.0

This guide provides you with the information needed to install and remove Enhanced Security Modules (Crypto cards) in Alcatel OmniAccess Wireless Switches and Appliances. Enhanced Security Modules provide extra processing power to support VPN, IPSec and other processor-intensive security options. This is a factory-orderable and field-installable option for all Alcatel OmniAccess Switches and Appliances.

Proceed with the following to install and remove Enhanced Security Modules in Alcatel OmniAccess Wireless Switches and Appliances:

- <u>Collecting Required Tools and Supplies</u>
- Installing the Enhanced Security Module
- Removing the Enhanced Security Module

#### **Collecting Required Tools and Supplies**

- For installations, one Enhanced Security Module per Alcatel OmniAccess Wireless Switch or Appliance.
- For removals, one Enhanced Security Module slot cover.
- Number 1 Phillips screwdriver.

Continue with *Installing the Enhanced Security Module* or *Removing the Enhanced Security Module*.

#### **Installing the Enhanced Security Module**

Complete the following to install an Enhanced Security Module into the rear panel of an OmniAccess Wireless Switch or Appliance:

Remove power from the Alcatel OmniAccess Wireless Switch or Appliance.



• Locate the slot for the Enhanced Security Module on the rear panel of the Alcatel OmniAccess Wireless Switch or Appliance.



• Using the Phillips screwdriver, remove the cover from the Enhanced Security Module slot by unscrewing the captive screws and sliding it out. Store the Enhanced Security Module slot cover for later use.



- Note the card rails on each side of the Enhanced Security Module slot.
- Note: The metal Enhanced Security Module guide must be installed between and below these rails.



03110805

• Insert the Enhanced Security Module in the slot. Make sure the Enhanced Security Module guide is between and below the slot rails.









04021702

• Gently but firmly press the Enhanced Security Module into the slot until it is firmly seated in the card electrical connector. Use the provided captive screws to secure the Enhanced Security Module to the Alcatel OmniAccess Wireless Switch or Appliance.



• Restore power to restart the Alcatel OmniAccess Wireless Switch or Appliance.



You have installed the Enhanced Security Module in the Alcatel OmniAccess Wireless Switch or Appliance. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Removing the Enhanced Security Module</u>.

#### **Removing the Enhanced Security Module**

Complete the following to remove the Enhanced Security Module from the rear panel of a 4012 or 4024 OmniAccess Wireless Switch:

Remove power from the OmniAccess Wireless Switch.



• Use the Phillips screwdriver to loosen the captive screws that secure the Enhanced Security Module to the rear panel of the OmniAccess Wireless Switch.



- Firmly pull the Enhanced Security Module out of the OmniAccess Wireless Switch.
- Using the Phillips screwdriver, secure the Enhanced Security Module slot cover to the rear of the OmniAccess Wireless Switch.



Restore power to restart the OmniAccess Wireless Switch.



You have removed the Enhanced Security Module from the OmniAccess Wireless Switch. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Installing the Enhanced Security Module</u>.

# 1000Base-SX Network Adapter Module Quick Installation Guide

System Release 2.0

This guide provides you with the information needed to install and remove 1000Base-SX Network Adapter Modules in 4012 and 4024 Alcatel OmniAccess Wireless Switches. 1000Base-SX Network Adapter Modules provide a 100/1000 Mbps wired connection to a network through a fiber-optic link. This is a factory-orderable option for the 4012 and 4024 Alcatel OmniAccess Wireless Switches.

Proceed with the following to install and remove 1000Base-SX Network Adapter Modules in 4012 and 4024 Alcatel OmniAccess Wireless Switches:

- <u>Collecting Required Tools and Supplies</u>
- <u>Installing the 1000Base-SX Network Adapter Module</u>
- Removing the 1000Base-SX Network Adapter Module

## **Collecting Required Tools and Supplies**

- For installations, one 1000Base-SX Network Adapter Module per 4012 or 4024 OmniAccess Wireless Switch.
- For removals, one Network Adapter Module slot cover.
- Number 1 Phillips screwdriver.

Continue with <u>Installing the 1000Base-SX Network Adapter Module</u> or <u>Removing the 1000Base-SX Network Adapter Module</u>.

## Installing the 1000Base-SX Network Adapter Module

Complete the following to install a 1000Base-SX Network Adapter Module into the rear panel of a 4012 or 4024 OmniAccess Wireless Switch:

Remove power from the OmniAccess Wireless Switch.



 Locate the slot for the 1000Base-SX Network Adapter Module on the rear panel of the 4012 or 4024 OmniAccess Wireless Switch.



• Using the Phillips screwdriver, remove the cover from the Network Adapter Module slot. Store the Network Adapter Module slot cover for later use.



- Note the card rails on each side of the Network Adapter Module slot.
- **Note:** The metal Network Adapter Module guide must be installed between and below these rails.



• Insert the 1000Base-SX Network Adapter Module in the slot. Make sure the 1000Base-SX Network Adapter Module guide is between and below the slot rails.









03110808

• Gently but firmly press the 1000Base-SX Network Adapter Module into the slot until it is firmly seated in the card electrical connector. Use the provided screws to secure the Network Adapter Module to the OmniAccess Wireless Switch.



03110812

• Restore power to restart the OmniAccess Wireless Switch.



You have installed the 1000Base-SX Network Adapter Module in the OmniAccess Wireless Switch. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Removing the 1000Base-SX Network Adapter Module</u>.

#### Removing the 1000Base-SX Network Adapter Module

Complete the following to remove the 1000Base-SX Network Adapter Module from the rear panel of a 4012 or 4024 OmniAccess Wireless Switch:

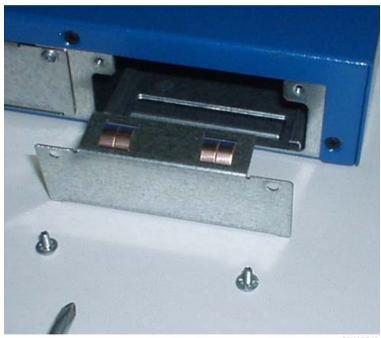
Remove power from the OmniAccess Wireless Switch.



• Use the Phillips screwdriver to remove the screws that secure the 1000Base-SX Network Adapter Module to the rear panel of the OmniAccess Wireless Switch.



- Gently pull the 1000Base-SX Network Adapter Module out of the OmniAccess Wireless Switch.
- Using the Phillips screwdriver, secure the Network Adapter Module slot cover to the rear of the OmniAccess Wireless Switch.



03110813

Restore power to restart the OmniAccess Wireless Switch.



You have removed the 1000Base-SX Network Adapter Module from the OmniAccess Wireless Switch. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Installing the 1000Base-SX Network Adapter Module</u>.

#### 1000Base-T Network Adapter Module Quick Installation Guide

System Release 2.0

This guide provides you with the information needed to install and remove 1000Base-T Network Adapter Modules in 4012 and 4024 Alcatel OmniAccess Wireless Switches. 1000Base-T Network Adapter Modules provide a 100/1000 Mbps wired connection to a network through a fiber-optic link. This is a factory-orderable option for the 4012 and 4024 Alcatel OmniAccess Wireless Switches.

Proceed with the following to install and remove 1000Base-T Network Adapter Modules in 4012 and 4024 Alcatel OmniAccess Wireless Switches:

- Collecting Required Tools and Supplies
- <u>Installing the 1000Base-T Network Adapter Module</u>
- Removing the 1000Base-T Network Adapter Module

## **Collecting Required Tools and Supplies**

- For installations, one 1000Base-T Network Adapter Module per 4012 or 4024 OmniAccess Wireless Switch.
- For removals, one Network Adapter Module slot cover.
- Number 1 Phillips screwdriver.

Continue with <u>Installing the 1000Base-T Network Adapter Module</u> or <u>Removing the 1000Base-T Network Adapter Module</u>.

#### **Installing the 1000Base-T Network Adapter Module**

Complete the following to install a 1000Base-T Network Adapter Module into the rear panel of a 4012 or 4024 OmniAccess Wireless Switch:

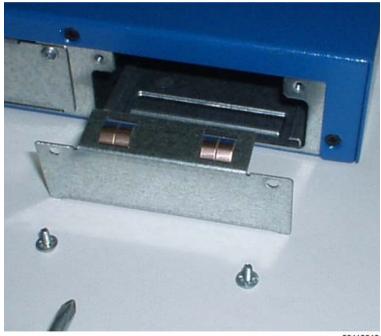
Remove power from the OmniAccess Wireless Switch.



 Locate the slot for the 1000Base-T Network Adapter Module on the rear panel of the 4012 or 4024 OmniAccess Wireless Switch.

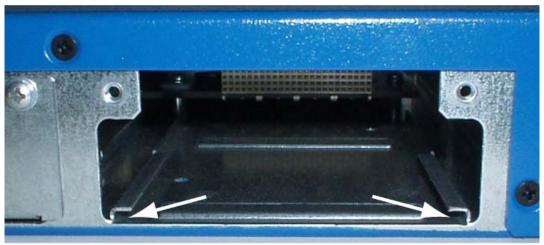


• Using the Phillips screwdriver, remove the cover from the Network Adapter Module slot. Store the Network Adapter Module slot cover for later use.



03110813

- Note the card rails on each side of the Network Adapter Module slot.
- Note: The metal Network Adapter Module guide must be installed between and below these rails.



03110814

Insert the 1000Base-T Network Adapter Module in the slot. Make sure the 1000Base-T Network Adapter Module guide is between and below the slot rails.









 Gently but firmly press the 1000Base-T Network Adapter Module into the slot until it is firmly seated in the card electrical connector. Use the provided screws to secure the Network Adapter Module to the OmniAccess Wireless Switch.



03110815

Restore power to restart the OmniAccess Wireless Switch.



You have installed the 1000Base-T Network Adapter Module in the OmniAccess Wireless Switch. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Removing the 1000Base-T Network Adapter Module</u>.

#### Removing the 1000Base-T Network Adapter Module

Complete the following to remove the 1000Base-T Network Adapter Module from the rear panel of a 4012 or 4024 OmniAccess Wireless Switch:

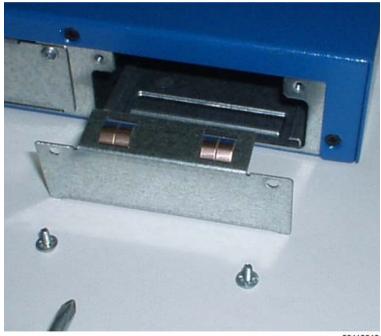
Remove power from the OmniAccess Wireless Switch.



 Use the Phillips screwdriver to remove the screws that secure the 1000Base-T Network Adapter Module to the rear panel of the OmniAccess Wireless Switch.



- Pull the 1000Base-T Network Adapter Module out of the OmniAccess Wireless Switch.
- Using the Phillips screwdriver, secure the Network Adapter Module slot cover to the rear of the OmniAccess Wireless Switch.



03110813

Restore power to restart the OmniAccess Wireless Switch.



You have removed the 1000Base-T Network Adapter Module from the OmniAccess Wireless Switch. Continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>, or refer to <u>Installing the 1000Base-T</u> Network Adapter Module.

#### **ACS Quick Installation Guide**

System Release 2.0

This Guide contains several sections allowing you to install the OmniVista Air Control System Software (ACS):

- <u>Overview</u>
- Step 1: Verifying the Workstation Configuration
- <u>Step 2: Installing Client and Server Software</u>
- Step 3: Starting and Stopping the ACS Software Server
- Step 4: Starting and Stopping an ACS Software Client
- Step 5: Where to Go From Here

## **Overview**

This guide is designed to provide you with the information needed to install the OmniVista Air Control System Software (ACS Software) Server and one or more ACS Software Clients. ACS Software is part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System).

The ACS Software Server runs the Alcatel OmniAccess Wireless System database and serves as an engine for one or more ACS Software Clients, while the ACS Software Clients provide the front end for the ACS Software Server on one or more workstations. The ACS Software Server can be run as a normal Windows application, or can be installed as a service, which operates continuously and resumes operating after a reboot. The following are required for proper operation:

- Requirements for OmniVista Air Control System Software Server Alcatel recommends a
  workstation/server class system: Pentium 4, 2.4 GHz or faster, with 512 MB or more RAM,
  running Windows 2000/SP4 with all critical and security Windows updates installed.
- Requirements for OmniVista Air Control System Software Client The ACS Software Client can run on a Pentium 4 desktop or laptop with 256 MB or more RAM running Windows 2000/SP4 or later, or running Windows XP/SP1 or later and equipped with Internet Explorer 6.0/SP1. Please install all critical and security Windows updates before installing the ACS Software Client.
- Requirements for OmniVista Air Control System Software Client and Server The ACS Software
   Client and the ACS Software Server can be run simultaneously on a workstation/server class
   system: Pentium 4, 2.4 GHz or faster, with 768 MB or more RAM, running Windows 2000/SP4
   with all critical and security Windows updates installed.

Because the ACS Software Client and ACS Software Server are installed on the same workstation, and the ACS Software Client can be installed on a separate workstation, the install script comes in two different .exe files, which ensures an easy install process.

Note that ACS Software uses the following ports:

Port Name	Port Number
RmiPort	1299
HttpPort	80 (can be changed during installation)
HttpsPort	443 (can be changed during installation)
WebContainerPort	8009
DatabasePort	1315
HttpConnectorPort	8456
HttpConnectorRedirectPort	8457
TomcatShutdownPort	8005
TftpPort	69

### Continue with the following steps:

- <u>Step 1: Verifying the Workstation Configuration</u>
- Step 2: Installing Client and Server Software
- Step 3: Starting and Stopping the ACS Software Server
- Step 4: Starting and Stopping an ACS Software Client

Step 5: Where to Go From Here

# **Step 1: Verifying the Workstation Configuration**

- Start your target workstation in Windows 2000 (or Windows XP, if you are installing only the ACS Software Client).
- Use **START/Programs/Windows Update** to display the Windows Update website. Select **Scan For Updates** to list the critical updates and Service Packs you can install on your Windows workstation. Follow the instructions on the website to install all outstanding critical updates and Service Packs on your Windows workstation.
- Select START/Settings/Control Panel.
- Select Add or Remove Programs.
- You are now ready to continue with <u>Step 2: Installing Client and Server Software or Step 3: Starting and Stopping the ACS Software Server</u>.

# **Step 2: Installing Client and Server Software**

When you are installing the ACS Software Client and ACS Software Server on the same workstation, continue with this process:

- Note: If you are reinstalling or updating the ACS Software Client and ACS Software Server, you must uninstall the old version first. Refer to <u>Using the OmniVista Air Control System Software</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u> for instructions.
  - Find the ACS-High-2.0.X.Y-install.exe (High-Accuracy Location ACS) or ACS-basic-2.0.X.Y-install.exe (Low-Resolution Location ACS) file, where 2.0.X.Y is the software build. This file may be found on an ACS CD-ROM.
- Note: For faster installation, you can copy the ACS-High-2.0.X.Y-install.exe or ACS-basic-2.0.X.Y-install.exe file to anywhere on your hard drive.
  - In Windows, navigate to the ACS-High-2.0.X.Y-install.exe OF ACS-basic-2.0.X.Y-install.exe file location.
  - Double-click the ACS-High-2.0.X.Y-install.exe or ACS-basic-2.0.X.Y-install.exe file to start the install script.
    - The install script prepares the install environment, and displays the **Installer** window.
  - In the Installer window, click Next>>.
  - In the Installer window, select the default C:\Program Files\ACS20 (or any other)
    directory. Click Install. The install script copies the ACS Software files to the selected directory
    and verifies them.
  - The Installer window displays the Install ACS as: prompt.
    - When you want to manually launch the ACS Software Server and have it run on the Desktop, select **Windows Application**.
    - When you want the ACS Software Server to launch as a Service at reboot and run in the background (especially useful when the ACS Software Server is to always be online), select Windows Service.

Click **Next>>** to continue installing ACS Software.

- The install script loads the required files into the selected directory and displays the Finished adding ACS to Windows Start Menu message. Click Next.
- The install script completes the installation and displays The installation is complete.
- Select Finished to close down the install script.

You have installed the ACS Software Client and ACS Software Server software on the target machine.

• If you are installing ACS Software <u>for the first time</u>, continue with <u>Step 3: Starting and Stopping the ACS Software Server</u>.

# **Step 3: Starting and Stopping the ACS Software Server**

- Before you can use an ACS Software Client, you must start the ACS Software Server, as described in <u>Starting the ACS Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- After you have closed down all ACS Software Clients (optional), you must shut down the ACS Software Server as described in <u>Stopping the ACS Software Server Application</u> or <u>Stopping the ACS Software Service</u>.

### Starting the ACS Software Server as an Application

When ACS Software has been installed as an application, you can start the ACS Software Server application at any time.

• From the Windows **START** button, select the **Programs** menu, and select **OmniVista Air Control System 2.0/Start ACS Server**.

The start ACS Software Server script opens a **Start ACS Server** DOS window, which displays many Created Table and Process Started messages.

When the **Start ACS Software Server** window displays the Please connect your client to the web server on port 80 message, the ACS Software Server has started and is ready to host ACS Software Clients.



**CAUTION:** The ACS Software Server may display **Start ACS Software Server** and **Apache** DOS windows, which you can minimize. DO NOT CLOSE either of these windows, or you can abnormally halt the ACS Software Server. When you plan to shut down the ACS Software Server, refer to <u>Stopping the ACS Software Server Application</u>.

If desired, continue with the <u>Step 4: Starting and Stopping an ACS Software Client</u> or <u>Using the OmniVista Air Control System Software</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

### Starting the ACS Software Server as a Service

After ACS Software has been installed as a service, you can start the ACS Software service at any time.

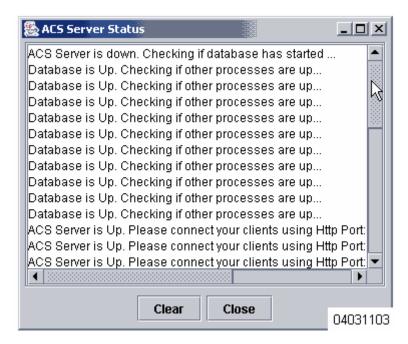
From the Windows START button, select the **Programs** menu, and select **OmniVista Air Control System 2.0/Start ACS Service**.

The start ACS Software Server script opens a **Start ACS Service** DOS window, which displays the following messages:

```
The ACS Software2.0 service is starting.... (in the background)
The ACS Software2.0 service was started successfully.

Launching Server Status Window
```

When the **Start ACS Software** window displays the Launching Server Status Window message, the ACS Software service has started and is ready to host ACS Software Clients. You can close the **Start ACS Service** DOS window, and view the current ACS Software Server status in the **ACS Server Status** window.



Note that the **ACS Software Server Status** window is updated about every five seconds. When the **ACS Software Server Status** window displays the ACS Software Server is Up message, the ACS Software service is ready to host ACS Software Clients.

Note: You can close the ACS Software Server Status window at any time, if you wish. When you want to view the current ACS Software status, from the Windows START button, select the Programs menu, and select OmniVista Air Control System Software 2.0/Check Server Status to view the ACS Software Server Status window again.

If desired, continue with the <u>Step 4: Starting and Stopping an ACS Software Client</u> or <u>Using the OmniVista Air Control System Software</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

### **Stopping the ACS Software Server Application**

You can stop the ACS Software Server application at any time.

- Note: If there are any ACS Software Clients logged in when you stop the Server, the ACS Software Client sessions will stop functioning.
  - From the Windows START button, select the Programs menu, and select OmniVista Air Control System 2.0/Stop ACS Server.
  - The Stop ACS Software Server window displays the Press any key to continue prompt.
  - Press any key to complete the stop ACS Software Server script.

You have shut down the ACS Software Server application. If desired, continue with the <u>Alcatel Omni-Access Wireless Product Guide</u>.

### **Stopping the ACS Software Service**

You can stop the ACS Software service at any time.

Note: If there are any ACS Software Clients logged in when you stop the Server, the ACS Software Client sessions will stop functioning.

 From the Windows START button, select the Programs menu, and select OmniVista Air Control System 2.0/Stop ACS Software Service.

The stop ACS Software Server script opens a **Stop ACS Service** DOS window and halts the ACS Software service.

You have shut down the ACS Software service. If desired, continue with the <u>Alcatel OmniAccess</u> <u>Wireless Product Guide</u>.

# **Step 4: Starting and Stopping an ACS Software Client**

Once you have an ACS Software Server started as described in <u>Step 3: Starting and Stopping the ACS Software Server</u>, starting and stopping an ACS Software Client are simple tasks. Continue with:

- <u>Starting an ACS Software Browser Client</u> This ACS interface is used by ACS operators as
  described in <u>ACS Software Browser Client</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- <u>Starting an ACS Software Java Admin Client</u> This ACS interface is used by ACS system administrators as described in <u>ACS Software Java Admin Client</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
- Stopping an ACS Software Browser Client.
- Stopping an ACS Software Java Admin Client.

### **Starting an ACS Software Browser Client**

- If not already done, start the ACS Software Server as described in the <u>Starting the ACS</u> <u>Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- Launch an Internet Explorer 6.0 (or other Web Browser).
- Note: Some documented features may not function properly if you choose to use any Web Browser other than Internet Explorer 6.0.
  - In the Web Browser address field, access the ACS Software Browser Client on port 80 by entering:

http://<localhost ACS Software Server IP Address>

where localhost is used when the ACS Software Server is on the same workstation as the ACS Software Client, and where <acs software Server IP Address> is the IP Address of the ACS Software Server on any workstation.

The ACS Software Server displays the **ACS Login** window.



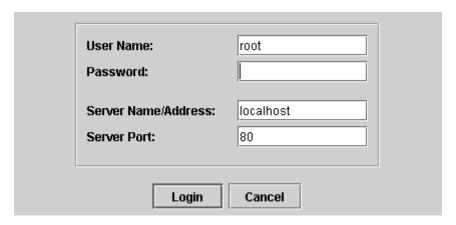
- In the ACS Login window, enter the following:
  - User Name: Your username (default root).
  - Password: Your password (default public).
- When you have made these entries in the ACS Login window, click Submit.

The ACS Software Browser Client is now active and available for your use. Continue with <u>Step 5: Where to Go From Here</u>.

### **Starting an ACS Software Java Admin Client**

- If not already done, start the ACS Software Server as described in the <u>Starting the ACS</u> <u>Software Server as an Application</u> or <u>Starting the ACS Software Server as a Service</u>.
- From the Windows START button, select the **Programs** menu, and then select **OmniVista Air Control System Software 2.0/Start ACS Client Application**.

The Start ACS Software Application script opens the **OmniVista Air Control System Login Dialog** window.



04031104

- In the OmniVista Air Control System Software Login Dialog window, enter the following:
  - User Name: Superuser username (default **Super1**).
  - Password: Superuser password (default **Super1**).
  - Server Name/Address: localhost, or <hostname> or IP Address if the ACS Software Server is on a remote workstation.
  - Port: Leave as 80.
- When you have made these entries, click Login to connect your ACS Software Client to the ACS Software Server and have your ACS Software Client display the OmniVista Air Control System Release 2.0 window.

The ACS Software Java Admin Client is now active and available for your use. Continue with <u>Step 5:</u> <u>Where to Go From Here</u>.

## **Stopping an ACS Software Browser Client**

### **Manually Stopping the Client**

When you are finished working in the ACS Software Browser Client application, exit the ACS
Software Browser Client application window by clicking **Logout** in the upper right corner of the
ACS Software Browser Client window. The ACS Software Server displays the **ACS Login**window.

Note that you can return to the previous cached screen in the Web Browser. However, if you attempt to access any of the parameters in that screen, you are returned to the **ACS Login** window.

Alternatively, you can shut down the Web Browser.

The ACS Software Client window shuts down, leaving the ACS Software Server running. If desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

### **ACS Software Server Shutdown Stopping the Client**

Occasionally, the system administrator may stop the ACS Software Server while an ACS Software Browser Client is logged in. Should this happen, the Web Browser displays a The page cannot be displayed message.



**Note:** When the ACS Software Browser Client has been stopped by an ACS Software Server shutdown, it does not reassociate with the ACS Software Server when the Server restarts. You must restart the ACS Software Browser Client as described in <u>Starting an ACS Software</u> Browser Client.

If desired, continue with the Alcatel OmniAccess Wireless Product Guide.

#### **Stopping an ACS Software Java Admin Client**

### **Manually Stopping the Client**

When you are finished working in the ACS Software Java Admin Client application, exit the ACS Software Java Admin Client application window by clicking **Logout.** The ACS Software Server displays the **ACS Login** window.

Note that you can return to the previous cached screen in the Web Browser. However, if you attempt to access any of the parameters in that screen, you are returned to the **ACS Login** window.

Alternatively, you can shut down the Web Browser.

The ACS Software Java Admin Client window shuts down, leaving the ACS Software Server running. If desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

### **ACS Software Server Shutdown Stopping the Client**

Occasionally, the system administrator may stop the ACS Software Server while an ACS Software Java Admin Client is logged in. Should this happen, the Web Browser displays a  $\[Delta]$  the  $\[Delta]$  cannot be displayed message.



**Note:** When the ACS Software Java Admin Client has been stopped by an ACS Software Server shutdown, it does not reassociate with ACS Software Server the Server restarts. You must restart the ACS Software Java Admin Client as described in <u>Starting an ACS Software Java Admin Client</u>.

If desired, continue with the Alcatel OmniAccess Wireless Product Guide.

# **Step 5: Where to Go From Here**

Continue with the <u>Using the OmniVista Air Control System Software</u> section in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# **ACS Floor Plan Editor Quick Installation Guide**

System Release 2.0

This guide provides you with the information needed to install and use the ACS Floor Plan Editor. The ACS Floor Plan Editor is part of the innovative Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System).

As described more fully in the <u>Alcatel OmniAccess Wireless Product Guide</u>, the ACS Floor Plan Editor takes rasterized bitmapped floor plan maps and converts them to vectorized .FPE wall files. You can then define the wall attenuation characteristics, and import the resulting .FPE files into the ACS database for more accurate RF prediction heatmaps.

 Requirements for the ACS Floor Plan Editor Software – Alcatel recommends any Windows 2000, Windows XP or later operating system running on a 300 MHz or faster workstation.

Continue with the following to install and start the ACS Floor Plan Editor:

- <u>Installing the ACS Floor Plan Editor</u>
- Starting the ACS Floor Plan Editor
- <u>Using the ACS Floor Plan Editor</u>
- Shutting Down the ACS Floor Plan Editor

# **Installing the ACS Floor Plan Editor**

The ACS Floor Plan Editor is distributed on the ACS CD-ROM, and requires a separate installation, typically on an operator workstation. Continue with the following to install and start the ACS Floor Plan Editor:

- 1. Find the Alcatel-FPE-2.9.exe file, where 2.9 is the software build. This file may be found on the Alcatel Web server or on an ACS CD-ROM.
- Note: For faster installation, you can copy the Alcatel-FPE-2.9.exe file to anywhere on your hard drive.
  - 2. In Windows, navigate to the Alcatel-FPE-2.9.exe file location.
  - 3. Double-click the Alcatel-FPE-2.9.exe file to start the install script.
  - 4. The install script prepares the install environment, and displays the **Welcome** window.
  - In the Welcome window, click Next> to have the Installer display the Choose Destination Location window.
  - In the Choose Destination Location window, select the default C:\Program Files\Alcatel (or any other) directory. Click Next> to have the Installer display the Select Program Manager Group window.
  - 7. In the Select Program Manager Group window, select the default Alcatel (or any other) program manager group. Click **Next>** to have the Installer display the **Start Installation** window.
  - 8. In the Start Installation window, click **Next>** to have the Installer load the ACS Floor Plan Editor in the selected directory, and display the **Installation Complete** window.
  - 9. In the Installation Complete window, click the **Finish** button to exit from the Installer.

You have installed the ACS Floor Plan Editor software on the target workstation. Continue with <u>Starting</u> <u>the ACS Floor Plan Editor</u>.

# **Starting the ACS Floor Plan Editor**

After you have installed the ACS Floor Plan Editor, start it by double-clicking the DocRdr.exe desktop icon, by selecting the ACS Floor Plan Editor application in the Start menu, or by double-clicking the AlcatelFPE.exe icon in the Floor Plan Editor directory.

 From the Windows START button, select the Programs menu, and then select Floor Plan Editor/AlcatelFPE.

The Start Alcatel FPE script opens the Alcatel FPE application window.

The Alcatel FPE application is now active and available for your use. Continue with <u>Using the ACS Floor Plan Editor</u>.

Þ

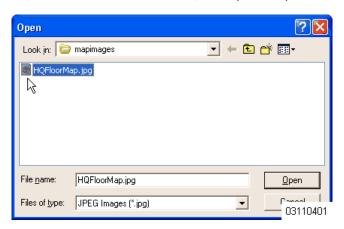
**Note:** Instead of using the ACS Floor Plan Editor as described in the <u>Using the ACS Floor Plan Editor</u> section, you can create a vectorized floor plan by drawing it directly in the ACS Floor Plan Editor. This may save some steps if you do not already have a bitmapped floor plan graphic.

Continue with *Using the ACS Floor Plan Editor*.

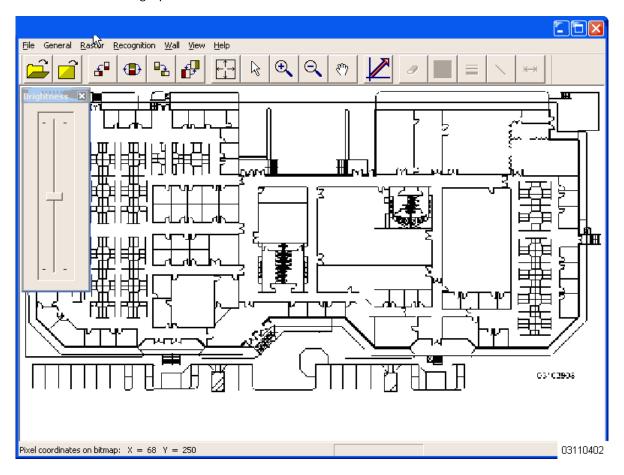
# **Using the ACS Floor Plan Editor**

Once you have started the ACS Floor Plan Editor, use it to convert bitmapped floor plan graphics to .FPE format as follows:

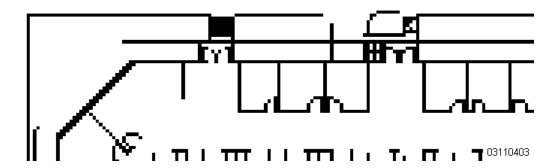
1. Open a bitmapped (.BMP, .TIFF, .JPEG, or .PNG) floor plan map.



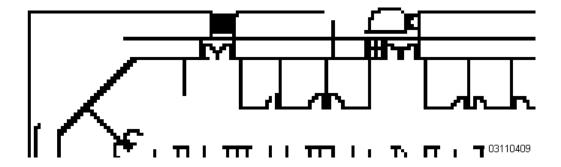
The ACS Floor Plan Editor displays the bitmap file in its main window, with the **Brightness** slider over the graphic for JPG files.



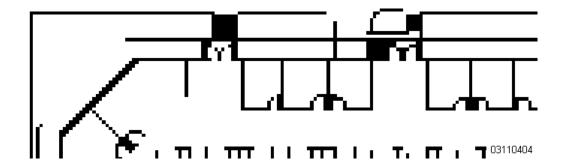
- 2. Clean up the graphic as desired.
- Note: All doors that are normally open and clear windows should be removed from the bitmap. Colored and/or tinted windows can remain in the graphic, as well as doors that are normally closed. Reduce all walls to one pixel width to make cleaner vector graphics.
  - Use the **Brightness** slider to add or remove bitmap detail.



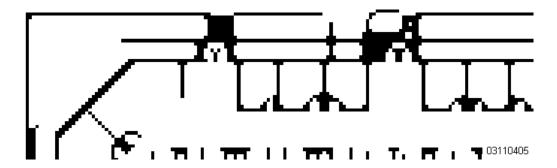
- Use the **Raster/Connect** command to fill in gaps between line segments.



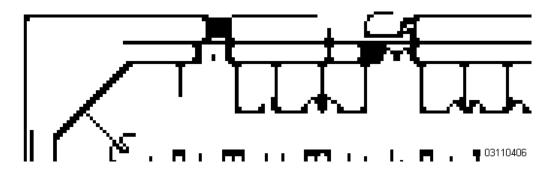
- Use the **Raster/Fill Small Holes** (F7) command to fill in gaps between line segments.



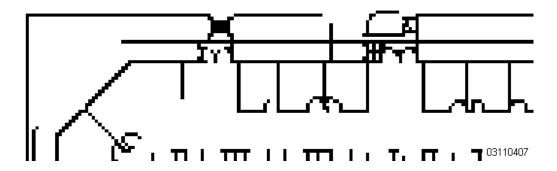
- Use the **Raster/Fill Holes** (F8) command to fill in large gaps between line segments.



- Use the **Raster/Clean** (F9) command to clean up graphics with many unnecessary dots and other marks.



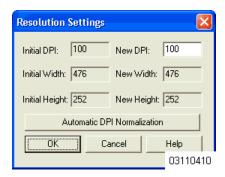
- Use the **Raster/Thin** (F10) command to make line segments the same thin width.



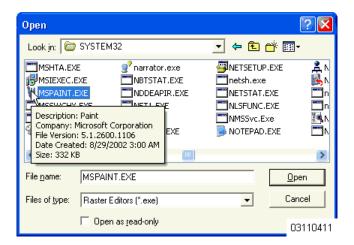
- Use the **Raster/Thicken** (F11) command to fill in gaps between line segments.



Use the Raster/Resolution command to change the resolution, width, and/or height using the Resolution Settings dialog.



Use the Raster/External Editor/Select command to select an external editor, such as Microsoft Paint.

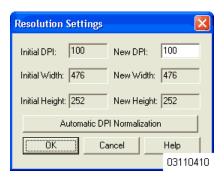


Then, use Raster/External Editor/Run command to use a selected external editor, such as Microsoft Paint to modify the map graphic. Use Save and Exit to return to the ACS Floor Plan Editor.

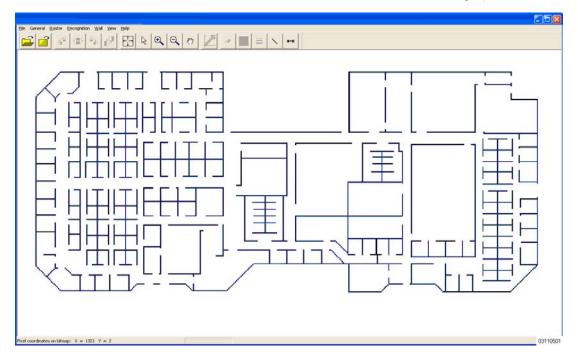
Use any other commands, as required, to clean up the bitmap graphic.

When you are done with the bitmap graphic cleanup, you should have a one-pixel wide outline of all walls, including doors, tinted and/or colored windows, and metal-lined cubicle walls. Any doors that are normally open and clear windows should be removed from the bitmap.

 Use the Raster/Resolution command to select Automatic DPI Normalization between 100 and 400 dpi.

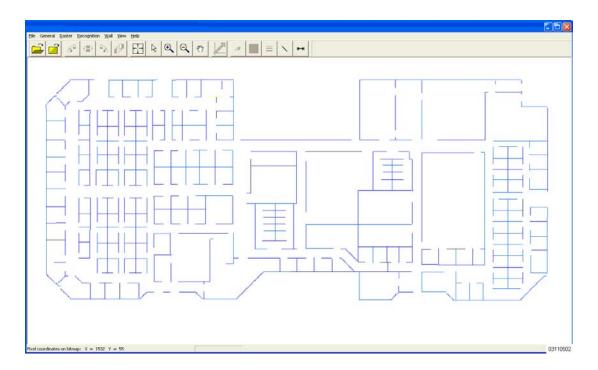


4. After you are done cleaning up the floor plan graphic and applying **Automatic DPI Normalization**, use the **Recognition/Vectorize** (F12) command to vectorize the graphic.



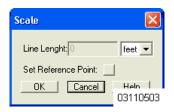
The ACS Floor Plan Editor overlays the modified bitmapped graphic with blue wall lines. You are going to edit these wall lines in the next step.

5. Use the **View/Show Raster** (R) command to toggle the bitmap background on and off to make editing easier.

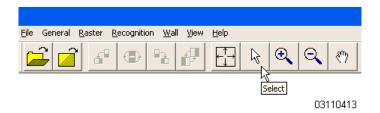


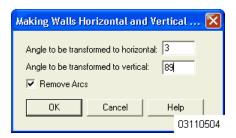
### 6. Scale your wall graphic:

A. Use the **Wall/Scale** command to display the **Scale** dialog box.

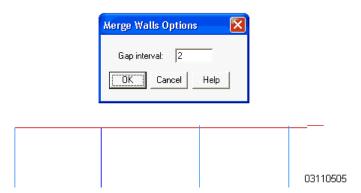


- B. On the wall graphic, draw a reference wall of known length (a long wall works best).
- C. In the **Scale** dialog box, enter the length of the reference wall.
- D. Click **OK** to apply the scale to the wall graphic. The ACS Floor Plan Editor closes the **Scale** dialog box and erases the reference wall.
- 7. Clean up any broken or misaligned walls:
  - If your walls are at right angles to each other, you can use the **Select** tool to select a wall or walls, and then use the **Wall/Horizontalizing** command to display the **Making Walls Horizontal and Vertical** dialog box. In the **Making Walls Horizontal and Vertical** dialog box, start with a shallow angle (3 degrees or less) for lines to be snapped to the horizontal, and another shallow angle (87 degrees or more) for lines to be snapped to the vertical. Click **OK** to snap the selected walls to the horizontal and the vertical. If the selected walls do not all snap to the horizontal and the vertical, try again with less shallow angles (3 degrees or more, or 96 degrees or less).

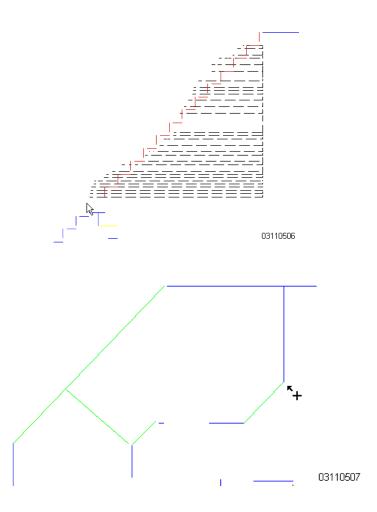




If your walls are broken, select all of the wall segments and use the **Wall/Merge Walls** command to display the **Merge Walls Options** dialog box. In the **Merge Walls Options** dialog box, start with a Gap Interval of 2 pixels, and click OK to merge the wall segments. If the selected wall segments do not merge, try again with a larger Gap Interval (3 or more pixels).



- If your walls are not on the horizontal or vertical axes, they may appear as broken lines. If so, use the **Select** tool to select the wall segments, and click **Delete** to delete the line segments. After you remove the line segments, use the **Add Wall** tool to add unbroken lines.



- 8. Define the RF characteristics of each wall on the floor plan:
  - A. Use the **Select** tool to select a wall or walls.
  - B. Use the **Select Wall Type** tool to assign characteristics to the selected wall:

Heavy Wall for metal and concrete walls and external building walls.

**Light Wall** for sheetrock/drywall walls, regardless if they are made with metal or wood studs.

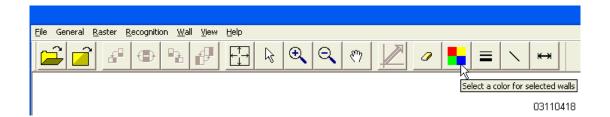
**Heavy Door** for metal doors.

**Light Door** for wood or composite doors.

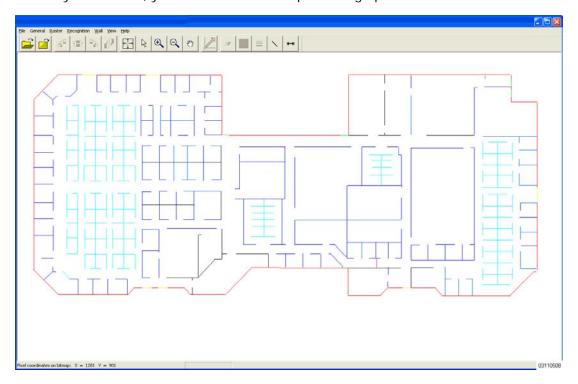
**Cubicle** for cubicle walls constructed with metal or foil sheets. Note that you can eliminate cubicle walls with no metal or foil sheets, and those cubicle walls under four feet (120 cm) tall.

**Glass** for tinted, colored and/or leaded glass. Note that you can eliminate segments that include clear, unleaded glass.

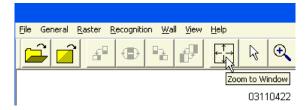
**Perimeter** for building exterior walls.



When you are done, you should have a floor plan wall graphic that looks similar the following:



- 9. If necessary, use the following Editing Tools to clean up the wall graphic:
  - Use the **Zoom to Window** tool to resize the wall graphic to the ACS Floor Plan Editor window.



- Use the **Zoom In** tool to zoom in on a selected area.



- Use the **Zoom Out** tool to zoom out on a selected area.



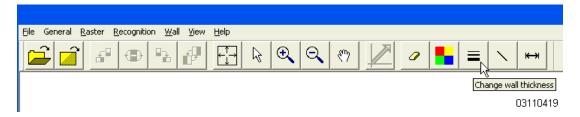
- Use the **Drag** tool to drag the graphic around in the ACS Floor Plan Editor window.



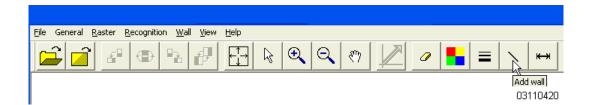
- After selecting a wall or walls, use the **Delete Selected Walls** tool to delete the wall(s).



- Use the **Change Wall Thickness** tool to change a selected wall's thickness.



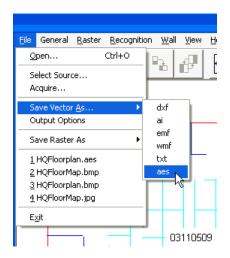
The **Add Wall** tool to add a straight wall.



- Use the **Measure Wall** tool to measure an existing wall segment.



10. When you are done, save the wall graphic as a .FPE file:



If desired, continue with the <u>Alcatel OmniAccess Wireless Product Guide</u>.

# **Shutting Down the ACS Floor Plan Editor**

Use the File/Exit or the Alt-F4 command to exit the ACS Floor Plan Editor.

Notes:

# **Alcatel Site Survey Tool User Guide**

System Release 2.0

Welcome to the Ultimate Site Survey Tool for the Wireless LAN. This User Guide explains how to setup and operate Alcatel Site Survey Tool software on Windows XP and 2000.

This User Guide consists of the following sections:

- <u>BEFORE YOU BEGIN</u>
- Getting Started
- Alcatel Client
- <u>Using Alcatel Client</u>
- Site Survey Tool User Interface
- Recording Data with the Site Survey Tool
- Analysis Features
- The Basics of Site Survey
- Site Survey Guidelines
- <u>Upgrading a License</u>
- <u>Troubleshooting</u>

## **BEFORE YOU BEGIN**

Alcatel Site Survey Tool software is a portable engineering tool for measuring and monitoring the air interface of Wireless Local Area Networks (IEEE 802.11). With Alcatel Site Survey Tool, you can quickly:

- Visualize the network coverage and other survey results with multi-color maps.
- Plan new wireless networks with single or multiple access points.
- Pinpoint locations where the network coverage is not optimal.
- Pinpoint your own access points and unknown access point locations.
- Find areas with channel interference.
- Find the optimal location and channel for new or existing access point.

The Alcatel Site Survey Tool collects real network data and stores it in a survey project. Survey visualizations provide useful information for network verification, tuning, and maintenance. The different visualizations can be easily viewed within the Site Survey Tool and exported for reporting.

Alcatel Site Survey Tool can be used with or without a map image (BMP, JPG, or PNG). If a map image is not available, the map features cannot be used. However, you can use the Signals Tab and Survey Charts to perform quick site surveys without a map image.

The Alcatel Site Survey Tool will from here on be referred to as the Site Survey Tool.

## **Site Survey Goals**

The goal of a site survey is to make sure that the number, placement, and channel configuration of your access points provide required network quality for the end user throughout the facility. In most implementations, "required quality" means a minimum data transfer rate. A site survey also detects the presence of radio interference coming from other sources that could degrade the network performance.

### **Supported Network Standards**

The supported network standards are IEEE 802.11a and IEEE 802.11b.

- Note: The IEEE 802.11a and IEEE 802.11b standards are measured separately.
- Note: The Site Survey Tool includes limited support for 802.11g networks. Based on the backward compatibility, 802.11g access points are displayed and treated as 802.11b access. When surveying with the 802.11g adapter, the following visualizations may not be displayed correctly:
  - Signal-to-Noise Ratio
  - Interference
  - Signals at Channel
  - Access Points Placement Tip
  - Transmission Speed

There are no overlapping channels that could cause channel interference in the 802.11a standard. Thus 802.11a interference is calculated only if there are two access points operating in the same space on the same channel.

## **Survey Safety**

Do not carelessly walk and operate the Site Survey Tool at the same time.

# **Operating Environment**

Always stop using the Site Survey Tool and disable the WLAN adapter when it is forbidden to use radio equipment or when it may cause interference or danger.

# **User Training**

The Site Survey Tool user should be appropriately trained and should be familiar with at least the basics of signaling technology in Wireless LAN.

## **Abbreviations and Definitions**

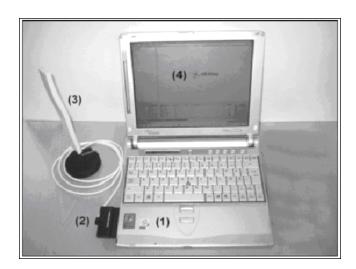
Term	Definition
AP	Wireless LAN Access Point.
dBm	Decibels relative to one milliwatt, where one milliwatt (1 mW) equals 1/1000 of a watt. This unit is commonly used in test laboratories to define signal strength. The dBm increment is based on the decibel, a logarithmic measure of relative power. Suppose a signal has a power level of P mW. Then the signal strength in dBm, symbolized SdBm, is: $S_{dBm} = 10 \; log_{10} \; \textbf{\textit{P}}$ A 1-mW signal has a level of 0 dBm. Signals weaker than 1 mW have negative dBm values; signals stronger than 1 mW have positive dBm values. The Site Survey Tool reports all signal strengths as dBm values.
RF	Radio Frequency
NL	Noise Level (non-802.11 signals, generally)
Rogue AP	Unauthorized or hostile access point
RSSI	Received Signal Strength Indication
SNR	Signal-to-Noise Ratio (SNR = RSSI - NL)
Wi-Fi	Wi-Fi (Wireless Fidelity) is the certification given by the Wi-Fi Alliance for wireless networking equipment that passes the Wi-Fi Alliance stringent tests for adherence to IEEE 802.11 standards and for real-world interoperability. Wi-Fi labeled equipment will work with any other piece of wireless networking gear that also has the Wi-Fi logo.

# **Getting Started**

Use the following topics to perform this activity:

- System Overview
- System Requirements
- Installing the Site Survey Tool
- Supported Adapters
- <u>Untested Adapters</u>
- <u>Updating the WLAN Adapter Driver</u>

## **System Overview**



- Light laptop PC with Windows XP or 2000 operating system.
- Wireless LAN adapter (see Getting Started for supported models)
- (Optional) external antenna for increased measuring accuracy. Recommended for site surveys only if the end users are expected to use similar antennas.
- The Site Survey Tool software, license key, and license file.

**NOTE:** Only the Site Survey Tool software is supplied by the vendor. All other system components are standard off-the-self items that can be sourced from any computer related resellers.

## **System Requirements**

- Light laptop PC with at least Windows XP or 2000 Professional, Pentium III, 256 MB RAM, 500 MB HD.
- The Site Survey Tool software (full install).
- Wireless LAN adapter (see Getting Started for supported models).
- At least one operational Wireless LAN access point (all 802.11a and b models supported).
  - Broadcast SSID must be enabled.

- Encryption should be disabled.
- (Optional) map image of the facility or area (BMP, PNG, or JPG).

**NOTE:** The Site Survey Tool adds each physical access point on the access point list only once. If you do two surveys with same access points first in 802.11a mode and then in 802.11b, the latter mode (here 802.11b) will always be displayed after the access point MAC and channel in the Browser View.

**NOTE:** To work around the problem, you can either save the two surveys (802.11b and 802.11a) into separate project files, or manually change the MAC property of each combo access point between the two surveys. This way the Site Survey Tool will treat the access points as different physical ones.

## **Installing the Site Survey Tool**

- 1. It is recommended to uninstall any old Site Survey Tool version before installing a newer version. This will not remove your survey files.
- 2. Insert your WLAN adapter to the PC slot and refer to the adapter documentation to properly install all default software.
- 3. Double-click SiteSurvey-installer-2.0.258.exe.
- 4. In case of CD installation, place the CD in the drive. If the installation does not start automatically, browse to the root folder on the CD and double-click SiteSurvey-installer-2.0.258.exe.
- 5. Follow the on-screen instructions and select the components you wish to install. It is highly recommended to install the included WLAN adapter drivers at this time. Refer to <u>Supported Adapters</u> to see which adapters and drivers are supported.

# **Supported Adapters**

The Alcatel software has been successfully tested with the following WLAN adapters and drivers on Windows XP and 2000.

The supported drivers can be installed with the Site Survey Tool and found under \Alcatel\Site Survey\drivers after installation.

Adapter	Supported Driver	Notes
Avaya Wireless World Card (b)	Agere 7.82.0.542	Scan speed 200 ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
		For unknown reason Symbol 802.11b AP using 1 mbps transfer rate can't connect with this driver.
Buffalo AirStation WLI-PCM-L11GP (b)	Agere 7.82.0.542	Scan speed 200 ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
Cisco AIRONET 350 (b)	Cisco 8.4.15.0	Scan speed 3 s, no hidden networks. Does not detect 802.11g APs even in b mode.
Cisco AIR-CB20A (a)	Cisco 3.7.48.0	Scan speed 5 s, no hidden networks.

Adapter	Supported Driver	Notes
D-Link AirXpert DWL-AG650 (a/b/g)	Atheros 2.4.2.14	Scan speed 1s for all three bands.
Enterasys RoamAbout (b)	Agere 7.82.0.542	Scan speed 200ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
IBM High Rate Wireless LAN PC Card (b)	Agere 7.82.0.542	Scan speed 200ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
Linksys Wireless-G Notebook Adapter WPC54G (g)	Linksys 3.10.27	Tested with 802.11b APs. Scan speed 500 ms, no hidden networks.
Nortel Networks Wireless LAN 2201 (a/b)	Atheros 2.4.2.14	Scan speed 5s. Detects hidden networks.
ORiNOCO (Classic) Silver/Gold (b)	Agere 7.82.0.542	Scan speed 200ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
ORINOCO PC Card Model 8462-WD (b)	Agere 7.82.0.542	Scan speed 150ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
ORINOCO USB Client (b)	Agere 7.82.0.542	Scan speed 200ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.
Proxim/ORiNOCO (b) Wireless PC Card Model 0111	Agere 7.82.0.542	Scan speed 150ms. Hidden APs can be detected with Scan Current option in the Site Survey Tool.

### **Untested Adapters**

Since there are hundreds of WLAN adapters on the market, the Site Survey Tool has not been tested with them all. Please see the Site Survey Tool Release Notes in Start > Programs > Alcatel > Site Survey for the list of adapters that might work but have not been tested.

If you find out that some of these adapters work with the Site Survey Tool, please send the adapter type, driver, and used operating system to **support@ekahau.com.** 

### **Updating the WLAN Adapter Driver**

An old adapter driver is the most common reason for not receiving network data. Always update the adapter driver before using the Site Survey Tool.

Follow these instructions if you did not install the included drivers during the Site Survey Tool installation, or want to change the adapter without re-installing the software.

- 1. Make sure your adapter works normally and you have completely installed the Site Survey Tool.
- Click Start > Settings > Network Connections.
   If the driver version number is lower than the one listed in <u>Supported Adapters</u>, you must update the driver.
- 3. Right-click an appropriate Wireless Connection in the list and select Properties.

4. Click the **Driver** tab sheet, then the **Update Driver** button.

The figure below shows Wireless Adapter Properties dialog on Windows XP. The driver version number must be same or higher than specified in <u>Supported Adapters</u>.



The figure below shows the Hardware Update Wizard on Windows XP.



- Click Install from a list or specific location, then Next.
- Browse to C:\Program Files\Alcatel\Site Survey\Drivers and select the appropriate driver for your adapter. Refer to <u>Supported Adapters</u> to see which driver works with your adapter.
- Click Next to install the new driver, then Finish to exit the Hardware Update Wizard.

The figure below shows the Hardware Update Wizard completed on Windows XP.



5. Open any adapter utility tool to confirm that the new driver was installed properly. If you have trouble updating the driver, please refer to the adapter and driver documentation before contacting support.

## **Technical Support**

If you encounter problems while using Alcatel software, or if you have improvement ideas, contact **support@Alcatel.com**. Alcatel Technical Support will respond within 24 hours on business days (Monday through Friday). Please include the following information in your Email:

- Detailed description and steps to repeat the problem.
- Operating system in use.
- Network adapter manufacturer, model, and driver version.
- Same information as viewed in the Alcatel Site Survey Client Windows Taskbar. (This may be different than actual.)
- Access point manufacturer and models.

Refer to <u>Alcatel Technical Support</u> in the <u>Alcatel OmniAccess Wireless Product Guide</u>.

## **Alcatel Client**

Use the following topics to perform this activity:

- Using Alcatel Client
- Working with Configuration Profiles
- Changing Adapter Settings

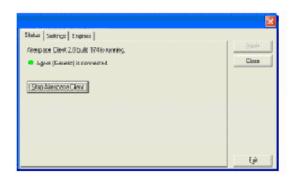
## **Using Alcatel Client**

Alcatel Client is a small program (Windows service) that allows the Site Survey Tool to retrieve network data from a WLAN adapter. Alcatel Client must be running whenever the Site Survey Tool is used. Starting the Site Survey Tool also starts the Client if the Client is not running.

Alcatel Client provides a separate Properties dialog that can be used for starting and stopping the Alcatel Client service and for enabling the writing of an Alcatel Client log file.

To open the Alcatel Client Properties dialog, click the Alcatel Client icon () in the Windows system tray. If the Alcatel icon is not displayed, start the Client by selecting **Start > Programs > Alcatel > Alcatel Client**.

The figure below shows the Alcatel Client Properties dialog on Windows XP.



If you need to manually view, start, or stop Windows service, right-click My Computer on the desktop, and select **Manage > Services and Applications > Services**.

**NOTE:** A red cross over the Alcatel Client symbol on system tray means that the Client service is not running. A yellow exclamation mark means an error. Open the Client Properties dialog to view error status.

# **Working with Configuration Profiles**

Your WLAN adapter's configuration profile affects site surveys. For example, enabling only 802.11a band in combo-adapter's Client Utility makes 802.11a the only available band in the Site Survey Tool as well.

Open the standard WLAN adapter utility, such as Agere Wireless Client Manager, Atheros Client Utility, or Cisco Aironet Client Monitor and create a suitable network profile for site surveys. For example, Atheros Client Utility allows scanning only specific bands such as 802.11a or 802.11b, or both. Depending on your adapter you may also need to provide valid security credentials to access the network you are about to survey.

The figure below shows the Orinoco Wireless Client Manager.

Use your standard WLAN adapter utility to create a suitable profile to survey specific network or 802.11 band (a/b).



Sometimes Windows XP causes configuration profile conflicts with its automatic Zero Configuration. To turn it off, right-click My Computer on the desktop and select Manage > Services and Applications > Services. Then open the Wireless Zero Configuration properties and Disable the service.

**NOTE:** Refer to the list of supported adapters to see which adapters can detect hidden, possibly unauthorized, networks.

### **Changing Adapter Settings**

Open the Site Survey Tool and click the Devices Tab to view the available WLAN adapters. Click a device to see its properties and settings. Different adapters may display different options:

The figure below shows the Device Properties and Settings in the Site Survey Tool with Agere Classic WLAN adapter.



- Adapter MAC and IP address are always displayed.
- Scan Interval is always displayed. Note that even with fastest (0s) setting the adapter will return new network scan results as quickly as possible. With some adapters this can be less than a second per 802.11(a/b) band, while others require many seconds per band.
- 802.11a checkbox is displayed only if the active WLAN adapter's configuration profile allows scanning a-band. Checking this box allows data from 802.11a access points to be observed.
- 802.11b checkbox is displayed only if the active WLAN adapter's configuration profile allows scanning b-band. Checking this box allows data from 802.11b access points to be observed.
- Scan Mode selection is displayed only when using certain Proxim/Orinoco adapters, such as
  Orinoco "Classic" 802.11b adapter. Scan All scans all access points, but cannot detect hidden
  networks. Scan Current Profile scans only the network (SSID) specified in the adapter's configuration profile. This network can be hidden but its name and possible security credentials must
  be set in the configuration profile to enable scanning.

# **Site Survey Tool User Interface**

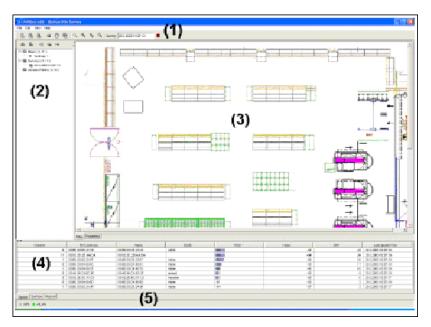
Use the following topics to perform this activity:

- Overview
- Projects and Surveys
- <u>Using Map Images</u>
- <u>Using the Browser View</u>
- <u>Exporting Map Image to a File</u>
- Exporting Survey Data to a File
- Printing a Map Image

#### **Overview**

### **Site Survey Tool User Interface**

The figure below shows the Site Survey Tool User Interface on Windows XP.



#### 1. Menu and Toolbar

The Menu and Toolbar provide the basic functions, such as opening and saving project files, printing or exporting images, recording network data, and manipulating the Map View.

#### 2. Browser View

The Browser View is a multi-purpose selection tool for maps, surveys, networks, and access points. You can select multiple items by holding down **CTRL** or **SHIFT**, and "lock" your selection to keep from being removed from the display. Only the selected or locked items are displayed in the Map View, or used for coverage display or data analysis. You can limit the number of displayed items by clicking the buttons Show All, Show Related, or Show Selected.

Learning how to use the Browser View takes a few minutes, but quickly allows powerful selection combinations. Please see <u>Using the Browser View</u> for further instructions.

#### 3. Map View

The Map View typically displays a map image, but can also display map, survey, and access point properties. Right-clicking on a map opens a context menu with zoom and other map features.

#### 4. Bottom View

The Bottom View has four Tab Sheets. **Signal** tab allows you to view all current WLAN signals. Surface tab is used for displaying the different visualizations for recorded data. Device tab allows viewing and changing the WLAN device settings, and Record tab shows the real-time access point RSSI. All Tabs can be used in real-time during a site survey.

#### 5. Surface Value

Surface Value is displayed in the bottom left corner of the Map View. It displays current dBm or other Surface visualization value range depending on the mouse location on the Map View. For example, Surface Value: [2.5 . . 8.5] means that the mouse cursor is at a map location that has value range between 2.5 and 8.5.

### **Projects and Surveys**

Each Site Survey Tool project can contain any number of site surveys and map images.

A new survey is created by selecting **File > New... > Survey**. Network data is recorded to the survey by pressing the record button:



and walking with the laptop while clicking on the laptop's location on the map between every 3-10 meters (10-30 ft.), or when changing speed or direction.



**Note:** Walk at a speed that ensures consistent data collection. Some cards collect data at a different rate depending on processor speed and/or very high-count AP networks.

### **Using Map Images**

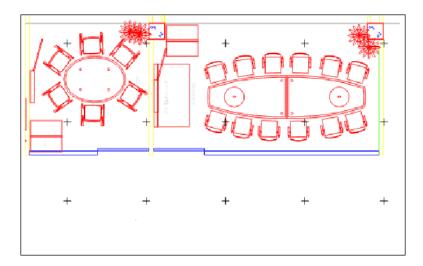
The Site Survey Tool does not require a map image, but using a map of the facility or area enables the advanced map features, such as coverage areas and access point placement tip. The supported map formats are PNG, JPG, and BMP.

Make sure that the map's normal viewing scale (1:1) is accurate enough for site survey usage. Below is an example of good map accuracy when the map is viewed without zooming.

You can get digital or paper maps from the facility management, national land survey, or other such authorities. If you do not have access to an actual floor plan or map, you can draw a rough map yourself with any drawing tool supporting the above file formats, such as Microsoft Paint.

The figure below shows an example of good map accuracy in normal viewing scale (1:1). If map objects such as doors or tables appear smaller than this on the application screen, open any image processing tool and enlarge the map before using it for site surveys.

Note that map details 6 inches or less are usually unnecessary.



**NOTE:** To maintain smooth map operation, keep each map image under 10 megabytes. If you have larger maps, split them with any suitable image processing tool.

### **Using the Browser View**

The Browser View (shown below) is used for selecting maps, site surveys, access points, and networks. You can select multiple items by holding down the **CTRL** or **SHIFT** key.

The Browser View takes a few minutes to learn, but provides powerful selection and grouping features.

The numbers after the folders represent the number of currently displayed items per all items in the folder.



1. Selecting map

Only one map can be displayed at a time. Double-click a preferred map in the Browser View to display it. (First be sure to add one from File > New... > Map).

2. Selecting active site survey

The active survey is displayed on the toolbar next to the Record button. This survey is used whenever recording data. To change the active survey, right-click the preferred survey in the Browser View, and click **Select as Active Survey** in the context menu.

3. Locking and unlocking your selection

After selecting a suitable set of items, such as a map, one or more surveys, and one or more networks or single access points, click the lock button.



to keep from losing your selection from being displayed when selecting or browsing additional items. Unlock your selection by selecting the items to be unlocked, and clicking the unlock button.



**NOTE:** Only the selected or locked items will be displayed on the map and used for the data visualizations. If you cannot see your survey on the map, make sure that you have locked or selected it. Changing the network or access point selection also immediately affects the visualizations.

4. Hiding unnecessary items

The numbers after the folders represent the number of currently displayed items / all items in the folder.

To hide items in a project for a given survey that are not related to the selected or locked items, click the **Show Related** button:



To hide all items that are not selected or locked, click the **Show Selected** button:



To view all items, click Show All:



5. Defining My Access Points and Other Access Points

By default, the Site Survey Tool adds all found networks and their access points under My Access Points folder, and considers them friendly. When you see foreign networks or access points appearing under the **My Access Points** folder, it is highly recommended to mark them as Other Access Points by moving them to the **Other Access Points** folder. To move items between folders, hold down the left mouse button and drag the selected item(s) to the new location.

**NOTE**: The Site Survey Tool visualization algorithms perform significantly more accurately if all access points other than your own are dragged to the Other Access Points folder before performing survey data analysis.

6. Grouping similar items in folders

To group your maps, surveys, or access points, you can right-click on a folder and select New Group from the context menu. This adds a new folder in the Browser View to be used for grouping similar items.

#### **Exporting Map Image to a File**

- 1. Open an existing project with surveys or record new.
- 2. Make selections in the Browser View and Surface Tab to display the appropriate visualization on the map.
- 3. Export the Map View to a file by selecting **File > Export Image...**
- 4. Type a name for the image file, select the format and click **OK**.

### **Exporting Survey Data to a File**

- 1. Open an existing project with surveys or record new.
- 2. Select the surveys you wish to export in the Browser View.
- 3. Export the survey data to a file by selecting **File > Export Data...**



4. Type a name for the data file and click **OK**.

#### **Printing a Map Image**

- 1. Open an existing project or create new.
- 2. Make selections in the Browser View and Surface Tab that display the appropriate visualization on the map.
- 3. Print map by selecting **File > Print**:



4. Click **OK** to print the Map View to the default printer. Note that printing may take up to two minutes depending on your printer.

# **Recording Data with the Site Survey Tool**

Use the following topics for this activity:

- Starting to Work with the Site Survey Tool
- Recording a Site Survey with Map
- Recording a Site Survey without Map
- Signals Tab
- Record Tab
- Survey Properties
- Marking Exact Access Point Locations
- Access Point Properties

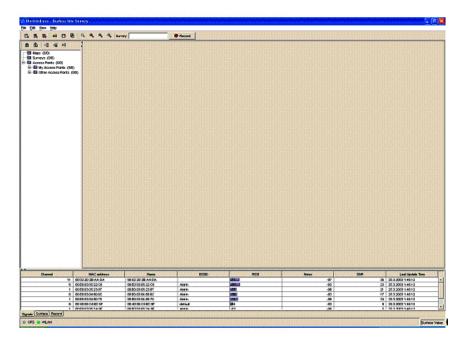
### Starting to Work with the Site Survey Tool

- Open the Site Survey Tool by selecting the Site Survey Tool icon in the Start > Programs >
   Alcatel > Site Survey 1.0 > Alcatel Site Survey. This will automatically launch Alcatel Client service that reads WLAN information from your adapter.
- 2. Make sure that Alcatel Client runs properly by clicking the blue icon in the Windows task bar:



- If you cannot see the icon, start Alcatel Client from Start > Programs > Alcatel > Client Controller.
- 4. After the Site Survey Tool has started, click the Signals tab in the lower part of the screen. If you can't see changing signal values, make sure that Alcatel Client is running, and your adapter and driver version are supported (see <u>Getting Started</u>).

The figure below shows the Site Survey Tool startup screen with the signals tab opened in the bottom view.



### **Recording a Site Survey with Map**

1. Add a new map image (BMP, PNG, or JPG) to the project by selecting **File > New... > Map**:



Each project can include any number of maps. Double-click a map image in the browser view to open the map in the map view.

2. Add a new site survey to the project by selecting **File > New... > Survey**:



Click the Record button (button will change color):



to start recording network data to the survey, or press **CTRL+R**. If you want to take a break, turn off data collection by clicking the Record button again.

- 4. Take your laptop with you and start walking around the facility or area. Click on the map accurately where you are (without stopping when clicking).
- 5. Always click the map again when:
  - You change your speed, stop or start moving.

- You change your walking direction.

**NOTE:** The survey recording is **ON** also between the map clicks. The purpose of the map clicking is to allow the software to interpolate the continuously recorded network data to your survey route. This speeds up data recording significantly.

**NOTE:** Occasionally look at the Record tab, client icon in tray, or time stamp signals to ensure that data is being collected.

- 6. When you have recorded enough data, click the Record button again to stop recording.
- 7. Save all surveys into a project file by selecting **File > Save**.

### Recording a Site Survey without a Map

The Site Survey Tool can record surveys without a map image, but then the survey visualizations, such as RSSI coverage areas and AP placement tip cannot be used. Working without a map is useful for quick or site surveys, or whenever a map image is unavailable.

Add a new site survey to the project by selecting File > New... > Survey:



You can rename the survey to describe the survey route or area by clicking the white textbox next to the **Record** button.

- 2. Double-click the survey name in Browser View to view the survey properties, and select the **Chart Tab**. You can alternatively right-click the survey and select View from the context menu.
- 3. Click the **Signals Tab** in the Bottom View to open it.
- 4. Click the Record button:

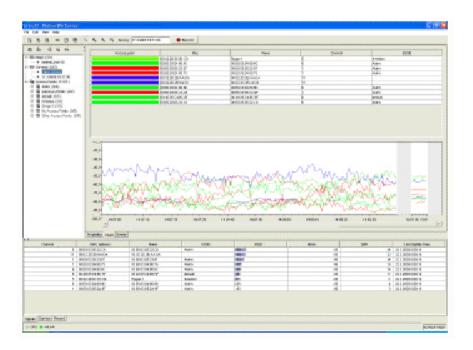


to start recording network data. If you want to take a break, turn off data collection by clicking the Record button again.

- 5. Take your laptop with you and start walking or driving around the facility or area.
- 6. Use the **Signals Tab** to observe how many APs are available at each location, their channel numbers, and how strong the signals are.
- 7. Use the **Chart Tab** to view the access point RSSI as a chart representation, helping you to spot changing signal strength.
- 8. When you have recorded enough data, click the Record button again to stop recording.
- Save project by selecting File > Save.

If a map image is not available, use the Signals Tab and Survey Properties to view the access point RSSI, SNR, and channel at different locations.

You can also change the survey name or properties to describe the recorded route and data.



### **Signals Tab**

The Signals Tab allows you to view all WLAN signals in real-time. You can click the header columns to sort the list by **Channel, MAC address, Name, ESSID, Band, RSSI, Noise Level, SNR, and Last Update Time** (last time the entry was refreshed).

**NOTE:** Sorting the Signal View allows quickly finding access points with the strongest RSSI, weakest noise level, or highest SNR. Sorting by MAC, Name, or ESSID helps finding unauthorized access points without a map.

#### Record Tab

The Record Tab shows the real-time access point RSSI as a RSSI-TIME diagram. Each curve describes an access point RSSI, while its color describes the used channel. Selecting a specific AP from the list displays just that AP.

### **Survey Properties**

Survey properties can be accessed by double-clicking a survey or right-clicking and selecting **Properties** from the context menu.

Survey Properties consists of 3 Tab Sheets: **Properties, Chart, and Events**. The Properties Tab can be used for storing any useful survey information, such as surveyor name, network card type, and any special comments. The Chart Tab is used for displaying the real-time RSSI of all access points, and the Events tab can be used for checking when the survey was started, stopped, etc.

### **Marking Exact Access Point Locations**

The Site Survey Tool produces a location estimate for each access point that has been audible at some point during a survey. To display the estimated locations, click the Surface Tab, select **Access Point** 

**Location** from the Type listbox, and select fine Grid size. Refer to <u>Site Survey Guidelines</u> for further instructions.

You can also manually mark the exact location of each access point for analysis, reporting, or documentation purposes. These access point locations do not affect any visualization or other calculation.

- 1. Select an access point from the Browser View.
- Right-click on the map at the exact location of the access point and select Place Selected Access Point from the context menu.

You can also find an access point in the Browser View by left-clicking the desired access point on the map:



You can select multiple access points by holding down CTRL.

### **Access Point Properties**

AP name, channel, and MAC address can be accessed by double-clicking an AP or right-clicking and selecting Properties from the context menu. You can modify the properties between two or more surveys for example to:

- Simulate different channel configurations without really changing the physical access point settings.
- Use the Notes text field to save any notes which may be relevant (AP make and model, transmit power, antenna type, engineer name, etc.).

# **Analysis Features**

Use the following topics for this activity:

- Performing Analysis
- Signal Strength (RSSI)
- Signal to Noise Ratio (SNR)
- Interference
- Strongest Access Point
- Access Point Count
- Signals at Channel
- Access Point Placement Tip
- Access Point Location
- Transmission Speed

### **Performing Analysis**

After recording a site survey, the Site Survey Tool analysis functions allow you to visualize the network performance and improve your Wireless LAN.

To visualize the recorded data, you must first select or lock:



the preferred survey(s) and network(s) or single access point(s) in the Browser View that you want to visualize - you can select multiple items by holding down the CTRL or SHIFT. Then open Surface Tab in the bottom view, and select a suitable survey visualization type.

The figure below shows the how the Surface Tab is used for analyzing the recorded network data.



### Signal Strength (RSSI)

The signal strength view displays the 802.11 Received Signal Strength Intensity (RSSI) of the selected access points. The strongest RSSI is shown per location.

The signal strength view displays the measured coverage of the wireless network, based on the recorded data, and helps find the specific areas with weak network coverage.

- Select Signal Strengths from the Type listbox.
- Select Viewed RSSI.

Viewed RSSI	Description
Strongest	Displays the strongest RSSI at each map location.
2nd Strongest	Displays the 2nd strongest RSSI at each map location. This measurement is useful for determining network redundancy and/or capacity.
3rd Strongest	Displays the 3rd strongest RSSI at each map location.

3. Select the appropriate Grid setting to set the scale for the visualization. Select a more **Rough** setting if the survey routes are far away from each other or a more **Fine** setting if survey routes exist very near to each other. The more survey routes you have, the finer you can set the grid to, and the more accurate your survey visualization will be.

The visual grid can be turned on or off from the View menu.

Grid Setting	Description
Rough	If you have surveyed a large outdoor (or indoor) area in a limited time, there are likely some spots that have not been visited. To display a continuous RSSI surface over the survey area, select rough. To see a more detailed surface near the surveyed routes only, select fine.
Fine	If you have surveyed a smaller indoor (or outdoor) area with lots of survey routes, select fine.

- 4. Optionally set the dBm value range and number of visualization colors by clicking the Legend Properties button. The default setting is between -90 (weak) and -10 (strong).
  - Alcatel recommends between -75 dBm and -35 dBm nominal to ensure good network performance.
- 5. Click the Legend Details button to display the accurate dBm ranges for different colors.

The figure below shows how Signal Strength View displays the strongest RSSI at each location for the selected access points. The dotted line is the recorded site survey route.

The grid lines are also turned on to see the accuracy of the visualization.



### Signal to Noise Ratio (SNR)

The SNR view displays the relationship between RSSI and 802.11 Interference and environmental noise as described in the next section. Under good circumstances, without adjacent, interfering access points configured on close channels (such as channels 1 and 2), the SNR value should be close to RSSI value. With high interference, the SNR can drop down to zero, making data transfer very slow or impossible. SNR is calculated as follows:

Signal to Noise Ratio (SNR) = RSSI - Noise Level

Please note that the SNR visualization is based on a computational worst-case estimate from the recorded data - not concrete SNR observations from the WLAN card. Momentary SNR values are not used because they may be affected by momentary variation such as varying number of clients transmitting data, or random radio interference, such as a microwave oven.

The figure below shows that if the Signal-to-Noise Ratio is significantly lower than the signal strength, there is radio interference affecting your network performance.

The grid and survey route visualizations have been turned off.

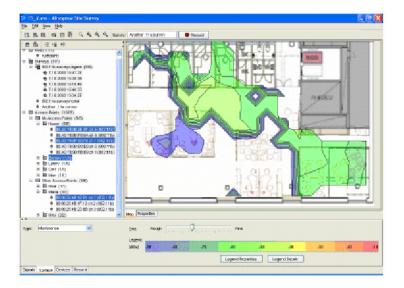


### Interference

The Interference view calculation assumes that the strongest signal of the My Access Points was the associated one, and all other signals (Other Access Points) were interfering with it by sending data at the same time.

The Interference view is a calculated estimate of a "worst-case scenario" for 802.11 interference - all access points do not typically send high amounts of data all the time, unless there is at least one user associated with each access point. **The Interface View displays what happens when all access points send data at the same time.** 

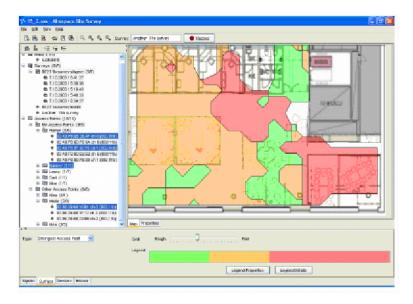
The figure below shows that by investigating the interference surface you can find the optimal channels with minimum interference.



### **Strongest Access Point**

The strongest access point view displays the strongest AP at each map location. The displayed AP is not necessarily the associated one, but typically the client device tries to associate with the AP that has the strongest signal. The color for each access point can be chosen from the <u>Access Point Properties</u>.

The figure below shows visualizing the strongest access points per location. Specific color can be defined for each AP.

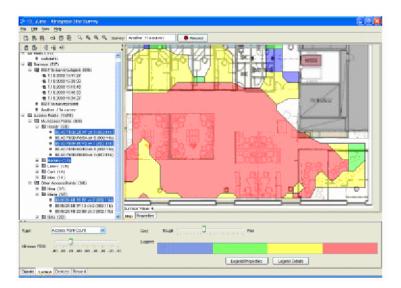


#### **Access Point Count**

The Access Point Count displays the number of access points at each location with respect to the selected **Minimum RSSI**. The feature is useful for visualizing overlapping coverage areas, for example to ensure "backup" coverage in case of an access point breakdown.

The figure below shows that the Access Point Count surface displays the number of overlapping access points per location.

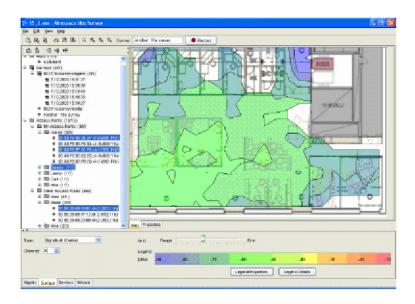
The number of access points can be seen in the bottom left corner of the map window, as well as in the Legend Details.



### **Signals at Channel**

The Signals at Channel displays the strongest signal strength (RSSI) at each location for each channel. Use the Channel list box to change the channel.

The figure below shows the strongest signal strength (RSSI) per location from all access points at channel 8 only.

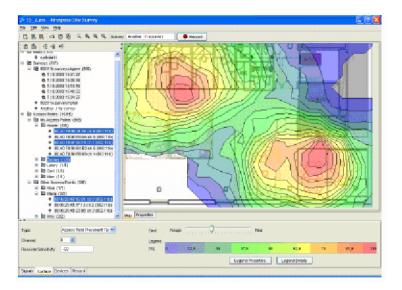


# **Access Point Placement Tip**

The AP Placement Tip helps to find the optimum location for a new or existing access point.

- Select the access point(s) from the Browser View that you wish to be treated as your "existing network". Even if you had more than 10 APs, you can select just a few of them, and see where the "next one" should be installed.
- 2. Select the channel that you would like to use with the access point. Try different channels to see how the suitability changes. Channels and locations with lower interference and signal strength are given better suitability. Higher suitability (near 100) is marked with red color (by default).

The figure below shows how the Access Point Placement Tip displays the most appropriate location(s) for a new or existing access point.

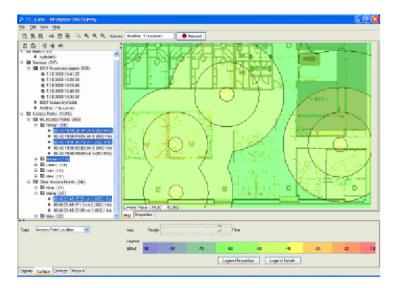


#### **Access Point Location**

The AP Location visualization helps to locate your own APs or unknown or unauthorized "rogue" access points. Refer to the list of Supported Adapters to see which adapters can detect hidden, possibly unauthorized, networks.

- 1. Select the networks or single APs that you wish to locate from the Browser View.
- 2. Select finer Grid size to calculate more accurate access point location.
- 3. Find the APs from the suggested locations.
- 4. After finding an AP you may mark its exact location on the map for reporting or documentation purposes. See <u>Access Point Location</u> for details. Note that marking the exact AP locations will not affect the Access Point Location visualization or any other visualization.

The figure below shows locating Access Points using the Site Survey Tool.

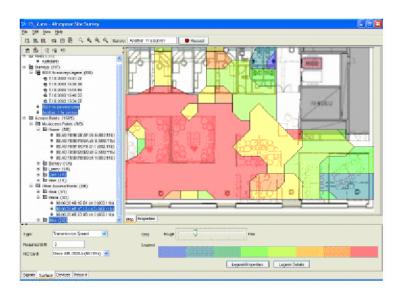


### **Transmission Speed**

The transmission speed estimation is based on the calculated SNR values and the selected receiver sensitivity values. The network card manufacturer reports the minimum RSSI values required for the network card to operate at a specific transmission speed (1, 2, 5.5, or 11 mbps in 802.11b).

- 1. Select the network card settings that are closest to the network cards to be used generally in the network, or add the receiver sensitivity values manually to the sensitivity.cfg file located in the conf folder under your Alcatel Site Survey Tool installation directory.
- 2. Type in your requirement for the SNR threshold for your network installation.
- 3. The Site Survey Tool will visualize the theoretical data transmission speed per location per client. The estimated Transmission Speed result assumes that only one access point serves per location.

Transmission speed quickly gives an estimate of the achievable throughput per location.



### The Basics of Site Survey

Use the following topics for this activity:

- Background of Site Survey
- When Site Survey is needed
- Defining WLAN Requirements

### **Background of Site Survey**

In wireless networks, it is difficult to predict the propagation of radio waves and detect interfering signals without the use of test equipment. Even if you're using omnidirectional antennas, radio waves don't travel the same distance in all directions. Walls, doors, elevator shafts, people, and other obstacles create varying degrees of attenuation, which cause the Radio Frequency (RF) radiation pattern to be irregular and unpredictable. As a result, it is often required and always recommended to perform an RF site survey to fully understand the behavior of radio waves within a facility before permanently installing the access points.

This is also why the Site Survey Tool 2.0 relies on collected network data, not on assumptions made by RF prediction models.

### When Site Survey is Needed

The need and complexity of a site survey varies depending on the facility. For example, a small three room office may not require a site survey, unless there are interference sources, such as other 802.11 devices nearby. This scenario can probably get by with a single access point located anywhere within the office and still maintain required coverage. If this access point encounters RF interference from another nearby wireless LAN, you can likely choose a different channel for the AP and eliminate the problem.

A larger facility, such as an office complex, apartment building, hospital, warehouse, or outdoor area, generally requires an extensive RF site survey. Without a survey, users will probably end up with inadequate coverage and suffer from low performance in some areas. You certainly wouldn't want to relocate and add access points to the facility after installing and interconnecting 20 or more access points.

### **Defining WLAN Requirements**

Always define the functional requirements before setting up a Wireless LAN. Requirements define what the WLAN must do, offering a foundation for network design. Re-engineering a solution that does not meet the needs of users or applications can be difficult and costly.

Below are some common Wireless LAN requirements for your consideration:

- **User applications.** This is the most important function for the WLAN. Be as specific as possible by defining information types (i.e., data, video, voice) and how much throughput they will require in different areas.
- **Backup requirements.** Having overlapping coverage of at least two access points at each location can avoid costly maintenance breaks in case of an access point crash. Also consider installing a file backup system to store your mobile users' valuable files.
- **Number of users.** Number of users and where they will use the WLAN. Mobile users will move about the facility and possibly roam across IP domains, creating a need to manage IP addresses dynamically. Some users may be stationary, such as wireless desktops. Remember that only certain number of users can connect to the same access point while still achieving reasonable throughput.

- **Coverage requirements**. This describes where users will need access to the wireless LAN. They might only need connectivity in their offices and conferences rooms, but they might be able to do without wireless connectivity inside power utility rooms and the cafeteria. By properly specifying coverage requirements, you'll avoid the unnecessary expense of installing access points where they're not needed, or cause unwanted coverage outside of the facility that could be used for hacking.
- **Security.** Describe the sensitivity of the information being stored and sent over the wireless network. You might need to identify a requirement for encryption if users will be transmitting sensitive information, such as credit card numbers. Give security requirements plenty of thought so that you design a solution that will protect the company's valuable information.
- **End User Devices.** Specify the end user devices (e.g., hardware and operating system) to ensure the solution accommodates them. For example, you could specify that users will have laptops running Windows XP or a particular brand of Pocket PCs with Compact Flash interfaces. This provides a basis for deciding on the type of WLAN adapter and drivers to use, as well as assessing the type of middleware that you can use.
- **Battery Longevity.** Depending on battery size and WLAN adapter model, batteries will last from a couple hours to a day or so. These are constraints for most applications, but it's beneficial to indicate the amount of battery life that users will realistically need. In the design, you can utilize this information to decide whether to activate power management, specify larger batteries, or determine an effective battery-charging plan.
- **System Interfaces.** In most cases, users will need to access information located in servers on the wired-side of the system. As a result, describe applicable end-systems and interfaces so that you can properly design the wireless system interfaces.
- Funding. The requirements stage of a Wireless LAN project is a good time to ask how much
  money is available. First define the requirements and design the system before giving a cost
  estimate.
- Schedules. Choose a realistic completion date and plan the project accordingly.

After defining these elements, you should have enough information to design the solution. Before proceeding, ensure you have consensus from all executives, users, and operational support staff. If requirements are not clear enough, consider some pilot testing to fully understand requirements before spending money on design and installation.

# **Site Survey Guidelines**

This section provides practical guidelines for performing a site survey, analyzing the results, and improving your network with the Site Survey Tool. Reference the following sections:

- General Wireless LAN Setup Steps
- Visual Site Inspection
- <u>Performing the Survey</u>
- Locating Access Points
- Verifying Network Coverage
- Network Quality and Channel Planning
- Improving the Network Based on Survey Results
- Finishing the Network Design and Documenting Results
- Implementing Location Aware Networks

### **General Wireless LAN Setup Steps**

- 1. Define WLAN requirements (see *The Basics of Site Survey*).
  - It is very important to define requirements at the beginning of the project. Re-engineering a solution that does not meet the needs of users or applications can be difficult and costly.
- 2. Design the WLAN (see Site Survey Guidelines).
  - A good network design facilitates implementation by describing how the solution will work, i.e. what components are necessary, where to place them, and how to configure them. The Site Survey Tool helps you to create a good network design by helping to find the access point locations, channels, antenna types, and any existing 802.11 networks that may cause interference.
- 3. Implement the WLAN (see manufacturer documentation).
  - Refer to the access point and other documentation to setup the Wireless LAN. Do not yet install the access points permanently.
- 4. Perform site survey (see <u>Site Survey Guidelines</u>).
  - Once you have a working Wireless LAN, perform a complete Site Survey to make sure that the access points are optimally placed and configured, and there is no interference.
- 5. Improve the network based on results (see <u>Site Survey Guidelines</u>).
  - Implement network changes based on the site survey analysis results. After the modifications, when the network works well, install the access points or antennas permanently.
- 6. Periodic Site Surveys (see Site Survey Guidelines).
  - To avoid performance problems, it is recommended to conduct a site survey every 3 months and always when changing the number of access points, their locations, channels, or antenna directions.

#### **Visual Site Inspection**

If the facility or area is larger than a few rooms, it is recommended that you use a map diagram to help plan AP locations, both manually and with the Site Survey Tool. By loading a map into the Site Survey Tool, you'll enable the advanced map features like coverage areas and AP placement tip. The Site Survey Tool supports BMP, PNG, and JPG image formats.

After obtaining a map image, walk or drive through the area to verify the map accuracy. Make notes of the following:

- Any potential barriers that may affect the propagation of RF signals. Look for obstacles such as metal racks and partitions and any other items that blueprints generally don't show.
- Possible access point locations: power outlets, data cables and antenna places. Try to ensure line-of-sight to the antennas wherever possible.
- RF interference sources: large metal objects, Bluetooth devices, microwave ovens, cordless phones and other devices operating in or near 2.4GHz.
- Estimated access point coverage areas (thickness of the walls, major reflections of the signal etc.).

The more experience you have on Wireless LANs, the better the result will be. This step is not supposed to be thorough or perfect, but will speed up the rest of the process when done as well as possible. For the following steps, you can either acquire an estimated number of access points (based on your visual inspection), or just use the one or few AP's you may already have and purchase the exact required number of AP's after the actual site survey has been performed (recommended).

### **Performing the Survey**

One major advantage of the Site Survey Tool is that you don't have to plug your APs to the Ethernet backbone before the site survey procedure. This saves both time and resources when you don't have to permanently place APs on the wall or ceiling and you're able to determine the Ethernet cable places and lengths. Another remarkable benefit is that you don't have to adjust the channels from the access points before performing the site survey - the channel separation can be simulated in the analysis phase. After a suitable channel combination is found, you can update the changes to the access points.

Place the access points to their preliminary locations to your best knowledge. If you are not sure about the number of APs to be installed, you can perform the survey using only one access point or a few access points. Both methods (single- and multi-AP) are described below.

If you want to survey both 2.4GHz and 5GHz access points, it is recommended to survey the area two times, one survey per band. Most network cards provide faster network scanning and thus a better quality survey when surveying different frequency bands separately. You can select the radio frequency to be used in the surveys from the Devices tab.

It is recommended to do the survey using more than one access point within different areas of the site to minimize the pre-installation survey time. The more experience you have, the better you can tell the reasonable AP and antenna places beforehand. Do not install the access points and antennas permanently at this phase - but do place simulating the final installation, in terms of height, antenna directions and such.

If your access points do not cover the whole area, you can perform several surveys having AP's in different locations and combine the information in the Site Survey Tool afterwards, as if you had more APs than you actually do. Here is the procedure for this virtual access point scenario:

- 1. Place the AP(s) in the most obvious good location(s), for example in the middle of an office room, or at the end of a corridor (always preferably at ceiling height or the actual installation height).
- Record a survey that covers the coverage area of the AP(s). (Have the Signal Strength visualization open to see the actual coverage(s) in real-time during the survey). Save the site survey when done.
- 3. By inspecting the surveyed coverage area visualization, move the AP(s) to location(s) that provides low RSSI, but needs to be covered.
- 4. Double-click the access point in the Browser View to display the AP properties. Change the MAC value(s) to something different, for example "loc 2". This makes it possible for the Site Survey

Tool to handle the single AP as multiple APs. You can optionally also change the channel number property to simulate that the AP was on another channel.

5. Repeat steps 2-4 to record multiple surveys - one every time you move AP(s) - to simulate a network with more access points than you actually have.

Select or lock all the surveys, or part of them, and use the Signal Strength and other visualizations to find out how many access points are needed, and how to place them.

### **Locating Access Points**

Locating your own access points and other APs outside your own network can be done using the Access Point Location feature. Unwanted access points at or near your facility may also be a security threat; An employee may have installed an AP without permission and connected it to the company backbone just to get a Wi-Fi access near his workspace, or an attacker may have installed a rogue access point inside or outside your facility for hacking purposes.

The more thorough the survey, the more accurately the Site Survey Tool can locate the access points. If you cannot find the AP in the area suggested by the Site Survey Tool then simply perform a quick survey near the access point to find its exact location.

**NOTE:** The location may be a floor above or below your current location.

After locating the access points, it is highly recommended to manually place the access point on the map. This helps you to immediately visualize the places of all the access points while analyzing the network performance without changing the current surface type.

Please note that different network cards use different scanning modes; the Agere-based adapters such as Lucent Orinoco (Classic) Silver/Gold 802.11b use active scanning and thus may not detect all access points that do not broadcast their ESSID. Refer to the list of Supported Adapters to see which adapters can detect hidden, possibly unauthorized, networks.

### **Verifying Network Coverage**

Usually the first step in the network performance analysis is verifying the network coverage. The goal of coverage analysis is to have sufficient and even coverage all around the required area. Using the Site Survey Tool, after surveying you can analyze the coverage areas of 1) all the APs, 2) only one AP, or 3) selected APs. It is obviously most important to determine the coverage of your own access points, although you can also determine the coverage of the foreign networks as well.

Usually a minimum RSSI value is set for the network. This can be visualized by using the Legend Properties button in the surface window. In this case visualization only shows the areas where signal strength is above the minimum value. Sometimes such conditions may be set to the network installation as redundancy by having two or three access points audible everywhere in case of any particular AP breakdown - or if more network throughput is needed per location than one AP can provide. This can be visualized with the Site Survey Tool using the Viewed RSSI functionality under the signal strength coverage visualization.

Unwanted coverage can also be visualized; just survey the area outside your facility (for example) and visualize if signals are leaking from your own access points there. Set the grid to dense to ensure the accuracy of the visualization.

The Strongest Access Point feature helps you to estimate the number of clients who will be associated with each AP - a rule of thumb is to have the serving area of each AP to be about of equal size to distribute the client load equally.

### **Network Quality and Channel Planning**

Good coverage is the first - but by no means the only - requirement for a well-performing network. The primary goal in channel planning is to avoid channel interference between the AP's and achieve better signal-to-noise ratio, resulting in optimal network throughput. Generally 802.11b Wi-Fi access points use in total eleven channels (thirteen are utilized in most of Europe). These channels overlap slightly, otherwise known as co-channel interference, which increases the importance of having proper channel spacing. AP's other than your own should also be taken into account when analyzing the overall interference level and planning the channels of your access points. In the unlicensed range where Wi-Fi operates, you have to accept the circumstances and maximize your network performance while taking other networks into account in terms of interference.

The Site Survey Tool helps you to get the most performance out of your network regardless of which channel separation you prefer. The features that help here are the interference and SNR maps. The SNR maps are based on the assumption, that the user is connected to the strongest audible access point and that the other access points are transmitting data all the time. In other words, instead of just looking at momentary, usually unreliable signal-to-noise ratio, the interference and signal to noise ratio is calculated for a "worst-case scenario". Assuming that all the AP's are transmitting data all the time may give you a pessimistic view to your network, but it also prepares you for the worst and - as the number of users grows - realistic scenario.

As the receiver sensitivity differs between network cards, you may want to use these values as guidelines when determining the desired signal-to-noise ratio. Just use the slider located in the bottom-left side of the window when SNR coverage visualization is selected. To find out how crowded the different channels are in terms of 802.11b signals, please use the Signals at Channel. It also takes into account the signal overlapping into neighboring channels using calculation.

As an estimation of data throughput use the Transmission Speed feature, which takes into account the NIC receiver sensitivity and the desired signal to noise ratio. You'll have to decide your desired SNR yourself - usually minimum values between 5 and 15 are used. The feature does not take into account the increased throughput achieved by having multiple AP's serving the same area.

You can simulate different channel settings by changing the channel number within the Site Survey Tool Access Point Properties. No manual modifications to the AP's are needed. Combining this information with Signals at Channel, SNR and Interference displays, you can investigate the interference levels and set up the optimal channel separation for your network.

**NOTE:** Using the Signals at Channel with just one access point you can visualize the 802.11 channel overlap.

### **Improving the Network Based on Survey Results**

Implement the necessary network improvements based on the site survey analysis results. When the network is modified to work optimally, install the access points or antennas permanently. The Site Survey Tool automatically helps in finding optimal locations and channels for your new or existing access points (discussed below).

To understand which places and channels are the most suitable for installation of your additional access points, use the Access Point Placement Tip. The AP placement tip will suggest the best placement location for your next AP, ensuring minimal channel interference and maximal coverage area. You can scan through all the channels to find the most suitable one. If nothing is shown on some channels, it means that no access points are recommended to be installed anywhere in that area on that particular channel, or that there are better channels available to be used.

The Access Point Placement Tip visualization can be used to relocate existing interfering access points also. Deselect only the interfering access point(s) to see where the AP Placement Tip suggests re-placing them: Try different channels to find the channel and location that provide the best suitability (0-100) for AP location.

**NOTE**: The Site Survey Tool will always recommend the best place for the next access point given the currently selected APs, regardless on the fact that you may not need any more APs for your network to meet the requirements you have.

To improve your network performance without Access Point Placement Tip, use the other visualization features, such as Interference, SNR and Signals at Channel to manually find the optimal places for AP's. Modifications such as turning antennas, changing AP power levels and changing antenna types are not automatically calculated, but can be estimated according to the existing results. It is recommended to do a new survey and analyze the results whenever network settings are significantly changed.

### **Finishing the Network Design and Documenting Results**

After carefully surveying and analyzing the network using the Site Survey Tool you will find an optimal network setup given the used hardware, network requirements, and the environment. This network design should be documented, and the Site Survey Tool can help. Use the Access Point Notes, Survey Notes and Image Export to create high quality network design documentation. You can also take screen captures (hold down **Alt** and press **Print Screen**) to export the contents of the whole Site Survey Tool window, including the browser view.

### **Implementing Location Aware Networks**

A regular Wi-Fi network can also be used for accurate positioning without additional hardware. If a location-aware wireless network is implemented, the required site calibration is recommended to be done along with the site survey. In addition to displaying the number of audible AP's with respect to the selected minimum RSSI, the Access Point Count feature is also useful when creating location-aware networks; Accurate Wi-Fi positioning may require a minimum number of audible access points per location - which can be easily visualized using this feature.

# **Upgrading a License**

#### **Purchasing a License**

The Site Survey Tool can be installed and evaluated for 14 days without a license. After this period a license must be purchased by contacting **sales@Alcatel.com**.

**NOTE:** License consists of a License Key and a matching license.xml file. After receiving the license file save it to any folder on the computer that has the Site Survey Tool installed.

#### **Upgrading the License**

- 1. Start the Site Survey Tool and select **Help > About > Upgrade License**.
- 2. Type your name, organization, and copy-paste or type the License Key exactly as given (remove any spaces before or after the key).
- 3. Click **Browse** and select the license.xml file you have purchased.
- 4. Click **OK** and restart the application to see the new license information on the startup splash screen and **Help > About** dialog.

# **Troubleshooting**

### I can't see any signals in the Site Survey Tool.

- Click the Alcatel Icon on the task tray to see if Alcatel Client has encountered errors.
- Check from <u>Supported Adapters</u> to see if your WLAN card is supported and that you have a correct driver for it.
- Using Agere (for Orinoco, Compaq and Avaya cards) Wireless Client Manager at the same time
  with the Site Survey Tool might cause network data reading problems. If you have problems
  with Site Survey, please exit the Agere Client Manager. This defect is under investigation and
  solution will be available later.
- If your access points are hidden, it depends on your adapter model how to proceed. With Agere-based 802.11b adapters, such as Orinoco, Avaya, Buffalo, Enterasys, or IBM, you need to do a separate survey for each hidden network. Create a suitable Configuration Profile for the first network with the Wireless Client Manager, and select option Scan Current Profile in the Site Survey Tool Device Properties Tab Sheet. With this setting, you will not see any other networks except for the current (hidden) one.
- Please refer to the list of <u>Supported Adapters</u> and <u>Using Alcatel Client</u> to see which adapters can
  detect hidden networks, and how to configure network settings.

# I can only see 802.11b (or 802.11a) access points even though I'm using 802.11a/b combo card.

- The available bands also depend on any limitations in the active configuration profile. Use your WLAN adapter's standard managing tools to create a configuration profile that allows reading all preferred 802.11 band(s).
- Make sure you have enabled the preferred band(s) in the Site Survey Tool Device Properties.

# I can only see 802.11b (or 802.11a) access points even though I'm using combo access points with 802.11a/b support.

- First make sure you are using a WLAN adapter configuration profile and the Site Survey Tool settings that allow using the preferred band. See <u>Alcatel Client</u> for details.
- The Site Survey Tool adds each physical access point on the access point list only once. If you
  do two surveys with same access points first in 802.11a mode and then in 802.11b, the latter
  mode (here 802.11b) will always be displayed after the access point MAC and channel in the
  Browser View.
- To work around the problem, you can either save the two surveys (802.11b and 802.11a) into separate project files, or manually change the MAC property of each combo access point between the two surveys. This way the Site Survey Tool will treat the access points as different physical ones.

# **Alcatel OmniAccess Wireless System Release Notes 2.0.113.3**

System Release 2.0

This Release Note covers Alcatel OmniAccess Wireless Switches and OmniAccess Wireless Appliances, OmniAccess APs, and OmniVista Air Control System Software, that comprise the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System). This document includes the following sections:

- Alcatel OmniAccess Wireless Enterprise Platform Components
- Requirements for Alcatel OmniAccess Wireless System Components
- New Features Available in Release 2.0
- <u>Features Not Available in this Release</u>
- Features Improved in this Release
- <u>Technical Notes</u>
- Open Issues in Alcatel Wireless Operating System Software
- Interoperability Tables

# **Alcatel OmniAccess Wireless Enterprise Platform Components**

- Alcatel Wireless Operating System (OmniAccess Wireless Switch, OmniAccess Wireless Appliance, and OmniAccess AP) Software, version 2.0.113.3.
- OmniVista Air Control System Software, version 2.0.67.0.
- 4012 and 4024 Alcatel OmniAccess Wireless Switches.
- 4102 OmniAccess Wireless Appliances.
- OAW-1200ABGE, OAW-1200BGE, OAW-1200ABG and OAW-1200BG Alcatel OmniAccess
  Wireless Access Point (OmniAccess AP), and OAW-1200ABGR Alcatel OmniAccess Remote Edge
  Access Point (OmniAccess AP 1200R).

# **Requirements for Alcatel OmniAccess Wireless System Components**

- Requirements for Alcatel Web Browser Interface Internet Explorer 6.0.2800.1106.xpsp2.030422-1633 or higher. Please note that there are known issues with 6.0.2800.1106 with SP1 with fixes for Q832894 and Q330994. A browser update will not be sufficient. To obtain the latest you may need to do a system update by going to <a href="http://windowsupdate.microsoft.com">http://windowsupdate.microsoft.com</a> and clicking on Scan for Updates. This will also work for Windows 2000. Also note that there are known issues with Opera, Mozilla and Netscape; these are unsupported.
- Requirements for Web Browser when using Web Authentication Internet Explorer 6.0 with SP1 or Netscape 7.2 There are known issues with Opera.

### **New Features Available in Release 2.0**

- <u>Layer 3 Support for OmniAccess APs</u> This feature enables access points to be located in subnets that are not directly connected to an Alcatel OmniAccess Switch or Appliance. You may position access points in the same subnet as an Alcatel OmniAccess Switch or Appliance as well as in remote subnets.
- Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R) You can place the Alcatel OmniAccess Remote Edge Access Point into a branch office, without a locally connected Alcatel OmniAccess Switch or Appliance. The OmniAccess AP 1200R automatically finds an Alcatel OmniAccess Switch or Appliance over a WAN link using DHCP extensions and LWAPP. The Alcatel OmniAccess Switch or Appliance uses WPA for local user authentication. If the WAN link fails, the OmniAccess AP 1200R continues to offer wireless 802.11a/b/g service from WLAN 1 only, provided that the users have the proper security settings and authentication.
- New Interface Structure Alcatel Wireless Operating System 2.0 provides you with the capability of defining an interface with multiple attributes including a VLAN tag and assigning this interface to a physical port. This effectively provides multiple DS ports. Alcatel Wireless Operating System 1.x only allowed VLAN tagging on a single DS port. In this release APs may also attach to the Alcatel OmniAccess Switch or Appliance over VLANs. The new interface structure will support up to 64 VLANs. This structure allows for greater flexibility in deployment.
- Access Control Lists This release allows the administrator to set up an access control list
  (ACL) for each interface with up to 64 rules per ACL. Users can permit and deny traffic based on
  source IP Address, destination IP Address, TOS/DSCP, destination TCP/UDP port, and source
  TCP/UDP port.
- <u>Customizable Web Authentication Screen</u> This release allows the administrator to customize the Web Authentication (Web Auth) Login Screen with logos and text.
- Rogue Location Detection Protocol (RLDP) This feature detects rogue access points that are
  on the same wired network which are broadcasting SSIDs within your coverage area. The
  Alcatel OmniAccess Wireless System operator can configure the Alcatel Wireless Operating
  System to automatically contain all such rogue access points. Note that this feature does not
  contain OmniAccess APs.
- <u>Ad-Hoc Rogue Containment</u> This release extends the Rogue Containment capabilities of OmniVista AirView Software to ad-hoc IBSS networks.
- <u>Port Mirroring</u> This feature allows you to capture all traffic from an OmniAccess AP, or from a client, and have it directed to a designated OmniAccess Wireless Switch port. All traffic is sent as 802.3 encapsulated traffic, allowing you to use any existing packet capture software.
- WLAN Override by OmniAccess AP This feature allows the user to specify which WLANs will operate on a specific 802.11a or 802.11b/g OmniAccess Radio. To configure this you will need to enable WLAN Override, and individually disable or enable WLAN operation on this 802.11a or 802.11b/g OmniAccess Radio. The OmniAccess AP must be reset after any change to the override configuration, including enable/disable of the override feature AND any changes to the WLANs to be advertised. (This feature is also known as SSID Advertisement by OmniAccess AP. Do not confuse SSID Advertisement and Disable SSID Broadcasts, which is defined below.)
- <u>Disable SSID Broadcasts</u> This feature allows the administrator to disable SSID broadcasts for the whole Alcatel OmniAccess Wireless Switch or Appliance as a security precaution. Users must know which SSID to associate with.
- <u>Identity Networking/AAA Override</u> When AAA Override is enabled client authentication is performed by the AAA server. As part of this authentication, a number of attributes can be changed on a per-client basis: VLAN tag, ACL, QOS. (Identity Networking is also known as Policy Granularity.)

This feature also allows for interfaces (VLANs and associated attributes) to be assigned on a per-client basis via MAC filtering.

- <u>TKIP Acceleration on the OmniAccess AP</u> This feature pushes TKIP acceleration into access points.
- Pre-shared Key support for WPA.
- Shared Authentication support for WEP.

### **Features Not Available in this Release**

- Management over Wireless is not supported for IPSec clients.
- <u>Debug commands</u> Debug commands and the **show tech-support** command are reserved for use only under direction of Alcatel personnel. Please do not use these commands without direction from Alcatel.

# **Features Improved in this Release**

- Corrected an issue in which a hidden AP-Manager Interface remained assigned to a port even after the Alcatel OmniAccess Switch or Appliance was placed in L2 LWAPP mode. One symptom of this problem was that port 1 could not be used for an OmniAccess AP until an Interface was assigned to that port.
- Removed a race condition that caused the message "Crypto Card Not Responding" on the console.
- Removed a rare condition in IPSec that caused Alcatel OmniAccess Switch and Appliance resets.
- Enhanced the message log information about mismatched WLAN configurations when clients are mobile between Alcatel OmniAccess Switches and Appliances.
- Added a trap to notify the operator when an OmniAccess AP is the target of a containment attack.
- Fixed a corner case where Over The Air Provisioning (OTAP) and the DHCP server options were conflicting and OmniAccess APs never associated with the Alcatel OmniAccess Switch or Appliance.
- Added the capability of the Alcatel OmniAccess Switch and Appliance to detect and respond to a TKIP-MIC attack from a malicious client.
- Fixed a corner case in which a WLAN using Web Authentication did not delete clients at the correct time during session timeout.
- Fixed a case where client to client communication stopped when one of the APs was a third-party AP (foreignAP) and was on a VLAN tagged network.
- Fixed a rare IPSec timing case in which rekeys caused the Alcatel OmniAccess Switch or Appliance to become unresponsive.
- Fixed a case with WPA and Dell True Mobile Systems in which clients intermittently lost connectivity.
- For the Web interface, fixed a header mislabeling in one of the Details pages on a specific port.
- Corrected the WLAN ID displayed in the MAC Filter ACS page.
- Fixed an Alcatel OmniAccess Switch or Appliance crash resulting from a race condition between the refresh of a web page during an upgrade and the generation of the content for that page.
- Fixed an instance where an SSH session could terminate, but a pointer to the connection remained, possibly crashing the Alcatel OmniAccess Switch or Appliance.
- Several fixes for the Alcatel Wireless Operating System code which detected error conditions in an Alcatel OmniAccess Switch or Appliance and reset it. This new code is able to recover from more situations and provide a more stable environment.
- When the Rogue Containment feature was turned on, a memory leak caused an OmniAccess AP
  to not accept new clients after many hours of containment. This has been corrected and Rogue
  Containment can be used without limitation.
- Fixed the condition for a 4101 or 4102 OmniAccess Wireless Appliance in which multicast traffic would not be passed to associated APs even when the "Enable Multicast" flag was turned on.
- Put a check in the Web interface to validate that complete and correct data is being returned to the server as it crafts the web page being requested during login. If there is incomplete or garbage data being returned (because of heavy load, network attacks, etc.) do not create the page and return an error to the user.

- Corrected an issue with intersubnet mobility with three or more Alcatel OmniAccess Switches and Appliances in the same mobility group.
- Increased the number of displayed characters in the Web interface for OmniAccess AP names.
- Fixed a race condition in the OmniAccess AP for up/down/new/delete events in LWAPP and the automatic processes like AireView Director.
- Fixed a counter reset error in 802.11 negotiations which might cause certain clients to think that they were the subject of a "replay" attack.

#### **Technical Notes**

- The Upgrade Process When an Alcatel OmniAccess Switch or Appliance is upgraded, the code on the associated OmniAccess APs is also upgraded. When an OmniAccess AP is loading code, each of its lights will blink in succession. Do not power down the an Alcatel OmniAccess Switch or Appliance or the OmniAccess AP during this process! Upgrading an Alcatel OmniAccess Switch or Appliance with a large number of OmniAccess APs can take as long as 30 minutes. The OmniAccess APs must remain powered and the an Alcatel OmniAccess Switch or Appliance must not be reset during this time.
- <u>Disable (Blacklist) Client Feature</u> If a client is not able to connect, and the security policy for the WLAN and/or client is correct, the client has probably been disabled. From the Web Management Interface, Monitor page under client summary, you can see the client's status. If they are disabled you can just do a "Remove" operation and the disable will then be cleared for that client. The client will automatically come back and, if necessary, reattempt authentication. Automatic disabling happens as a result of too many failed authentications. Note that clients disabled due to failed authorization do not show up on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.
- <u>IPSec Clients Supported in this Release</u> This release has been tested with the following IPSec clients:
  - NetScreen v8.0.0
  - Cisco Unity v3.6.2
  - SSH Sentinel v1.3.2(1)
  - Movian v3.0

Please note that the Netscreen client does not handle fragmented ICMP packets, doesn't respond to large ping packets, and does not work with certificates. Other IP fragmented traffic works fine.

- XAuth Configuration with NetScreen Do not enable XAuth on the NetScreen client. Configure XAuth on the Alcatel OmniAccess Switch or Appliance. The Alcatel OmniAccess Switch or Appliance initiates the XAuth session and the NetScreen client responds and begins interoperating. Configure the NetScreen client with pre-shared keys only. You also need to set up a separate connection in the clear to your DHCP server.
- Rekeys are not supported with Cisco VPN client If a rekey occurs clients must re-authenticate. To mitigate this problem, log into the Web Browser interface, navigate to the WLANs page, select Edit to display the WLANs > Edit page, choose Advanced Configuration, and change Lifetime (seconds) to a large value, such as 28800 seconds (this is the default), depending upon your security requirements.
- RADIUS Servers This product has been tested with the following RADIUS servers:
  - Odyssey Server and Odyssey Client v1.1 and 2.0 from Funk Software
  - Steel-Belted RADIUS from Funk Software version 4.40.337 Enterprise Edition
  - FreeRADIUS version 0.8.1 and 0.9.3, with OpenSSL 0.9.7B
  - Microsoft Internet Authentication Service (IAS) Version 5 on Windows 2000 Server/ SP4.
  - CiscoSecure ACS, v3.0, 3.1 and 3.2.
- Management Usernames and Local Netuser Usernames must be unique, because they are stored in the same database. That is, you cannot assign the same name to a Management User and a Local Netuser.

- When an Alcatel OmniAccess Switch or Appliance reboots, dropped OmniAccess 1200R APs attempt to associate with any available Alcatel OmniAccess Switch or Appliance. If the OmniAccess 1200R APs cannot contact an Alcatel OmniAccess Switch or Appliance, they continue to offer 802.11a/b/g service on WLAN 1 only.
- <u>WEP Keys</u> This release supports four separate WEP index keys. These keys cannot be duplicated between WLANs. At most four WEP WLANs can be configured on an Alcatel OmniAccess Switch or Appliance. Each of these WLANs must use a different key index.
- <u>DCA and Transmit Power Algorithms are designed to work with four or more OmniAccess APs</u> If there is a need to enable these algorithms for a smaller number of OmniAccess APs, please contact Alcatel Technical Support.
- <u>Using the Backup Image</u> The Alcatel OmniAccess Switch or Appliance ppcboot Bootloader stores a copy of the previous image. If the current image should get corrupted you can use ppcboot to boot with the backup image. After you have booted with the backup image, be sure to download a new current image. If you do not, then if the system resets it will come up with the corrupted current image once again.
- <u>Home page retains Web Auth login with IE 5.x</u> This is a caching issue in the user's Internet Explorer version 5.x browser. Clearing history will correct it, or upgrade your user to Internet Explorer version 6.x.
- RLDP Enable/Disable RLDP Enable/Disable refers to the RLDP protocol which detects rogues
  on your wired network. Autocontainment enable/disable indicates whether you want the Alcatel
  OmniAccess Switch or Appliance to automatically contain new Rogues that it finds on the wire.
  Disabling RLDP or autocontainment does not disable containment for Rogues that are being
  contained. When Rogues are being contained, you must manually disable containment for each
  Rogue individually.
- <u>Ad-hoc Rogue Containment</u> Client card implementations may mitigate the effectiveness of ad hoc containment.
- Apple iBook Note that some Apple OSs require shared key authentication for WEP. Other
  versions of the OS actually do not work with shared key WEP set unless the users saves the key
  in their key ring. How you should configure your Alcatel OmniAccess Switch or Appliance is
  based on the client mix you expect to use. Alcatel recommends testing these configurations
  before deployment.
- <u>Multicast</u> Only supported for voice applications.

## **Open Issues in Alcatel Wireless Operating System Software**

- VLAN trunks require Filters (9365) You must limit your trunks to only pass VLAN traffic to the
  Alcatel OmniAccess Switch or Appliance for those VLANs used by the Alcatel OmniAccess Switch
  or Appliance on that link. For example, Cisco switches will require filters to be placed on trunks
  going into the Alcatel OmniAccess Switch or Appliance. Failure to do this may result in
  unexpected behavior when large numbers of OmniAccess APs try to join the Alcatel OmniAccess
  Switch or Appliance.
- <u>AP-Manager and Management Interfaces must be on the same network and on the same port</u> (8028) This affects Layer 3 only.
- The Alcatel OmniAccess Switch or Appliance may need to be reset when disabling Web management (http/https) while using Web Authentication (4750) If you have WLANs that use Web Authentication, and you decide to disable management over the http/https (http + SSL) protocol that Web Authentication is using, a reset will be required before Web Authentication will work.
- <u>Client statistics are not updated for third-party AP clients (6027)</u> Administrators should note that this is a display issue only.
- <u>Client Totals (6823)</u> There is a very brief window when listing clients via either web or CLI, where a client may disassociate while the list is being generated. When this happens, the total number of clients may not match the number of clients list. Executing the command again or doing a refresh on the web case will provide you with a consistent list.
- <u>Centrino and other clients do not load balance (7172, 8885)</u> This may require a client card driver update. Please contact Alcatel Technical Support for more information.
- <u>Avaya client cannot connect under some circumstances using WPA-PSK (7890)</u> Alcatel is investigating this issue.
- Client must re-initiate IKE once IPSec lifetime has expired on the Switch (8113) When the Alcatel OmniAccess Switch or Appliance IPSec lifetime is expired, the client will need to reinitiate IKE to connect. Some clients provide that facility or the user may also stop and re-insert their WLAN cards to start a new session. To minimize this issue ensure that the lifetime setting on the Alcatel OmniAccess Switch or Appliance is high. Clients may rekey at a faster rate if desired.
- <u>WPA issues with some clients (8078, 8127)</u> We have seen issues with some of the latest WPA drivers from reference vendor Atheros. The Atheros 2.4.2.x drivers do not demonstrate these problems. This problem may effect many types of wireless cards.
- Link Test does not work with OmniAccess 1200R APs (8159).
- Client Statistics are not provided with OmniAccess 1200R APs (8160).
- <u>Issue with client to client multicast (7660, 8739)</u> Multicast works for server to client for Layer 2 LWAPP. Client to client multicast for Layer 3 LWAPP is not supported. There is no work around for the client to client issue.
- MAC Filtering does not work on Third-Party APs with 802.1x enabled on the Third-Party AP (8490).
- <u>Incompatibility with Vocera and aggressive load balancing (8746)</u> Please turn off aggressive load balancing when using Vocera.
- IBM 802.11 a/b/g card does not reassociate after being load balanced (8856) Either use other client cards or turn off aggressive load balancing.
- <u>Mobility issues with 802.11 a/b/g client card (8799)</u> This problem requires a client card driver upgrade. Please contact Alcatel Technical Support for more information.

- Session Time does not work when provided by Radius for Web Authentication (9121) The session time that is set on the WLAN is used instead.
- Show ARP does not always show ARP entry for APs (9332) This is a display issue only.
- Interoperability issues with Baystack 5510 switch and GigE (8793) Baystack 5510 switches are not supported in this release.
- <u>GigE interface is sometimes reported as down in the interface but the port is passing traffic (8972)</u> In this case the link light on the front of the Alcatel OmniAccess Switch or Appliance is a more accurate indicator of the status of the port.
- <u>Dell True Mobile 1300 will not authenticate with WPA/TKIP (9238)</u> Please use a different client card that supports WPA.
- <u>Spanning Tree is not fully functional (9347)</u> It does work for a short period of time but does not continue to work over night.
- Rare intermittent connectivity issues with Vocera (9213) This is not common and is under investigation.
- <u>Intermittent issues with Nortel clients doing 802.1x (9035)</u> sometimes the authentication does not go through. User should retry authentication.
- <u>AP crash during upgrade (9158)</u> On rare occurrences we have observed an AP crash during upgrade. The AP resets itself, comes up and provides service. There is no action required on the part of the administrator.
- <u>Semaphore messages in error log (9505)</u> Under some circumstances you may see error messages in the error log for semaphore or mutex timeouts. These messages can be safely ignored.
- <u>Enabling/Disabling Blacklisting can cause client disconnects (9467)</u> Enabling or disabling blacklisting on a WLAN causes the WLAN to be reset temporarily, which disconnects users. No warning is currently displayed.

# **Interoperability Tables**

The following table shows which WLAN cards have been tested and tracked for the Release 2.0 Alcatel Wireless Operating System.

WLAN Card	Radio	Status		
Cisco – Air-CB20A	802.11a	tested		
Orinoco Gold	802.11a/b	tested		
Centrino	802.11b	tested		
Linksys WPC11	802.11b	tested		
Linksys	802.11a/b	tested		
Netgear Prism 2.5 – MA401	802.11b	tested		
NetGear - WAG 511	802.11a/b/g	tested		
NetGear - WAB 501	802.11 a/b	tested		

The following table lists the 802.1X RADIUS Server - Supplicant support matrix.

Supplicant	Steel Belted				Odyssey			Microsoft IAS		Cisco ACS				
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	TTLS	PEAP	LEAP
Odyssey Client	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	not sup- ported	pass	not sup- ported
XP Native	pass	not sup- ported	pass	not sup- ported	pass	not sup- ported	pass	not sup- ported	pass	pass	pass	not sup- ported	pass	not sup- ported
win2k Native		not sup- ported		not sup- ported		not sup- ported		not sup- ported				not sup- ported		not sup- ported
Cisco ACU		not sup- ported		not sup- ported		not sup- ported						not sup- ported		not sup- ported

Notes:

### **ACS Software Release Notes 2.0.67.0**

System Release 2.0

This Release Note covers the OmniVista Air Control System Software (ACS), which can be used to configure, monitor, and control the Alcatel OmniAccess Wireless Enterprise Platform (Alcatel OmniAccess Wireless System). This document includes the following sections:

- Alcatel OmniAccess Wireless Enterprise Platform Components
- Requirements for OmniVista Air Control System
- New Features
- Improvements in this Release
- <u>Technical Notes for OmniVista Air Control System</u>
- <u>Technical Notes for Alcatel Site Survey Tool</u>
- Technical Notes for ACS Floor Plan Editor
- Open Issues in the OmniVista Air Control System Software

## **Alcatel OmniAccess Wireless Enterprise Platform Components**

- Alcatel Wireless Operating System (OmniAccess Wireless Switch, OmniAccess Wireless Appliance, and OmniAccess AP) Software.
- OmniVista Air Control System Software, Version 2.0.67.0.
- 4012 and 4024 Alcatel OmniAccess Wireless Switches.
- 4102 OmniAccess Wireless Appliances.
- OAW-1200ABGE, OAW-1200BGE, OAW-1200ABG and OAW-1200BG Alcatel OmniAccess Wireless Access Point (OmniAccess AP), and OAW-1200ABGR Alcatel OmniAccess Remote Edge Access Point (OmniAccess AP 1200R).

# Requirements for OmniVista Air Control System

- Requirements for OmniVista Air Control System Server The ACS Software Server can be run on a workstation/server class system: Pentium 4, 2.4 GHz or faster, with 1 GB or more RAM, running Windows 2000/SP4 with all critical and security Windows updates installed.
- <u>Requirements for ACS Software Browser Client</u> The ACS Software Browser Client requires Internet Explorer 6.0/SP1 or later.

## **New Features**

• There are no new features in this maintenance release.

# Improvements in this Release

• The ACS database took up 100% of the CPU cycles and the system appeared to hang (9122) – This issue has been fixed in this release.

## **Technical Notes for the OmniVista Air Control System**

- <u>ACS Software Server Upgrade</u> ACS Software Server Upgrade instructions are included in the <u>ACS Quick Installation Guide</u> When you are upgrading from Release 2.0.44.14 or later, the existing ACS database and floorplan map backup procedure is in the <u>Alcatel OmniAccess Wireless Product Guide</u>, and the new Restore and Update instructions are in the <u>ACS Quick Installation Guide</u>, which is also included in the <u>Alcatel OmniAccess Wireless Product Guide</u>.
  - When restoring the database from ACS Release 2.0.65.1, the user receives a warning message: "The version of the restored database is different from the installed software version. If these are incompatible, the software will fail to start". This message may be ignored since the database schema in Release 2.0.67.0 is compatible with the database from ACS Release 2.0.65.1.
- <u>Compatibility</u> This version of ACS Software is compatible with Alcatel Wireless Operating System Release 2.0.90.13 or later.
- ACS Software Server Location and IP Addresses The ACS Software Server is intended to be
  run on a robust desktop or rack-mount machine in a server room, while the ACS Software
  Browser Client and the ACS Software Java Admin Client are intended be run on an administrator's desktop. If you need to change the IP parameters on the ACS Software Server
  workstation, such as the IP Address or the default gateway, please shut down the ACS Software
  Server before making the change, and bring the ACS Software Server up after your IP configuration changes are complete.
- Restoring Alcatel OmniAccess Switch or Appliance Configurations For security reasons, the Alcatel OmniAccess Switch or Appliance does not allow community strings and shared keys to be read through SNMP once they are created. As a result, if any of these were created through SNMP or CLI interfaces and subsequently a restore configuration (after clearing configuration on the device) was done on the Alcatel OmniAccess Switch or Appliance from ACS, these changes will have to be manually reapplied to the Alcatel OmniAccess Switch or Appliance. This is because the ACS configuration database does not retain these values if they are applied through other interfaces.

#### Client Location Notes:

- Power management of Laptops can sometimes affect the client transmit output power, which may affect the location accuracy as the client may seem farther away from each AP
- Location of some clients will not be displayed correctly under Recent Map. Immediate effect can be obtained by using Present Map.
- Using the location Present Map to locate some clients like Linksys WPC55AG will result in only the associated AP detecting the client.
- Adding Floor Maps to the OmniVista Air Control System Software When using the ACS coverage map feature, you can import a copy of your floor maps in .FPE, .JPG, .GIF or .PNG format from anywhere in your file directory structure. After that, the images will be available through the ACS Software Browser Client when Configuring AP Areas, and the images will be automatically backed up when an ACS backup is performed.

## **Technical Notes for the Alcatel Site Survey Tool**

- These Technical Notes apply to Release 2.0.258.0 of the Alcatel Site Survey Tool.
- Please refer to the <u>Alcatel Site Survey Tool User Guide</u> for more information on doing site surveys using Version 2.9 of the Alcatel Site Survey Tool.
- For optimal performance, use the D-Link DWL-AG650 card.
- Surveys for 802.11a and 802.11b must be run independently. Perform two separate surveys and save as two separate projects. You may need to select and deselect the "in use" box to get the 802.11a and 802.11b band selection to appear.
  - To select 802.11a or 802.11b band, go to the Site Survey device tab and select the device first.
  - Click on the device description and you will see the band list in the lower right window. If the device use button is deselected, no signal strength is recorded.
- Client utilities (including zero config) should not be used with the Site Survey tool. When installing Atheros drivers, please choose the "install only driver" option and not the recommended "install driver and application" option.
- When switching from 802.11a to 802.11b site survey mode or vice versa, please completely shut down the Site Survey application and restart it.

#### **Technical Notes for the ACS Floor Plan Editor**

- The Version 2.9 ACS Floor Plan Editor is distributed with ACS to provide accurate RF prediction on ACS floor maps. To install just run Alcatel-FPE-2.9.exe from the top level directory of your ACS CD-ROM.
- Recommendation for Floor Maps Make the long side of the building map the horizontal direction to optimize the display in ACS.
- The perimeter wall-type is not functional in this release It is reserved for future use.

## Open Issues in the OmniVista Air Control System Software

- The ACS Software Server Hostname Cannot Begin with a Number (6205) The ACS Software Client cannot attach to an ACS Software Server with a hostname that starts with a number. If the ACS Software Server is installed as a Service, the service will not start. Please install the ACS Software Server only on a machine whose hostname begins with a letter. This is a bug with Java version 1.4.1 and will be fixed in a later release.
- <u>Issue with Special Characters in Names (6430)</u> Alcatel OmniAccess Switches and Appliances
  that have names with special characters in AP names, SSIDs, etc. cannot be imported into the
  ACS database.
- <u>User May Experience a Login Delay After Starting the ACS Software Server (6713)</u> After starting the ACS Software Server, the first login may take longer than usual. Subsequent logins will be much quicker. This will be resolved in a future release
- <u>Cannot manage IOS-based Cisco APs</u> The Cisco 1200 AP now allows the user to upgrade to an IOS-based OS. This software is not compatible with ACS.
- ACS server should be on the same side of a firewall as the Alcatel OmniAccess Switches and Appliances it is managing (7967) This is true unless the firewall can be configured to handle fragmented packets.
- <u>Unable to add IPSec Certificates (6969)</u> There is an issue with adding IPSec CA and ID Certificates via the ACS. Please use the Switch Web Browser Interface.
- <u>ACS installer fails when Kanji characters are in the directory path (9496)</u> ACS fails to install if the directory path containing the executable or the path to the target install directory contains Kanji characters. As a workaround, please install ACS from and to a directory that contains only English characters.
- MAC address filter added from ACS shows as read-only (9474) If you create a Client MAC address filter in ACS, it gets labeled as read-only. This can be ignored since read-write access privileges do not apply to MAC filters.

Notes: