

AirMagnet[®] Enterprise

User Guide



© 2003-2012 Fluke Corporation. All Rights Reserved.

AirMagnet® Enterprise User Guide.

This *User Guide* is furnished under license and may be used or copied only in accordance with the terms specified in the license. The content of this document is for information only and should not be construed as a commitment on the part of AirMagnet, Inc.

No part of this document may be reproduced, transmitted, stored in a retrievable system, or translated into any language in any form or by any means without the prior written consent of AirMagnet, Inc. Further, AirMagnet, Inc. reserves the right to modify the content of this document without notice.

AIRMAGNET, INC. SHALL NOT BE HELD LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THIS CONTENT.

This product includes software developed by David Young. Copyright 2003, 2004. All rights reserved.

This product includes software developed by Atsushi Onoe. Copyright 2001. All rights reserved.

This product includes software developed by Sam Leffler, Errno Consulting. Copyright 2002-2005. All rights reserved.

This product includes software developed by Bill Paul <wpaul@ctr.columbia.edu>. Copyright 1997, 1998, 1999. All rights reserved.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm. Copyright 1990-1992 RSA Data Security, Inc. All rights reserved.

Registered users may log into [MyAirMagnet](#) to download the available open source software utilized in AirMagnet Enterprise.

AirMagnet® and AirWISE® are registered trademarks, and the AirMagnet logo is a trademark, of AirMagnet, Inc. All the other product names mentioned herein may be trademarks or registered trademarks of their respective owners.

U.S. Patent Numbers 7,009,957, 7,130,289, and 7,613,139

AirMagnet, Inc.

2575 Augustine Drive

Santa Clara, CA 95054

USA

Compiled in the United States of America

Part Number: AME-v10.1-USG-01-0412

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, RETURN THE UNUSED AIRMAGNET SOFTWARE WITHIN 30 DAYS TO THE PLACE WHERE YOU OBTAINED IT FOR A REFUND.

1. GRANT OF LICENSE.

Fluke Networks, a division of Fluke Electronics Corporation grants you a non-exclusive right to install and use the AirMagnet Software on a single computer at a time. The software, documentation and any fonts accompanying this License whether on disk, in read only memory, on any other media or in any other form (the "AirMagnet Software") are licensed to you by Fluke Networks.

2. TITLE, COPYRIGHT, AND TRADEMARK.

Software is owned by Fluke Electronics Corporation and is protected by United States copyrights laws and international treaty provisions. Therefore you must treat the Software like any other copyrighted material. You own the media on which the AirMagnet Software is recorded but Fluke Networks and/or Fluke Networks' licensor(s) retain title to the AirMagnet Software. The AirMagnet Software in this package and any copies which this License authorizes you to make are subject to this License.

3. PERMITTED USES AND RESTRICTIONS.

This License does not allow the AirMagnet Software to exist on more than one computer at a time. You may make one copy of the AirMagnet Software in machine-readable form for backup purposes only. The backup copy must include all copyright information contained on the original. Except as expressly permitted in this License, you may not decompile, reverse engineer, disassemble, modify, rent, lease, loan, sublicense, distribute or create derivative works based upon the AirMagnet Software in whole or part or transmit the AirMagnet Software over a network. You may not disclose any information relating to the performance or operation of the AirMagnet Software (including any benchmarking or other testing results) to any third party without Fluke Networks' express prior written consent. You may, however, transfer your rights under this License provided you transfer the related documentation, this License and a copy of the AirMagnet Software to a party who agrees to accept the terms of this License and destroy any other copies of the AirMagnet Software in your possession. You may not use or otherwise export or re-export the AirMagnet Software except as authorized by United States law and the laws of the jurisdiction in which the AirMagnet Software was obtained. In particular, but without limitation, the AirMagnet Software may not be exported or reexported (i) into (or to a national or resident of) any U.S. embargoed country or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders. By using the AirMagnet Software, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

4. TERMINATION.

Your rights under this License will terminate automatically without notice from Fluke Networks if you fail to comply with any term(s) of this License.

5. LIMITED WARRANTY.

Fluke Network warrants the media on which the AirMagnet Software is recorded to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of original retail purchase. Fluke Networks does not warrant any downloading errors or that the Software will be error free or operate without interruption. Fluke Networks' entire liability and your exclusive remedy shall be, at Fluke Networks' option, a refund of the purchase price of the product containing the AirMagnet Software or replacement of the AirMagnet Software which is returned to Fluke Networks or an authorized representative with a copy of the receipt. This limited warranty is void if failure of the products has resulted from accident, abuse, or misapplication. Any replacement product will be warranted for the remainder of the 90 day original warranty period or 30 days, whichever is longer.

6. DISCLAIMER OF WARRANTY ON AIRMAGNET SOFTWARE.

Other than as provided in the Limited Warranty above, The AirMagnet Software is provided "AS IS" and without further warranty. FLUKE NETWORKS EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE AIRMAGNET SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE AIRMAGNET SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE AIRMAGNET SOFTWARE WILL BE CORRECTED. FURTHERMORE, FLUKE NETWORKS DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE AIRMAGNET SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY AIRMAGNET OR AN AIRMAGNET AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL FLUKE NETWORKS BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Fluke Networks total liability to you for all damages exceed the amounts paid by you hereunder.

8. GOVERNMENT END USERS.

If the AirMagnet Software is supplied to the United States Government, the AirMagnet Software is classified as “restricted computer software” as defined in clause 52.227-19 of the FAR. The United States Government's rights to the AirMagnet Software are as provided in clause 52.227-19 of the FAR.

9. CONTROLLING LAW AND SEVERABILITY.

This License shall be governed by the laws of the United States and the State of Washington, U.S.A. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

10. COMPLETE AGREEMENT.

This License constitutes the entire agreement between the parties with respect to the use of the AirMagnet Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Fluke Networks.

Disclaimer

AirMagnet DoD (Department of Defense), GLBA (Gramm, Leach, Bliley Act), HIPAA (Health Information Portability and Accountability Act), and SOX (Sarbanes Oxley Act 2002) Policy Compliance Reports provide a security framework intended to assist you in complying with various regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on wireless network security and aim to guide network administrators in documenting their security policies and responding to security threats and incidents.

AirMagnet's customers are responsible for ensuring their own compliance with applicable laws and regulations. While the AirMagnet Policy Compliance Reports provide information about the law and are designed to help users satisfy government regulations, such information is not legal advice, and it is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant law or regulation. AirMagnet does not represent or warrant that its services, products or any other information it provides to a customer will ensure that the customer is in compliance with any law or regulation.

The information contained in the Policy Compliance Reports is furnished under and subject to the terms of the Software License Agreement ("License"). The Policy Compliance Reports do not create a binding business, legal, or professional services relationship between you and AirMagnet, Inc.

Because business practice, technology, and governing laws and regulations vary by industry and location, full compliance with regulations will depend on an organization's particular circumstances. AirMagnet Policy Compliance Reports document an organization's wireless network security framework for authentication, access control, and encryption. The Reports are intended to provide useful information to determine whether wireless network security policies are implemented correctly and provide an integral framework to guide network administrators to respond to security threats and incidents in a consistent, compliant, and approved manner.

AirMagnet System Level and Device Level Compliance Reports provide information to assist its customers in determining whether they are in compliance with various standards, laws and regulations applicable to wireless networks and devices operating in the unregulated radio frequencies (2.4 – 5 GHz). It is intended to assist customers in identifying wireless networks and devices not in compliance with security frameworks such as FISMA (Federal Information Security Management Act) and US federal regulations implementing laws such as GLBA, HIPAA, SOX, and more.

AirMagnet is **not** responsible for an organization's compliance with industry standards or legal regulations. AirMagnet should be used by organizations as an aid in satisfying the organization's compliance requirements for standards, laws, and regulations.

AirMagnet operation is limited to wireless networks and devices operating in the unregulated radio frequencies (2.4 – 5 GHz). It operates and reports on networks and devices that use wireless technologies. It does **not** apply to wire-line networks and devices **not** operating in the wireless spectrum.

AirMagnet, Inc.

Table of Contents

Software License Agreement	i
Disclaimer	v
Part I: AirMagnet Enterprise System	xxv
Chapter 1: AirMagnet Enterprise Overview	1
Enterprise-hardened Wireless Intrusion Prevention	1
Automated Intrusion Prevention	1
Superior Detection	1
Automated, Active Defenses	1
3D Rogue Control	2
Detect	2
Disable	2
Document	2
Full Disclosure Policy View	3
Tailored Policy Creation	3
Security- or Performance-Only User Role	3
Streamlined Analysis and Investigation	3
Notification and Escalation	3
Integrated Reporting	3
Compliance Reporting	4
SmartEdge Architecture	4
Local Analysis	4
Fast, Secure Deployments	4
Protect Your Bandwidth	4
Enterprise Scalability and Fail-over	4
Device-Specific Alarm List	5
Embedded AirMagnet Spectrum Analyzer Sensor	5
SSH Support on Sensors	5
Database Backup/Restore/Reset	5
Device Locator	5
“Rogue AP Detected Inside” Alarm	6
Server to Console Data Compression	6
Managing Network ACL Groups	6
Showing Rogue-Detecting Sensors	6
Oracle Database Support	6
PostgreSQL Database Support	6

Software Update from Enterprise Console	7
Adding Comments to GPS Log Files	7
Addition of Two New Policy Profiles	7
AirMagnet Enterprise System Components	8
AirMagnet Enterprise Server	8
AirMagnet Enterprise Console	9
AirMagnet SmartEdge Sensor	9
Product Documentation	9
Online Help	9
AirMagnet WLAN Policy Reference Guide	10
Release Notes	10
AirMagnet SmartEdge Sensors	10
Frequently Asked Questions (FAQs)	10
Chapter 2: Installing AirMagnet Enterprise	11
Product Package Contents	11
Product Registration	11
Technical Support	12
Contact Customer Support	12
AirWISE Community	13
AirMagnet Enterprise Installation Overview	13
Database Server Prerequisite	14
Performing Product Upgrades or Downgrades	14
Downgrade Procedure	15
AirMagnet Enterprise Server Installation	15
Notes on AirMagnet Enterprise Server Installation	16
Special Notes on Backup Server Installation	17
AirMagnet Enterprise System Requirements	17
Server operating systems*	17
Supported databases	17
Console operating systems*	17
Installing AirMagnet Enterprise Server	20
Using a Backup AirMagnet Enterprise Server	28
Registering Your AirMagnet Enterprise	28
AirMagnet Enterprise Server Web Page	29
AirMagnet Enterprise Console Installation	29
AirMagnet Enterprise Console System Requirements	29
Downloading AirMagnet Enterprise Console	29
Installing AirMagnet Enterprise Console	31
Verifying AirMagnet Enterprise Console Installation	32
AirMagnet SmartEdge Sensor Configuration	34
Configuring SmartEdge Sensor via Web Browser	34
Configuring SmartEdge Sensor via Sensor Serial Console Port	40

Verifying Sensor Configuration Using Show Commands	42
Maintenance Commands	42
FIPS-Required Features	45
Zeroizing an AirMagnet Sensor	47
International Power Standards	48
Verifying AirMagnet SmartEdge Sensor Installation	48
Software Sensor Agent (SSA)	50
Introduction	50
Special Notes	50
Installation Methods	51
SSA System Requirements	51
SSA Installation	51
Unattended method	51
Manual method	51
AirMagnet Console and SSA	52
Getting Software and License from My AirMagnet	53
Chapter 3: Deploying AirMagnet Enterprise	55
Preparation for System Deployment	55
Scenarios for AirMagnet Enterprise Server Setup	57
How Many SmartEdge Sensors Do I Need?	57
Basic Concepts	57
Sensor Field of View (FOV)	58
Trusted Devices	58
Unauthorized WLAN Devices	58
Radio Receiver Sensitivity/Link Budget	58
802.11 RF Media Types	58
WLAN Device Detection Science 101	59
WLAN Device Detection Science 102	59
Sensor FOV Types	59
Type A: All Trusted Traffic Monitoring	59
Type B: Trusted AP Monitoring	60
Type C: Unauthorized Device Detection	60
Factors Affecting SmartEdge Sensor FOV Performance	60
SmartEdge Sensor Installation Restrictions	61
Office with Dense Central Core	61
Microcell Network	61
SmartEdge Sensor Network Design Objectives	61
Measurement Process Overview	62
Unauthorized Device Detection Measurements	62
Sample Design Results Review and Conclusion	63
Part II: AirMagnet Enterprise Console	65

Chapter 4: Enterprise Console Basics.....	67
Introduction	67
Launching AirMagnet Enterprise Console	67
Console UI Components	68
Navigation Bar	68
Network Tree.....	70
Server Status Indicator	70
Sensor Filter	71
Network Building Tools	72
Enabling 802.11n Support.....	73
Connect Menu	74
Manage Menu.....	74
View Reports	76
The Toolbar	76
Help Menu	77
Using the View Filter.....	77
Setting Up a Network Tree	79
Managing Console-Server Connection	80
Adding AirMagnet Enterprise Servers to the Console.....	81
Removing Servers from the Console.....	82
Changing Server Login Settings	82
Connecting to AirMagnet SmartEdge Sensors	83
Exiting AirMagnet Enterprise Console.....	84
Accessing Network Audit Log.....	84
Audit Log Screen Components.....	85
Customizing an Audit Log	86
Printing an Audit Log	86
Exporting an Audit Log	86
Managing ACL Groups.....	87
Creating ACL Groups	87
Deleting ACL Groups.....	88
Wired ACL.....	89
Assigning Devices to ACL Groups	90
Adding Devices to Your AirMagnet Enterprise System	90
AirMagnet Enterprise Console User Management.....	92
User Roles and Privileges	93
Adding Users to AirMagnet Enterprise Console	94
Removing Users from the Console User List.....	103
Choosing User Display Options	103
Managing AirMagnet SmartEdge Sensors.....	103
Accessing the Manage Sensors Screen.....	103
Sensor Screen Control Buttons.....	104
Sensor Table Data Fields.....	105

Monitoring Sensors on the Network.....	105
Modifying Sensor Properties.....	106
Deleting Sensors.....	109
Finding Sensors	110
Importing Sensor Data	112
Exporting Sensor Data	112
Managing AirMagnet Enterprise Database	113
Backing Up the Current Database	114
Restoring a Database Backup File	115
Deleting a Database Backup File	117
Cleaning Up Database Tables	117
Chapter 5: Using the Start Screen	121
Introduction	121
Overall View	121
Major UI Components.....	122
The Toolbar.....	122
Network Tree.....	122
Network Information	123
Network Information Components.....	123
Server Summary.....	123
Security Status	124
Rogue Device Status.....	124
Compliance Status	124
Performance Status	124
VIP Device Status.....	124
Problem Device Status	125
Chart Display.....	125
Classic View.....	125
Major UI Components.....	126
Network Tree.....	126
Time Frame Selector	127
Alarm Overview	127
AP Information by Hour.....	128
STA Information by Hour	129
Most Events per AP/STA/AdHoc.....	130
Most Active APs/SSIDs.....	131
New AP/STA/AdHoc.....	132
Using the AirMagnet Alert Window	132
Controls on the Alert Window.....	135
Customizing Alert Window Display	136

Chapter 6: Using the AirWISE Screen139

Introduction	139
Major UI Components.....	140
Easy View Options.....	140
General Alarm Views	141
Security Views	142
Performance Alarm Views	143
Problem Device Views	143
VIP Views.....	144
Compliance Views	144
Policies & Alarms Tree.....	145
Policy/Alarm Description	147
Alarm Tab	147
Live Stats	148
Live Graphs.....	151
Association Tab	152
Sensor Tab	153
Using Forensics Information	154
Activating Forensic Logging	154
Adding Forensics Notifications	154
Configuring Forensics Notifications on Specific Alarms.....	154
Viewing Forensics Data	156

Chapter 7: Using the Infrastructure Screen.....159

Introduction	159
Major Components of the Infrastructure Screen	159
Network Tree.....	160
Easy View Options.....	160
Infrastructure View	161
Infrastructure Hierarchy List Tab.....	162
Rogue View	162
Device Management Tools	163
Importing and Exporting ACL Data	164
Device List.....	165
Device Information	167
Adding Devices to the Device List	167
Re-categorizing Devices	170

Chapter 8: Rogue Management View173

Introduction	173
Rogue Management View Sections	174
Rogue	174

Newly Detected Rogue	176
Rogue Management.....	176
Establishing Multi-layered Tracing to Identify Rogue Devices.....	177
Rogue Identification by Wireless Tracing	177
Rogue Identification by Switch Tracing	178
To establish Sensor-based switch tracing.....	179
To establish Server-based switch tracing.....	180
Rogue Identification by Wired Listening (hub correlation)	180
Rogue Identification by Passive Detection.....	181
Rogue Identification by Enhanced Rogue on wire	181
To establish Enhanced Rogue on Wire:	181
Automatic Rogue Traffic Blocking	182
Wired Traffic Blocking	182
Enabling Wired Blocking.....	182
Wireless Traffic Blocking	183
Enabling wireless blocking.....	183
Defining Policy Profiles to Detect Rogue Devices	184
Rogue Management Examples	186
Chapter 9: Viewing Top Analyses	193
Introduction.....	193
Major UI Components.....	193
Using the Easy View.....	194
Chart Display.....	195
Working in the Top Analysis Screen.....	196
Sample Analysis Charts	196
Chapter 10: Locating Rogue Devices	199
Introduction.....	199
Enabling the Device Locator	199
Major UI Components.....	200
Network Tree.....	200
Toolbar.....	201
Map Frame.....	201
Probability Meter	201
Configuring the Floor Plan.....	202
Configuring a Floor Map	202
Configuring the Network Space	204
Configuring Site Boundaries	205
Placing Sensors on the Floor Plan.....	206
Locating Rogue APs	206
Locating Rogue Stations.....	208
Displaying AirMagnet Survey Heat Maps.....	208

Chapter 11: Using the Reports Screen.....211

Introduction	211
Major UI Components.....	211
Managing Report Books.....	212
Creating a Report Book	213
Adding Reports to a Book	214
Deleting Reports from a Book.....	214
Searching Text through a Report.....	214
Modifying Book Properties	215
Modifying Report Contents.....	215
Printing Data Reports.....	216
Exporting a Report or Report Book.....	217
Automatic Report Generation.....	217
Configuring the Report Email Server	218
Scheduling a New Auto Report Task.....	219
Compliance Reports	221
Department of Defense Directive 8100.2	221
Health Insurance Portability and Accountability Act	222
Gramm-Leach Bliley Act.....	222
Sarbanes-Oxley Act.....	222
Payment Card Industry Data Security Standard	222
Basel II	222
EU CRD/CAD3.....	223
ISO 27001.....	223
FISMA.....	223
Compliance Reports Disclaimer	224
Customizing Compliance Reports.....	224

Chapter 12: Managing Policy Profiles.....227

Introduction	227
Policy Profile Creation Procedures.....	227
Creating Network Policy Profiles	228
Creating a Policy Profile from Scratch	228
Using a Pre-Configured Policy Profile.....	230
Exporting and Importing Policy Profiles	231
Exporting Policy Profiles and Notifications.....	231
Importing Profiles and Notifications	233
Managing Network Policies	234
Working with the Policy Wizard.....	237
Working with the Notification Wizard.....	240
Assigning Notifications to Alarms.....	240
Adding Notification Options	241
Modifying Existing Notification Settings.....	242

Deleting a Notification	242
Working with the Score Wizard	242
Configuring Policy Options	243
802.11 Settings	243
Configuring WEP Authentication	245
Rogue Management.....	246
Channel Scan	246
Scanning Extended 802.11a Channels.....	247
Implementing Policy Profiles.....	247
 Chapter 13: Configuring System Settings	251
Introduction.....	251
Console Settings	251
Server Settings	252
Configuring a Hot-Swap Server	255
Sensor Settings.....	255
Configuring Notification List.....	257
Configuring SysLog Notification.....	258
Configuring Email Notification	259
Configuring SNMP Notification.....	261
Configuring SMS-via-Email Notification	264
Configuring Page-Over-Phone Notification	265
Configuring Page-over-Internet Notification	266
Configuring Sound Notification.....	268
Configuring Instant Messenger Notification	268
Configuring Event Log Notification	270
Configuring Print Notification.....	270
Configuring Device Block Notification	271
Configuring Forensics Notifications	273
Configuring Device Classification Notification	274
Configuring the Shared Secret Key	275
Database Settings	275
Enabling Sensor Zero Configuration	277
Pre-Installation Model.....	277
Post-Installation Model.....	278
Vendor IEEE OUIs	279
AP Grouping.....	280
Auto Group Rules.....	282
Manual Group Rules	283
Device Classification	283
Importing ACL from Other Vendors	285
Custom Settings	287
WLC Settings	289

Chapter 14: Automated Health Check (AHC)	295
Introduction	295
Enabling AHC mode on a sensor	295
Configuring AHC in the AME console	295
Assigning AHC jobs to a sensor	299
Viewing AHC Results	300
Trends	301
 Part III: AirMagnet Remote Analyzer	 303
 Chapter 15: Introducing Remote Analyzer	 305
Chapter Summary	305
Launching Remote Analyzer	305
Navigation Bar	306
View Filter	308
Applying Filters	308
Channel Tab	308
SSID Tab	309
Device Tab	309
AirWISE Tab	309
How-To Guide	309
Toolbar	310
Working on Start Screen	312
Start Screen UI Components	312
Toolbar Options	312
Text-Search Tool	312
Easy View Button	313
OK/R(ogue) Buttons	313
RF Signal Meter	313
RF Signal Quality Codes	314
Expanded RF Graphs	315
802.11n 20-/40-MHz Channels	316
802.11 Information	316
AirWISE Advice	317
Pie Chart	317
Packet Frames Summary	318
Device Data	319
Using Bubble Help	324
AirWISE Details	325
Changing Operating Frequency	325
802.11 Protocols and Operating Frequencies	326
Changing RF Signal Unit of Measurement	326

Worldwide 802.11 a/b/g/n Radio Channel Allocation	327
Accessing Data Reports.....	327
Working on Channel Screen.....	328
Channel Utilization and Throughput	328
Channel Selection Pane	328
Link Speed and Media Type	330
Channel Data Summary	330
Device Data Graph.....	331
Analyzing Channel Occupancy	332
Working on Interference Screen	333
Interference Score.....	334
Channel Interference Calculation.....	335
Channel Interference Summary	336
Interfering Devices.....	339
Hidden Devices.....	339
Graph Pane	340
Working on the Infrastructure Screen	341
Network Tree Structure	342
Network Infrastructure Color Codes	343
Analyzing Data of Individual Devices	343
The Infrastructure Data Graphs.....	343
Infrastructure Data Summary	344
Infrastructure Data Pie Chart.....	345
Alarm Status	345
802.11d/h Information.....	345
Viewing Connections between Devices.....	345
Peer-to-Peer Connections.....	345
Peer-AP-Peer Connections	346
Working on AirWISE Screen.....	347
AirWISE Screen Viewing Options.....	348
Managing Alarm List	349
Analyzing Network Policy Alarms	350
Expert Advice.....	350
Data Analysis.....	351
Viewing All Alarms Generated by a Specific Device	351
Working on Top Traffic Analysis Screen.....	353
Top Traffic Analysis Screen UI Components.....	353
Viewing Device Charts.....	354
Exporting Chart Data	355
Choosing a Graph Option.....	355
Chart Data Tabulation.....	356
Viewing Compliance Charts	357
Basel II	357
DOD 8100.2	357

EU-CRD	358
FISMA	358
GLBA	358
HIPAA	358
ISO 27001	358
PCI DSS	359
SOX	359
Viewing Compliance Charts	360
Viewing Compliance Reports	360
Compliance Reports Disclaimer	360
Working on Decodes Screen	361
Filtering Packet Captures	362
Basic Procedures for Using Filters	363
Creating Custom Filers	363
Using a Custom Filter	363
Deleting a Custom Filter	364
Conducting Packet Decoding	364
Finding Packets on Decodes Screen	365
The Embedded AirMagnet Remote Spectrum Analyzer	366
Enabling AirMagnet Remote Spectrum Analyzer	366
Launching AirMagnet Remote Spectrum Analyzer	367
Accessing Remote Spectrum Analyzer User Documentation	368
Device Detection	369
Non-WiFi (Spectrum) Devices	370
Bluetooth Devices	370
RF Spectrum Pattern	370
Impact on 802.11b/g WLAN	371
Recommended Courses of Action	371
Digital Cordless Phones	372
RF Spectrum Pattern	372
Impact on 802.11 WLAN	373
Recommended Courses of Action	373
Analog Cordless Phones	374
RF Spectrum Pattern	374
Impact on 802.11 WLAN	375
Recommended Courses of Action	375
Microwave Ovens	376
RF Spectrum Pattern	376
Impact on 802.11b/g WLAN	376
Recommended Courses of Action	376
Wireless Cameras	377
RF Spectrum Pattern	377
Impact on 802.11b/g WLAN	378
Recommended Courses of Action	378

Baby Monitors	378
RF Spectrum Pattern.....	378
Impact on WiFi Networks	379
Recommended Courses of Action	379
RF and Narrowband Jammer	379
RF Spectrum Pattern.....	379
Impact on WiFi on WiFi Networks	380
Recommended Course of Actions	381
Digital Video Monitors	381
RF Spectrum Pattern.....	381
Impact on 802.11b/g WLAN.....	382
Recommended Courses of Action	382
Zigbee	382
RF Spectrum Pattern.....	382
Impact on 802.11b/g WLAN.....	383
Recommended Courses of Action	383
Radar.....	384
Introduction	384
Impact on 802.11 WLAN.....	384
Recommended Courses of Action	384
Motion Detector	385
RF Spectrum Pattern.....	385
Impact on 802.11 WLAN.....	386
Recommended Courses of Action	386
RF Signal Generator.....	386
Recommended Courses of Action	386
Impact on 802.11 WLAN.....	387
Recommended Course of Action.....	387
Non-Bluetooth Wireless Mouse.....	388
RF Spectrum Pattern.....	388
Impact on 802.11 WLAN.....	389
Recommended Course of Action.....	390
Game Controller.....	390
RF Spectrum Pattern.....	390
Impact on 802.11b/g WLAN.....	391
Recommended Courses of Action	391
WiFi Devices	391
802.11 a/g/n APs.....	391
RF Spectrum Pattern.....	392
Impact on WiFi Networks	393
Recommended Courses of Action	393
802.11b APs	394
RF Spectrum Pattern.....	394
Impact on WiFi Networks	395

Recommended Courses of Action	395
Chapter 16: Configuring Remote Analyzer	397
Introduction	397
Sensor Settings	397
General Settings	397
Configuring SmartEdge Sensor's 802.11 Settings	399
Configuring WEP Settings	401
Configuring SmartEdge Sensor Packet Capture Filters	402
Removing an Existing Filter	404
Configuring Sensor Channel Scan Settings	404
Customizing the User Interface	406
Chapter 17: WLAN Management Tools.....	409
Introduction	409
Troubleshooting the Link Connection	409
Diagnosing Network Connectivity Problems.....	409
Verifying Station-AP Association.....	409
Verifying DHCP IP Address Acquisition.....	411
Verifying DNS Name Resolution	412
Reaching an End Node with Default Gateway	412
Tracing Network Devices	413
802.11n Network Tools.....	413
802.11n Efficiency	413
802.11n Analysis.....	416
Simulating WLAN Throughput.....	418
Configuring WLAN Throughput Simulator.....	418
Conducting WLAN Throughput Simulations	419
Simulated WLAN Throughput.....	420
Calculating Device Throughput	421
Chapter 18: Managing Data Files.....	425
Introduction	425
Saving Captured Data	425
AirMagnet-Supported File Formats	425
Saving a New .amc File.....	425
Saving an Existing File in a Different Format	425
Opening a Saved File.....	426
Previewing Data Prior to Printing.....	426
Part IV: Appendices & Index	429

Appendix A: Secure Communication	431
Firewall Configuration.....	431
Proxy Servers.....	431
Outgoing Proxy	431
Incoming Proxy	431
Static NAT.....	431
Port Forwarding.....	432
Appendix B: System Troubleshooting.....	433
Appendix C: Enterprise Deployment.....	435
Introduction	435
AirMagnet Enterprise Server Deployment	435
Notes on AirMagnet Enterprise Server Installation	435
Special Notes on Backup Server Installation	435
Configuring AirMagnet Sensors.....	436
Zero Configuration Options.....	436
Manual Configuration Options	437
Working with Firewalls, VPNs, and NATs.....	437
Firewall Configuration.....	437
Proxy Servers.....	438
Wireless Policies and Enforcement	439
System Troubleshooting	440
Database Issues	441
Sensor Issues.....	441
General and Administrative Issues.....	442
Appendix D: SNMP Integration	445
SNMP Support	445
Enabling SNMP.....	445
Appendix E: Manual Rogue Trace.....	447
Appendix F: FIPS 140-2 Secure Operation	449
Information for Local Crypto Officers	449
Installing and Configuring the Sensor.....	449
Maintaining the Sensor in FIPS Approved Mode	450
Setting the Shared Key	451
Removing the Sensor from Service	451
Information for Remote Crypto Officers.....	451
Installing and Configuring the Sensor.....	452

Setting the Shared Key	452
Removing the Sensor from Service	453
Maintaining the Sensor in FIPS Approved Mode	453
Setting the Browser to Use TLS.....	453
Information for Users	454
Protect Your Password.....	454
Reference Information.....	454
Appendix G: Installing Oracle Database	455
Creating an Oracle Database	455
Creating User Profiles	462
Configuring Oracle Client	466
Using an Oracle Database Server	471
Appendix H: Installing PostgreSQL Database.....	475
Setting up the PostgreSQL Database	475
Creating a new AirMagnet Database.....	477
Installing AirMagnet Enterprise	479
Appendix I: Third-Party Copyrights	483
D. Young Copyright	483
A. Onoe & S. Leffler Copyright.....	483
S. Leffler Copyright	484
B. Paul Copyright.....	484
Apache License.....	485
APPENDIX: How to apply the Apache License to your work.....	488
GNU Library General Public License	488
GNU LESSER GENERAL PUBLIC LICENSE.....	499
Go Ahead License Agreement	506
Libpcap License.....	511
NetSNMP License	511
OpenSSL License.....	516
PuTTY License.....	520
SSH Server License	521
ZipArchive License.....	521
ZLib License.....	523
Appendix J: A. Onoe & S. Leffler Copyright.....	525
Appendix K: S. Leffler Copyright.....	527

Appendix L: B. Paul Copyright	529
Index	531

Part I: AirMagnet Enterprise System

Chapter 1: AirMagnet Enterprise Overview

Enterprise-hardened Wireless Intrusion Prevention

Wireless technology poses a critical test to the enterprise. Businesses must respond to a rising wave of new threats and vulnerabilities at a time when wireless expertise and manpower are in short supply. AirMagnet Enterprise tames this complexity and exposure with a true zero-tolerance approach to wireless security that is tied to the policies and needs of your business. AirMagnet Enterprise detects every threat in the network, worldwide, and then automatically takes action with multiple layers of automated threat response. An intuitive global interface provides full disclosure of all wireless events, making it easy to make the right decisions while cutting through the time required to manage your networks. The end result is a system that brings simplicity, accountability, and bullet-proof defense to any wireless deployment.

Automated Intrusion Prevention

AirMagnet Enterprise creates an airtight seal over your wireless networks, quickly identifying and neutralizing any threats that arise. This is done through the marriage of continuous threat detection with a suite of active defenses that respond to any event automatically.

Superior Detection

WLANs can expose any enterprise to a new class of security threats where the rogue AP represents only the tip of the iceberg. AirMagnet answers this challenge by continuously monitoring for hundreds of potential threats using the only sensors in the industry to perform a complete, independent local analysis of all wireless traffic. This firsthand view provides a stateful analysis of all conversations and all devices in the network to identify more than 135 classes of threats in real-time. The result is the deepest, most accurate library of wireless events in the industry, covering all aspects of WLAN security.

Automated, Active Defenses

When threats arise, AirMagnet Enterprise actively protects the network with multiple layers of defenses. This layered approach insures that every threat is addressed and technical teams are always armed with the professional tools needed to protect their networks.

- **Wireless Blocking**—Wireless blocking gives managers the ability to reach out and stop wireless threats at the source. When a device is blocked wirelessly, it is unable to make or maintain any wireless connections, effectively locking it out of the network. Any client, AP, or Ad-hoc device can be selectively targeted and blocked without impacting the normal operation of the network.
- **Wired-Side Blocking**—AirMagnet Enterprise also includes the ability to block threats at the wired port. This provides a complementary layer of protection and ensures that the wired network is shielded from threats in the WLAN.
- **Locate Threats**—AirMagnet lets users see the location of rogues and intrusions on a map of their location. Staff can now immediately see if a threat is inside or outside the premises, and can target responses appropriately.

- **Device Tracing**— When a threatening device is identified in the network, AirMagnet can launch an active analytical trace to expose where the device is attached to the wired infrastructure. Traces can span multiple switches, ensuring that every corner of the network is inspected.
- **Automated Response**— AirMagnet's defensive suite can be tied to policy and triggered automatically. This insures networks are protected 24 hours a day, even when staff is not readily available. When an attack is detected, AirMagnet comes into action to immediately defend the network.

3D Rogue Control

Rogue devices are a constant threat to every wireless network, and require a trusted system to detect, disable, and document every rogue, every time. To this end, AirMagnet's unique 3D Rogue Control provides a truly fail-safe approach to rogue management, built on a concept of operational redundancy in each step of the process.

Detect

AirMagnet Enterprise employs multiple layers of rogue detection to insure every rogue device is identified, immediately and accurately. Users can easily import access control lists from other management systems, making it easier to define rogues based on your overall network policy.

Rogues can be identified based on:

- MAC address
- Hardware vendor
- Channel
- SSID
- 802.11 band (a/b/g)

Disable

AirMagnet actively disables rogue devices on both the wireless and wired sides, keeping rogues completely isolated from your network. All blocking and tracing can be automated to provide around-the clock active protection from rogues.

Rogues can be blocked with:

- Wireless Blocking
- Wired Blocking
- Automated Blocking

Document

AirMagnet fully documents every rogue device with a consolidated view of every rogue including the location of the rogue on a map, its blocking status, the switch and port where the rogue is connected, security measures in place on the rogue, as well as the MAC address, channel, SSID and much more.

Full Disclosure Policy View

AirMagnet's Full Disclosure Policy View brings easy, policy-based management and accountability to any wireless LAN. Instead of tracking hundreds of individual alarms, users can create, document, and enforce coordinated wireless policies that integrate with their existing processes.

Tailored Policy Creation

AirMagnet Enterprise makes it easy to create and enforce policies tied to your specific business needs and regulatory requirements. The system includes a library of pre-configured policies tailored to specific industry needs (government, retail, warehouses, etc.), as well as regulatory standards such as HIPAA and GLBA. Policies can be applied to any level of the network, from policies that span the entire organization to policies that target specific VLANs within a single device.

Security- or Performance-Only User Role

Network administrators can now fine-tune and assign WLAN management responsibilities to staff members in two separate categories. A user who is assigned the security-only role can only view and manage the security policies and alarms of the network, and vice versa.

Streamlined Analysis and Investigation

The AirMagnet Console makes it easy to see the Who, What, When, Where, and Why of wireless problems in the network. Users can then drill down for additional details, including event correlation, hardware analysis, and configurable graphs of trends in the network.

Notification and Escalation

AirMagnet Enterprise delivers targeted, actionable information to network staff and management systems via a comprehensive notification system. Notification methods including SNMP versions 1, 2, and 3, SysLog, EventLog, Email, Pager, Instant Message, SMS, Print, and more. Notification rules can be set on a per- alarm basis, allowing individual alerts to be routed to specific recipients. As situations change, the notification targets can change in response, allowing for logical event escalation.

Integrated Reporting

AirMagnet's Reports screen quickly turns your Wi-Fi data into professional customized reports. Users can leverage a library of pre-built reports or generate their own custom reports by selecting the appropriate items from the user interface. The reports cover all areas of WLAN management and can be output in a variety of formats including PDF, HTML, XML, MS Word, MS Excel, Text, and more.

Compliance Reporting

AirMagnet Enterprise includes detailed compliance reports covering a variety of regulatory standards including Sarbanes-Oxley, HIPAA, DoD, Payment Card Industry, FISMA, and GLBA. These reports step through each section of the respective standards, providing a pass-fail assessment of each device and policy, while illustrating any needed corrective actions. As a result, IT staff can easily verify regulatory compliance and maintain detailed records of their efforts.

SmartEdge Architecture

AirMagnet Enterprise is built on a truly revolutionary architecture that provides superior intelligence and unmatched scalability. The system consists of three major components — AirMagnet SmartEdge Sensors, deployed throughout the network to analyze your wireless networks, a centralized Enterprise Server that correlates events and integrates to other systems, and Enterprise Consoles that provide the user interface to the system.

Local Analysis

AirMagnet Enterprise is the only solution in the world to perform a complete wireless analysis at the source, in the sensor itself, instead of chopping and forwarding data for remote analysis. As a result, AirMagnet always has access to a complete set of firsthand data, and never drops important information.

Fast, Secure Deployments

AirMagnet SmartEdge Sensors are plenum-rated and FIPS 140-2 compliant, insuring they can be deployed in any environment. SmartEdge Sensors also include native support for 802.3af Power-over-Ethernet and include a zero configuration option for fast, painless deployments. Sensors come standard with removable antennas, allowing users to use external antennas to meet any unique monitoring requirements.

Protect Your Bandwidth

AirMagnet's local analysis drastically reduces the volume of data sent between the Sensor and Server. AirMagnet typically generates only a few packets per second (about 2% of which is required by other sensors), conserving wired bandwidth even during peak WLAN use.

Enterprise Scalability and Fail-over

AirMagnet Enterprise meets the needs of any organization regardless of size. A single AirMagnet Enterprise Server can support up to 1,500 sensors (each monitoring hundreds of wireless devices). Multiple servers can be monitored through a single Enterprise Console, and the system supports redundant management servers for automatic fail-over. Additionally, since each SmartEdge Sensor performs an independent local analysis, each sensor continues to protect the network even in the event that remote connectivity is lost.

Device-Specific Alarm List

The user can view all the alarms that are triggered by a specific device (AP or station). It provides an easy way to keep track of the overall security and performance status of individual selected devices. This feature is available in the Remote Analyzer.

Embedded AirMagnet Spectrum Analyzer Sensor

The AirMagnet Spectrum Analyzer Sensor integrates AirMagnet's advanced spectrum-sensing hardware and analytical and visual display software into one application. This new sensor platform brings AirMagnet Enterprise system to a new level and allows network professionals to use the AirMagnet Enterprise system to monitor and collect spectrum data as the basis for network design and planning, troubleshooting, and optimization. Unlike the regular AirMagnet SmartEdge Sensor which comes with only one wireless network card for monitoring network traffic, the AirMagnet Spectrum Analyzer Sensor comes with an additional wireless card dedicated for spectrum data analysis. The AirMagnet Enterprise system is able to differentiate the Spectrum Analyzer Sensors from the regular SmartEdge Sensors and display them on the Enterprise Console using different icons

SSH Support on Sensors

AirMagnet Enterprise comes with enhanced security by offering SSH support on the AirMagnet SmartEdge Sensor. This ensures that all communication between the Command Line Interface (CLI) client and the SmartEdge Sensor is encrypted, making it impossible to eavesdrop or sniff critical information. The AirMagnet SmartEdge Sensor uses SSH Server Version 2.0 at Port 22. It has been fully tested to work smoothly with the following SSH clients:

- Linux SSH Client (Fedora Core 4, Debian Sarge 3.1)
- OpenSSH Client
- SecureCRT
- Putty
- Cygwin

Database Backup/Restore/Reset

This feature is designed to make it easy for users to back up, restore, or reset their AirMagnet Enterprise Server database all from one simple user interface. Currently, it is available for the Microsoft Access and SQL database servers.

Device Locator

This is an enhancement to the Rogue Triangulation feature in the AirMagnet Enterprise 6.x releases. Using a new calculation algorithm, the program now is able to track and locate all kinds of devices (i.e., AP, station, Ad Hoc) of any type (i.e., Rogue, Neighbor, Monitored, and In-ACL) with greater accuracy.

“Rogue AP Detected Inside” Alarm

This alarm is associated with the Device Locator feature. To enable AirMagnet Enterprise to generate this alarm, all you need to do is to specify an area on the floor plan. Once the area is set, the program will automatically send an alarm whenever a rogue AP is detected within the borders of the area. It's a great feature to fortify a specific area on a wireless network or even the entire network.

Server to Console Data Compression

Significant breakthrough has been made in compression of data transmitted from the AirMagnet Enterprise Server to the Enterprise Console. As a result, data traffic from Server to Console can now be reduced by 80~90% of what it used to be. This is achieved by using zlib, a free, general-purpose, legally unencumbered, lossless data-compression library that can be used on virtually any computer hardware and operating system.

Managing Network ACL Groups

An Access Controls List, or ACL, provides an easy way for network administrators to effectively manage the security of their networks. With this feature, users can create and manage/group their networks' access control lists (ACLs) from the AirMagnet Enterprise Console using the ACL Groups Management dialog box, where the user can create or delete ACLs and add devices to or delete devices from a selected ACL group.

Showing Rogue-Detecting Sensors

This feature correlates Sensors with rogue devices that have been detected on the network, making it easier for the user to identify the Sensor or Sensors that have detected a certain rogue device. The feature is available on the AirMagnet Enterprise Console's Infrastructure screen.

Oracle Database Support

This release of AirMagnet Enterprise comes with support for Oracle Database server, in addition to the Microsoft Access and SQL servers. It not only offers more database options for the user to choose from, but also makes AirMagnet Enterprise more scalable, making it ideal for managing large-scale enterprise wireless networks.

PostgreSQL Database Support

This release of AirMagnet Enterprise comes with support for PostgreSQL Database server, in addition to the Oracle, Microsoft Access and SQL servers. It not only offers more database options for the user to choose from, but also offers the user a free open source database management system.

Important Notes:

[1] PostgreSQL must be installed and the database you wish to use must be created prior to installing the AirMagnet server software. For steps on installing the server software see Chapter 2. Simply follow the prompts on the screen.

[2] Before you can connect to a PostgreSQL repository, you must first set up a PostgreSQL ODBC driver. Therefore, during AirMagnet Enterprise installation, you will be prompted to install the ODBC driver.

Software Update from Enterprise Console

All AirMagnet software comes with a one-year free technical support plan which entitles users to all patches and new releases during that period. This AirMagnet Enterprise release includes a useful tool for checking for any available updates to the AirMagnet software. This can be done (from the Enterprise Console) simply by navigating to **Help>Check Update**. The user will receive a message indicating if an update is available or not. If there is an update, detailed instructions will be given on the screen to guide the user through the update process.

Adding Comments to GPS Log Files

A “Comment to log file” field has been added to the GPS Log Options dialog box, which allows the user to add text descriptions to GPS log files, if they want to.

Addition of Two New Policy Profiles

- The **Educational Institution Policy Profile**—is designed to provide technical teams with the systems and tools needed to stay in control of the wireless networks in the Educational environment. Colleges, universities, and K-12 school districts have been among the early adopters of the Wi-Fi technology. Depending on the school policy, even though the students and faculty members will be allowed to bring in personal access points, the wireless administrator needs to ensure that these devices do not affect the performance of those authorized devices or pose any security threat to the campus-wide network. The AirMagnet Enterprise Educational Institution Profile addresses WLAN policy issues in the education sector.
- The **Zero Wireless Policy Profile**—is designed to provide technical teams with the systems and tools needed to ensure no wireless network is present in certain environments. Enterprises that enforce this policy need to be assured of protection from any Denial-of-Service attacks, Man-in-the-Middle attacks, ad-hoc nodes, or any issue that may compromise the security of the corporate network. For this reason, enterprises need to continuously monitor their networks to ensure the “zero wireless policy”. AirMagnet Enterprise will alert network administrators when any wireless device is detected on their network.

AirMagnet Enterprise System Components

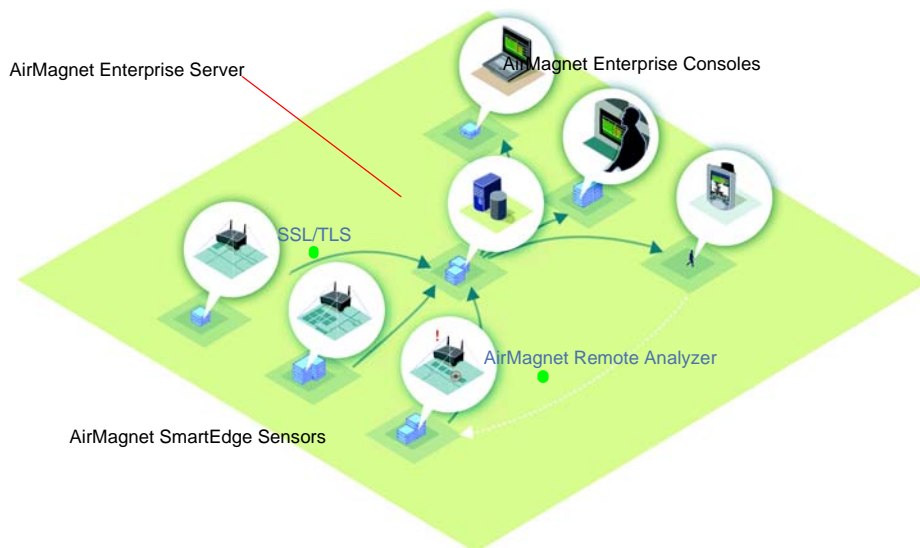


Figure 1-1: Topology of the AirMagnet Enterprise system

Figure 2-1 illustrates the network topology of the AirMagnet Enterprise system. The entire AirMagnet Enterprise system consists of three major components:

- AirMagnet Enterprise Server
- AirMagnet Enterprise Console, and
- AirMagnet SmartEdge Sensor

AirMagnet Enterprise Server

The AirMagnet Enterprise Server is the central component of the AirMagnet Enterprise system and holds all the network data collected by AirMagnet SmartEdge Sensors. AirMagnet SmartEdge Sensors send alarms and trending information to the AirMagnet Enterprise Server, which maintains a database of all network data and securely delivers the information in real time to AirMagnet Enterprise Consoles deployed throughout the network. The AirMagnet Enterprise Server is a Windows-based software program running on Windows Server 2000, 2003, or 2008 operating systems. It provides the following key services:

- Centralized alarm view – provides an eagle-eyed view of the most critical activities in the entire wireless LAN.
- Sensor management – provides sensor configuration profile, profile distribution, and software upgrade to sensors to facilitate effective policy distribution.
- User administration – provides role-based user profile management which gives IT managers the flexibility of delegating network monitoring and troubleshooting tasks to IT staff who have various classes of security clearance and skill sets.

- Sensor network trending information aggregation — is an Enterprise Server database that saves network performance information as a data source for producing various baseline reports.

AirMagnet Enterprise Console

The AirMagnet Enterprise Console provides the user interface to the system, allowing users to view network activities by location or sensor throughout the network. When more detailed information is required, the Enterprise Console can directly connect to any individual sensor for real-time analysis and remote troubleshooting, using the AirMagnet Remote Analyzer. The AirMagnet Enterprise Console is flexible enough to be deployed and launched securely from a NOC on a Laptop or PC for complete anytime-anywhere control.

AirMagnet SmartEdge Sensor

The AirMagnet SmartEdge Sensors are deployed in the wireless network to proactively monitor the environment for more than 135 alarms that could impact the security and performance of the network. Unlike simple packet sniffing probes, each AirMagnet SmartEdge Sensor has an built-in intelligent AirWISE analysis engine, allowing it to automatically monitor the network environment. This unique ability allows the “heavy lifting” of the analysis to be performed locally at the edge of the network and avoids the additional bandwidth overhead of capturing and re-sending each and every packet to a central server for processing. The AirMagnet SmartEdge Sensors are placed throughout the network and report back to the AirMagnet Enterprise Server using the 10/100 Ethernet.

Product Documentation

This *AirMagnet Enterprise User Guide* contains comprehensive information about the AirMagnet Enterprise application and all the utilities that are integrated in it. It provides detailed instructions and vivid graphical illustrations on how to use the various features of the product. It is highly recommended that the user print out the *User Guide* and have it handy as a reference for their daily work.

In addition to this *User Guide*, AirMagnet Enterprise also comes with the following documents:

Online Help

AirMagnet Enterprise also comes with a complete HTML-based online help system. It includes all the information found in the *AirMagnet Enterprise User Guide*, plus context-sensitive help for the software’s major user interfaces. The entire help system consists of two separate files: one for the AirMagnet Enterprise Console and the other for the AirMagnet Remote Analyzer.

You can access AirMagnet Enterprise Console’s online help, from the Console’s user interface, by clicking **Help>Contents**. To access the online help for the Remote Analyzer, you must first bring up the AirMagnet Remote Analyzer and then click **Help>Contents**.

You can also activate the online help for the AirMagnet Enterprise Console or the Remote Analyzer by pressing the **F1 Key** on your keyboard from their respective interfaces.

AirMagnet WLAN Policy Reference Guide

The *AirMagnet Enterprise WLAN Policy Reference Guide* contains descriptions of all the WLAN security IDS/IPS and performance intrusion alarms that could be triggered by the AirMagnet Enterprise system. It describes in detail all the security threats and performance anomalies that have been identified so far in the typical enterprise wireless LAN environment and provides proven strategies on how to deal with those threats and anomalies.

An electronic copy of the *Policy Reference Guide* in Adobe PDF format is included on the AirMagnet Enterprise software CD. It can also be accessed by clicking **Start>All Programs>AirMagnet Enterprise Console> Policy Reference Guide**.

Release Notes

The *AirMagnet Enterprise Release Notes* contains the most up-to-date information about the product. It reflects the overall status of AirMagnet Enterprise at the time of release. The user should always refer to the *Release Notes* for all the last-minute enhancements, known issues, and important notes.

A hard copy of the *Release Notes* is included inside your product package. The user is also encouraged to log on to AirMagnet's Website for the latest release notes regarding software update and upgrade.

AirMagnet SmartEdge Sensors

AirMagnet SmartEdge Sensor user guides (including technical specifications) are located in the Documents/Drivers section of your My_AirMagnet account.

Frequently Asked Questions (FAQs)

We at AirMagnet take great pride in providing our customers with the best customer service experience possible. Towards that end, we have an FAQ section on our Website to address product-related questions commonly asked by our customers. The entries are listed by product and are in a question-and-answer format. We encourage our customers to use those FAQs when they have product-related questions before contacting us for technical support. The FAQs can be accessed from <http://airmagnet.flukenetworks.com/faq/>.

We take great pride in providing our customers with the best IDS/IPS products available on the market. Towards that end, we are constantly adding new features and enhancements to our products in response to market needs. Therefore, our product documentation is updated regularly to reflect the latest status of our products. We strongly recommend that our customers visit our website for the latest version of all our product literature.

Chapter 2: Installing AirMagnet Enterprise

Product Package Contents

Thank you for choosing AirMagnet Enterprise!

Prior to installing AirMagnet Enterprise, make sure that the following items are included in your product package:

- AirMagnet Enterprise Software CD*
- *AirMagnet Software License Agreement*
- *AirMagnet Enterprise Read Me First*
- *AirMagnet Enterprise Quick Crib Sheet*

If any of these items is missing or damaged, contact your AirMagnet product reseller or AirMagnet technical support immediately.

The CD contains a copy of the AirMagnet Enterprise User Guide and the AirMagnet Enterprise WLAN Policy Reference Guide. Both documents are in Adobe PDF format. The Adobe Acrobat Reader software is required in order to view and print the documents. The software can be downloaded free of charge from Adobe's Website at <http://www.adobe.com>.

Product Registration

Registering your AirMagnet Enterprise will ensure your eligibility for product support and updates as well as other benefits.

To register your product:

- 1) Open your Web browser.
- 2) In the **Address** field, go to: http://airmagnet.flukenetworks.com/support/register_product/index.php
- 3) Follow the instructions on-screen to complete the registration.

The AirMagnet Product Registration screen appears automatically on-screen upon the installation of the AirMagnet Enterprise Server, providing an easy way for registering your product. For more information, see “[AirMagnet Enterprise Server Installation](#)” on page 15.

Technical Support

Fluke Networks' Gold Support is our comprehensive support and maintenance program that offers expanded coverage for all AirMagnet products. All existing AirMagnet customers with products under the annual maintenance and support program are automatically migrated to the new Fluke Network's Gold Support program.

Benefits of the Gold Support program include:

- Access to live 24 X 7 technical support*
- Highly trained technical experts to help with product installation, configuration, best practices & troubleshooting on call 24 hrs a day including weekends and through the night.
- Multilingual technical support team**
- Free software updates/upgrades (new features and product enhancements) when available.
- Hardware support, repair and replacement for AirMagnet products***
- Free access to “AirMagnet Certified Professional” web-based training for certain AirMagnet products.
- MAC Address Reset assistance.

** Except United States holidays (New Years Day, Memorial Day, Labor Day, 4th of July, Thanksgiving, Christmas)*

*** Multilingual support not available on weekends*

**** Must meet terms and conditions as defined in the hardware warranty*

Contact Customer Support

- Phone Support: Sign-in to MyAirMagnet at http://airmagnet.flukenetworks.com/my_airmagnet/ to access the “Exclusive” Gold-member only phone numbers for your region.
- Submit a support request at <http://airmagnet.flukenetworks.com/support/submit-report.php>
- Send email to support@AirMagnet.com.

When contacting AirMagnet Technical Support, please have the following information ready so we may assist you quickly:

- Server hardware configuration
- Operating System

- Database
- AirMagnet Management Server version prior to updating (if updating to a new version caused the problem)
- Current version of AME
- Type(s) of sensors that are deployed in the enterprise environment (if the issue is sensor-related)

AirWISE Community

From the help menu, users can directly link to the AirWISE Community <http://www.airwisecommunity.com> created by AirMagnet for wireless experts. The AirWISE Community includes discussion forums, blogs and additional resources for the security, performance and compliance of wireless networks.

AirMagnet Enterprise Installation Overview

The AirMagnet Enterprise System consists of the following system components:

- AirMagnet Enterprise Server
- AirMagnet Enterprise Console
- AirMagnet SmartEdge Sensor, and
- Database server (Microsoft Access, SQL, PostgreSQL, or Oracle database)

Microsoft SQL Service Pack 3 or later is required when installing Microsoft SQL 2000 Server on a Windows 2003 Server.

AirMagnet Enterprise system installation involves the following tasks:

- Installing an AirMagnet Enterprise supported database server or having the database access information to a supported database server (e.g., IP address, login) is required before installing the AirMagnet Enterprise Server.
- Installing the AirMagnet Enterprise Server.
- Installing the AirMagnet Enterprise Console (can be downloaded from <https://<Enterprise Server name or IP address>> once the AirMagnet Enterprise Server has been installed).
- Configuring the AirMagnet SmartEdge Sensor(s).

Each of these tasks requires separate procedures, which will be covered in detail in the following sections.

Database Server Prerequisite

A prerequisite to AirMagnet Enterprise Server installation is to have a database server that will be used to create the AirMagnet Enterprise database. The only exception to this is that the user may choose to use a Microsoft Access database.

For a list of AirMagnet Enterprise supported databases, see [“Supported databases” on page 17](#).

As a convenience for PostgreSQL database server installation, PostgreSQL 8.4.2.x for Windows 32-bit support and the PostgreSQL 9.0.3.x for Windows 64-bit support may be accessed from the AirMagnet Enterprise autorun installer or from the associated PostgreSQL folder on the installation CD. For specific instructions about configuring the AirMagnet Enterprise database on a PostgreSQL database server, see [Appendix H, “Installing PostgreSQL Database”](#)

For specific instructions about configuring the AirMagnet Enterprise database on an Oracle database server, see [“Installing Oracle Database” on page 455](#).

During AirMagnet Enterprise installation the user will be required to select an existing database server and provide the required database access information (e.g. IP address, login).

Performing Product Upgrades or Downgrades

Before upgrading to AirMagnet Enterprise version 10, it is necessary to perform the following back-up procedure. Once upgraded to AirMagnet Enterprise version 10, the product may be downgraded to a lower version. In the case of a downgrade, current data will be lost, however, once a downgrade is completed, the pre-upgrade, back-up files may be restored.

Pre-Upgrade Back-up Procedure

- 1) Backup the full AME database, and ensure the backup copy functions fine.
- 2) Backup the entire \\Program Files\\AirMagnet Inc\\AirMagnet Management Server\\web\\AMom\\Configs directory.
- 3) Export the following items (if applicable) using the AirMagnet Enterprise Console:

Switch list:

- **If server tracing is enabled:** Go to Manage > Server Options > Server and click **Configure Switch List** (note that the button is enabled only if the "Auto trace APs from Server box" is checked - meaning server tracing is enabled). Click **Export**. Save the exported text file (save the file to a name that can be easily identified for server tracing use).
- **If sensor tracing is enabled:** Go to Manage > Policy Profiles > and double-click the policy profile name. This opens the Policy Management screen. Click **Options**. Click the **Rogue Management** tab. Click **Configure Switch List** (this button is enabled if the "Use the configured list of switches and settings" box is checked meaning sensor tracing is enabled). Save the exported text file (save the file to the name that can be easily identified for the sensor tracing use).

WLC integration: Go to Manage > Server Options > **WLC** tab. Click **Export**. Save the exported .csv file.

WCS ACL integration: Go to Manage > Server Options > **Device Classification** tab. Click **Configure** (note that this button is enabled only if the "Enable ACL integration with other vendors" box is checked). Double-click the Cisco WLAN Controller entry. Click **Export**. Save the exported text file. Make sure you repeat this step if there is more than one Cisco WLAN Controller entry.

Device Classification Rules: Go to Manage > Server Options > **Device Classification** tab. Click **Device Classification Rules**. Click **Export All Rules**. Save the exported xml file.

Downgrade Procedure

Note: Downgrading from AirMagnet Enterprise version 10 to version 8.5.x or 9.x is not desirable. In the case of a downgrade, current data will be lost, however, once a downgrade is completed, the pre-upgrade, back-up files may be restored.

- 1) Uninstall the AirMagnet Enterprise server.
- 2) Restore the backup AirMagnet Enterprise database.
- 3) Re-install the AirMagnet Enterprise server, and make sure to point the AirMagnet Enterprise server to use the restored database in item 2 above.
- 4) Stop the AMWebserver service and AMMonitor service.
- 5) Replace the existing \\Program Files\\AirMagnet Inc\\AirMagnet Management Server\\web\\AMom\\Configs directory with the backup copy (from before the upgrade).
- 6) Restart the AMWebserver service and AMMonitor service.
- 7) From the pre-upgrade backup, re-import the Switch list, WLC integration, WCS integration, and Device Classification Rule (whichever apply).
- 8) Manually un-install SSA (one of the new features introduced in AME version 10) from the client machine(s).

*For AirMagnet Enterprise Hot Swap server users: Follow the downgrade procedure. Also, after the re-install of AirMagnet Enterprise server on the AirMagnet Enterprise Hot Swap Server machine, you need to re-configure the Hot Swap Server setting in AirMagnet Enterprise Console. Go to Manage > Server Options > **Server** tab. Check **Act as Hot Swap Server** and enter the Primary Server information.*

AirMagnet Enterprise Server Installation

The AirMagnet Enterprise Server can be installed from the AirMagnet Enterprise CD. To ensure that the installation goes smoothly, it is advised that the user read the following important notes prior to starting the installation.

Notes on AirMagnet Enterprise Server Installation

- We recommend that the AirMagnet Enterprise Server should be installed on a machine dedicated to running the AirMagnet services only.
- The AirMagnet Enterprise Server should have a **static IP** address and should NOT have any other Web servers running on it, including the Microsoft® Internet Information Service (IIS) which may have been added to the system while installing the Microsoft Windows operating system.
- No other AirMagnet application, such as the AirMagnet WiFi Analyzer, should be installed on the same machine on which the AirMagnet Enterprise Server is installed.
- If you are installing the AirMagnet Enterprise Server from AirMagnet's Website, make sure that you have **WinZip** installed on the machine before downloading the AirMagnet Enterprise Server.
- Make sure that the "**proxy server**" option within the LAN settings for Microsoft Internet Explorer on the AirMagnet Enterprise Server is turned OFF for your network setup.
- Make sure that the "**automatic detect settings**" option within the LAN settings for Microsoft Internet Explorer on the AirMagnet Enterprise Server is NOT checked.
- When running the AME server on a Windows 2003 or 2008 Server environment, the Data Execution Prevention feature must be set to "Turn on DEP for essential Windows programs and services only". To configure this setting:
 - a Right-click **My Computer** and select **Properties**
 - b Select the **Advanced** tab and click **Settings** from the Performance section.
 - c Click the **Data Execution Prevention** tab and modify the setting as described above.
- In order to download and set up a self-signed SSL certificate from VeriSign® (resulting in increased security for web server access), refer to the following link: <http://www.verisign.com/ssl/>
- AirMagnet Enterprise installs Microsoft Visual C++ 2005 Redistributable.
- AirMagnet Enterprise uses SSL port 443 for its communication between the sensors and the server.
- Using an Internet browser to navigate to <https://localhost/> on the Enterprise Server may not access the server web page properly. To work around this, use the server's IP address (i.e., <https://<IP>/>).
- Web access to the server and sensor web pages may not work properly with Mozilla browsers. To work around this, use Internet Explorer.
- Users may be unable to properly migrate Microsoft Access databases to SQL 2005 or Oracle.

Special Notes on Backup Server Installation

You need to install a backup AirMagnet Enterprise Server in order to take advantage of AirMagnet Enterprise's server redundancy feature. All the notes on AirMagnet Enterprise Server installation outlined in the previous paragraph also apply when installing the back-up server. In addition, you must also keep the following important points in mind if you choose to use the server redundancy feature:

- You must set up a Microsoft SQL/Oracle/PostgreSQL Database server on your network on a dedicated PC, prior to installing the AirMagnet Enterprise Servers (primary and backup), if you do not already have one.
- You must install a primary AirMagnet Enterprise Server and a backup AirMagnet Enterprise Server, making sure that they are installed on two separate PCs.
- You must select Microsoft SQL/Oracle (Server)/PostgreSQL as your database server when configuring the primary AirMagnet Enterprise Server and the back Server.
- Make sure that the primary AirMagnet Enterprise Server and the backup Server point to the *same database* on the Microsoft SQL/Oracle/PostgreSQL server using the same username and password.
- The same administrator password and the shared secret key must be used for both the primary AirMagnet Enterprise Server and the backup server.

AirMagnet Enterprise System Requirements

For optimal performance, it is recommended that AirMagnet Enterprise run in a Server/Database/Client configuration where the server, database and console run on separate machines.

Server operating systems*

Microsoft® Windows Server® 2008 (Standard or Enterprise, 32 or 64 bit), Windows Server 2003 (Standard or Enterprise, 32 bit, Service pack 2) or Windows® XP Professional (Service Pack 3). Windows Server 2003 or Windows Server 2008 is required for a deployment with more than 20 AirMagnet sensors.

Supported databases

Microsoft SQL Server® (2000, 2005, 2008), Oracle® 10g -11g, PostgreSQL® (64 bit use v9.0.5, 32 bit use v8.4.9-1) or Microsoft Access® (Access not recommended for larger deployments).

Console operating systems*

Microsoft Windows 7 (Service Pack 1), Windows Server 2003 (Service Pack 2), Windows XP (Service Pack 3).

* Server and console installations require local admin rights.

Table 2-1: Hardware Specifications

		Small business Up to 100 sensors	Medium Sized Business Up to 500 sensors	Enterprise Up to 1000 sensors
Server	Processor	Intel® Xeon® Processor E3	Intel Xeon Processor 5000 or greater recommended	Intel Xeon Processor 5000 or greater recommended
	RAM	2 GB available for the AME application	2 GB available for the AME application	2 GB available for the AME application
	Hard disk space	146 GB available	300 GB available	300 GB available
	Ethernet	10/100 Mb or higher	1 Gb or greater	1 Gb or greater
Database				
	Processor	Intel Xeon Processor E3	Intel Xeon Processor E3	Intel Xeon X5600 Series CPU
	RAM	4 GB / 1333 MHz or faster	8 GB / 1333 MHz or faster	12 GB / 1333 MHz or faster
	Hard disk space	146 GB available 10,000 RPM SAS recommended	146 GB available 10,000 RPM SAS recommended	300 GB available 15,000 RPM SAS recommended
	Database max size	5 GB	10 GB	15 GB
	Ethernet	1 Gb or greater, full duplex	1 Gb or greater, full duplex	1 Gb or greater, full duplex
Console				
	Processor	Intel Core i5 or greater	Intel Core i5 or greater	Intel Core i5 or greater
	Ram	3 GB	3 GB	3 GB
	Hard disk space	500 MB	500 MB	500 MB
	Ethernet	Ethernet connection	Ethernet connection	Ethernet connection

Important Notes:

- Deployments over 100 sensors require that the Enterprise server software and database are installed on separate physical machines.
- Drive partition for AME server must have at least 25 GB free disk space for software install, page file, logs, forensics files and floor maps.
- Intel server CPU info here:

<http://www.intel.com/content/www/us/en/processors/xeon/xeon-processor-5000-sequence.html>

<http://www.intel.com/content/www/us/en/processors/xeon/xeon-processor-e3-family.html>

Table 2-2: VMWare Specifications

VMware ESX or ESXi 3.5-4.1		100 Sensors	300 Sensors	Up to 500 sensors per virtual machine
Per VMware Server	Processor	Intel Xeon Processor X5000 series or greater recommended	Intel Xeon Processor X5000 series or greater recommended	Intel Xeon Processor X5000 series or greater recommended
	RAM	4 GB available for the AME application	8 GB available for the AME application	8 GB available for the AME application
	Hard disk space	60 GB available 10,000 RPM SAS recommended	80 GB available 15,000 RPM SAS recommended	120 GB available 15,000 RPM SAS recommended
	Ethernet	10/100 Mb or higher	1 Gb or greater	1 Gb or greater
Per VMware Database	Processor	Intel Xeon Processor X5000 series or greater recommended	Intel Xeon Processor X5000 series or greater recommended	Intel Xeon Processor X5000 series or greater recommended
	RAM	4 GB /1333 MHz or faster	8 GB /1333 MHz or faster	8 GB /1333 MHz or faster

Table 2-2: VMWare Specifications

VMware ESX or ESXi 3.5-4.1	100 Sensors	300 Sensors	Up to 500 sensors per virtual machine
Hard disk space	80 GB available 10,000 RPM SAS recommended	120 GB available 15,000 RPM SAS recommended	160 GB available 15,000 RPM SAS recommended
Database max size	5 GB	10 GB	15 GB
Ethernet	1 Gb or greater, full duplex	1 Gb or greater, full duplex	1 Gb or greater, full duplex

Important Notes:

- Requires VMware Software version: ESX or ESXi 3.5-4.1.
- The AirMagnet Enterprise Server can require significant CPU resources. Care should be taken to ensure at least 90% of the Host System CPUs assigned to the AME Virtual Machine will be available for use at any time.
- The network interface should not be shared with any other VM on the host system.
- The specifications above require that the Enterprise Server and Database are running on separate VM's. For the best performance, the database server should be on a separate ESX installation.

Installing AirMagnet Enterprise Server

This section discusses the installation of the AirMagnet Enterprise Server, which is the first and most important step in AirMagnet Enterprise system installation.

To install the AirMagnet Enterprise Server:

- 1) Insert the AirMagnet Enterprise CD in your CD-ROM drive, and the installation program will start automatically (autorun). If autorun is disabled, you can install the program by opening the AirMagnet Enterprise folder. Double-click **Setup.exe**.
- 2) You must agree to the AirMagnet, Inc. Software License to continue.
- 3) The database server selection dialog appears. Select a database option and click Next. See Figure 2-1.

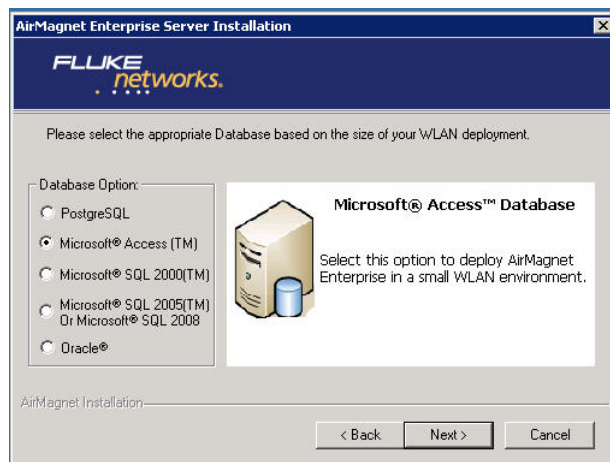


Figure 2-1: Selecting a database server

Microsoft SQL Server or Oracle Database Server must be used if you want to use AirMagnet Enterprise's server redundancy feature.

- 4) The Setting Up Database Server message box appears. See Figure 2-2.
- 5) .

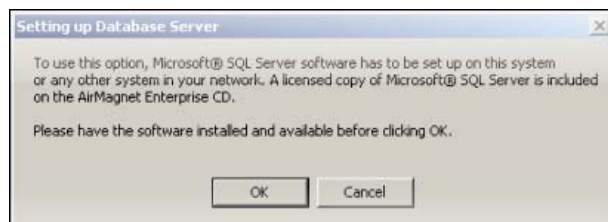


Figure 2-2: Database server setup reminder

- 6) Read the message, and click **OK**. The AirMagnet Database Connection Utility screen appears. The type of connection utility presented depends on the database option previously selected. See Figure 2-3.

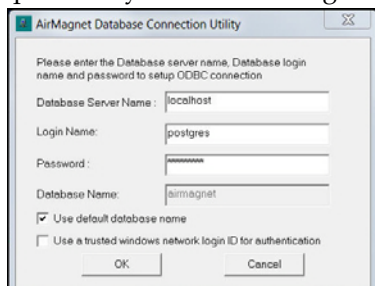


Figure 2-3: Configuring database server connection

- 7) Make the entries and/or selections as described in Table 2-3.

Table 2-3: Database Server Connection

Parameter	Description
Database Server Name	Enter the name of the Microsoft SQL database server to which you connecting.
Login Name	Enter the login name of the Microsoft SQL database server. Note: This field will be disabled if the Use a trusted Windows login ID for authentication check box is checked.
Password	Enter the password of the Microsoft SQL database server. Note: This field will be disabled if the Use a trusted Windows login ID for authentication check box is checked.
Database Name	Enter a unique name for the database. Note: This field will be automatically interpolated with the default database name (i.e., airmagnet) if the Use default database name check box is checked. See below.
Use default database name	Check this check box only if you want to use the default database name. Note: The Database Server Name field will be automatically interpolated with the default database name (i.e., airmagnet) when this option is selected. See Database Server Name above.

Table 2-3: Database Server Connection

Parameter	Description
Use a trusted Windows network login ID for authentication	<p>Check this check box only if you want to use a trusted Windows network login ID for authentication.</p> <p>Note:</p> <ul style="list-style-type: none">Both the Login Name and Password fields will be disabled when this option is selected. See Login Name and Password.To use this option, the SQL server must be installed with Windows Authentication.The machine used to install the AirMagnet Enterprise Server must belong to the same domain defined by Windows Authentication.You must be a network administrator of the domain to do the installation.

- 8) Click **OK**. The AirMagnet Enterprise Server Installation screen appears. To accept the default destination folder for your AirMagnet Enterprise Server, click **Next**. Otherwise, browse for a location of your choice and then click **Next**. See Figure 2-4.

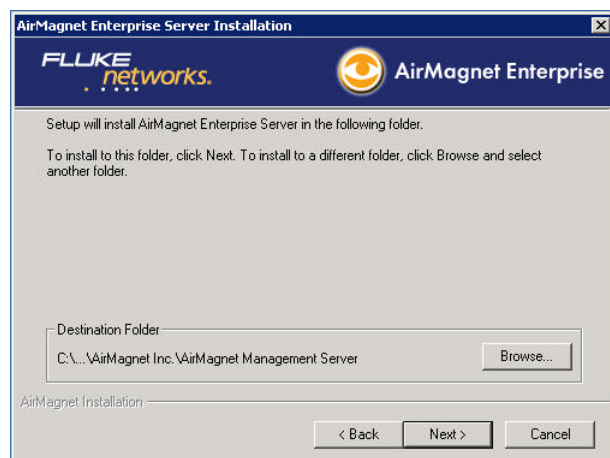


Figure 2-4: Setting server installation destination

- 9) The pre-configured policy profiles selection screen appears. See Figure 2-5.

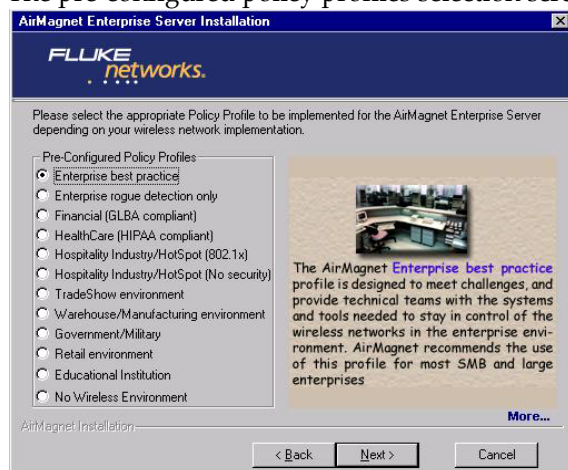


Figure 2-5: Selecting a pre-configured policy profile

- 10) Select a pre-configured policy profile that best matches your WLAN environment, and click **Next**. The license file installation screen appears. See Figure 2-6.

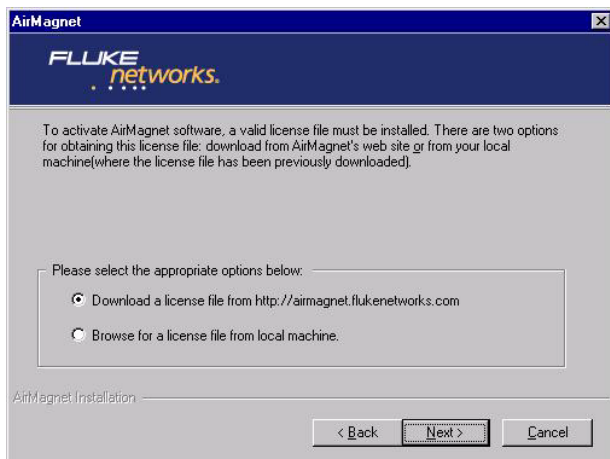


Figure 2-6: Obtaining server license file

- 11) Select **Download a license file from airmagnet.flukenetworks.com** or select **Browse for a license file from local machine** and click **Next**.

*Normally, the user should select **Download a license file**. The **Browse for a license file from local machine** option is used **ONLY** when the user already has a valid license file on a local machine. In that case, the user will need to locate the file on the machine and install it from there.*

The license information screen appears. See Figure 2-7.

Figure 2-7: Providing license information

- 12) Make the entries as described in Table 2-4. If a support contract was purchased, check the box and enter the AirMagnet Gold Support serial number and serial key

Table 2-4: AirMagnet License Information

Parameter	Description
Serial Number	Enter the 13-digit product serial number (e.g., A0000-00000000). Note: The Serial Number can be found on a label inside your AirMagnet Enterprise Server software package.
Serial Key	Enter the 12-digit alphanumeric serial key. Note: The Serial Key can be found on a label inside your AirMagnet Enterprise Server software package.
Adapter	Select the WLAN adapter from the drop-down list. Note: The AirMagnet Enterprise system is able to capture information, such as vendor name and MAC address, of all the adapters installed on your WLAN.
MAC Address	This field will be automatically interpolated with the MAC address of the selected adapter.

- 13) Click **Next**. This will download and install the license file. The installation continues. See Figure 2-8.

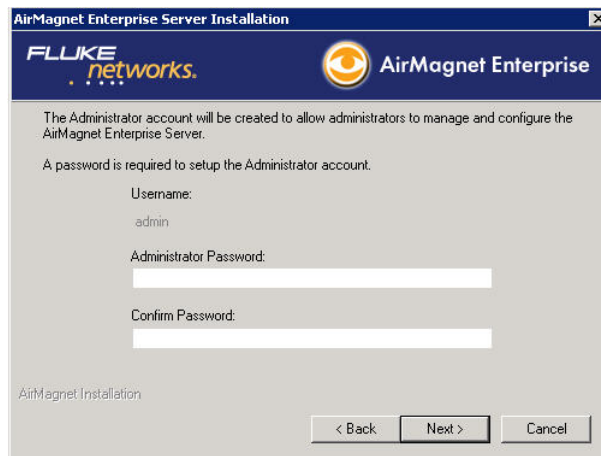


Figure 2-8: Setting user password

- 14) Make the entries as described in Table 2-5.

Table 2-5: Server Account Information

Parameter	Description
Username	This field will be automatically interpolated with the default value “ admin ”, which is not meant to be changed.
Administrator Password	Enter the administrator password. Note: The Administrator Password should be granted by the person who assumes the ultimate management responsibility of your WLAN.
Confirm Password	Re-enter the same the administrator password as you did above.

- 15) Click **Next** to continue. The installation continues. See Figure 2-9.

Figure 2-9: Specifying Sensor shared secret key

- 16) Make the entries as described in Table 2-6.

Table 2-6: Sensor Shared Secret Key

Parameter	Description
Sensor Shared Secret Key	<p>Enter a shared secret key for the AirMagnet Enterprise Server.</p> <p>Note:</p> <ul style="list-style-type: none"> The Sensor Shared Secret Key can contain 6 to 36 characters. Make sure you remember the Sensor Shared Secret Key you have entered, for it will be required during Sensor installation. All AirMagnet SmartEdge Sensors on your WLAN will use this Shared Secret Key to connect to the AirMagnet Enterprise Server.
Confirm Sensor Shared Secret Key	Re-enter the same Sensor Shared Secret Key you have entered above.

- 17) Click **Next**. The installation continues.
- 18) When the **AirMagnet Enterprise Server Setup Complete** message appears, click **Finish**.

Using a Backup AirMagnet Enterprise Server

Large-scaled deployment of the AirMagnet Enterprise system requires server redundancy to prevent loss of data in case the primary AirMagnet Enterprise Server has to be taken off the network (e.g., routine maintenance, etc.). With server redundancy, the backup server will automatically take over and the sensors will automatically report to the backup server when the primary server goes down. Once the primary AirMagnet Enterprise Server is restored, the sensors will resume communicating with it, leaving the backup Server in its normal standby mode.

Each copy of the AirMagnet Enterprise Server software comes with two sets of serial numbers and serial keys: one for the primary Server and the other for the backup server. You can install a backup AirMagnet Enterprise Server by following the same procedures used for installing the primary server outlined above. The following paragraph outlines the major steps involved in setting up a backup AirMagnet Enterprise Server.

To use a backup AirMagnet Enterprise Server:

- 1) Install Microsoft SQL or Oracle Database Server on a PC, if you have not already done so.
- 2) Install the primary AirMagnet Enterprise Server on a second PC, making sure it points to a database on the Microsoft SQL or Oracle Database Server. Refer to Figure 2-1.
- 3) Install the backup AirMagnet Enterprise Server on a third PC, making sure it points to the same database on the Microsoft SQL or Oracle Database Server as the primary AirMagnet Enterprise Server. See Step 2 above.
- 4) From the AirMagnet Enterprise Console, connect to the backup Server and set it as a hot-swap server.

Registering Your AirMagnet Enterprise

AirMagnet is committed to providing the best products and services in WLAN intrusion detection and prevention and performance management. To enable us to better serve your needs, we strongly recommend that you register your product as soon as possible.

Timely registration of your AirMagnet product will ensure your eligibility for product support and updates and unlimited access to our registration-only online knowledge base. It may also allow us easy access to feedback from our customers on our products and services, which in turn will help us enhance our product offerings to meet the new challenges in the rapidly evolving WLAN world.

You can register your AirMagnet Enterprise system at any time. For your convenience, the AirMagnet Product Registration Web page appears automatically once the AirMagnet Enterprise Server installation is completed. You may register your AirMagnet Enterprise system right away by following the instructions on the screens. You can also register at a later time by logging onto <http://airmagnet.flukenetworks.com>.

*Once the AirMagnet Enterprise Server is installed, the system will automatically create an AirMagnet Enterprise Server page on your network. The page displays all the resources of the AirMagnet Enterprise system, and can be accessed from any PC on the network via a Web browser at **https://<AirMagnet Enterprise Server name or IP address>**. See the following sections for more information.*

AirMagnet Enterprise Server Web Page

As a Web-based client-server application, the AirMagnet Enterprise system will automatically create a Web server page on your network for your AirMagnet Enterprise Server once the AirMagnet Enterprise Server installation is completed. This page contains important resources for your AirMagnet Enterprise system. The page can be accessed from any PC on your network at **https://<Enterprise Server name or IP address>** using Microsoft Internet Explorer.

It is strongly recommended that users completely close all internet browser windows after logging out of the Enterprise Server or Sensor web interfaces. Additionally, users are discouraged from opening multiple tabs in the browser window while logged into the web interface. the user should not use the Internet browser's History function to navigate to the web interface.

AirMagnet Enterprise Console Installation

Once the AirMagnet Enterprise Server is successfully installed, the next step is to download the AirMagnet Enterprise Console from the AirMagnet Enterprise Server Web page (**https://<Enterprise Server name or IP address>**) and install it on client stations on your network.

Since each AirMagnet Enterprise Server can support an unlimited number of AirMagnet Enterprise Consoles, customers can virtually install it on as many PCs as they need.

AirMagnet Enterprise Console System Requirements

See [Table 2-1 on page 18](#) for Console system requirements.

Downloading AirMagnet Enterprise Console

AirMagnet Enterprise Console can be downloaded at **https://<Enterprise Server name or IP address>** onto any PC on your network using a Web browser.

To download the AirMagnet Enterprise Console:

- 1) Launch your Web browser (e.g., Microsoft Internet Explorer).
- 2) In the Address field, enter **https://<Enterprise Server name or IP address>** and press **Enter**.

- 3) If a Security Alert page appears, click **Yes** to continue. The AirMagnet Enterprise Server Web page appears. See Figure 2-10.

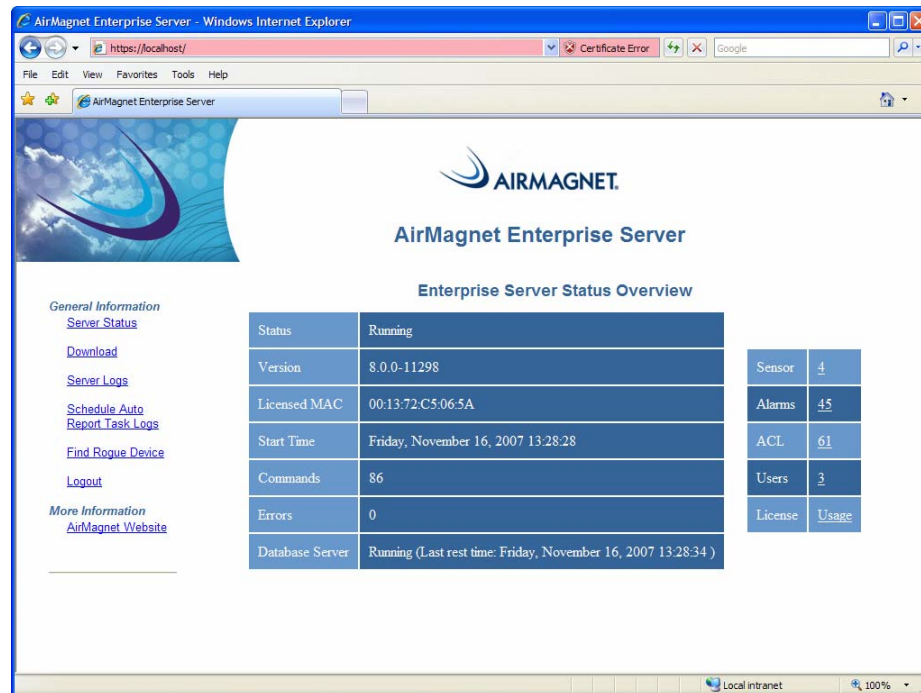


Figure 2-10: AirMagnet Enterprise Server page

- 4) Click the **Download** link. The Download AirMagnet Software page appears. See Figure 2-11.

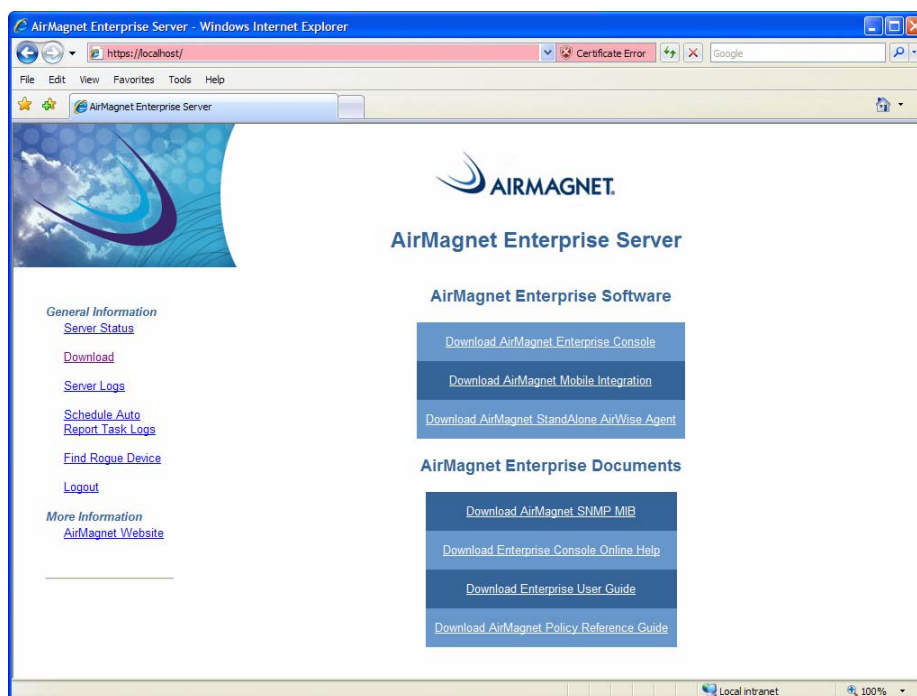


Figure 2-11: Downloading AirMagnet Enterprise Console

- 5) Click **Download AirMagnet Enterprise Console**. The File Download screen appears.
- 6) Click **Save** to continue. The Save As dialog box appears.

*You may also click **Run**, which lets you install the file directly from the AirMagnet Enterprise Server page. However, clicking **Save** allows you to download (save) the file onto your machine first. You can then open and install the file from there. This option will let you keep a copy of the file on your machine so that you can easily reinstall the program if you need to.*

- 7) To download the file to the default destination, click **Save**; to download it to another location, specify the location of your choice and then click **Save**. The download starts.
- 8) Wait until the file download is completed.

Installing AirMagnet Enterprise Console

Once you have downloaded AirMagnet Enterprise Console software onto a PC, the next step is to install it on the machine.

To install the AirMagnet Enterprise Console:

- 1) From the PC, locate the **Enterprise Console.exe** file and double-click to open it. The installation starts.
- 2) When the Open File – Security Warning screen appears, click **Run**. The AirMagnet Enterprise Console Installation screen appears.
- 3) Click **Next**. The AirMagnet Destination Folder screen appears.
- 4) To install the AirMagnet Enterprise Console in the default location, click **Next**; to install it in a location of your choice, browse to the location and then click **Next**. The installation continues.
- 5) When the AirMagnet Enterprise Console Setup Complete message appears, click **Finish**.

Verifying AirMagnet Enterprise Console Installation

The AirMagnet Enterprise Console must be able to communicate with the AirMagnet Enterprise Server in order to fulfill its management functions. It is for this reason that we make the verification of AirMagnet Enterprise Console-Server communication an integral part of the system installation. This is done by having the AirMagnet Enterprise Console login screen automatically pop up on the screen once the user click **Finish** on the finishing screen of the AirMagnet Enterprise Console installation. See Figure 2-12.

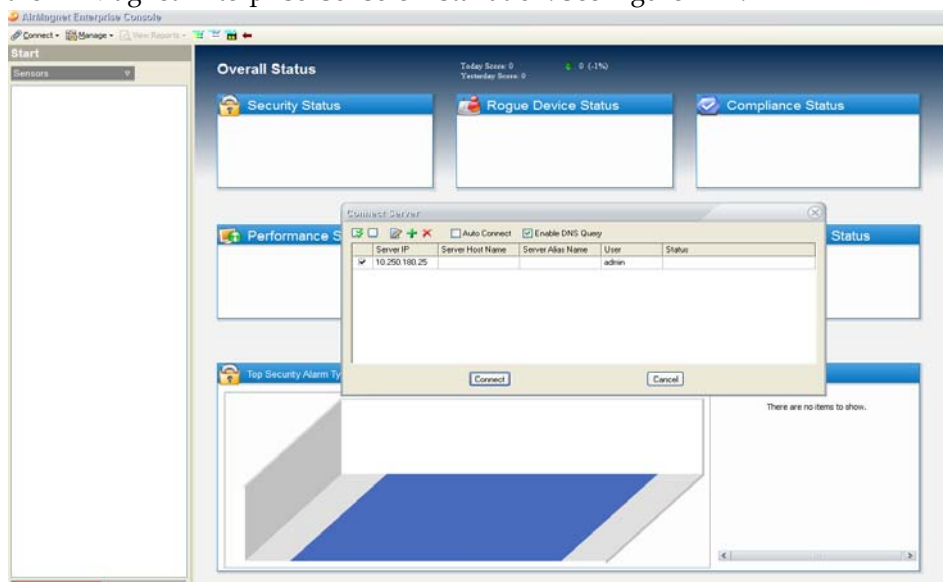


Figure 2-12: Connecting to AirMagnet Enterprise Server

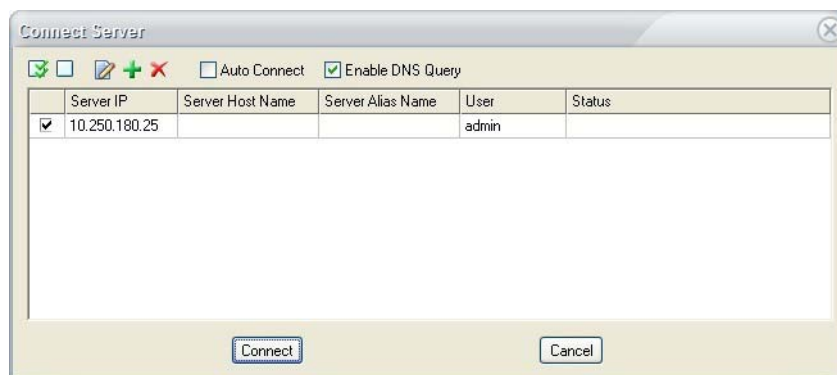
To verify AirMagnet Enterprise Console-Server communication:

- 1) On the Server Login screen, make the entries as described in Table 2-7.

Table 2-7: Enterprise Server Login Parameters

Parameter	Description
Server	The domain name or IP address of the AirMagnet Enterprise Server to be connected to.
Server Alias Name	If desired, give the server a name. This is not the same as the server host name (DNS query).
User Name	The user name created during AirMagnet Enterprise Server installation.
Password	The password created during AirMagnet Enterprise Server installation. Check "Remember Password" to automatically populate the password when connecting to this server IP.

- 2) Click **OK**. The Connect Server screen appears. See Figure 2-13.

**Figure 2-13: Connect Server table**

- 3) If you desire to display the Server Host Name, check **Enable DNS Query**. Click **Connect**. The AirMagnet Enterprise Console starts to connect to the AirMagnet Enterprise Server.

If the connection is successful, the Connect Server screen will close and the AirMagnet Enterprise Console's Start screen will appear. If the AirMagnet Enterprise Server is working properly, the round dot next to the name of the Server will be green. A red dot means a connection problem and requires immediate attention.

AirMagnet SmartEdge Sensor Configuration

Note: AirMagnet Sensor user guides (including sensor technical specifications) are located under the Documents/Drivers section of your My_AirMagnet account.

Prior to installing the AirMagnet SmartEdge Sensor, make sure that the AirMagnet Enterprise Server is installed and running on the network. The initial setup procedure also requires a computer to communicate to the AirMagnet SmartEdge Sensor. The user has the option of using the Web-based configuration or the Sensor Serial Console Port configuration method, as described in the following sections.

SmartEdge Sensors are configured to use DHCP by default when shipped. Users who wish to manually specify IP information for the Enterprise Server must alter this setting, as described in [Table 2-11 on page 39](#).

Configuring SmartEdge Sensor via Web Browser

The instructions in this section apply only if you choose to configure the AirMagnet SmartEdge Sensor using a Web browser. To configure the Sensor for use in FIPS-approved mode, use the configuration method in the AirMagnet AirMagnet Enterprise User Guide, Appendix H, "FIPS 140-2 Secure Operation"

Since the AirMagnet SmartEdge Sensor comes with a factory-default DHCP IP address setting, the IP address of the computer used to communicate with the AirMagnet SmartEdge Sensor must be configured in such a way that the computer can communicate with the AirMagnet SmartEdge Sensor.

To configure the AirMagnet SmartEdge Sensor:

- 1) From your computer, click **Start>Control Panel**. The Control Panel screen appears.
- 2) Double-click **Network Connections**. The Network Connections screen appears.
- 3) Double-click **Local Area Connection**. The Local Area Connection Status screen appears.
- 4) Click **General>Properties**. The Local Area Connection Properties screen appears.
- 5) Double-click **Internet Protocol (TCP/IP)**. The Internet Protocol (TCP/IP) Properties screen appears.

- 6) Check **Use the following IP address**, make the following entries as suggested in Table 2-8, and click **OK**.

Table 2-8: Internet Protocol (TCP/IP) Properties

Parameter	Description
IP address	Assign a static IP address to the computer in the same subnet as the AirMagnet SmartEdge Sensor, e.g., 192.168.0.77.
Subnet mask	Use 255.255.255.0 as the subnet mask.
Default gateway	Use 192.168.0.1 as the gateway IP address.

- 7) Now connect the AirMagnet SmartEdge Sensor to a separate network hub or switch for the initial configuration using a RJ-45 Ethernet straight-through cable or connect the Sensor directly to the computer using the supplied RJ-45 Ethernet crossover cable.
- 8) Power ON the AirMagnet SmartEdge Sensor.

The AirMagnet SmartEdge Sensor communicates with the AirMagnet Enterprise Server by using SSL and TLS at TCP Port 443.

- 9) Launch your Web browser, and enter **https://<sensor's IP address>** in the address field.
- 10) When a Security Alert message appears, click **Yes** to continue. A login screen appears. See Figure 2-14.



Figure 2-14: Connecting to a SmartEdge Sensor

11) Make the following entries as described in Table 2-9.

Table 2-9: AirMagnet SmartEdge Sensor Login Information

Parameter	Description
User name	Enter AirMagnetSensor as the user name. Note: AirMagnetSensor is one word.
Password	Enter airmagnet as the password.

12) Click **OK**. The Sensor Information Page appears. See Figure 2-15.



Figure 2-15: AirMagnet SmartEdge Sensor page (1)

- 13) From the left-hand side of the page, click **Configuration**. The Sensor Information Page refreshes. See Figure 2-16.

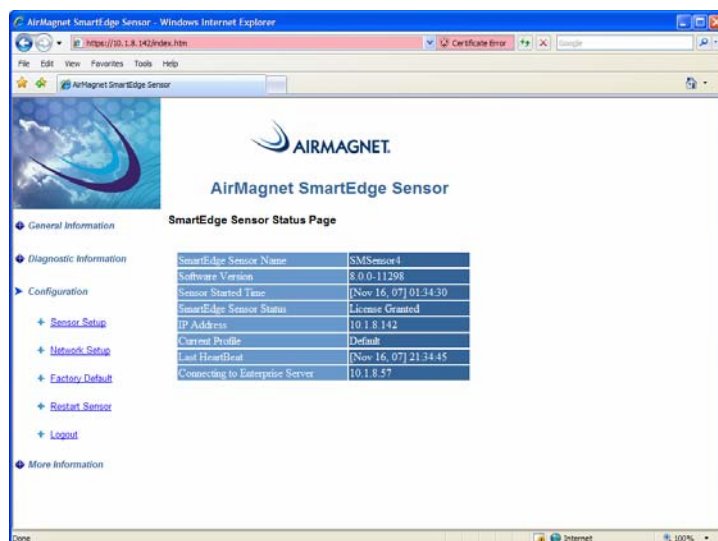


Figure 2-16: AirMagnet SmartEdge Sensor page (2)

- 14) Click **Sensor Setup**. The Sensor Information Page refreshes. See Figure 2-17.

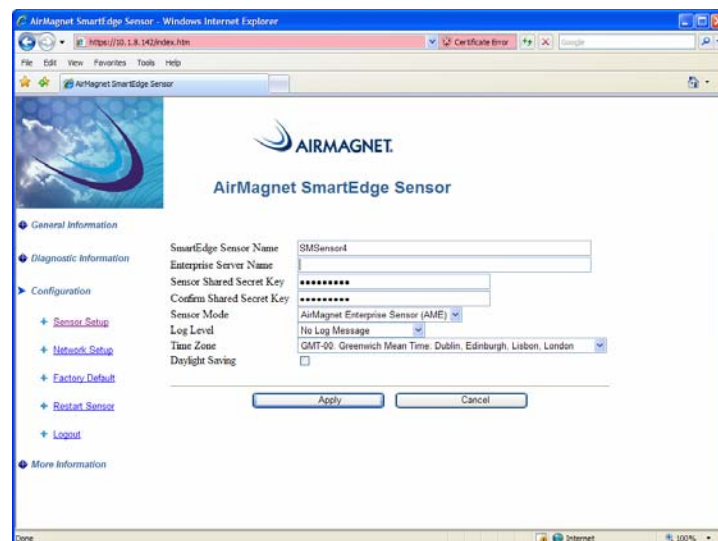


Figure 2-17: AirMagnet SmartEdge Sensor page (3)

- 15) Make the following entries or selections as described in Table 2-10.

Table 2-10: Sensor Configuration

Parameter	Description
Sensor Name	Change the default Sensor name “amsensor” to a unique a name in reference to its physical location.
Enterprise Server Name	Enter the name of the AirMagnet Enterprise Server. It can also be the IP address of the server (i.e., 192.168.0.1 by default) or a DNS-assigned name.
Sensor Shared Secret Key	Enter the Sensor Shared Secret Key. Note: This should be identical to the value you entered during AirMagnet Enterprise Server installation, which is AirMagnetSensor in our case. Refer to Figure 2-14 and Table 2-5.
Confirm Shared Secret Key	Re-enter the Sensor Shared Secret Key to confirm it.
Log Level	Select Log Important Event .
Time Zone	Select a time zone that corresponds to the region the AirMagnet SmartEdge Sensor is deployed.
Daylight Saving	Check this check box, if applicable.

- 16) Click **Apply**. The system will start to reboot. The Sensor Information Page pops up again once the reboot is completed
- 17) Upon Sensor reboot, click **Network Setup**. The Sensor Information Page refreshes. See Figure 2-18.

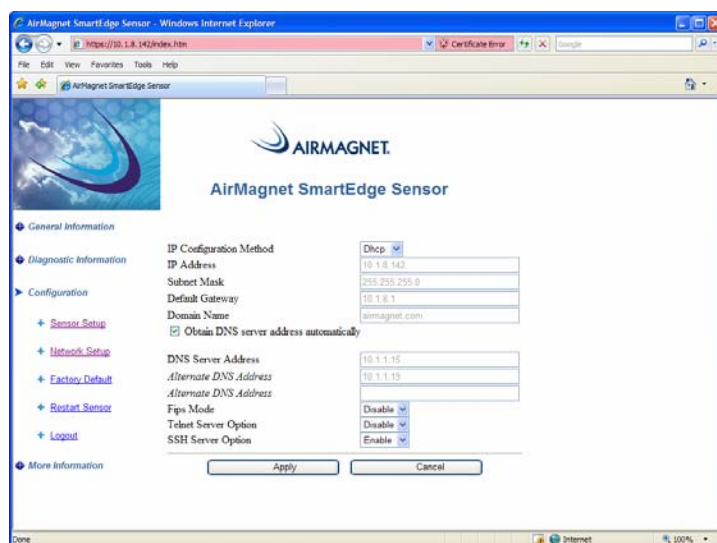


Figure 2-18: AirMagnet SmartEdge Sensor page (4)

- 18) Make the following entries as described in Table 2-11.

Table 2-11: Setting Up Network Parameters

Parameter	Description
IP Configuration Method	Select Static or DHCP from the drop-down list. Note: If Static is selected, then specify the IP address, subnet mask, and gateway address; if DHCP is selected, the system will get the IP address, subnet mask, and gateway address automatically.
IP Address	Enter the IP address ONLY if Static is selected as the IP Configuration Method. See Above.
Subnet Mask	Enter the subnet mask ONLY if Static is selected as the IP Configuration Method. See Above.
Default Gateway	Enter the gateway IP address ONLY if Static is selected as the IP Configuration Method. See Above.
Domain Name	Enter the domain name of your enterprise network, e.g., mydomain.com
Fips Mode	Enable Fips mode on your sensor.
Telnet Server Options	Select Enable if you want to use the Telnet Server on the AirMagnet SmartEdge Sensor.
SSH Server Option	Select Enable if you want to use the SSH Server on the AirMagnet SmartEdge Sensor.
Obtain DNS server address automatically	Check this check box if you want the system to automatically get the DNS server address. Note: This check box will be disabled when Static is selected as the IP address configuration method.
DNS Server Address	Enter the DNS server address ONLY if Obtain DNS server address automatically is NOT checked.
Alternate DNS Address	Enter an alternate DNS server address ONLY if Obtain DNS server address automatically is NOT checked.
Alternate DNS Address (2)	Enter a secondary alternate DNS server address (if needed).
Ethernet Auto Negotiation	Allow the sensor to automatically negotiate with your ethernet settings.

- 19) Click **Apply**. The AirMagnet SmartEdge Sensor will start to reboot, and the Sensor Information Page refreshes once the reboot is completed.
- 20) Continue using the crossover cable if you have an autosensing MDI/MDIX hub/switch. Otherwise, connect the AirMagnet SmartEdge Sensor to the corporate network hub/switch using a straight-through cable.

- 21) Change the computer's static IP address of 192.168.0.XXX back to your corporate network IP settings.
- 22) Browse to the AirMagnet SmartEdge Sensor Web page (<https://<Sensor IP address>>) to check if the license has been granted to the AirMagnet SmartEdge Sensor. Use **admin** as the username and use the **password of the AirMagnet Enterprise Server**.

If the DHCP option is selected, the new IP address assigned to the AirMagnet SmartEdge Sensor will be displayed on the AirMagnet Enterprise Server Page under Status>Sensor List.

If a license has been granted, the name of the newly installed AirMagnet SmartEdge Sensor will appear in the Sensor List under the Enterprise Server on the left-hand side of the AirMagnet Enterprise Console's Start screen.

It is strongly recommended that users completely close all internet browser windows after logging out of the Enterprise Server or Sensor web interfaces. Additionally, users are discouraged from opening multiple tabs in the browser window while logged into the web interface. the user should not use the Internet browser's History function to navigate to the web interface.

Configuring SmartEdge Sensor via Sensor Serial Console Port

The instructions in this section apply only if you choose to configure the AirMagnet SmartEdge Sensor using the Sensor Serial Console Port. To configure the Sensor for use in FIPS-approved mode, use the configuration method in The AirMagnet User Guide, Appendix H, "FIPS 140-2 Secure Operation".

To configure the AirMagnet SmartEdge Sensor using Sensor Serial Console Port:

- 1) Connect the Sensor Serial Console Port of the AirMagnet SmartEdge Sensor to the serial port of the computer using the supplied serial cable.
- 2) Click **Start>Programs>Accessories>Communication>Hyper Terminal**.
- 3) Select the appropriate COM port to which the AirMagnet SmartEdge Sensor is connected.
- 4) Make the following entries or selections for the Hyper Terminal session as described in Table 2-12.

Table 2-12: Hyper Terminal Session Parameters

Parameter	Description
bits per second	115200

Table 2-12: Hyper Terminal Session Parameters

Parameter	Description
data bits	8
parity	no
stop bit	1
flow control	none

- 5) Now connect the AirMagnet SmartEdge Sensor to the corporate network using a straight-through RJ-45 Ethernet cable.
- 6) On the Hyper Terminal screen, you will get the “**config>**” prompt.
- 7) **config>set network**
This command is used to set the IP address parameters (IP address, subnet mask, and the default gateway) and to enable the Telnet server on the AirMagnet SmartEdge Sensor.
- 8) **config>set time**
This command is used to set the SmartEdge Sensor time zone and daylight savings option. The time on the SmartEdge Sensor is set when the AirMagnet SmartEdge Sensor communicates with the AirMagnet Enterprise Server.
- 9) **config>set sensor**
This command is used to configure the SmartEdge Sensor name, AirMagnet Enterprise Server name or IP address, and the Sensor Shared Secret Key.

Figure 2-19 is an sample of the screen command on the Hyper Terminal screen for AirMagnet SmartEdge Sensor configuration.

```

config>set network
DHCP Enabled (Y/N)?n
IP Address(192.168.0.100):10.1.1.207
Subnet Mask(255.255.0.0):255.255.255.0
Default Gateway(192.168.0.1):10.1.1.1
Domain Name(my.domain):airmagnet.com
Primary DNS Server():device eth0 left promiscuous mode
10.1.1.19
Optional DNS Server():
Do you want to enable Telnet Server(Y/N)?y
The system is setting the following configuration:
  IP Address:      10.1.1.207
  Subnet Mask:     255.255.255.0
  Gateway:        10.1.1.1
  Domain Name:     airmagnet.com
  Primary DNS Server: 10.1.1.19
  Telnet Server Enabled: Yes
Is the above information correct (Y/N)?n
config>_

```

Figure 2-19: Sample screen commands for Sensor configuration

- 10) Reboot the AirMagnet SmartEdge Sensor when prompted.
- 11) Once the Sensor is rebooted, browse to the AirMagnet SmartEdge Sensor Web page (<https://<Sensor IP address>>) to check if the license has been granted to the AirMagnet SmartEdge Sensor. Use **admin** as the username and use the **password of the AirMagnet Enterprise Server** as the login password.

The user can also telnet to the AirMagnet SmartEdge Sensor to verify its configuration. However, if the Sensor is configured for use in FIPS-approved mode, you can only use the Sensor Serial Console Port to verify the Sensor's configuration because telnet is disabled in FIPS-approved mode. SSH must also be disabled in FIPS-Approved mode.

Verifying Sensor Configuration Using Show Commands

This section introduces the commands used to verify AirMagnet SmartEdge Sensor configuration.

To verify AirMagnet SmartEdge Sensor configuration settings:

- 1) `confi g>show sensor`

This command will display Sensor name, software and system version, and Sensor uptime.

- 2) `confi g>show network`

This command will display the current network configuration.

- 3) `confi g>show ti me`

This command will display the Sensor current time, time zone and whether the daylight savings option has been enabled or not.

Maintenance Commands

The following are the commands commonly used for maintaining the AirMagnet SmartEdge Sensor:

- 1) `confi g>reboot`

This command is used to reboot the AirMagnet SmartEdge Sensor.

- 2) `confi g>restore`

This command is used to restore the AirMagnet SmartEdge Sensor to its factory default. It does NOT zeroize the password or the associated AES key. Instead, it will restore the password to `ai rmagnet` while leaving the AES key unchanged.

- 3) `confi g>pi ng [-s|-c] host-i p`

This command is used to ping other hosts on the network.

- 4) `confi g>update [sys|app]`

This command is used to update the kernel and the AirMagnet application software. The user is prompted for the location of a TFTP server to get the latest update. You must have a TFTP server set up prior to using this command.

There are two files that must be put on the TFTP server: `rlmage.bin` and `amwebsensor.tar.gz`. The `rlmage.bin` file is used for the "update sys" command; the `amwebsensor.tar.gz` file is used for the "update app" command.

Since the AirMagnet Enterprise Server supports different models of AirMagnet SmartEdge Sensors and the two files are stored at different locations on the AirMagnet Enterprise Server, it is of vital importance that you point the TFTP server to the correct location and rename the files properly. Failure to do so may lead to system crash, making it impossible to update the system and the application. Table 2-13 explains the actions you need for each model of the AirMagnet SmartEdge Sensors.

Table 2-13: Sys and App Update Files Locations and Procedures

Sensor	Location of Files	Actions to be Taken
A5010	\program files\AirMagnet Inc\AirMagnet Management Server\web\AM5010	Copy the files to the TFTP server, and rename "AM5010-rlmage.bin" to "rlmage.bin"
A5012	Same as A5010.	Same as A5010.
A5020/5120	\program files\AirMagnet Inc\AirMagnet Management Server\web\AM5020	Copy the files to the TFTP server, and rename "AM5020-rlmage.bin" to "rlmage.bin".
A5023/5123	\program files\AirMagnet Inc\AirMagnet Management Server\web\AM5023	Copy the files to the TFTP server, and rename "AM5023-rlmage.bin" to "rlmage.bin"
A5200	\program files\AirMagnet Inc\AirMagnet Management Server\web\AM5200	Copy the files to the TFTP server, and rename "AM5200-rlmage.bin" to "rlmage.bin"
A5225	\program files\AirMagnet Inc\AirMagnet Management Server\web\AM5225	Copy the files to the TFTP server, and rename "AM5225-rlmage.bin" to "rlmage.bin"

5) `config>diag`

This command initiates the following important system tests:

- The test of Sensor's ability to scan 802.11 a/g channels to verify if the Sensor can scan all available channels.
- The test of the Ethernet interface to make sure that it works properly.

- The test of the DHCP feature to verify if the Sensor can obtain IP addresses dynamically.
- The test of the DNS feature.
- The test of the PING feature to verify the connectivity between the AirMagnet Enterprise Server and the SmartEdge Sensor.
- The test of connection through the firewall and verify the AirMagnet Enterprise service status (i.e., up or down).
- The verification of the Sensor license status, which includes license granted, no license, host mismatch, software version mismatch, license file not found, bad license, license expired, device count exceeded, etc.
- The download speed from the AirMagnet Enterprise Server.

This command also triggers the Sensor to perform self checking and module checking. Self checking verifies encryption algorithms to ensure that they function correctly and have not been tampered, whereas module checking is used to ensure that no binary file is corrupted. This command is in compliance with FIPS requirement.

6) `confi g>set fi psmode`

This command is used to toggle the AirMagnet SmartEdge Sensor between FIPS and non-FIPS Modes. When set in the FIPS mode, the Sensor will automatically perform self-checking and module checking at system start. You will see self-checking messages on the CLI. When the Sensor is set the non-FIPS mode, it will not perform any self-checking or module checking.

The following is a sample screen command:

```
confi g>set fi psmode
```

```
Sensor is in non-fips mode. Do you want to set to fips mode (y/n):  
y
```

```
The sensor has been set to fips mode.
```

```
The Shared Secret Key has been set to default value.
```

```
You need to re-enter your shared secret after the sensor is  
rebooted.
```

```
The Telnet Server has been disabled.
```

```
You must configure internet browser to use TLS protocol in order  
to communicate.
```

```
You must reboot the sensor to take the setting effects.
```

```
Do you want to reboot now (y/n)?
```

*For FIPS mode, the password will be encrypted; for non-FIPS mode, it will be in plain text. Each time the user switches from one mode to the other, the password will be reset to **ai rmagnet** (default). By default, the AirMagnet Smartedge Sensor is in non-FIPS mode. For instructions on how to configure the TLS protocol, see the next section.*

7) `confi g>show fi psmode`

This command is used to verify whether the AirMagnet SmartEdge Sensor is set in the FIPS mode. The following is a sample screen command:

```
confi g>show fi psmode
```

```
FI PS mode: ON
```

FIPS-Required Features

The features discussed here are required by the Federal Information Processing Standards (FIPS).

1) Use of TLS protocol for secure communication

FIPS requires the use of TLS protocol for secure communication. Otherwise, there would be no communication among the AirMagnet SmartEdge Sensor, the AirMagnet Enterprise Console, and the AirMagnet Enterprise Server.

To comply with the FIPS requirement, you must configure your Internet Explorer using these commands: **Start>Internet Explorer>Tools>Internet Options...>Advanced>Security>Use TLS 1.0**. See Figure 2-20.

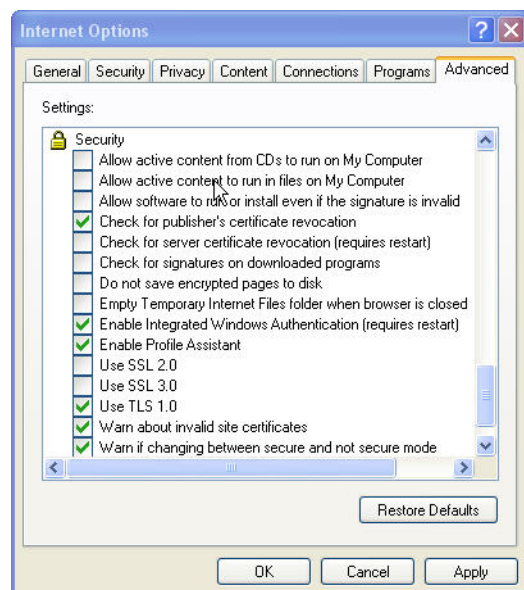


Figure 2-20: Configuring Security Settings

As shown in Figure 2-22, the user must check Use TLS 1.0. and uncheck Use SSL 2.0 and Use SSL 3.0.

2) Limited logon attempts

The user is allowed a maximum of 3 log-on attempts per minute.

3) Length of password word

The password used to access the AirMagnet Enterprise system must be between 6 and 36 characters in length.

4) Automatic self checking and module integrity checking on system start (or reboot).

The AirMagnet SmartEdge Sensor will automatically perform self checking and module integrity checking upon the start or reboot of the AirMagnet Enterprise system to ensure system security and integrity.

If your Command Line Interface is open, the following commands will be displayed on the screen:

Start FIPS Self Test for Encrypted Algorithm. . .

Passed.

AmWebserver Module Integrity Checking. . .

Passed.

AmConfig Module Integrity Checking. . .

Passed.

AmMonitor Module Integrity Checking. . .

Passed.

Checking Done.

If an error occurs during the self checking, then the AirMagnet SmartEdge Sensor will enter an error state, in which all communication among the Sensor, Server, and Console will be disabled since NO secure communication is allowed in an error state. The Sensor will keep generating the same error message. If this occurs, contact AirMagnet Technical Support for assistance.

5) Change of the shared secret key through secure communication only.

FIPS does NOT allow the change of the shared secret key through Telnet due to lack of encryption in the Telnet communication protocol. If, for some reason, the user needs to change the shared secret key, it can be done either through the Sensor Serial Console Port or a browser interface.

6) Password Encrypted in FIPS-approved algorithms

All passwords used to access the Sensor will be encrypted using a FIPS-approved algorithm and saved in a file. Passwords entered using a Web browser and the TLS protocol and those entered using the Sensor Serial Console Port meet the requirement.

7) Securing the Sensor with tamper-evident seals

To prevent your AirMagnet SmartEdge Sensor from tampering that may jeopardize the security and integrity of your corporate network, use the supplied tamper-evident seals to cover the screws at the bottom of each Sensor. At least two seals should be applied on each Sensor. **For instructions on how to apply the tamper-evident seals, see the section that follows.**

8) Periodical inspection of the module for evidence of tampering

Tamper evidence includes unexpected scratches on the cover and damage to the tamper-evident seals on the back of the module. Compare the seal serial numbers against the recorded numbers to determine whether an unauthorized replacement has occurred, which may indicate a tamper condition. If tampering is suspected, zeroize the cryptographic keys and shared key following the steps detailed in [“Zeroizing an AirMagnet Sensor” on page 47](#). Then remove the module from service and contact AirMagnet Technical Support for assistance.

When operating the Sensor in FIPS-approved mode, administrators and users must take precaution to avoid disclosure of sensitive authentication data, including the shared secret key and passwords. Follow all of the guidance in this section to ensure that the module is installed and operated in a secure manner.

Zeroizing an AirMagnet Sensor

The Zeroize operation is used to wipe out all the passwords and their associated AES keys and then delete them from the Sensor’s memory. It is important that users zeroize sensors only when necessary (such as in order to ensure FIPS compliance), as the Sensor will require its firmware to be restored after the operation has completed.

In order to initiate the zeroization process, the Sensor must **not** be actively connected to a valid Enterprise server. Thus, the user must direct the Sensor to an invalid IP before the process can begin. Follow the steps below corresponding to the desired process:

This command is in compliance with FIPS requirement. Note that The zeroize command will only be available to Sensors operating in FIPS mode.

To zeroize a Sensor via serial connection:

- 1) Establish a serial connection to the Sensor and log into the device using the shared secret key.
- 2) Type `set sensor` and press Enter.

- 3) When asked to enter the server IP, enter the IP of a nonexistent server. Reboot the Sensor when prompted.
- 4) After the reboot has completed, log in to the sensor using the shared secret key.
- 5) Type zeroize and press Enter.
- 6) Confirm the zeroization process. The Sensor will begin zeroization and reboot when complete. Note that after zeroization, the Sensor prompt will appear as follows:

/ #

To zeroize a Sensor via the web interface:

- 1) Open an internet browser and navigate to
`https://<Sensor IP>`
Confirm any security or certificate exceptions required.
- 2) Log into the sensor with username AirMagnetSensor (case sensitive) and the Sensor's shared secret key.
- 3) Click the Configuration link on the left-hand portion of the window and click Sensor Setup.
- 4) Change the IP address of the Sensor's management server to the IP of a nonexistent server.
- 5) Click Apply and reboot the Sensor when prompted.
- 6) Close and relaunch the internet browser to ensure that the session has been closed.
- 7) Navigate to `https://<Sensor IP>` again and click the Configuration link.
- 8) Click Zeroize and confirm the zeroization process. The Sensor will reboot itself after it has completed.

International Power Standards

Contact AirMagnet technical support for power specification for locations outside USA. For information about the AirMagnet SmartEdge Sensor, see the AirMagnet Enterprise User Guide, Appendix F, "Sensor Specifications"

Verifying AirMagnet SmartEdge Sensor Installation

Upon the installation of each and every AirMagnet SmartEdge Sensor, it is important to verify that it is installed correctly and that it is communicating with the AirMagnet Enterprise Server.

To verify Sensor installation:

- 1) Open your Web browser, enter **https://Enterprise Server name or IP address**, and press the **Enter** key on your keyboard. The AirMagnet Enterprise Server page appears.
- 2) From the left-hand side of the AirMagnet Enterprise Server page, click **Status**, and then click **Sensor**. The AirMagnet Enterprise Server page refreshes, showing the Sensor List. See Figure 2-21.

Sensor Name	Wireless MAC Address	Wired MAC Address	IP Address	Last Heartbeat	Last License Granted	Gateway
amsensor-2012	00:02:6F:20:32:22	00:02:6F:2E:07:5A	192.168.2.37	Tuesday, June 07, 2005 15:34:34	Monday, June 06, 2005 15:45:17	192.168.2.1
QA2011	00:02:6F:20:1F:58	00:0D:CB:00:01:46	192.168.2.12	Tuesday, June 07, 2005 15:34:17	Monday, June 06, 2005 15:45:18	192.168.2.1

Figure 2-21: Server-Sensor connection list

- 3) Make sure that the Sensor name and IP address are correct and that a license has been granted.
- 4) Alternatively, start the AirMagnet Enterprise Server, connect it to the AirMagnet Enterprise Server to which the Sensor is connected.
- 5) From the AirMagnet Enterprise Server Start screen, see if the Sensor appears under the Enterprise Server and if it is functioning properly.

If the Sensor is installed successfully and working properly, the name of the sensor should appear under the Server in the upper-left corner of the AirMagnet Enterprise Console's Start screen, as

shown in Figure 2-22. A Sensor icon in red always indicates the sensor itself is experiencing some problem. It may be marked as “no license”, “down”, etc. and requires immediate attention.

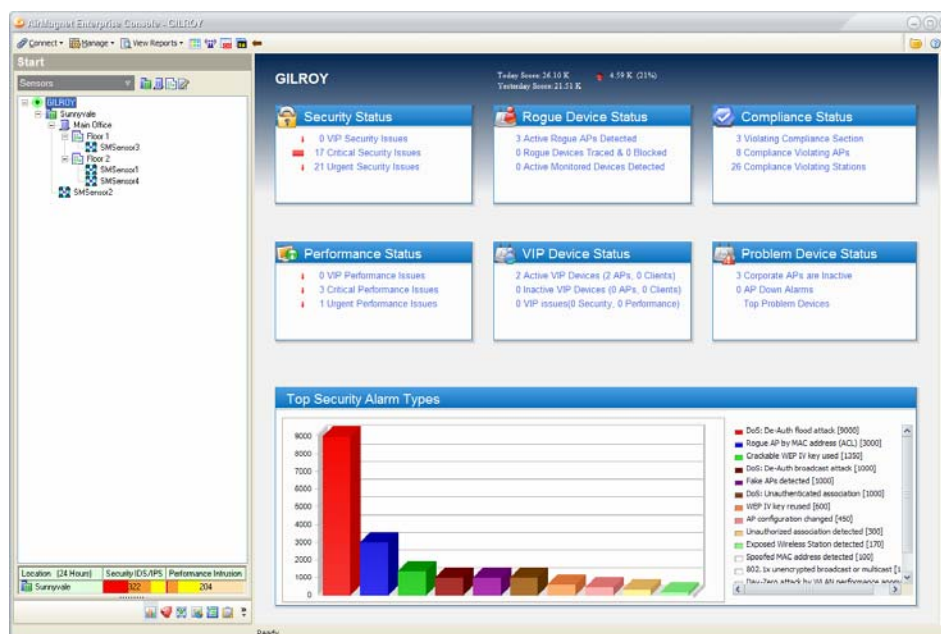


Figure 2-22: AirMagnet Enterprise Console Start screen

Software Sensor Agent (SSA)

Introduction

The Software Sensor Agent (SSA) enables a Windows client computer to act as an AirMagnet Enterprise sensor for some basic WIPS functionality such as rogue detection and tracing. The SSA uses the computer's WiFi adapter to collect wireless security information about the surrounding access points (APs) in its environment and reports to the AirMagnet Enterprise Server.

Special Notes

- There is an SSA client age-out setting for removing the inactive SSA client from the sensor tree in AME console -> Manage -> Server Options -> Server tab.
- The tracing feature in SSA only performs auto wired tracing and no blocking function.
- SSA only scans for APs (no station and no ad hoc devices).
- Currently, there are no alarms available for SSA.
- SSA only uses the rogue detection configuration from the policy profile.

- Before using the SSA wired tracing feature, the WinPcap tool must be installed on the SSA machine that will perform the wired tracing function. You can download a copy of the WinPcap 4.1.2 version from AME server web page -> Download page.

Installation Methods

- **Unattended:** No user interaction. Generally pushed out by network administrators to be installed automatically on multiple stations.
- **Manual:** It can be manually installed on a machine by an individual user.

SSA System Requirements

- Microsoft Windows XP or Windows 7.
- Enabled 802.11 a/b/g/n wireless adapter.
- Since SSA client is run as Window services, the user needs to have administrative rights on the machine in order for the SSA client to be installed successfully.

Note: In order to run an AHC job on an SSA client, the wireless network profile for the SSID must be already configured in Windows Zero Config on the SSA client machine. This applies to both Microsoft Windows XP and Windows 7.

SSA Installation

- 1) Log into the AirMagnet Enterprise Server webpage (https://<IPAddress_AMEserver>).
- 2) Click "Download" link shown on the left hand panel. There are two options:

Unattended method

From the AME server download page, click **Download AirMagnet Software Sensor Agent ZeroConfig Install Zip File (with VC redist package)** and save the download file. The network administrator can utilize this package (in which the install batch file contains AirMagnet Enterprise Server IP address) to push the install onto multiple stations.

When the SSA client is installed on a laptop, the SSA icon is displayed in the system tray area on the machine. The user can right-click or double-click the SSA icon to select the configuration option.

Manual method

From the AME server download page, click **Download AirMagnet Software Sensor Agent Install EXE File (with VC redist package)**. Save the download file. Double-click **Enterprise SSA.exe** to run the installation.

At the conclusion of installation, a dialog is opened requesting the AirMagnet Enterprise server IP and Shared Key.

*Note: The Shared Key is created by the user during AirMagnet Enterprise server installation. The Shared Key may be reset using the AirMagnet Enterprise Console. Go to Manage > Server Options and click the **Shared Secret** tab.*

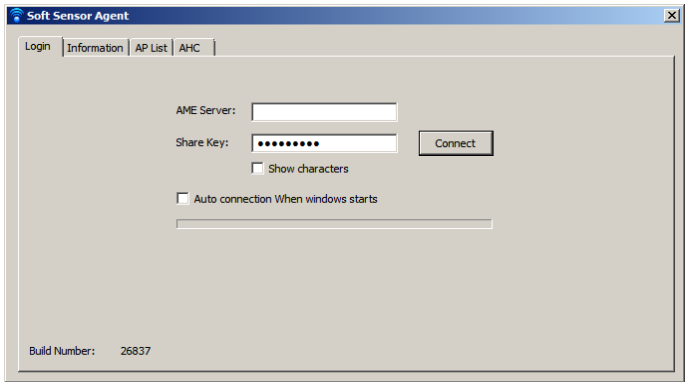


Figure 2-23: SSA Dialog

Table 2-14: SSA Dialog tabs

Tab	Description
Login	AME Server: IP Address Share Key: Share code created during installation
Information	Wireless adapter information pertaining to the adapter on the SSA host machine and its AHC status.
AP List	AP detected by SSA.
AHC	List of AHC jobs

Once the SSA client is installed on laptop, the SSA icon  is displayed in the system tray area. The user may double-click the SSA icon to open the SSA dialog.

AirMagnet Console and SSA

When an SSA is running on a station, the Sensor Tree in the AirMagnet Enterprise Console will display an SSA icon along with its machine name. If more than one machine in the same network subnet is running SSA, those machines will be grouped together under the subnet IP address.

To view APs reported by SSAs, open the Infrastructure view, click on the SSA sensor, and all detected APs will be listed in the AP list.

If the machine hosting SSA stops running (such as shutdown or hibernation), you may configure the period of time to wait before the SSA icon is removed from the console tree view.

- 1) From the Enterprise Console, click Manage>Server Options.... The Manage Server Configuration screen appears.
- 2) Click Server tab.
- 3) Next to **Remove Inactive SSA in** select a time duration from the drop-down menu.
- 4) Click OK.

Getting Software and License from My AirMagnet

The product software and license(s) may be obtained from your My_AirMagnet account. Refer to “[Product Registration](#)” on page 11.

Chapter 3: Deploying AirMagnet Enterprise

Preparation for System Deployment

Deploying the AirMagnet Enterprise system involves careful planning. The following checklist can be used to organize the installation and configuration process. It also can be used as a directory to the details in the remaining parts of this guide. The following must be kept in mind when planning a WLAN deployment:

- 1) Scale of the WLAN – The first step in planning a deployment is to consider the physical layout and available resources for the project:
 - a. Determine how many sites are to be covered by the deployment.
 - b. Determine how many AirMagnet SmartEdge Sensors will be used to collect data.
 - c. Depending on whether or not the sites span multiple buildings and campuses, VPN and firewall settings may be important.
 - d. If NAT is used, care must be taken when determining which network devices are capable of addressing one another.
 - e. See Appendix A: “Secure Communication” for a summary of VPN/Firewall issues.
- 2) Users – User management will permit planned and controlled access to the AirMagnet Enterprise system:
 - a. Consider the users who will be granted access and assigned passwords and user roles.
 - b. Make sure that all users can connect to the AirMagnet Enterprise Server and the AirMagnet SmartEdge Sensors from their locations in the network.
 - c. For details on users and roles, see the section “Assigning Management Responsibilities” in Chapter 5.
- 3) AirMagnet Enterprise Server Administration – Consider the basic requirements of the AirMagnet Enterprise Server administration:
 - a. The AirMagnet Enterprise Server should be physically located at a central point in a wired network, ideally a network operations center (NOC) with proper Ethernet and AC power connections. This may be a NOC that is staffed full-time or it may be a network closet in the basement.
 - b. The AirMagnet Enterprise Server should have uninterrupted AC power and be wired for 10/100 Ethernet.
 - c. The AirMagnet Enterprise Server should be a machine dedicated to running AirMagnet services only.
- 4) SmartEdge Sensor Administration – Consider the basic requirements for AirMagnet SmartEdge Sensor administration:
 - a. Make sure that the AirMagnet SmartEdge Sensor is deployed close to a power source (i.e., AC power or PoE) and a 10/100 Ethernet connection.

Scenarios for AirMagnet Enterprise Server Setup

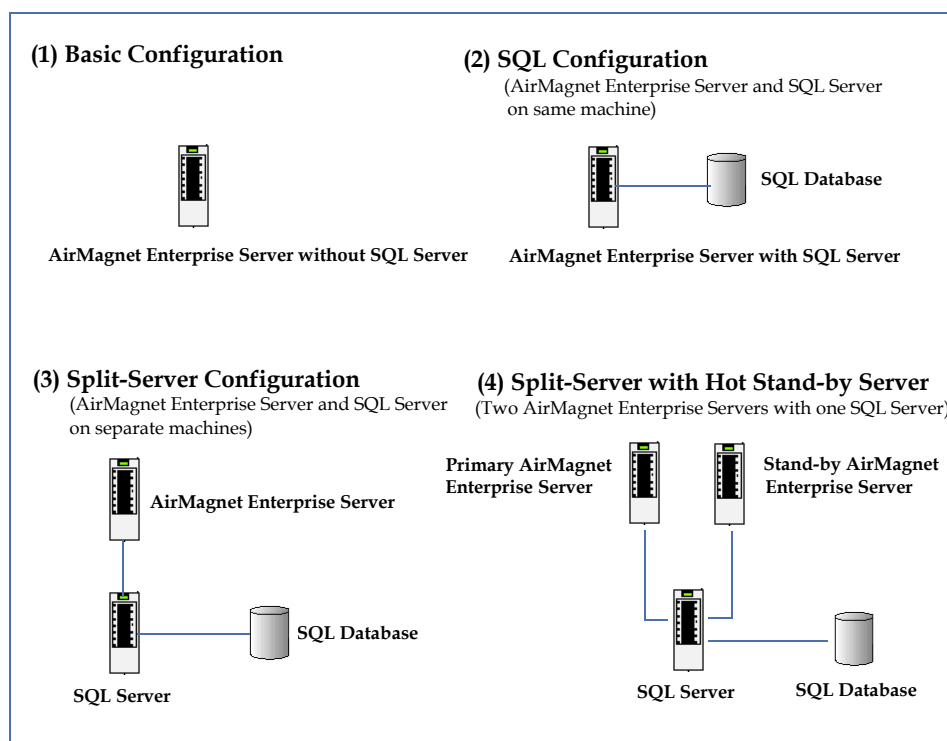


Figure 3-1: AirMagnet Enterprise system hardware components

How Many SmartEdge Sensors Do I Need?

The AirMagnet Enterprise system is a comprehensive system for intelligently monitoring all operating characteristics of a WLAN environment. Sophisticated security intrusion detection and policy conformance is continuously monitored, along with many network and device-specific performance metrics. The AirMagnet SmartEdge Sensor is the edge device which captures and analyzes wireless packets. The number of SmartEdge Sensors required to monitor a given WLAN environment is a design point of great interest to network and budget planners when considering this technology. This section covers the basic technical background and design methods required to understand the process for determining the optimal WLAN monitoring network design, including the number of AirMagnet SmartEdge Sensors required.

Basic Concepts

Normal design goals apply to building a WLAN monitoring system using AirMagnet Enterprise — “cover” the largest possible area with the least amount of equipment. The same thinking is usually applied to building a WLAN with access points (APs) or other infrastructure elements. When considering deployment of a WLAN infrastructure, it may be tempting to “eyeball” a floor plan or the outside of a building and come up with an estimate of the number of APs required to provide coverage for very basic WLAN services. The reality is

that few successful WLAN deployments are achieved using this design method. Carefully executed AP and antenna site surveys are required to ensure proper coverage for all users. This same principle applies to the design of AirMagnet SmartEdge Sensor networks for monitoring WLAN environments.

Sensor Field of View (FOV)

The FOV is the physical area that can be monitored for WLAN activity by the Sensor. The Sensor FOV is analogous to the coverage for an AP.

Trusted Devices

A trusted device is an AP or WLAN computing station (STA) provisioned by an authorized network deployment organization to provide WLAN services.

Unauthorized WLAN Devices

They can be any WLAN device (AP or STA) that is transmitting or receiving an 802.11 signal in the 2.4-GHz or 5-GHz bands, which is observable inside the physical area defined as the trusted zone of operation. There are several classes of unauthorized devices. For example, the “friendly” rogue AP, which is an AP that is part of another organization’s network but happens to be radiating into the trusted zone. Common examples of friendly rogue APs include neighboring tenants in a multi-use office building or business park, or a home or hot-spot AP that radiates into an adjacent office in a dense urban area.

Radio Receiver Sensitivity/Link Budget

The SmartEdge Sensor contains a multi-mode radio that can receive 802.11b, 11g, and 11a frames from the air. As with every WLAN radio, the SmartEdge Sensor radio has a receiver sensitivity profile, which specifies a receiver sensitivity value for each data rate supported by each 802.11 mode. Combined with the SmartEdge Sensor antenna characteristics, this profile defines the RF link budget threshold for detection of 802.11 traffic for each of the modes.

802.11 RF Media Types

The SmartEdge Sensor captures 802.11 packets transmitted using 802.11b or 11g modes in the 2.4-GHz band, and 802.11a in the 5-GHz band. Since the 5-GHz band has different RF propagation characteristics and radio performance parameters compared to the 2.4-GHz band, the Sensor FOV will be different for 11a devices. It is important to consider this when designing SmartEdge Sensor networks, because even though most existing WLAN infrastructures use the 2.4-GHz 802.11b/g modes, it is critical that the SmartEdge Sensor network be able to accurately detect unauthorized 11a devices.

In most cases, the Type C boundary will encompass the largest area, with the Type B boundary smaller, and the Type A boundary enclosing the smallest area. Figure 3-3 illustrates the three FOV boundary types.

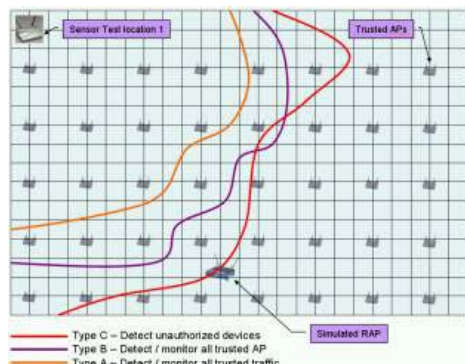


Figure 3-3: Illustration of Sensor FOV types

It is possible to mix Sensor FOV types. For example, a design may specify Type A FOV for interior areas, and have additional Sensors in place to monitor lobbies or adjacent parking areas which are designated with Type C FOV.

Type B: Trusted AP Monitoring

The edge of the Type B Sensor FOV is defined as the boundary for the SmartEdge Sensor to reliably monitor trusted APs at a signal level at least equal to a minimum specified in the design. For example, a minimum signal level of -88 dBm is sufficient for monitoring all 802.11b traffic transmitted from a popular enterprise AP using a 2.5 dBi diversity antenna configuration.

Type C: Unauthorized Device Detection

The edge of the Type C Sensor FOV is defined as the boundary for the SmartEdge Sensor to reliably detect “under-desk” rogue APs for indoor areas, and the boundary for the SmartEdge Sensor to reliably detect AP or STA devices in open areas for outside areas.

Factors Affecting SmartEdge Sensor FOV Performance

Just like the coverage created by an AP, there are many factors that influence the exact FOV pattern which a SmartEdge Sensor will achieve at a given location. These factors can be divided into four categories:

- Sensor RF specifications;
- Sensor installation methods;
- In-building structural composition and type;
- WLAN network operational characteristics, if present.

Due to the large variations created by these factors from one WLAN environment to another, it is clear that the Sensor FOV measurement process is essential for a well designed WLAN monitoring network. Some of these factors can have a very great impact on the Sensor FOV and must be carefully evaluated in the design, measurement, and verification process.

SmartEdge Sensor Installation Restrictions

Some corporate office environments require that technical equipment be installed so that it is completely hidden from view. This may restrict potential SmartEdge Sensor locations to completely enclosed areas such as above acoustic-tile drop ceilings. Blocking the SmartEdge Sensor antennas in this way would reduce the FOV, sometimes dramatically, compared to an exposed mounting location. A similar example can be found in some government sites and public access venues such as airports, where it is often required that communication devices be installed only in designated cabinets or rooms, usually with tight physical access control.

Office with Dense Central Core

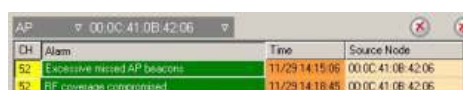
Many office towers are constructed with a central engineering core, a very dense area containing elevators, electrical and mechanical equipment, air handling ducting, telco and data cable conduits, etc. Often this central core area completely blocks 802.11 signal propagation, usually requiring that the area be divided into at least 2 physical sectors for a WLAN. One floor of an office tower as small as 25,000 sq. ft. may require 2 SmartEdge Sensors to get the desired FOV.

Microcell Network

Some WLAN designs use a microcell configuration, where the coverage created by each AP is purposely made very small to increase overall available throughput, or to carefully “paint” coverage into the perimeter of a building, minimizing the chance that signal is available outside. In order to provide Type B or A FOV for this type of network, SmartEdge Sensors would have to be carefully positioned to guarantee reliable monitoring of this microcell coverage environment.

SmartEdge Sensor Network Design Objectives

WLAN monitoring systems may be first considered by the IT security group specifically for the wireless intrusion detection system (WIDS) features. Type C Sensor FOV design is appropriate if this is the only intended use of the system. AirMagnet Enterprise contains a rich set of WLAN health and performance management capabilities, as well as the ability to perform real-time remote diagnostics. For example, a change to building structure (such as moving a wall, reconfiguring cube areas, installing new machines, etc.) can affect WLAN coverage. With a Type B Sensor design, AirMagnet Enterprise can immediately recognize resultant AP signal level changes and provide very detailed alerts to the NOC or network engineers. Figure 3-4 shows an example of the alarm types generated by the SmartEdge Sensor.



CH	Alarm	Time	Source Node
52	Excessive missed AP Beacons	11/29 14:15:06	00:0C:41:0B:42:06
52	RF coverage compromised	11/29 14:18:45	00:0C:41:0B:42:06

Figure 3-4: AP signal level alarms

In addition to alarming on many performance compliance precursor event signatures, the AirMagnet Enterprise allows remote connection directly to the SmartEdge Sensor to observe the real-time network connectivity and traffic characteristics. Figure 3-5 shows a small sample of the information that can be viewed, a display of all the APs observed in the Sensor FOV, along with STA association, STA type and SSID information. This information can be used to instantly verify STA and user connectivity status and connection states.

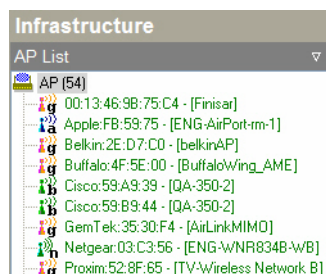


Figure 3-5: SmartEdge Sensor live remote WLAN monitoring

The largest “bang-for-the-buck” is clearly obtained by designing the AirMagnet SmartEdge Sensor network to achieve both the WIDS and proactive health and performance monitoring functions. A Type-A Sensor FOV design can often be achieved with a small, or in many cases, a zero percentage increase in the total number of SmartEdge Sensors.

Measurement Process Overview

The actual Sensor Measurement procedure varies according to the FOV type desired and the characteristics of the physical space and any WLAN in service. The overall procedure can be carried out in these steps:

- 1) Collect system design data.
- 2) Design WLAN monitoring network operating specifications/Sensor FOV types. Plan measurement process.
- 3) Perform Sensor FOV measurements.
- 4) Analyze measurement data.
- 5) Create SmartEdge Sensor network design: SmartEdge Sensor locations, wired network connectivity design.
- 6) Post-deployment verification.

Unauthorized Device Detection Measurements

It is essential to include measurements that validate the reliable detection condition. This is typically done by selecting a set of test locations for the reference AP (used to simulate an unauthorized device) for a given SmartEdge Sensor location and position. A test power-on duration ($T_{ON-Test}$) is then determined based on the value of T_{ON} . The number of beacon frames received by the SmartEdge Sensor, N_{Test} is then recorded during $T_{ON-Test}$. If it is greater than N_p , the threshold computed from the P value specified, then reliable detection is achieved at the given test location. The test locations are usually chosen around the perimeter of the desired total FOV.

Sample Design Results Review and Conclusion

Table 3-3 on the following page summarizes a set of actual SmartEdge Sensor Design measurements. Here are some observations:

- Across these real designs, the Sensor FOV Avg. area varies over more 2 orders of magnitude. This validates very strongly that SmartEdge Sensor density is highly dependent on the specific design requirements and physical characteristics of each application project.
- Greater than any other factor, SmartEdge Sensor density is most strongly affected by the physical structure of the desired area. Open areas or buildings with high ceilings generally require the lowest SmartEdge Sensor density. This is no surprise, as the same is true for AP density, and is a basic result of RF propagation science.
- No easy rule of thumb has been obtained for the required ratio of SmartEdge Sensor to APs in a given network.
- While it is sometimes possible to estimate the required number of SmartEdge Sensors from floor plans or quick walkabouts, performing a set of well planned measurements is the only reliable method of verifying that the number and locations of SmartEdge Sensors chosen will accurately provide the desired monitoring capabilities. The best estimating tool is a review of an existing design with comparable building structure and configuration and similar monitoring specifications. The numeric FOV distance and area specifications are provided as guidelines only, and are not a substitute for the measurement process.

Table 3-1: SmartEdge Sensor FOV Measurements Summary

Project Title	Interior Area (K sq. ft.)	Number Floors	Number APs	FOV Type	Number Sensors	Sensor FOV Avg. (K sq. ft.)	Notes
Office 1	120	9	32	B/C	20	6	Major corporate office tower; WLAN service deployed on Floors 2-9; very dense central core requires 2 Type A Sensors per floor; large open areas on ground floor with cafes, parking, 2 Type C Sensors deployed in these areas.
Office 2	95	1	16	B/C	3	47	This is a 3-story office complex. WLAN service deployed on the middle floor only. Two Type B Sensors used for the office area, 1 Type C Sensor for the adjacent parking areas and public lobby.
Distr. Ctr. 1	100	N/A	3	C	3	33	Regional distribution center with steel racking to within 4 feet of ceiling; narrow aisles, very dense product packing. Two Sensors used for the DC, 1 for the adjoining office space.
Plant 1	575	N/A	40	B	5	115	WLAN supports critical material transfer and manufacturing process applications. Small vehicle fabrication and assembly plant. High density heavy machinery and overhead conveyor lines; fairly open finishing areas with high ceilings.

Table 3-1: SmartEdge Sensor FOV Measurements Summary

Project Title	Interior Area (K sq. ft.)	Number Floors	Number APs	FOV Type	Number Sensors	Sensor FOV Avg. (K sq. ft.)	Notes
Plant 2	2,400	N/A	29	A	7	342	WLAN supports critical material transfer and manufacturing process applications. Large vehicle fabrication and assembly plant. High density heavy machinery and overhead conveyor lines; fairly open finishing areas with high ceilings.
Outside 1	N/A	N/A	N/A	C	1	1,154	Open outdoor area in a multi-building office campus. Sensors mounted on a roof corner, placed to optimize 270 degree FOV away from building edges.

For additional Enterprise deployment information, refer to [Appendix C, “Enterprise Deployment”](#).

Part II: AirMagnet Enterprise Console

Chapter 4: Enterprise Console Basics

Introduction

This chapter discusses the major portions of the AirMagnet Enterprise Console User Interface. The sections below help show the user various configuration and navigation options to help view the enterprise network most effectively.

Launching AirMagnet Enterprise Console

The AirMagnet Enterprise Console can be launched from any PC on which the software is installed.

To launch the AirMagnet Enterprise Console:

- 1) From your desktop, click **Start**, and select **All Programs>AirMagnet Enterprise Console>Console**. The AirMagnet Enterprise Console screen appears, with the Connect Server dialog box on top of it. See Figure 4-1.

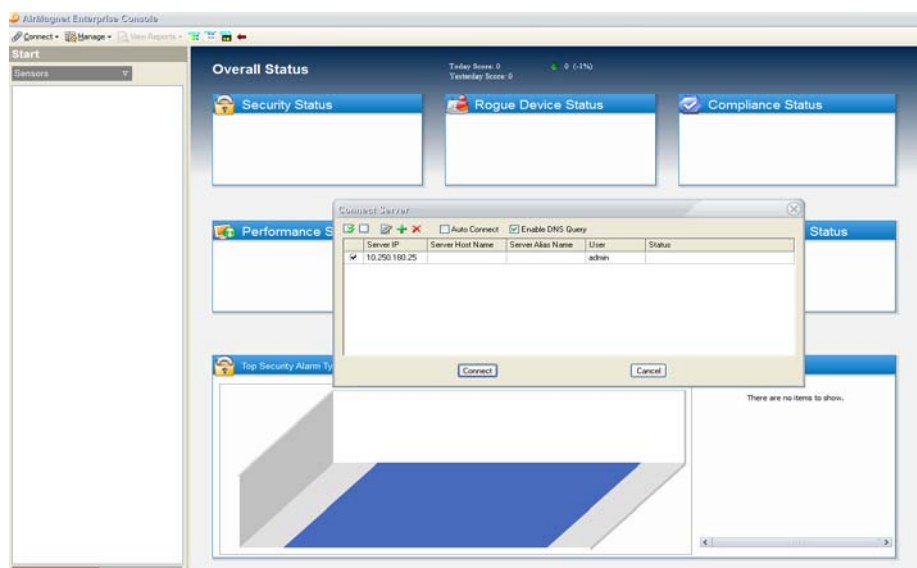


Figure 4-1: Connecting to AirMagnet Enterprise Server

- 2) Select an AirMagnet Enterprise Server, and click **Connect**. The AirMagnet Enterprise Console's Start screen appears once the Console-Server connection is established. See Figure 4-2.

If you have multiple AirMagnet Enterprise Servers installed, you can connect to any of them using the `Connect>Server...` command. For more information, see "Managing Console-Server Connection" on page 80.

Console UI Components

This section discusses the UI components that are common to all the major screens of the AirMagnet Enterprise Console. UI components that are specific to a certain screen will be discussed only in the chapter dedicated to that screen.

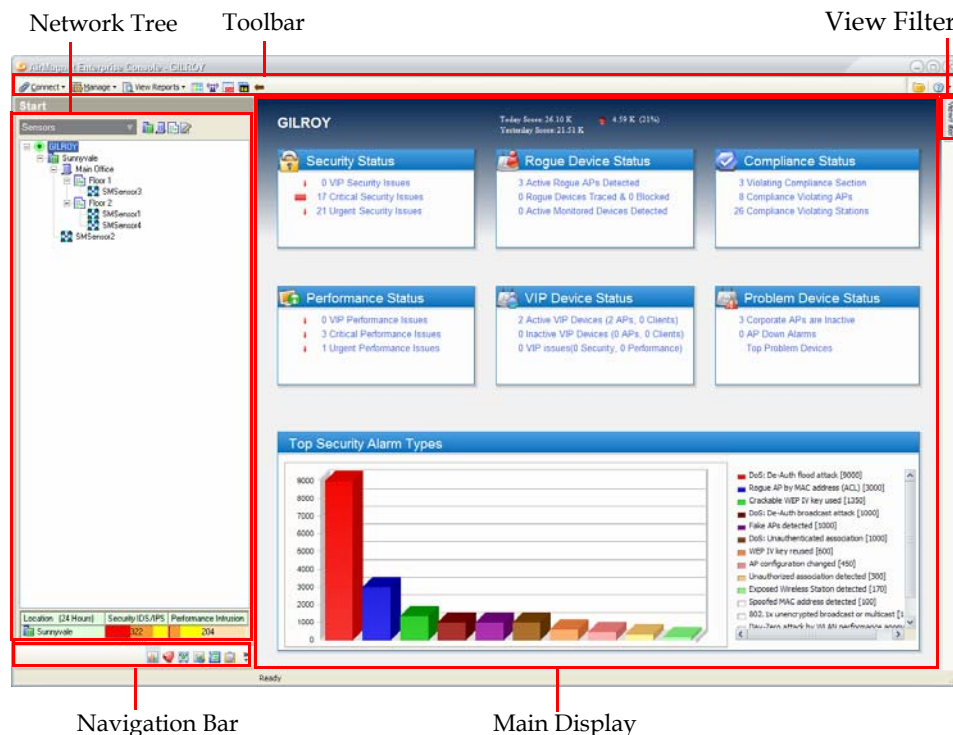


Figure 4-2: AirMagnet Enterprise Start screen (default)

As illustrated in Figure 4-2, the AirMagnet Enterprise Console UI can be divided into two main parts: the Network/Policy Tree on the left and the Data Display on the right. Across the top of the screen are a number of control buttons and menus. Located at the bottom right of the screen is the Navigation Bar with seven navigation buttons. The following sections highlight the functions of these major UI components.

Navigation Bar

The Navigation Bar allows the user to navigate to the various screens provided in AirMagnet Enterprise. Clicking on a button will open the corresponding screen.

The Navigation Bar can be viewed in either expanded or compact mode, depending on the requirements of the user. By default, the Console displays compact mode; to view it in expanded mode, drag the resizing bar (marked with a series of dots) above the buttons upwards until all the

buttons required are displayed. Each mode is shown in Figure 4-3.

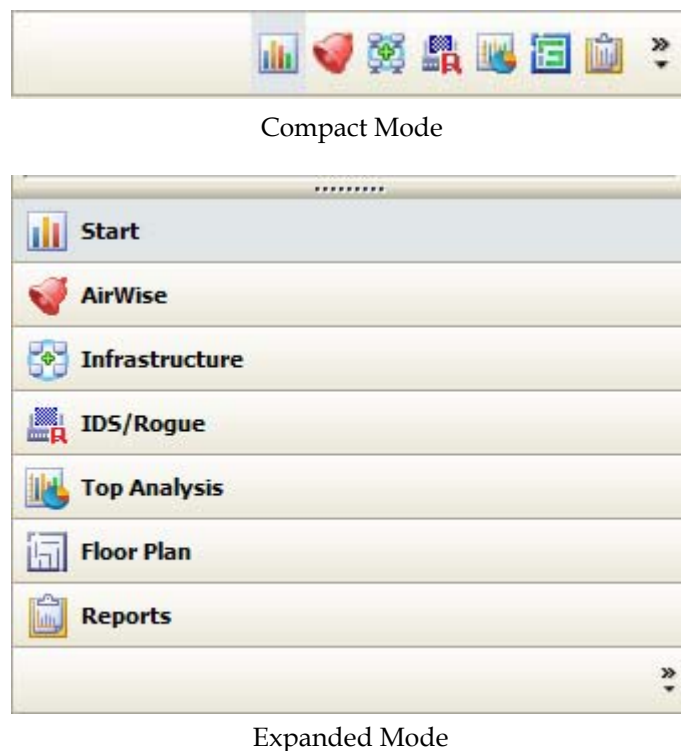


Figure 4-3: Navigation Bar Views

The following is a brief description of the functions of the navigation buttons and the screens associated with them.

- **Start**—brings up the Start screen (the default initial screen), where you can view the all components of your wireless network and a summary of security and performance alarms detected on the network. Here you can create or modify your Network Tree to organize your WLAN components and get a quick overview of your network status. For more information, see Chapter 5, “Using the Start Screen”.
- **AirWISE**—opens the AirWISE screen, where you can inspect policy compliance and network events in detail. The AirWISE expert analysis engine automatically identifies and alerts you on more than 130 security and performance issues based on the policy profile in use. (See Chapter 12, “Managing Policy Profiles”.) It also provides context-driven expert advice to help WLAN administrators quickly understand all the issues and events on their network. You can choose to view the information based on location or policy. For more information, see Chapter 6, “Using the AirWISE Screen”.
- **Infrastructure**—takes you to the Infrastructure screen, where you can have an in-depth look at all your wireless assets: APs, stations, and SSIDs. You can get detailed information on all these assets at any chosen location, e.g., who they are, where they

are, and how they are functioning. More importantly, you can select a specific policy and then drill down to find out who is violating the policy and where. Like the AirWISE screen, the Infrastructure screen also gives you the option to view the information based on location or policy. For more information, see Chapter 7, “Using the Infrastructure Screen”.

- **IDS/Rogue** – This view provides a quick summary of devices classified as Rogue and Unknown along with summaries of wired traced and blocked devices. It also enables quick access to rogue management configuration dialogs.
- **Top Analysis** – takes you to the Top Analysis screen, where you can view and analyze your network data using charts. The charts can be based on data about the security and performance alarms, wireless devices, and regulatory compliance status of your network. Like the AirWISE and Infrastructure screens, the Top Analysis screen also allows you to view information based on location or policy. For more information, see Chapter 9, “Viewing Top Analyses”.
- **Floor Plan** – allows you to access the Device Locator feature. Users can add a floor plan image for the enterprise network and Enterprise will automatically place each detected device at the appropriate location on the image. This feature requires that users distribute sensors at the boundaries of the floor in order to properly detect devices within the sensor grid.
- **Reports** – allows you to access various device and compliance reports to view the current and past status of the network. For more information, see Chapter 11, “Using the Reports Screen”.

Network Tree

The Network Tree displays the various buildings, floors, and sensors contained in the enterprise network. Users can organize these objects into a tree structure, making it easy to determine where sensors (and therefore, devices) are located. Selecting a specific portion of the tree will cause the console to display information pertaining only to that area; in other words, selecting a floor will display data detected by sensors located on that same floor. To view data regarding the entire network, simply select the root of the enterprise server, which is located at the root of the tree.

Server Status Indicator

The color of the icon next to the AirMagnet Enterprise Server name (or IP address) at the top of the Network Tree indicates the health status of the AirMagnet Enterprise Server:

- **Green** – The Server is in normal working condition.
- **Red dot inside a green circle** – The Server is experiencing a database problem.
- **Red** – The Server is down.

Figure 4-4 shows that AirMagnet Enterprise Server GILROY is in perfect operating status, as indicated by the green dot.

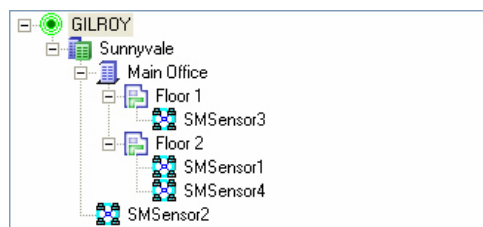


Figure 4-4: The Enterprise Server in good working condition

Figure 4-5 shows that Enterprise Server GILROY is down, as indicated by the red dot.

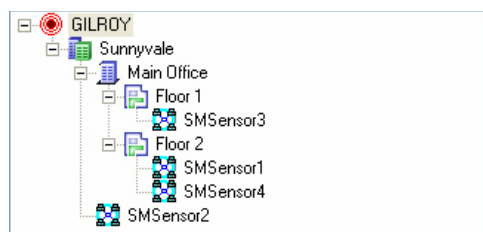


Figure 4-5: The Enterprise Server down

Sensor Filter

The sensor filter drop-down located above the Network Tree provides four options for displaying information of the AirMagnet SmartEdge Sensors, as shown in Figure 4-6.



Figure 4-6: Sensor filters

- **Sensors [Grade]** – shows the health status of the sensors as indicated by letters A to F, with A being the best (healthiest) and F the worst.
- **Sensors [Policy Profile]** – shows the WLAN policy profiles the sensors are using. If a manufacturer-preconfigured policy profile is in use, the name of the policy will always be marked as “Default”.
- **Sensors [Alarm Severity]** – shows the number of alarms detected at each of the four severity levels, which are, from left to right, Critical, Urgent, Warning, and Informational.
- **Sensors** – shows the names of the sensors only.

Network Building Tools

Figure 4-7 illustrates the tools used to construct a WLAN network tree. These buttons are located directly above the Network Tree structure.

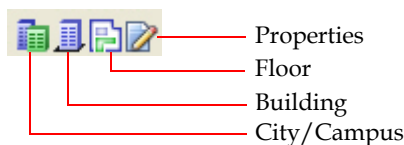






Figure 4-7: Network tree building tools

- **City/Campus**—adds cities or campuses to the network tree.
- **Building**—adds buildings to cities or campuses in the network tree.
- **Floor**—adds floors to buildings in the network tree.
- **Properties**—displays the information about the selected entry in the network tree.

The network building tools, i.e.,  (**City/Campus**),  (**Building**), and  (**Floor**), represent different levels of the network hierarchy. They are intended to make it easier for creating a layered network structure. When constructing your network tree, you can create a nesting structure by adding cities below a city and, buildings below a city, and floors below a building, and then drag and drop Sensors under any of these components. For instructions on how to use these tools, see “Setting Up a Network Tree” on page 79.

To view the properties of an entry in the network tree, simply highlight it and then click the  (**Properties**) button. A window will pop up, showing some basic information about the selected entry. Depending on the entry you select, the information shown in the window may be different. Figure 4-8 shows the properties window for the AirMagnet Enterprise Server.

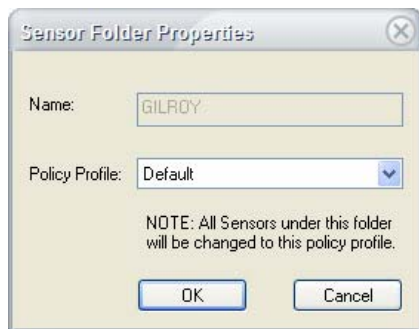



Figure 4-8: Properties window for AirMagnet Enterprise Server

The Properties Window above shows the name and the network policy profile of the AirMagnet Enterprise Server. Although you cannot change the name of the Server from within AirMagnet Enterprise, you can modify its policy profile by clicking the down arrow and selecting a different policy profile from the list menu.

If a Sensor is selected from the network tree, clicking the  (**Properties**) button will bring up the Sensor Properties window where you can view and modify certain properties of the Sensor. See Figure 4-9.

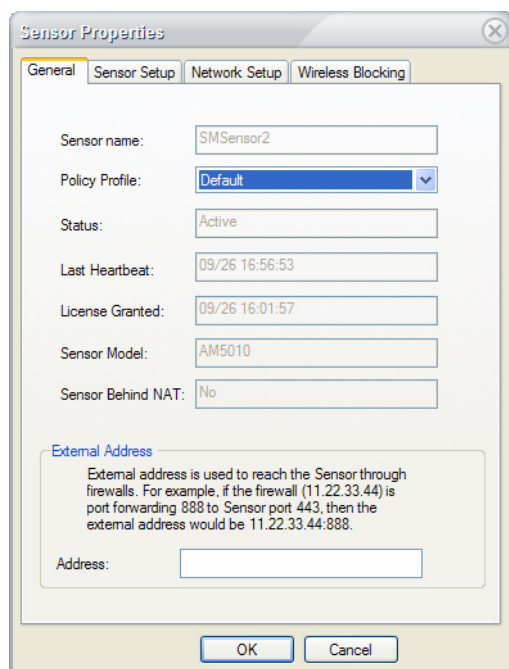


Figure 4-9: Viewing the properties of a Sensor

Enabling 802.11n Support

Users who have purchased 802.11n-enabled sensors with their corresponding licenses must configure the new sensors to activate the 802.11n features.

To enable 802.11n support on a sensor:

- 1) From the Start screen, right-click the desired sensor in the Network Tree.
- 2) Select Grant N-license. A '[n]' appears at the end of the sensor name, indicating the new support.
- 3) Repeat Steps 1 through 2 for all additional sensors desired.

To view a list of all sensors that currently have 802.11n support, click Manage>Sensors... and assess the NLicense column.

Connect Menu

The Connect Menu allows the user to remotely connect to devices that are not located on the current enterprise network. See Figure 4-10.

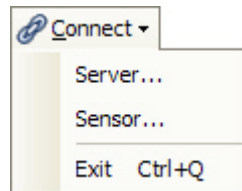


Figure 4-10: Connect Menu

- **Server**—Opens the Connect Server dialog box, which allows the user to connect to a different server. This box is automatically shown when the console is launched.
- **Sensor**—Opens the Connect Sensor dialog box, which allows the user to remotely connect to a sensor that is not in the current tree. If successfully connected, the sensor's Remote Analyzer window appears.
- **Exit**—Exits the enterprise console.

Manage Menu

The Manage drop-down contains access to the bulk of AirMagnet Enterprise's configuration controls. See Figure 4-11.

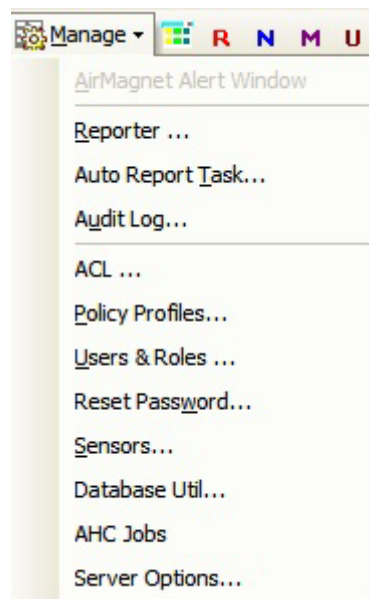



Figure 4-11: Manage Menu Options

The table below describes each option in detail.

Table 4-1: Manage Menu Options

Option	Description
AirMagnet Alert Window	Allows you to show or hide a floating screen that displays real-time network data such as the latest alerts from selected sensors, Sensor statistics, rogue device statistics, and device statistics. <i>This option is only available when viewing the Classic Start screen.</i>
Reporter...	Opens the Reports screen, where you can view all the pre-defined report books and create your own custom report books. See Chapter 11, “Using the Reports Screen” for more details.
Auto Report Task...	Allows the user to create a task that will automatically generate a specified report book and email it to the desired users. For more information, see “Scheduling a New Auto Report Task” on page 219.
Audit Log...	Opens the AirMagnet Audit Log screen, where you can view records of a variety of activities and events that have happened on your network system.
ACL Groups...	Opens the ACL Group Management dialog box, where you can manage ACL groups.
Policy Profiles...	Allows you to create new security and performance policy profiles and assign them to various locations of your WLAN. It also lets you modify or remove existing policy profiles. For more information on how to create and assign policies, see Chapter 12, “Managing Policy Profiles.”
Users and Roles...	Allows you to add new users to the AirMagnet Enterprise Console and assign specific roles to them. For more information, see “User Roles and Privileges” on page 93.
Reset Password...	Allows the user to change the password for the current user account.
Sensors...	Opens the Manage Sensors screen where you can view various data about the Sensors which are connected with the AirMagnet Enterprise Server.
Database Util...	Opens the Database Utilities dialog box, where you can manage the system’s database. Note: Not supported for Oracle.
AHC Jobs	Opens the AHC Jobs dialog where you can manage Automated Health Check jobs.
Server Options...	Allows you to set or change the configuration settings of your AirMagnet Enterprise Server and Console. See Chapter 13, “Configuring System Settings.”

View Reports

The  **View Reports** button provides direct access to the integrated AirMagnet Enterprise Reports. To open the Reports screen, simply click this button and select a report option from the list menu. See Figure 4-12.

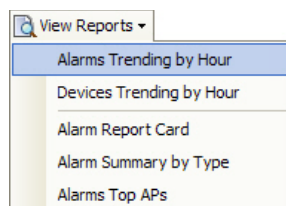


Figure 4-12: Selecting a report option

The contents of the View Report list menu vary depending on the screen you are on. Figure 4-12 shows the report options that are available for the Start screen.

The Toolbar

AirMagnet Enterprise's toolbar is located at the top of each screen and contains various tools to help navigate through the console interface. The tools within the toolbar vary from screen to screen, and therefore screen-specific tools will be discussed in the individual screen chapters later in this book. This section details the tool buttons that are available to (nearly) every screen. See Figure 4-13.



Figure 4-13: Common Screen Tools

Table 4-2 describes the functions of each button in the common toolbar.

Table 4-2: Common Screen Tools






Tool	Description
 (Full Screen)	The Full Screen toggle allows the user to show or hide the Network Tree portion of the screen.
 (AP Grouping)	The Enable/Disable AP Grouping button allows the user to easily enable or disable AP groups within the Enterprise Console.
 (Back)	The Back button returns the user to the last screen visited.
Find in this View	This field allows the user to search for specific text within the current screen. This is most particularly useful for finding devices on the Infrastructure screen, as the text entered can be an IP, MAC Address, SSID, or AP Group.

Table 4-2: Common Screen Tools

Tool	Description
 (Bubble Help)	Click this button to activate the Enterprise Console's built-in help pop-ups. These bubbles provide additional details about any object the mouse is hovered over.
 (Help)	The Help button provides access to Enterprise's online help interface. See the next section for more details.

Help Menu

The Help menu has several options:

- **About**—opens the About AirMagnet Enterprise Console screen which shows the version and build number of the AirMagnet Enterprise Console you are using.
- **Contents**—opens AirMagnet Enterprise Console's online help.
- **User Guide**—opens this User Guide.
- **Policy Reference Guide**—opens AirMagnet Enterprise's Policy Reference Guide.
- **Check Update**—Checks for updated software versions.

Using the View Filter

The View Filter located in the upper right-hand corner of the Enterprise Console user interface is available on all major screens of the application. It provides a number of easy-to-use options for filtering data to be displayed on the screen.

To apply View Filter options:

- 1) Mouse over or click the View Filter tab in the upper right-hand corner of the screen. The View Filter pane expands onto the left-hand side of the screen. See Figure 4-14.

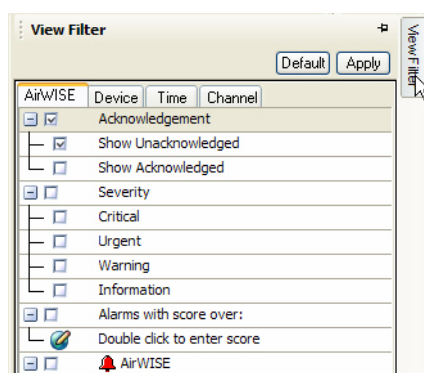


Figure 4-14: Accessing the View Filter Options

- 2) If desired, click the pushpin button to “pin” the View Filter to the Console interface. This forces the View Filter tab to remain open even when the mouse is not actively hovering over it.

- 3) Use the View Filter tabs to access the type of filter desired. By default, the AirWISE tab is selected.
- 4) Check the boxes for the types of data to filter on. Note that users can select multiple options, even spanning across different tabs. For example, to view Urgent alarms generated by APs in the last 30 minutes, the user can check the corresponding boxes in the AirWISE, Device, and Time tabs.
- 5) A new type of filter “Custom dates” has been added where the user can specify an exact time to filter. Users may also Filter by MAC, entering a partial MAC address and Filter by SSID, entering a partial SSID, and the values are not case sensitive.

Example: Filter by MAC

- 1) Select device tag in View Filter.
- 2) Check Filter by MAC
- 3) Under Filter by MAC, double click to enter MAC. You can enter a partial MAC address e.g. 00:0f and it is not case sensitive. See Figure 4-15 for reference.
- 4) Click Apply.

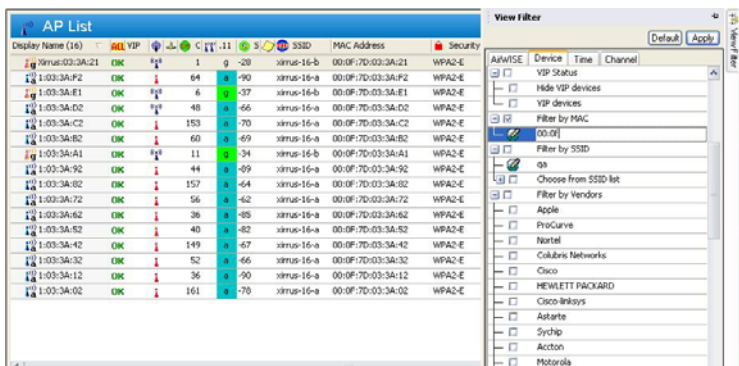


Figure 4-15: Filter by MAC

Example: Filter by SSID

- 1) Select device tag in View Filter.
- 2) Check Filter by SSID.
- 3) Under Filter by SSID, double click to enter SSID. You can enter a partial SSID e.g. cisco, and it is not case sensitive. See Figure 4-16 for reference.
- 4) Uncheck “Choose from SSID list”.
- 5) Click Apply.

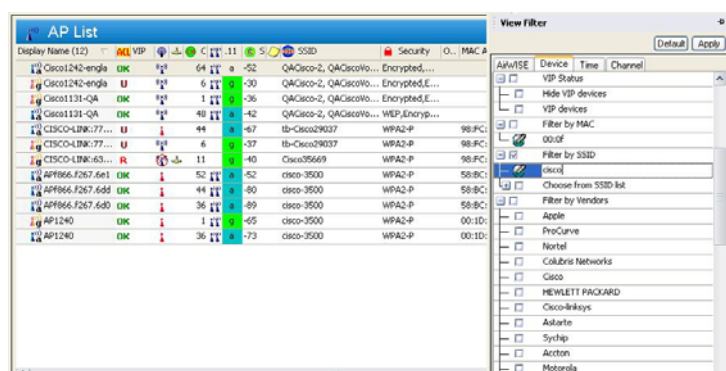


Figure 4-16: Filter by SSID

If nothing is checked in the View Filter options, the filter acts in the same manner as if all options were checked. That is, all data is displayed.

- 6) Click Apply to apply the filter to the current Console session. If desired, click the pushpin button again to unlock the tab. It will vanish as soon as the mouse is clicked anywhere else in the Enterprise Console.

An easy way to clear any custom View Filters currently applied is to use the Default button on the View Filter tab.

Setting Up a Network Tree

This section discusses how to create a network tree that reflects the structure of your WLAN from the AirMagnet Enterprise Console.

When you launch the AirMagnet Enterprise Console for the first time after system installation, all the AirMagnet SmartEdge Sensors on your WLAN will appear under the Enterprise Server on the left-hand side of the Start screen, as shown in Figure 4-17.

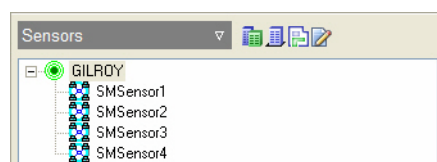





Figure 4-17: An unconfigured network tree

In order to manage your WLAN using the AirMagnet Enterprise Console, you need to organize your network components using the network building tools, and then drag and drop the Sensors to where they virtually belong on the network.

The following procedures are intended to help set up your network tree.

To set up a network tree:

- 1) Click the  **(City/Campus)** button. A “New City” appears under the sensors.
- 2) Click the  **(Building)** button. A “New Building” appears.
- 3) Click the  **(Floor)** button. A “New Floor” appears.
- 4) Organize your network structure by dragging and dropping the New Building, New City, and the New Floor to their respective locations.
- 5) Right-click the New City, New Building, and New Floor and rename them one by one.
- 6) Drag and drop the Sensors to their respective locations.

You can modify your network structure at any time using the same way. Figure 4-18 is a sample network tree setup.

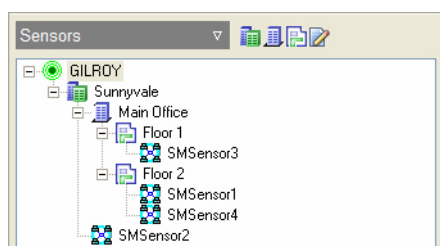


Figure 4-18: A sample network tree

Managing Console-Server Connection

A single AirMagnet Enterprise Console can support multiple AirMagnet Enterprise Servers. Each Server is identified by its name or IP address in the network tree on the left-hand side of the AirMagnet Enterprise Server UI.

The **Connect>Server...** menu provides an effective means for managing the connection between the AirMagnet Enterprise Console and the AirMagnet Enterprise Servers. It opens the Connect Server dialog box (Figure 4-17) that contains a table showing the information of all AirMagnet Enterprise Servers you have entered. You can choose to connect to any AirMagnet Enterprise Server as long as you provide valid login information (i.e., server name or IP address, user name, and password). You can also add servers to or remove them from the table as needed.

Adding AirMagnet Enterprise Servers to the Console

To add an AirMagnet Enterprise Server to the Enterprise Console:

- 1) Select **Connect> Server....** The Connect Server screen appears. See Figure 4-19.

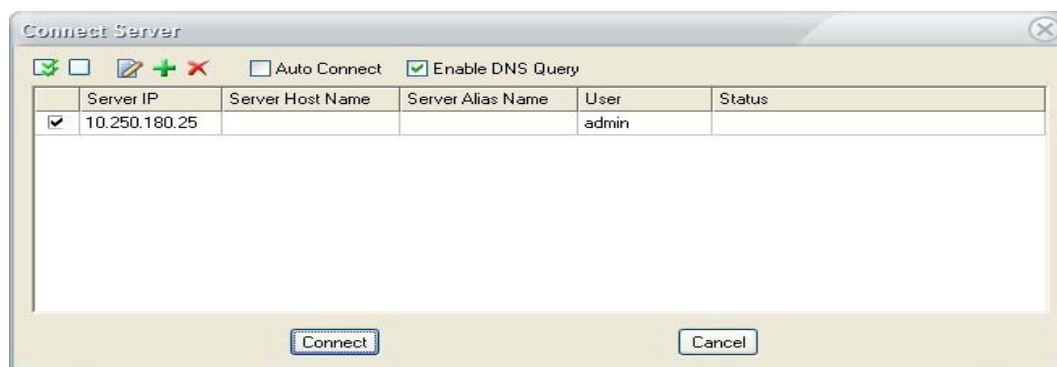


Figure 4-19: Connect Server screen

The Auto Connect option in Figure 4-17 allows the user to automatically connect to the selected server any time the Console is launched. The user can connect to a different server by using the Connect menu, if needed.

- 2) Click **+** (Add Server). The Server Logon Details dialog box appears. See Figure 4-20.



Figure 4-20: Server Logon Details screen

- 3) Make the entries as described in Table 4-3.

Table 4-3: Enterprise Server Login Settings

Parameter	Description
Server	Enter the name or IP address of the AirMagnet Enterprise Server.

Table 4-3: Enterprise Server Login Settings

Parameter	Description
Server Alias Name	If desired, give the server a name. This is not the same as the server host name (DNS query).
User Name	Enter your user name.
Password	Enter your password. Check “Remember Password” to automatically populate the password when connecting to this server IP.


- 4) Click **OK**. The newly added AirMagnet Enterprise Server will appear on the Connect Server dialog box. Refer to Figure 4-17.

*To connect to the newly added server, select it from the Connect Server dialog box, and click **Connect**. If the connection is successful, the Server will appear in the network tree section on the left-hand side of the AirMagnet Enterprise Console UI.*

Removing Servers from the Console

You can remove an AirMagnet Enterprise Server from the Enterprise Console if the Server is no longer in service.

To remove an Server from the Console:


- 1) From the Connect Server dialog box (Figure 4-15), highlight the Server.
- 2) Click  (**Delete Server**). The entry will be removed from the dialog box.

*If the Enterprise Console is already connected to an Server at the time when it is deleted from the Connect Server dialog box, the connection will remain until you click the **Connect** button in the Connect Server dialog box. The deleted server will disappear from the network tree once the system refreshes.*

Changing Server Login Settings

You may need to change server login settings from the Connect Server dialog box if you want to connect to a different server, or to connect to the same server but as a different user (or even in a different role). Whatever the case, you need to provide valid information (i.e., server name or IP address, user name, and password) in the Connect Server dialog box in order to establish a new connection.

To change Server login settings:

- 1) From the Connect Server dialog box (Figure 4-17), highlight the server, and click  (**Edit Server**). The Server Login Details dialog box appears. See Figure 4-21.

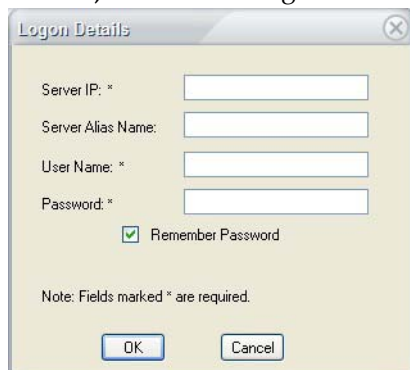


Figure 4-21: Changing Server login information

- 2) Make the desired changes in the Server, User Name, and/or Password fields.
- 3) Click **OK**. The changes will appear in the Connect Server dialog box (Figure 4-17).

Connecting to AirMagnet SmartEdge Sensors

Connecting to an AirMagnet SmartEdge Sensor allows you to launch the AirMagnet Remote Analyzer so that you can conduct detailed data analysis by drilling down to the specifics captured by the SmartEdge Sensor.

To connect to an AirMagnet SmartEdge Sensor:

- 1) Click **Connect> Sensor....** The Connect Sensor dialog box appears. See Figure 4-22

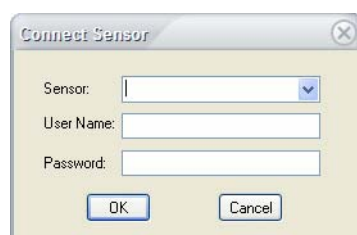


Figure 4-22: Connect Sensor screen

- 2) Make the selection and/or entries as described in Table 4-4.

Table 4-4: Connect Server Parameters

Option	Description
Sensor	Click the down arrow and select a Sensor (name or IP address) from the drop-down list.
User Name	Enter your user name for the sensor.

Table 4-4: Connect Server Parameters

Option	Description
Password	Enter your password for the sensor.

- 3) Click **OK**. This will launch the AirMagnet Remote Analyzer of the selected SmartEdge Sensor. See Chapter 15, “Introducing Remote Analyzer” for more information.

Exiting AirMagnet Enterprise Console

For security reasons, it is recommended that you log out of the AirMagnet Enterprise Console after each management session.

To log out of the AirMagnet Enterprise Console:

- 1) Click **Connect>Exit**. This will let you log out of the AirMagnet Enterprise Console securely.

Accessing Network Audit Log

AirMagnet Enterprise’s Audit Log automatically records more than a dozen major activities and events that could happen on the enterprise network, allowing network administrators and security officers to effectively track and monitor the security and usage status of the network. It is a feature that helps enterprise networks comply with a series of government regulations on network security and safeguard the integrity of their networks.

To view the Audit Log:

- 1) Click **Manage>Audit Log....** The AirMagnet Audit Log screen appears. See Figure 4-23.

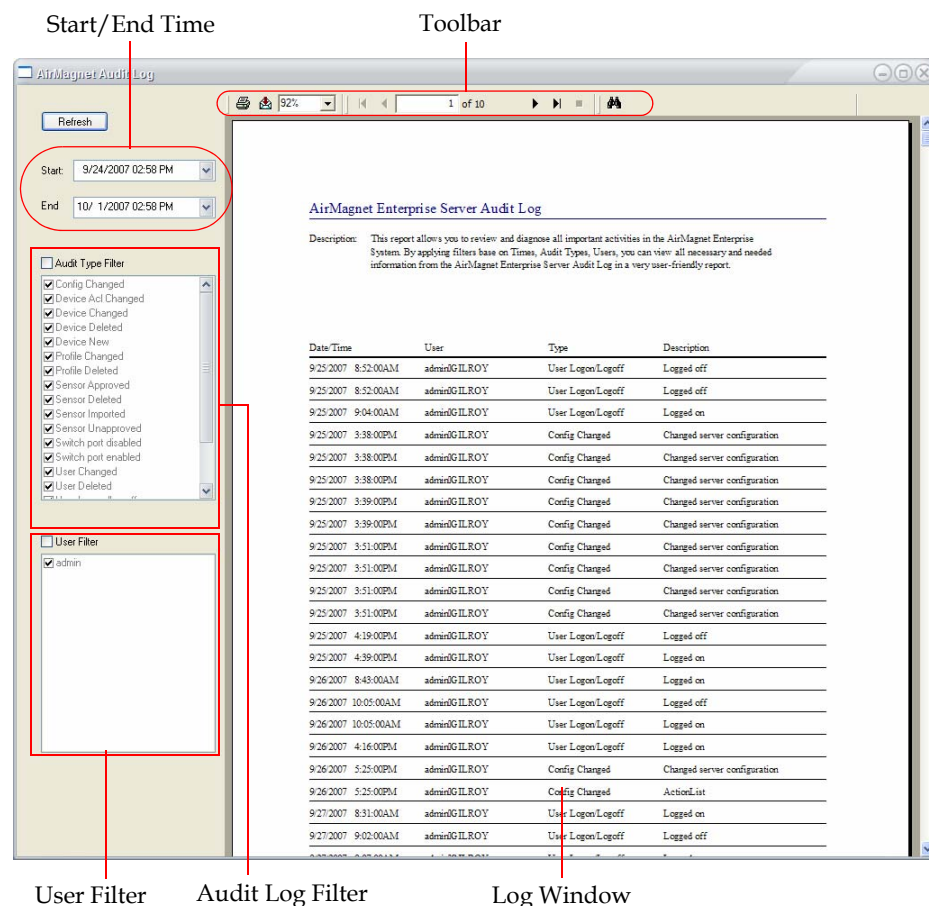


Figure 4-23: AirMagnet Audit Log screen

Audit Log Screen Components

As seen from Figure 4-21, the AirMagnet Audit Log screen has the following components:

- **Refresh Button**—allows you to update the content in the log window.
- **Start (Time)**—allows you to select the starting date and time of the logs you want to display.
- **End (Time)**—allows you to set the ending date and time of the logs.
- **Audit Type Filter**—contains all types of logs AirMagnet Enterprise has generated.
- **User Filter**—contains all types of users of the AirMagnet Enterprise on the network.
- **Toolbar**—contains tools for viewing, printing, and exporting logs.
- **Log Window**—displays the currently selected log.

Customizing an Audit Log

By default, the AirMagnet Audit Log screen displays all types of audit logs that the system has generated in the past seven days, relating to all users of the Console. However, you can customize the log display using the controls on the AirMagnet Audit Log screen.


To customize the display of audit logs:

- 1) From the AirMagnet Audit Log screen, click the **Start** and **End** down arrows to set the starting and ending date and time of the logs.
- 2) Check the **Audit Type Filter** check box and uncheck the types of logs that you want to exclude.
- 3) Check the **User Filter** check box and uncheck the users that you want to exclude.
- 4) Click the button. The changes you have made will be reflected in the log window once the screen refreshes.

Printing an Audit Log

You can print the logs that are displayed in the log window directly from the AirMagnet Audit Log screen so that you can share and back up the log files using a hard copy.

To print the audit logs displayed on the screen:

- 1) From the AirMagnet Audit Log screen, click  (Print Log) button. The Print dialog box appears. See Figure 4-24.

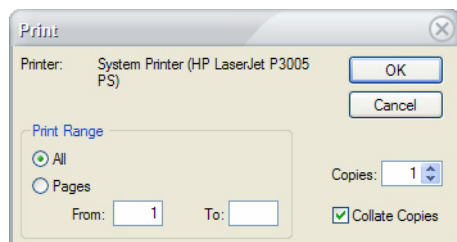



Figure 4-24: Printing an audit log

- 2) Make the required selection from the screen, and click **OK**.

Exporting an Audit Log

AirMagnet Enterprise Console provides a built-in file export utility that allows the users to export audit logs directly from the Audit Log screen.

To export audit logs:

- 1) From the AirMagnet Audit Log screen, click the  (Export Log) button. The Export dialog box appears. See Figure 4-25.

**Figure 4-25: Exporting audit logs**

- 2) Click the upper down arrow and select a file format from the drop-down list.
- 3) Click the lower down arrow and select an appropriate export destination of the log.

Each of the log export destinations may open a different dialog box that may require a different procedure for the user to specify the designating information. Make sure that the option you select is applicable to your network.

- 4) Click OK.

Managing ACL Groups

An Access Control List, or ACL, provides an easy way for network administrators to effectively manage the security of their networks. With this feature, users can create and manage/group their networks' ACLs from the AirMagnet Enterprise Console using the ACL Groups Management dialog box, where the user can create or delete ACLs and add devices to or delete them from a selected ACL group.

Creating ACL Groups

In order to manage your wireless network assets using the ACL concept, you must create ACL groups so that you can assign devices to the appropriate ACL groups where they belong.

To Create ACL groups:

- 1) From the AirMagnet Enterprise Console screen, click **Manage>ACL....** The Manage ACL Groups dialog box appears. See Figure 4-26.

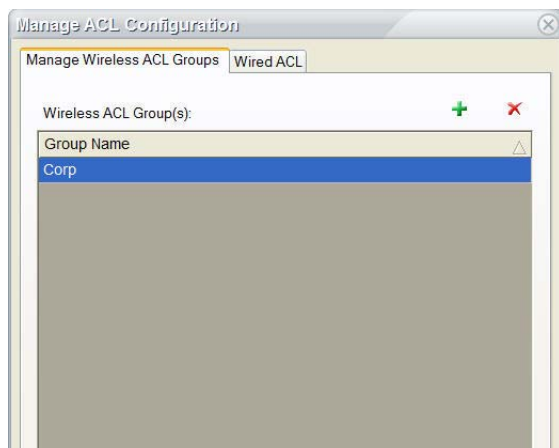


Figure 4-26: The Manage ACL Groups dialog box

- 2) Click **+** (Add ACL Group). An entry marked “New Group” appears in the dialog box.
- 3) Highlight the “New Group” entry and type a unique name over it.
- 4) Repeat Steps 2 through 3 to create as many ACL groups as applicable. See Figure 4-27.

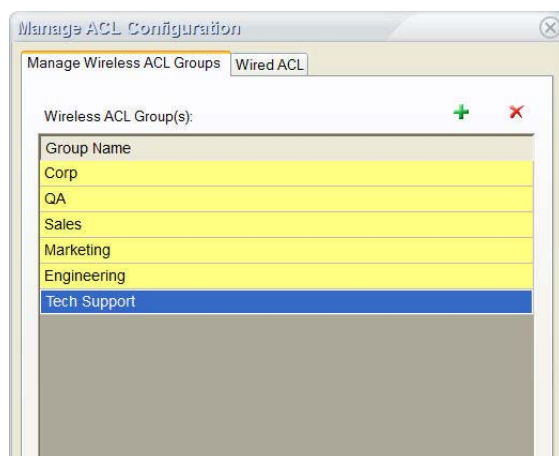



Figure 4-27: Newly created ACL groups

- 5) Click **OK** when completed.

Deleting ACL Groups

As your network evolves, some of the ACL groups you have created in the past may become obsolete as time passes. In that case, you may want to remove those ACL groups that are no longer applicable.

To delete an ACL group:

- 1) From the Manage ACL Groups dialog box, highlight the ACL group to be removed and click  **(Delete ACL Group)**.
- 2) Repeat Step 1 to remove any other ACL groups, if applicable.
- 3) Click **OK** when completed.

Wired ACL

AirMagnet Enterprise monitors the network for unauthorized AP's plugged into the wired network. When you enable configure the alarm "Rogue AP Traced Using Passive Detection" in the policy profile, AirMagnet Enterprise detects that an unauthorized AP has been plugged into the corporate wired network, you will be alerted of this threat so that as a Network Administrator you can take appropriate action against this unauthorized Access Point. If this wireless device is indeed authorized, you may add it the wired MAC address of the device to Wired ACL list.

To add a wired MAC address:

- 1) From the AirMagnet Enterprise Console screen, click Manage>ACL.... The manage ACL groups dialog box appears.
- 2) Click Wired ACL tag.
- 3) Click + to add wired MAC address using the format xx:xx:xx:xx:xx:xx
- 4) Repeat step 3 if you need to add as many as applicable.



Figure 4-28: Wired ACL screen configure

Assigning Devices to ACL Groups

Once ACL groups have been created, you can organize your wireless network devices simply by assigning them to the appropriate ACL groups where they belong. This can be done from AirMagnet Enterprise Console's Infrastructure screen.

To assign devices to ACL groups:

- 1) From the AirMagnet Enterprise Console's Infrastructure screen, highlight the device or devices of interest and then right-click it or them. A pop-up menu appears. See Figure 4-29.

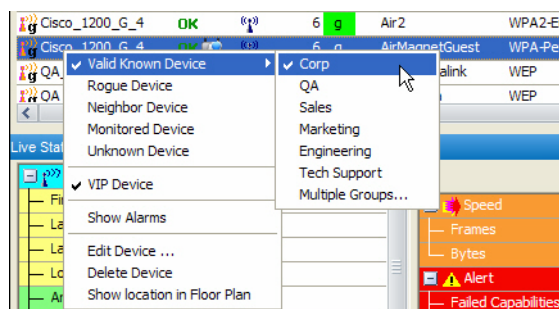


Figure 4-29: Assigning devices to ACL groups

- 2) From the pop-up menu, select **Valid Known Device** and then select an option from the ACL pop-up list. You may also assign it to multiple ACL groups by selecting the last option.

Once assigned to an ACL group, the ACL status of those devices originally marked with a "U" (Unknown) will change to "OK", meaning that they are now valid known devices on the network.

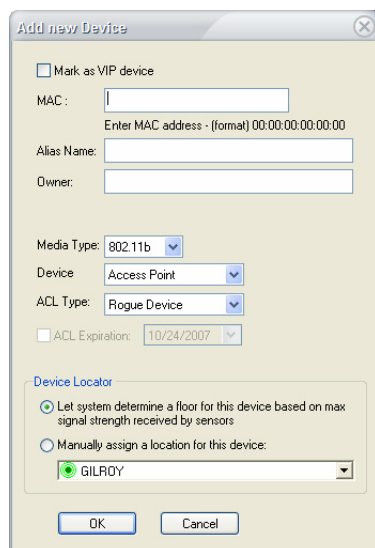
If a device belongs to multiple different areas, you can assign it to multiple ACL groups. Simply select the "Multiple Groups..." option when assigning the device to a group and check the areas it belongs to.

Adding Devices to Your AirMagnet Enterprise System

From time to time, new wireless devices may be added to your network. In order to effectively manage those newly added devices using the ACL group concept, you must first add those devices onto your AirMagnet Enterprise system and then assign them to the appropriate ACL groups using the procedures mentioned in the previous section.

To add new devices to your AirMagnet Enterprise system:

- 1) From the Infrastructure screen, click  (Add New Device). The Add New Device dialog box appears. See Figure 4-30.



The 'Add new Device' dialog box contains the following fields and options:

- ☐ Mark as VIP device
- MAC: (Placeholder: Enter MAC address - (format) 00:00:00:00:00:00)
- Alias Name:
- Owner:
- Media Type:
- Device:
- ACL Type:
- ☐ ACL Expiration:
- Device Locator**
 - ☒ Let system determine a floor for this device based on max signal strength received by sensors
 - ☐ Manually assign a location for this device:
- Buttons: OK, Cancel

Figure 4-30: Adding devices to AirMagnet Enterprise system

- 2) Make the following entries as described in Table 4-5.

Table 4-5: Adding Devices

Option	Description
MAC	The device's MAC address.
Alias Name	The device's alias, if applicable.
Owner	The owner or user of the device.
Media Type	The device's media type (802.11a, b, g, a/b, or a/g).
Device	The type of device selected (AP, Station, or Ad-Hoc).
ACL Type	The device's ACL status (Valid, Rogue, Neighbor, Monitored, or Unknown).
ACL Expiration	This option is available only for devices in the Valid Known Device category. In that case, you may check the check box and specify an expiration time for the device's Valid Known Device status. AirMagnet will treat such devices as rogue devices once their "Valid Known Device" status expires. This feature is very useful for managing devices used by visitors to your organization who may need to access your wireless network for a certain period of time.

Table 4-5: Adding Devices

Option	Description
Device Locator	<ul style="list-style-type: none"> • Let system determine a floor for this device based on max signal strength received by sensors—If selected, in situations in which the device is detected by sensors deployed on different floors, the AirMagnet Enterprise Server will automatically assign the device to the floor where sensors detect the strongest signal strength from it. • Manually assign a location for this device—If selected, you can manually assign the device to a floor of your choice in case it is detected by sensors from different floors.

3) Click **OK** when completed.

Once a device is added to your AirMagnet Enterprise system, you can then assign it to the appropriate ACL group using the procedures discussed in the previous section.

AirMagnet Enterprise Console User Management

Each AirMagnet Enterprise Console can be used by multiple users. Each user can have her or his own user name and password assigned by the network administrator, who can also assign different roles and privileges to different users and make such changes at any time. This not only helps delegate network management responsibilities but also protects the integrity of your network.

You can add or remove users, and assign or modify their roles and privileges using the **Manage>Users & Roles...** menu on the AirMagnet Enterprise Console screen.

Notes: Only 1000 objects can be queried in Active Directory at a time.

User Roles and Privileges

There are three kinds of users: Administrators, Power User, and Basic User. Table 4-6 illustrates their roles and privileges.

Table 4-6: AirMagnet Enterprise Console User Roles & Privileges

Privileges	User Role		
	Administrator (WLAN Administrators)	Power User (Engineers)	Basic User (Technicians)
Manage Policy Profiles	x		
Manage Users and Roles	x		
Manage Sensor Tree	x		
Manage Location	x		
Manage Server Configuration	x		
Manage Sensor (Including Shared Secret Key)	x		
ACL Export and Import	x		
Enterprise Server Web Logon	x		
Sensor Web Page Configuration	x		
Acknowledge Alarms	x		
Database Utilities	x		
Manage Location Services	x		
Delete Forensic Files	x		
Configure Compliance Report	x		
Configure Report Book	x		
Manage ACL	x	x	
Remote Analyzer Tools	x	x	
Disable Switch Port	x	x	
Wireless Block	x	x	
Open Remote Analyzer	x	x	x
Remote Analyzer Decodes	x	x	x
Remember password on login	x	x	x

Table 4-6: AirMagnet Enterprise Console User Roles & Privileges

Privileges	User Role		
	Administrator (WLAN Administrators)	Power User (Engineers)	Basic User (Technicians)
Display Security Policies and Events	x	x	x
Display Performance Policies and Events	x	x	x
User can Change Password	x	x	x
View Scheduled Auto Report Task	x	x	x
View Report	x	x	x
Manage AHC Job	x		

Adding Users to AirMagnet Enterprise Console

Network administrators can add new users to the Console at any time as needed. This can be easily done using the Manage menu.

To add a user to AirMagnet Enterprise Console:

- 1) Click **Manage>Users & Roles....** The Manage Users and Roles dialog box appears. See Figure 4-31.

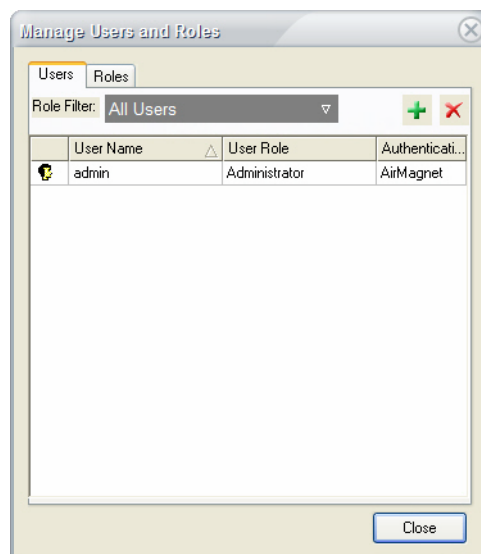


Figure 4-31: Manage Users and Roles dialog box

Each AirMagnet Enterprise Console comes with a default “admin” user account with the Administrator role. This account is empowered with all the privileges the system allows for and, therefore, should be handled by a person with the highest level of management responsibility of the network. No change is allowed for this account.

- 2) Click  (New User). The New User screen appears. See Figure 4-32.

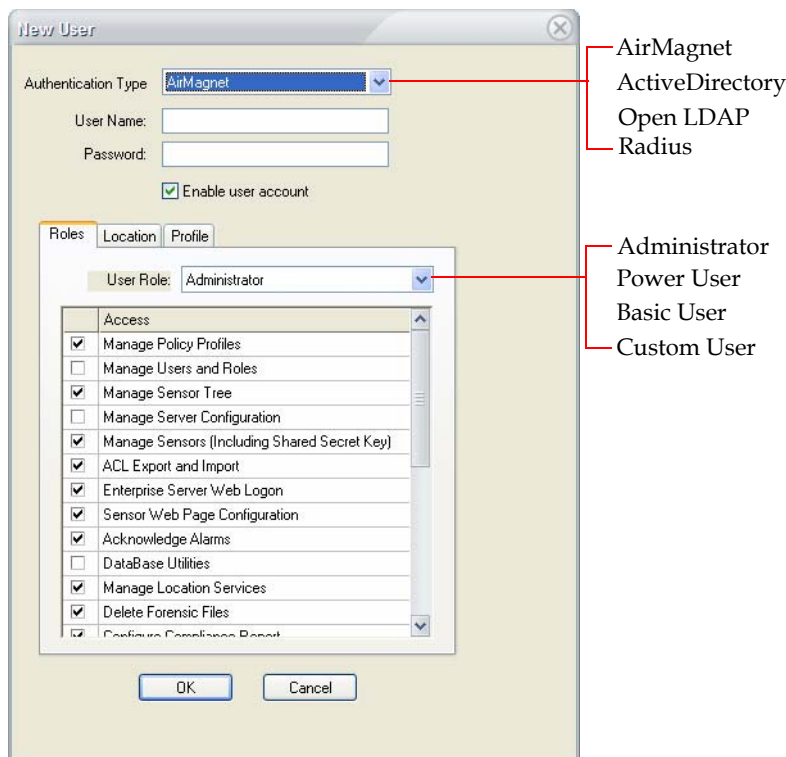


Figure 4-32: Using AirMagnet for user authentication

- 3) Click the down arrow and select an Authentication Type from the drop-down list, as described in Table 4-7.

Table 4-7: Authentication Types

Type	Description
AirMagnet	If selected, the user needs to create a user name and a password which will then be stored in the AirMagnet Enterprise Server database. When the user logs in, the Server will verify the log-in information against the data in the database to determine whether to grant or deny his or her access.

Table 4-7: Authentication Types

Type	Description
ActiveDirectory®	<p><i>In order to use this option, make sure that the user information is in the Active Directory service database.</i></p> <p>If selected, the administrator needs to find the user name in the ActiveDirectory service and add it to AirMagnet Enterprise Server. Later, when the user logs onto the AirMagnet Enterprise Server through an AirMagnet Enterprise Console, the AirMagnet Enterprise Server will contact the Active Directory server to authenticate the user.</p>
Open LDAP	<p><i>In order to use this option, make sure that the user information is in the Open LDAP (Lightweight Directory Access Protocol) service.</i></p> <p>If selected, the administrator needs to find the user name in the Open LDAP service and add it to AirMagnet Enterprise Server. Later, when the user logs onto the AirMagnet Enterprise Server through an AirMagnet Enterprise Console, the AirMagnet Enterprise Server will contact the Open LDAP service to authenticate the user.</p>
Radius	<p>If selected, the password box will be disabled and a “Find User” button will appear. Clicking the button will take you to the Radius Authentication User screen. The administrator needs to fill out the information on the Radius Authentication User dialog properly. The Verify button can be used to make sure that the user is in the Radius server. The list of users can be on the radius server itself or can be linked from the radius server to Active directory or LDAP server database.</p>

- 4) If AirMagnet is selected as the Authentication Type, enter the user name and password and click **OK**.
- 5) If Active Directory or Open LDAP is selected as the Authentication Type, the screen will refresh the moment you make the selection.
- 6) If you know the user information in the Active Directory or Open LDAP, enter the complete string of the user name of the Active Directory or Open LDAP service in the

format as shown on the screen. See Figure 4-33.

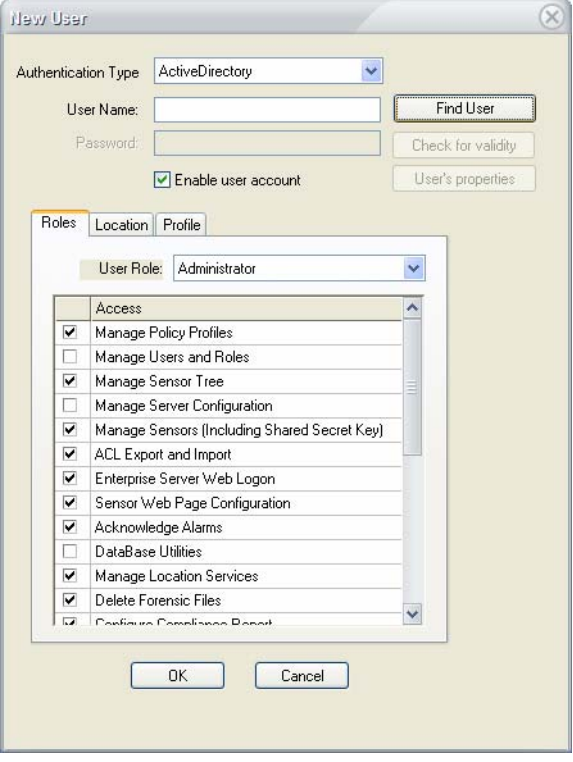
The 'New User' dialog box is shown with the 'Authentication Type' set to 'ActiveDirectory'. The 'User Name' and 'Password' fields are empty. The 'Find User' button is highlighted. The 'Enable user account' checkbox is checked. The 'Roles' tab is selected, showing a list of roles with 'Administrator' selected. The list includes 'Access', 'Manage Policy Profiles', 'Manage Users and Roles', 'Manage Sensor Tree', 'Manage Server Configuration', 'Manage Sensors (Including Shared Secret Key)', 'ACL Export and Import', 'Enterprise Server Web Logon', 'Sensor Web Page Configuration', 'Acknowledge Alarms', 'Database Utilities', 'Manage Location Services', 'Delete Forensic Files', and 'Configure Compliance Report'. The 'OK' and 'Cancel' buttons are at the bottom.

Figure 4-33: Entering Active Directory user name

- 7) If you do not know the user name or the related information in the Active Directory or Open LDAP, click **Find User**. This will open a Find User screen. See Figure 4-34.

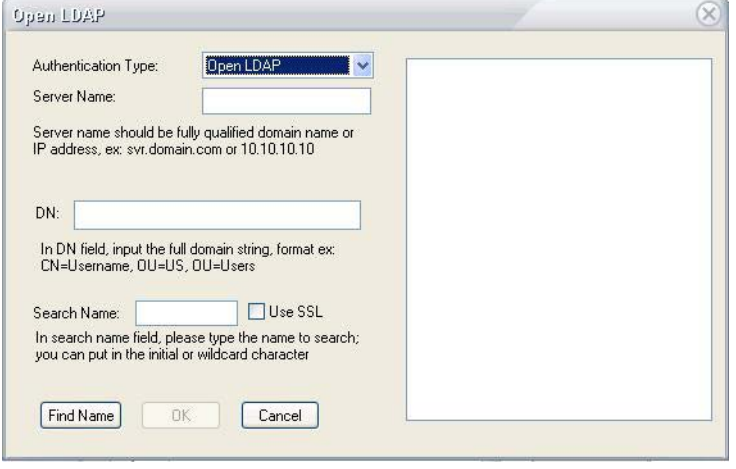
The 'Open LDAP' dialog box is shown. The 'Authentication Type' is set to 'Open LDAP'. The 'Server Name' field is empty. A note states: 'Server name should be fully qualified domain name or IP address, ex: svr.domain.com or 10.10.10.10'. The 'DN' field is empty. A note states: 'In DN field, input the full domain string, format ex: CN=Username, OU=US, OU=Users'. The 'Search Name' field is empty. A note states: 'In search name field, please type the name to search; you can put in the initial or wildcard character'. The 'Find Name', 'OK', and 'Cancel' buttons are at the bottom.

Figure 4-34: Searching users in Open LDAP

- 8) Make the following entries as described in Table 4-8.

Table 4-8: Searching for Users in Active Directory

Entry	Description
Authentication Type	Select either ActiveDirectory or Open LDAP.
Server Name	Enter the name of the Active Directory or Open LDAP server, e.g., svt.domain.com
Object Type	Use the drop-down to select whether you are finding user(s) based on the Active Directory group structure or searching all users in the Active directory.
User Name	Enter the user name of the account granted access to the Active Directory database.
Password	Enter the password for the user name entered above.
Use SSL (Secure Socket Layer)	<ul style="list-style-type: none"> • If unchecked, AirMagnet will communicate with the Active Directory or Open LDAP server through a standard connection (Port 389). • If checked, AirMagnet will communicate with the Active Directory or Open LDAP through a secure connection (Port 636).
Remember	Check this box to have the console store the user name and password credentials entered the next time the Active Directory dialog box is accessed. This is useful for adding multiple different users or groups in a row.
Location	After the logon credentials have been entered, click the Location button to connect to the Active Directory server to retrieve all Container or Organization Units defined in the directory.
Use Criteria	The Search Criteria section allows you to search for specific text within the Active Directory results. You can search based on text within the user's Display Name, First Name, Last Name, email address, or logon name.

- 9) Click **Find Name**. The user list on the right displays the accounts detected that match the specified criteria. See Figure 4-35.

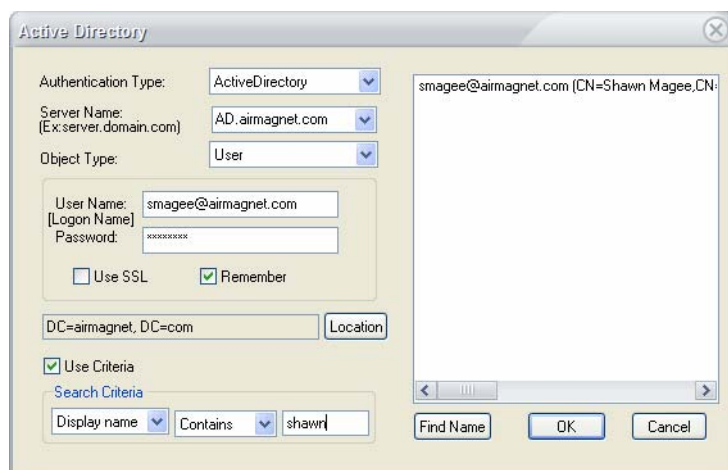


Figure 4-35: Account Located

- 10) Select the account(s) to be added and click **OK**.
- 11) Click the User Role drop-down list, and select one of the following:
- Administrator
 - Power User
 - Basic User
 - Custom User (role defined manually)
- 12) Assign privileges to the user as described in Table 4-9.

Table 4-9: User Privileges

Option	Description
Manage Policy Profiles	Has the authority to create and modify WLAN security and performance policy.
Manage Users and Roles	Has the authority to add and delete users, and to assign and modify their management roles.
Manage Sensor Tree	Has the authority to modify the network tree structure, allowing the user to move sensors and add or remove floors, buildings, or cities/campuses.
Manage Server Configuration	Has the authority to set or change Enterprise Server configuration.
Manage Sensors	Has the authority to manage sensor list as well as change the Sensor Shared Secret Key.

Table 4-9: User Privileges

Option	Description
ACL Export and Import	Has the authority to import or export ACL to or from the AirMagnet Enterprise.
Enterprise Server Web Logon	Has the authority to log onto the AirMagnet Enterprise Server Web page.
Sensor Web Page Configuration	Has the authority to log onto the AirMagnet SmartEdge Sensor Web page.
Acknowledge Alarms	Has the authority to acknowledge alarms that have been reviewed.
Database Utilities	Has the authority to back up and restore the database from the Database Utilities screen, which can be accessed by selecting <i>Manage>Database Utilities....</i>
Manage Location Services	Has the authority to change location information within your network.
Delete Forensic Files	Has the authority to delete files generated by the forensic analysis.
Configure Compliance Report	Has the authority to modify the alarms included in Compliance Reports.
Configure Report Book	Has the authority to change the contents of report books.
Manage ACL	Has the authority to create or modify the WLAN's access control list.
Remote Analyzer Tools	Has the authority to use the active tools from the AirMagnet Remote Analyzer screen.
Disable Switch Port	Has the authority to disable the switch port on the wired side of the network.
Wireless Block	Has the authority to conduct wireless rogue block.
Open Remote Analyzer	Has the authority to launch the AirMagnet Remote Analyzer from the Enterprise Console.
Remote Analyzer Decodes	Has the authority to use view decodes packets from the AirMagnet Remote Analyzer interface.
Remember Password on Login	If checked, the system will automatically remembers/enters the password each time you log in to AirMagnet Enterprise Console.
Display Security Policies and Events	If <u>unchecked</u> , all security-related policies and events will NOT be displayed on the AirMagnet Enterprise Console user interfaces.
Display Performance Policies and Events	If <u>unchecked</u> , all performance-related policies and events will NOT be displayed on the AirMagnet Enterprise Console user interfaces.

Table 4-9: User Privileges

Option	Description
User Can Change Password	Has the authority to change the server password.
View Scheduled Auto Report Task	Has the authority to view scheduled auto reports.
View Report	Has the authority to access and view reports.
Manage AHC Jobs	Has the authority to manage AHC jobs.

Although a user in the Administrator or Power User role could have more privileges than a user in the Basic User role, the network administrator may still tailor their privileges. However, the privileges of the Administrator in the default “admin” account cannot be modified.

- 13) Click the **Location** tab, the New User dialog box refreshes. See Figure 4-36.

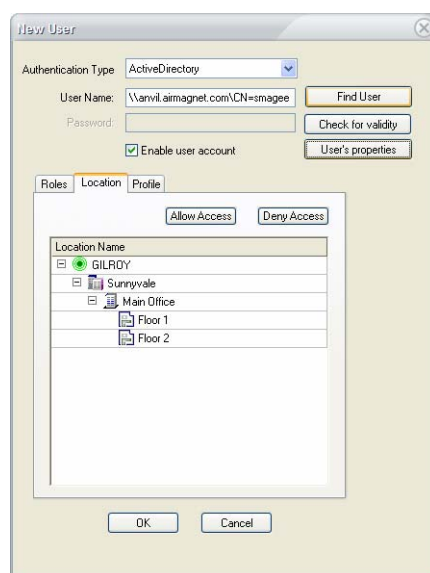


Figure 4-36: Designating location of user access

- 14) Expand the structure of the network, highlight the node where you want to allow or deny the user the access and click **Allow Access** or **Deny Access**.

In order to have a network tree structure shown under the Location tab, a network tree must be constructed first. Otherwise, only the name or IP address of the AirMagnet Enterprise Server shows on the screen when you click the Location tab.

- 15) Click the Profile tab, the New User dialog box refreshes. See Figure 4-37

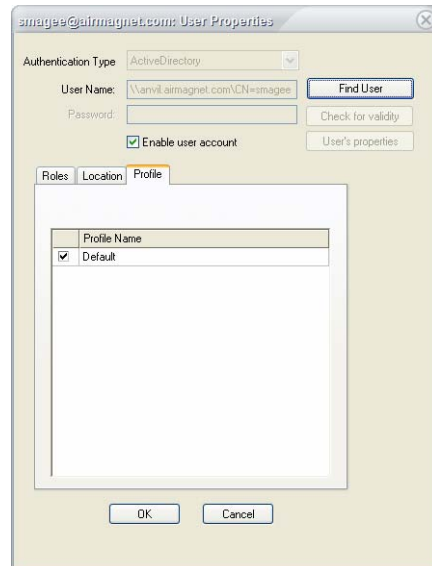


Figure 4-37: Assigning policy profiles to user

- 16) Select the policy profile(s) by checking the check box(es).

The Profile dialog box will display the default policy profile and any newly created policy profiles. For this reason, the network administrator should have all the policies configured prior to adding users to the AirMagnet Enterprise Console. For information on how to create policy profiles, see Chapter 12, "Managing Policy Profiles."

- 17) Check **Enable user account** to activate the account.


***Enable user account** must be checked in order to activate the account.*

- 18) Click **OK**. The newly added user will appear in the user list in the Manage User screen.

Removing Users from the Console User List

The Manage Users and Roles dialog box makes it easy to manage your AirMagnet Enterprise Console users and their responsibilities. To make it useful, it is important that the information be kept up to date. This involves the removal of users who are no longer using the Console.

To remove a user from the Console user list:

- 1) From the Manage Users and Roles dialog box, highlight the user account, and click  (Delete User).

Choosing User Display Options

If you have multiple users, you may want to have a quick way to differentiate one type of users from the another. This is where the user filter can help. It allows you to choose to display the users in the Manage Users and Roles dialog box.

To filter users for display:

- 1) From the Manage Users and Roles dialog box, click the down-arrow on top of the screen to display the user list. See Figure 4-38.

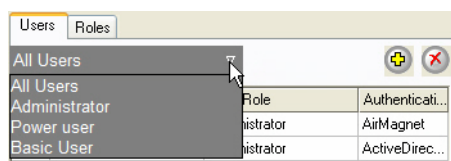


Figure 4-38: Selecting user display category

- 2) Select a user category (e.g., Power Users). The Manage Users and Roles dialog box refreshes, displaying all the users in the selected category.

Users can add additional categories by using the Roles tab in the Manage Users and Roles dialog box.

Managing AirMagnet SmartEdge Sensors

AirMagnet Enterprise allows network administrators to easily monitor the operating status of all AirMagnet SmartEdge Sensors deployed on various locations on their network directly from the AirMagnet Enterprise Console. They can know in real time the status of any Sensor and perform some basic management tasks on the Sensors remotely.

Accessing the Manage Sensors Screen

You need to bring up the Manage Sensors screen in order to view and manage the Sensors deployed on your network.

To access the Manage Sensors screen:

- 1) From the AirMagnet Enterprise Console, click **Manage>Sensors**. The Manage Sensors screen appears. See Figure 4-39.

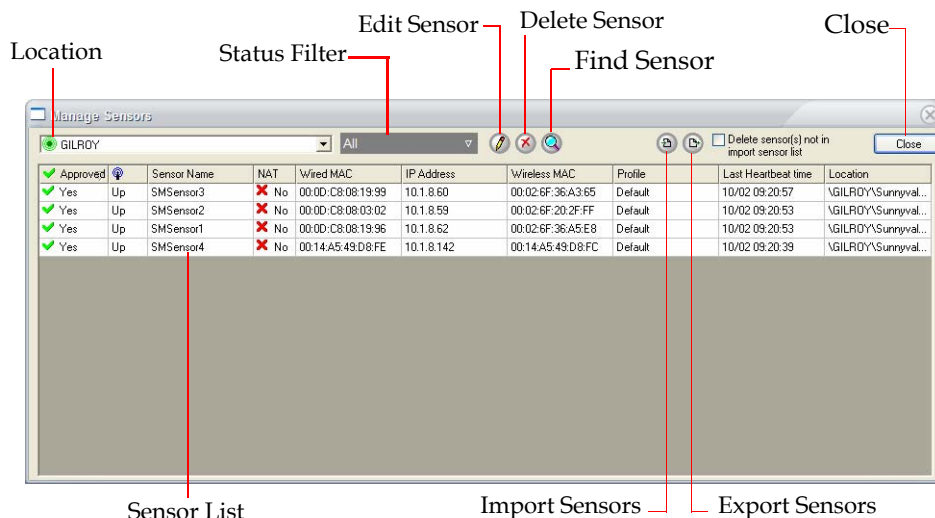


Figure 4-39: Manage Sensors screen

Sensor Screen Control Buttons






As shown in Figure 4-36 above, the Manage Sensors screen contains the following components:

- **Location** (Filter) – allows you to select Sensors by location on the network.
- **Sensor Status** (Filter) – allows you to select Sensors by operating status.
- **Edit Sensor** – brings up the Sensor Properties dialog box which allows you to modify the parameters of a Sensor selected from the Sensor Table.
- **Delete Sensor** – allows you to delete all data related to the Sensor or Sensors selected from the Sensor Table.
- **Find Sensor** – brings up the Find Sensor dialog box which displays information about all the sensors deployed near the Enterprise Console. You can then open the Web page of any sensor to configure it or change its existing configuration. See “Finding Sensors” on page 110 for more information.
- **Export Sensors** – allows you to export Sensor data as a .txt file.
- **Import Sensors** – allows you to import Sensor data (i.e., a .txt file) into AirMagnet Enterprise Server.
- **Close** – allows you to close the AirMagnet Sensors screen with a click of the button.

Sensor Table Data Fields

The AirMagnet Sensors screen provides an interface for monitoring and managing Sensors that are deployed in your network. It displays some basic information about the Sensors that match the location and the operating status of your choice. Table 4-10 briefly describes the information contained in the Sensor Table.

Table 4-10: Sensor Table Data Fields

Field	Description
Approved	Allows you to approve or disapprove (i.e., enable or disable) a sensor by clicking this field. <i>Note: A Sensor must be enabled in order to communicate with the AirMagnet Enterprise Server. This field toggles between two options:</i> <ul style="list-style-type: none">  Yes — Enabled  No — Disabled
 (Operating Status)	Indicates the working status of the Sensors. <ul style="list-style-type: none"> Up — In service. Down — Out of service.
Sensor Name	Shows the names of the Sensors, which are identical to the Sensor names in the network tree.
NAT	Allows you to turn on or off the Sensor behind NAT feature. <ul style="list-style-type: none">  Yes — Enabled  No — Disabled
Wired MAC	The MAC address of the Sensor's Ethernet interface which connects the Sensor to the wired corporate network.
IP Address	The Sensor's IP address.
Wireless MAC	The MAC address of the Sensor's wireless network card which connects the Sensor to the wireless network.
Profile	The AirMagnet policy profile used on the Sensor.
Last Heartbeat Time	The time when the Sensor's last heartbeat was detected.
Location	The location of the Sensor on the network tree.

Monitoring Sensors on the Network

The intuitive design of the Manage Sensors screen enables network administrators to view and monitor AirMagnet SmartEdge Sensors with great ease. By default, the Manage Sensors screen displays all the Sensors that report to the AirMagnet Enterprise Server to which the AirMagnet Enterprise Console is connected. You can customize the contents of the Sensor List using the Location and Sensor Status filters on top of the screen to show Sensors at a specific location or in a specific status or both.

To customize the list of Sensors on the Manage Sensors screen:

- 1) From the Manage Sensors screen, click the Location down arrow and select a location of interest from the network tree. See Figure 4-40.

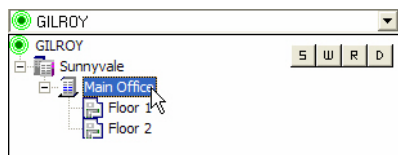


Figure 4-40: Selecting a location from the network tree

The drop-down network tree will collapse and the selected location will appear in the Location filter once you click the location of your choice.

- 2) Click the Sensor Status down arrow and select a status option from the drop-down list. See Figure 4-41

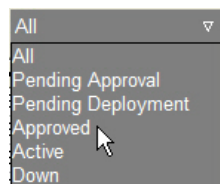


Figure 4-41: Selecting a Sensor status option


By default, the Manage Sensors screen displays all the Sensors that report to the AirMagnet Enterprise Server, regardless their operating status. With the Sensor Status filter, you can easily fine-tune the list of Sensors displayed on the screen using any of the options in the drop-down list.

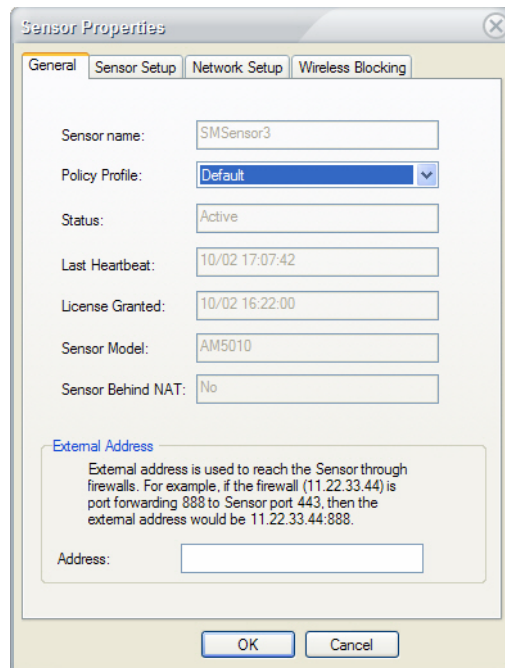
The Pending Approval and Pending Deployment filter options are very similar and could be easily confused. The former option displays sensors that already exist on the network and have been detected by AirMagnet Enterprise, and they simply await the user's approval. The latter displays sensors that have been added manually but are not yet connected to the network.

Modifying Sensor Properties

The Manage Sensors screen also allows you to make some changes to the configuration of the selected Sensor remotely from the AirMagnet Enterprise Console.

To modify the properties of a Sensor:

- 1) From the Manage Sensors screen, highlight the Sensor of interest and click  (**Edit Sensor**). The default Sensor Properties dialog box appears. See Figure 4-42.



The image shows the 'Sensor Properties' dialog box with the 'General' tab selected. The fields are as follows:

Field	Value
Sensor name:	SMSensor3
Policy Profile:	Default
Status:	Active
Last Heartbeat:	10/02 17:07:42
License Granted:	10/02 16:22:00
Sensor Model:	AM5010
Sensor Behind NAT:	No

External Address
External address is used to reach the Sensor through firewalls. For example, if the firewall (11.22.33.44) is port forwarding 888 to Sensor port 443, then the external address would be 11.22.33.44:888.

Address:

Buttons: OK, Cancel

Figure 4-42: Changing Sensor Policy Profile

- 2) Click the down arrow and select a different policy profile, if desired.
- 3) Enter the external address of the Sensor, if applicable. This field is only necessary if your network requires that connections be established through a proxy server.

- 4) Click the Sensor Setup tab. The Sensor Properties dialog box refreshes. See Figure 4-43.

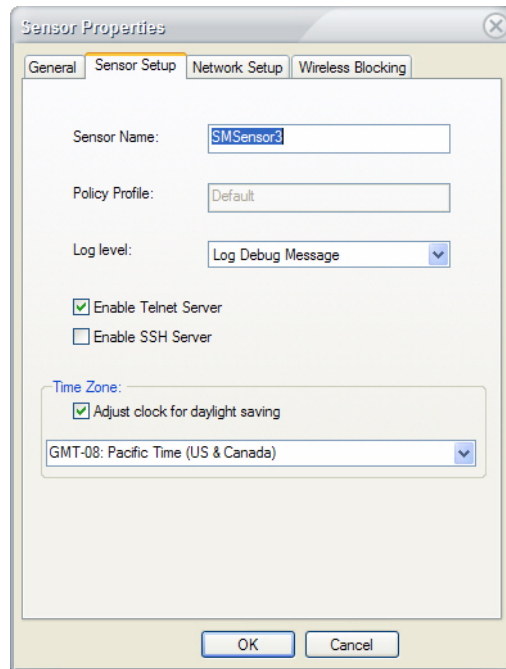


Figure 4-43: Changing Sensor Setup

- 5) If desired, highlight the sensor name and overwrite it with a new one.
- 6) Click the **Log Level** down arrow and select an option from the drop-down list. See Figure 4-44.

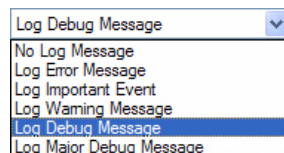


Figure 4-44: Selecting a log level for the Sensor

- 7) Check the Enable Telnet Server check box or Enable SSH Server check box, if applicable.
- 8) If applicable, click the down arrow to select a different time zone from the drop-down list.
- 9) Check the **Adjust clock for daylight saving** check box, if applicable.

- 10) Click the Network Setup tab. The Sensor Properties dialog box refreshes. See Figure 4-45.

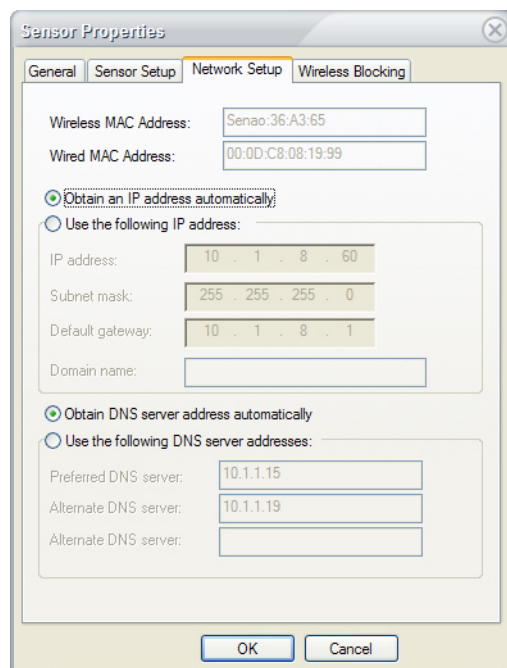


Figure 4-45: Modifying Sensor's network settings

- 11) Make the applicable changes, and click OK.


All the changes you have made will be reflected on the AirMagnet Sensors screen once the screen refreshes. You can refresh the screen by closing it and then opening it again.

The Wireless Blocking tab shown in Figure 4-42 allows the user to view a list of the devices that the selected sensor is currently blocking.

Deleting Sensors

You can remove from the network Sensors that are not functioning or are physically taken off the network for repair. However, the Sensors will show up in the Sensor List once they are re-deployed on the network.


To delete a Sensor from the network:

- 1) From the Manage Sensors screen, highlight the Sensor in the Sensor List.
- 2) Click  (Delete Sensor).

Finding Sensors

AirMagnet Enterprise allows you to view all sensors deployed in the vicinity of the Enterprise Console from the Console user interface. You can then log on to the Web page of any of the sensors to perform a number of tasks about the sensor, including configuring or modifying the sensor's settings. This feature is especially useful for users of A5023 sensors which do not have a Sensor Serial Console Port interface.

To find sensors close to your AirMagnet Enterprise Console:

- 1) From the Manage Sensor screen, click  (Find Sensor). The Find Sensor dialog box appears. See Figure 4-46.

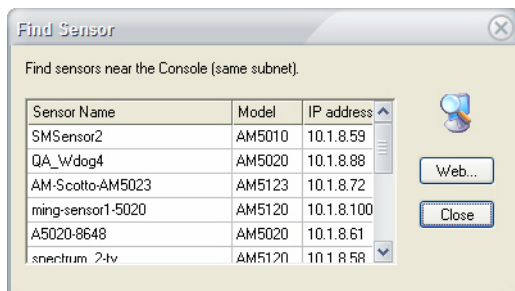


Figure 4-46: Finding sensors close to the Console

- 2) Highlight a sensor of interest from the list of sensors on the screen, and click the **Web...** button. An Internet browser is launched. See Figure 4-47.

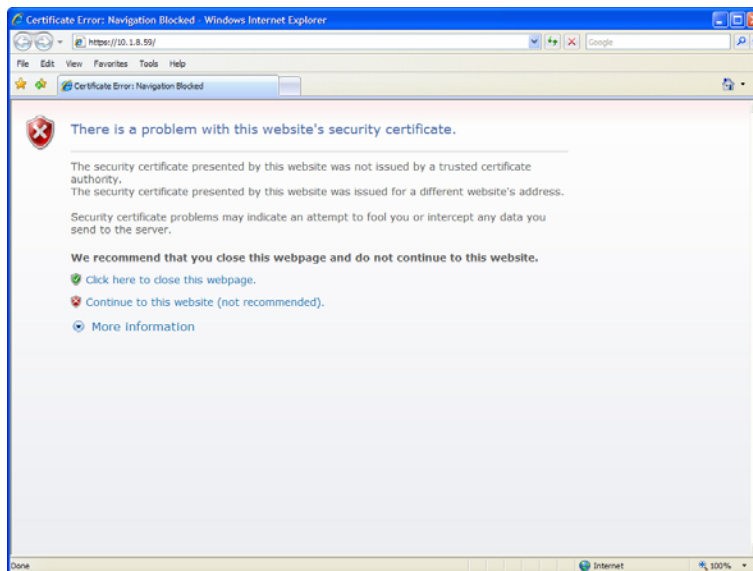


Figure 4-47: Launching Microsoft Internet Explorer

- 3) Click **Continue to this website** to continue. The Sensor login dialog box appears. See Figure 4-48.



A Windows-style dialog box titled "Connect to 10.1.8.59". It features a blue header bar with a question mark icon. The main area has a light beige background. At the top left is a key icon. Below it, text reads: "The server 10.1.8.59 at AirMagnet SmartEdge Sensor requires a username and password." There are two input fields: "User name:" with a dropdown arrow and a small user icon, and "Password:" with a standard text box. Below the password field is a checkbox labeled "Remember my password". At the bottom are "OK" and "Cancel" buttons.

Figure 4-48: Logging onto a sensor

- 4) Enter the user name and password of the sensor, and click **OK** to continue. The sensor's Web page appears. See Figure 4-49.

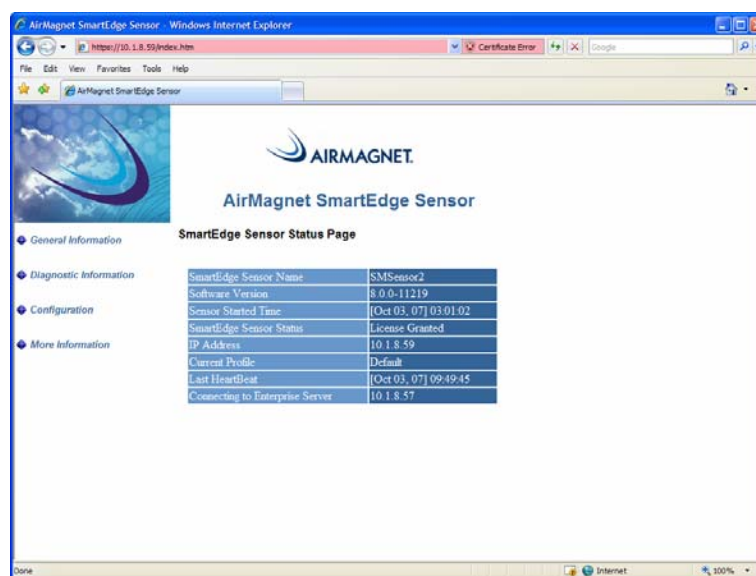


Figure 4-49: AirMagnet SmartEdge Sensor Web page

Once you are on the AirMagnet SmartEdge Sensor Web page, you can perform a number of tasks using the menu buttons on the left-hand side of the Web page.

Importing Sensor Data

The Import Sensor feature allows network administrators to create and save the plan of their wireless networks in a text file and then import it into the AirMagnet Enterprise system before the Sensors are physically deployed on the network. The file contains some basic information of all the AirMagnet SmartEdge Sensors to be deployed, their names, MAC addresses, policy profiles, and location on the network. In this way, once the Sensor are physically deployed on the network, they will automatically find their respective locations on the network tree and start to communicate with the AirMagnet Enterprise Server.

To import Sensor data into the AirMagnet Enterprise system:

- 1) From the Manage Sensors screen, click  (**Import Sensors**). The Import Sensors dialog box appears. See Figure 4-50.

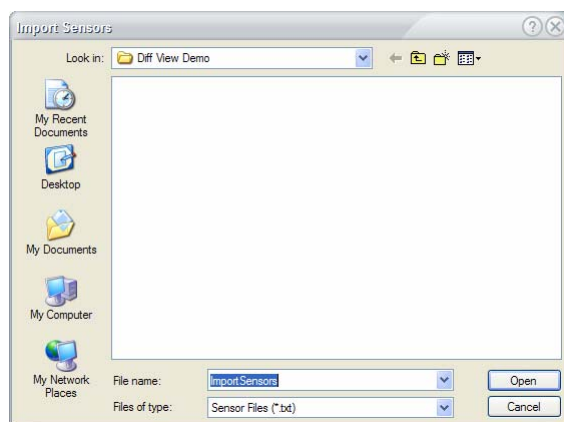


Figure 4-50: Importing Sensor data

- 2) Locate and select the Sensor data file on your machine or network, and click **Open**. The Sensors contained in the imported Sensor data file appear in the Sensor List on the Manage Sensors screen.

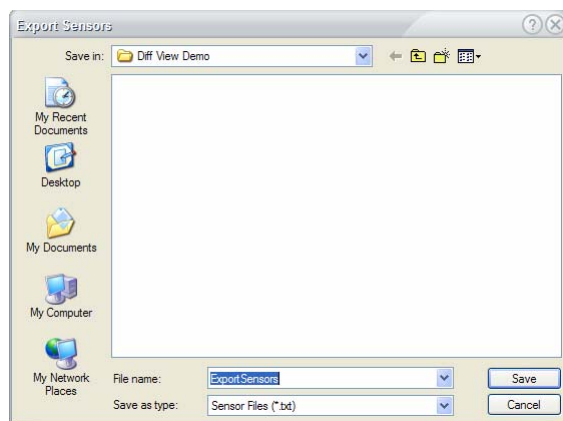
When you import sensors, information about all Sensors contained in the imported Sensor data (.txt) file appears not only on the AirMagnet Sensors screen, but also in the network tree on the Start screen.

Exporting Sensor Data

Not only can you plan your network deployment ahead of time, but also back up the configuration of your network by exporting data of your Sensors in a text file in the same format as illustrated in Figure 4-47. This also can be done from the Manage Sensors screen.

To export your Sensor data:

- 1) From the Manage Sensors screen, click  (**Export Sensors**). The Export Sensor dialog box appears. See Figure 4-51.

**Figure 4-51: Exporting Sensor data**

- 2) Specify an export location and a file name, and click **Save**.

*Make sure that the .txt file extension is selected in the **Save as type** field.*

Managing AirMagnet Enterprise Database

The AirMagnet Enterprise database contains important data of the system parameters used on your AirMagnet Enterprise as well as various events that have occurred on your network. However, as time passes by, the size of the database can grow significantly as more data are added into the database. As a result, your database may become less efficient to operate and need more staff to maintain. Therefore, it is important that you manage your database properly to ensure that your AirMagnet Enterprise system operates smoothly and provides the security and performance services you need. This section discusses how to manage your AirMagnet Enterprise database using the Database Utilities on the Enterprise Console. Managing AirMagnet Enterprise database involves the following tasks:

- Backing up the current database;
- Restoring an database backup file;
- Deleting a database backup file; and
- Resetting the database table.

Although AirMagnet Enterprise supports Microsoft Access, SQL, PostgreSQL, and Oracle databases, the Database Utilities discussed here apply to the Microsoft Access, SQL, and PostgreSQL databases ONLY, and cannot be used with the Oracle database.

The following paragraphs provides detailed instructions for performing each of the tasks.

To access the Database Utilities:

- 1) From the Enterprise Console screen, click **Manage>Database....** The **Database Utilities** dialog box appears. See Figure 4-52.

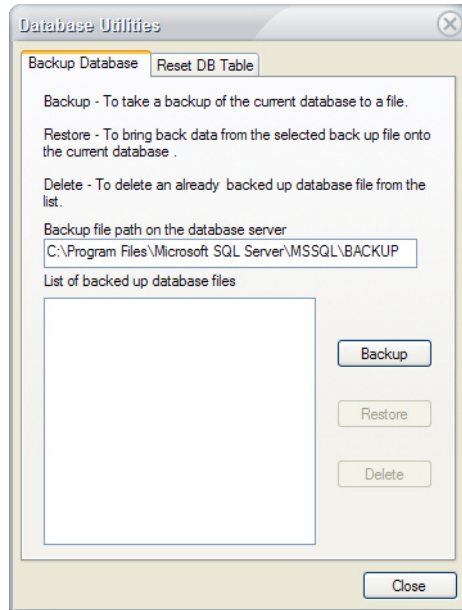


Figure 4-52: AirMagnet Database Utilities

Backing Up the Current Database

The AirMagnet Enterprise Database, whether it is on a Microsoft Access Server or SQL Server, consists of more than half a dozen tables, each containing a specific type of data. Backing up your database means storing the current data on the AirMagnet Enterprise into a file so that you can revisit the data at a later time if you wish. It also keeps a record of data on your network at different times so for future auditing purposes.

To back up your current AirMagnet Enterprise database:

- 1) From the **Database Utilities** dialog box, highlight the path of the backup file and overwrite it with a unique path of your choice.

You may also accept the default destination for the backup file. However, if you want to back up the file at a location of your choice, it is important that you make a note of it because you need this information in order to restore the file. For illustration purposes, we just use the default path.

- 2) Click the **Backup** button. The current database will be stored to a backup file at the specified location and the name of the backup file appears the Database Utilities dialog

box. See Figure 4-53.

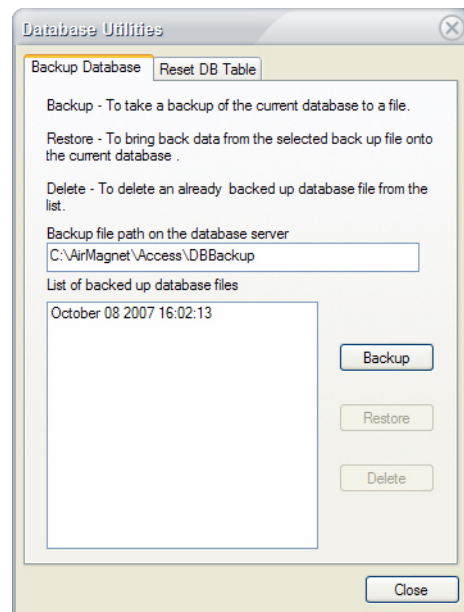


Figure 4-53: A database backup file

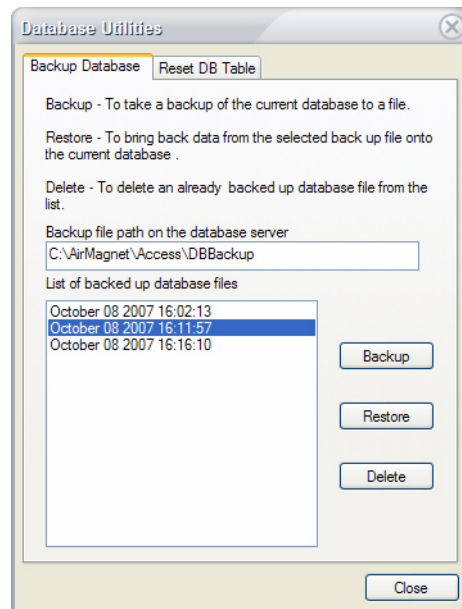
The current database is backed up each time you click the Backup button, and the name of the database backup file automatically appears in the Database Utilities dialog box when the backup is completed. By default, the time of the backup is used as the name of the backup file, which makes it easier for differentiating the database backup files made at different times in the past. Also, all backup database files are linked to the locations they are stored, and AirMagnet Enterprise can automatically locate the path of a database backup file and displays it in the Database Utilities dialog box.

Restoring a Database Backup File

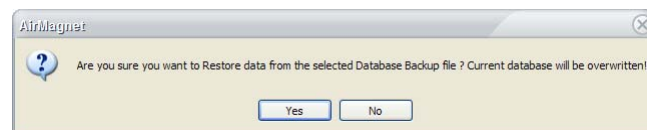
The Database Utilities also allows you to restore any database backup file so that you can restore your AirMagnet Enterprise database to a certain point of time in the past. In this way, you can revisit some historical data that AirMagnet Enterprise has captured in your network.

To restore a database backup file:

- 1) From the Database Utilities dialog box, highlight the name of the database backup file of interest. See Figure 4-54.

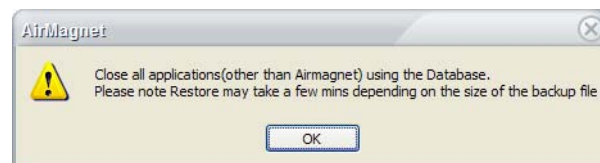
**Figure 4-54: Selecting a database backup file**

- 2) Click the **Restore** button. A warning message appears. See Figure 4-55.

**Figure 4-55: A warning message on database Restoration**

Make sure you read the message on the screen before you proceed with restoring the old database.

- 3) Click **Yes** to continue. Another message may appear. See Figure 4-56.

**Figure 4-56: A reminder on database restoration**

- 4) Click **OK** to continue.

Upon restoration of the database backup file, the data contained in the backup file appear on the Enterprise Console.

Deleting a Database Backup File

As mentioned earlier, a database backup file is created each time you click Backup button, and the name of the file automatically appears in the Database Utilities dialog box. As a result, the Database Utilities dialog box may become over-crowded, making it difficult to find the correct database backup file you want. To solve this problem, you may want to delete those database backup files that you may not need any more.

To delete a database backup file:

- 1) From the Database Utilities dialog box, highlight the name of the database backup file.
- 2) Click the **Delete** button. A message appears on the screen. See Figure 4-57.

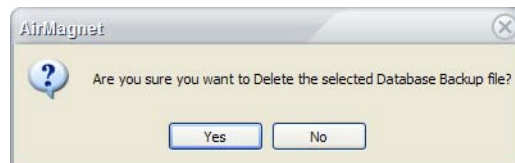


Figure 4-57: A reminder on deleting a database backup file

- 3) Click Yes to continue. The Database Utilities dialog box refreshes, with the selected database backup file removed.

Cleaning Up Database Tables

AirMagnet Enterprise uses tables to organize your network data. Each database table contains a specific type of data. As the amount of data grows, so does the size of the database table. It is for this reason that AirMagnet Enterprise provides the option for cleaning up some or all the database tables from the Database Utilities dialog box.

To clean up database tables:

- 1) From the Database Utilities dialog box, click the Reset DB Table tab. The dialog box refreshes. See Figure 4-58.

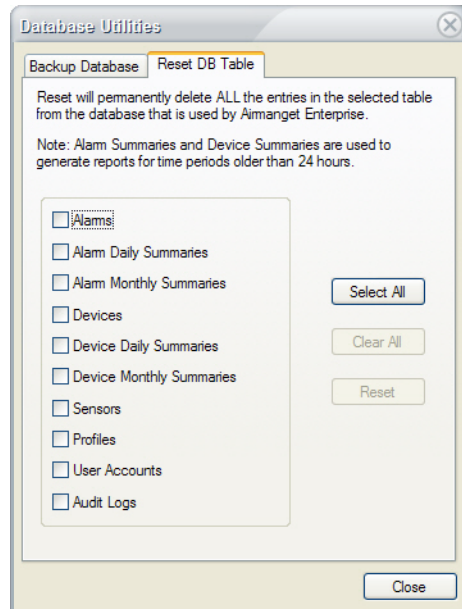


Figure 4-58: Resetting database table

- 2) Read the instructions on the screen.

- 3) Select the database table or tables to be cleaned up. See Figure 4-59.

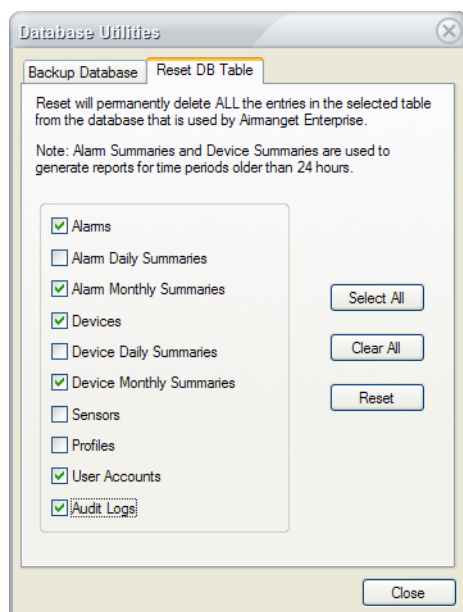


Figure 4-59: Selecting database tables

You must exercise caution when deleting the Sensors and User Accounts tables because they contain very important system configuration data which, if deleted, will be gone forever. If that happened, you would have to re-create your network (Sensor) tree structure and reconfigure all the user accounts. For this reason, a warning message automatically pops up on the screen when you select either of the tables.

- 4) Click **Reset** to proceed. A message appears on the screen. See Figure 4-60.



Figure 4-60: A reminder on resetting database table

- 5) Click **Yes** to continue. Another message appears on the screen. See Figure 4-61.

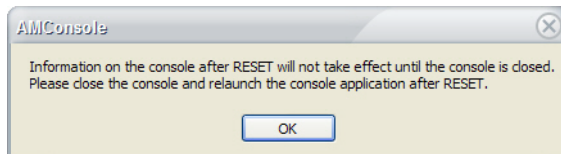


Figure 4-61: A message box

- 6) Click **OK** to close the message box.
- 7) Exit the AirMagnet Enterprise Console and then restart it.

The database tables that have been reset will appear empty when the Console restarts. You may need to wait for a few seconds for data to start appearing in the tables. However, if you reset the Sensors table, then the network tree you had created would be gone and you have to reconstruct your network hierarchy from the scratch. If you reset the User Accounts table, then all information related to the accounts will be wiped out and those users can no longer access the AirMagnet Enterprise.

Chapter 5: Using the Start Screen

Introduction

This chapter discusses the major sections of the AirMagnet Enterprise Console Start screen, and describes how to use the various sections of the screen to identify, analyze, and solve your WLAN security and performance issues.

The Start screen provides network administrators with a quick overview of all network activity detected within the last 24 hours. Note that the Start screen contains two viewing options: Overall View and Classic View. By default, the Overall View is displayed, but users can switch to the Classic View by using the tools provided at the top of the screen. Each view option is discussed in its own section of this chapter.

By default, the AirMagnet Enterprise Console's Start screen automatically appears once the Console is successfully connected to the AirMagnet Enterprise Server. If you are working on any of the other screens, you can switch to the Start screen by clicking  **Start**.

Overall View

The Overall View is divided into several sections that each provide a summary of specific network information. The links displayed by the Overall View allow the user to focus on the problems displayed, making it easier to remedy network issues as quickly as possible.

Major UI Components

The Overall View has several main components, as shown in Figure 5-1.

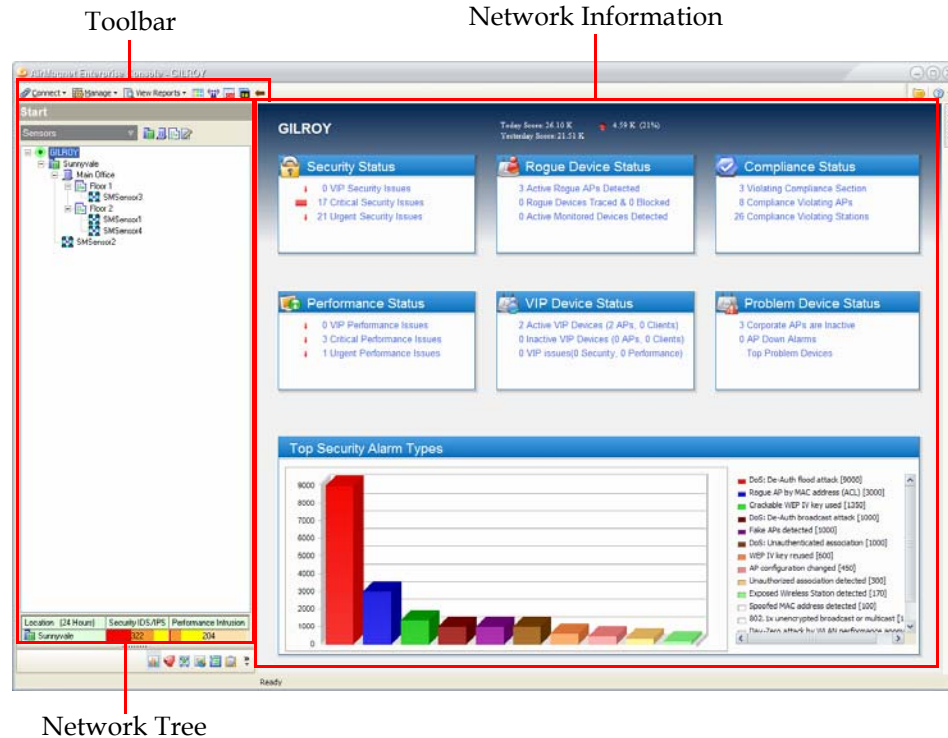




Figure 5-1: Overall View Components

Each portion of the interface is described in a section below.

The Toolbar

As most of the Toolbar's major buttons have been discussed in "The Toolbar" on page 76, this section describes the two buttons specific to the Start screen. These buttons simply allow users to toggle between Overall View and Classic View.

To switch Start screen views:

- To access the Overall View, click  (Overall View).
- To access the Classic View, click  (Classic View).

Network Tree

The Start screen's Network Tree operates in the same manner as described in "Network Tree" on page 70. Users can select specific cities, buildings, floors, or sensors to view data from.

Network Information

The Network Information section provides data regarding a variety of categories on the network. Users can view a summary of network activity over the past 24 hours, and by using the links provided on the screen can drill-down to analyze specific issues as they are detected. The Network Information is described in greater detail in the following section.

Network Information Components

The Network Information portion of the screen is divided into eight major components, as shown in Figure 5-2.

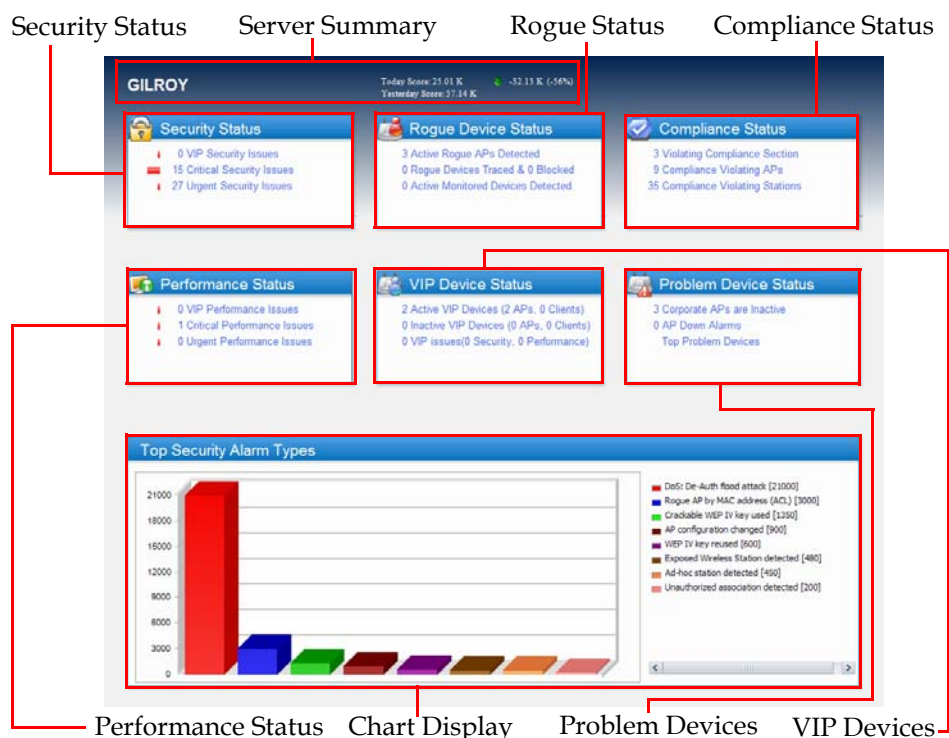


Figure 5-2: Network Information Components

The fields highlighted in Figure 5-2 are described in the following sections.

Server Summary

The Sever Summary shows a summary of the network's status over the course of the past 24 hours. These data are based on the alarm scores generated in that time interval. As shown in Figure 5-2, the portion of the Network Tree selected is displayed at the far left of the Server Summary section. This allows the user to easily determine the location that data are being displayed for.

Security Status

The Security Status frame shows a summary of security alarms currently detected on the network. By clicking the title of the frame, users can display the top security alarm types in the Chart Display frame. Clicking the links contained in the Security Status frame filters the chart further, allowing users to view security issues specific to VIP devices, critical issues, or urgent issues.

Users can drill-down on the issues listed by double-clicking each link. This opens the AirWISE screen with a filter set up to display the information that was double-clicked.

Rogue Device Status

The Rogue Device Status frame shows a summary of rogue device information currently detected on the network. By clicking the title of the frame, users can display the top rogue device alarm types in the Chart Display frame. Clicking the links contained in the Rogue Device Status frame filters the chart further, allowing users to view data specific to rogue APs, traced and blocked devices, or monitored devices.

Users can drill-down on the device issues listed by double-clicking each link. This opens the Infrastructure screen with a filter set up to display the information that was double-clicked.

Compliance Status

The Compliance Status frame shows a summary of the network's compliance with the directive selected in Enterprise's configuration (for more details, see ["Server Settings" on page 252](#)). Users who must follow a specific compliance type can use this field to easily view and fix issues that cause compliance violations.

By clicking the Compliance Status title, users can display the compliance issues by section of the compliance report. Clicking the links contained in the frame filters the chart further, allowing users to view the sections violated, APs causing violations, or stations causing violations. Double-clicking any of the links opens the AirWISE screen with a filter set up to display the information that was double-clicked.

Performance Status

The Performance Status frame shows a summary of performance alarms currently detected on the network. By clicking the title of the frame, users can display the top performance alarm types in the Chart Display frame. Clicking the links contained in the Performance Status frame filters the chart further, allowing users to view security issues specific to VIP devices, critical issues, or urgent issues.

Users can drill-down on the issues listed by double-clicking each link. This opens the AirWISE screen with a filter set up to display the information that was double-clicked.

VIP Device Status

The VIP Device Status frame shows a summary of VIP device information currently detected on the network. By clicking the title of the frame, users can display the top VIP device alarm types in the Chart Display frame. Clicking the links contained in the VIP Device Status frame filters the chart further, allowing users to view data specific to active VIP devices, inactive VIP devices, or the types of issues associated with VIP devices.

Users can drill-down on the device issues listed by double-clicking each link. This opens the Infrastructure screen with a filter set up to display the information that was double-clicked.

Problem Device Status

The Problem Device Status frame shows a summary of devices currently experiencing unusual problems on the network. By clicking the title of this frame, users can display the top problem devices in the Chart Display frame.

Users can drill-down on the device issues listed by double-clicking each link. This opens the Infrastructure screen with a filter set up to display the information that was double-clicked.

Chart Display

As described in the preceding sections, the Chart Display frame adjusts to display any data that has been selected by the user in the status frames. The chart displays a graphical view of the selected data, with chart entries listed in order of alarm score.

Classic View

The AirMagnet Enterprise Console's Classic View serves as a WLAN Network Operating Center (NOC). It provides WLAN network administrators with comprehensive information about their WLAN network security and performance status, WLAN assets, and aggregated data about any selected segment on the WLAN in the following categories:

- Security IDS/IPS policy violations, separated into each IDS/IPS category;
- Performance policy violations, separated into each Performance category;
- The top 10 APs with the most events;
- The top IDS/IPS events detected;
- The top performance intrusion events detected;
- The top 10 active APs, as listed by the number of stations associated to them;
- APs detected on the network, sorted by ACL status;
- Stations detected on the network, sorted by ACL status;
- New devices detected within the last hour.

Major UI Components

This section discusses the various sections of the Classic Start screen and the information that each of these sections contains as well as the ways to use the screen to identify, analyze, and solve your WLAN security and performance issues.

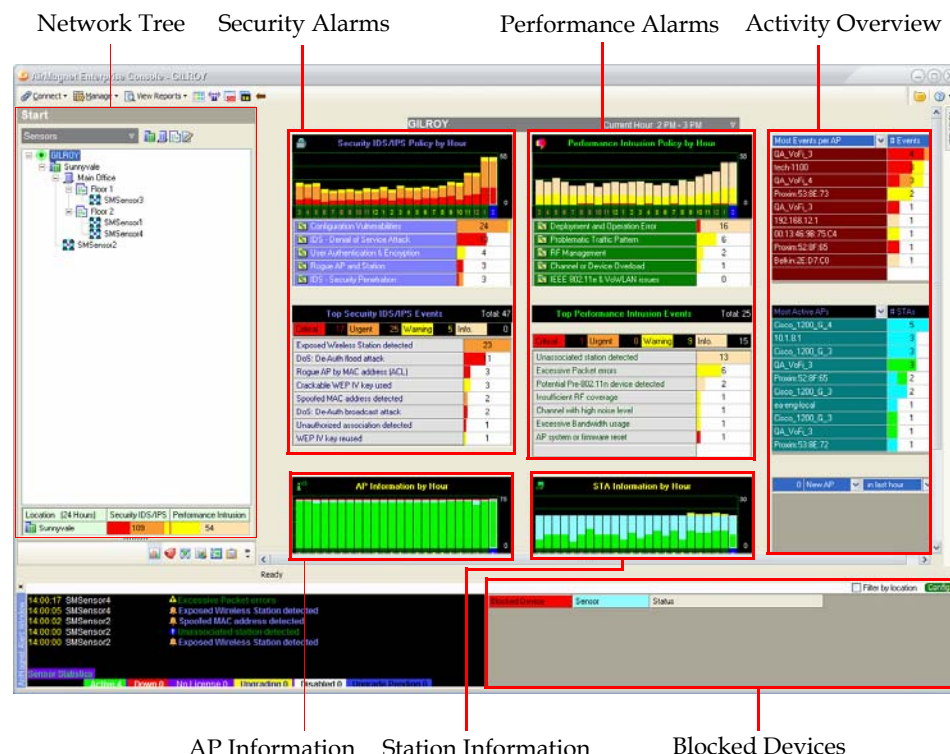


Figure 5-3: Classic View Components

As shown in Figure 5-3, the Classic Start screen can be divided into several main sections. These sections are interrelated and presents WLAN data from different perspectives. The following is a summary of the main functions of each of these sections.

The screens of the AirMagnet Enterprise Console vary depending on the roles or privileges of the user who is using the Console. For a user who is assigned to manage only performance policies and events, the screen will not show any security-related policies or events, and vice versa.

Network Tree

The Start screen's Network Tree operates in the same manner as described in "Network Tree" on page 70. Users can select specific cities, buildings, floors, or sensors to view data from.

Time Frame Selector

The Time Frame Selector shows the time period of the data shown on the current screen. You can change the time frame by clicking a bar in a bar chart (e.g., Security Policy by Hour, AP Information by Hour, etc.), or by choosing a time period from the Time Frame Selector drop-down list. See Figure 5-4.

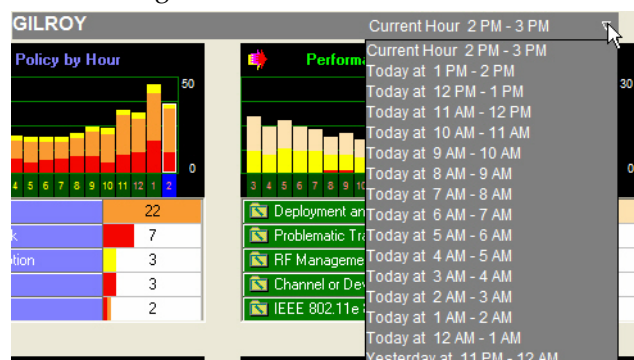


Figure 5-4: Time frame selector drop-down list

Alarm Overview

The Alarm Overview shows what problems have occurred on your WLAN and when they occurred. This section contains three parts. The top part displays in bar charts the number of security and performance alarms that have occurred in the last 24 hours. Each bar indicates the density and severity of alarms at a given hour. Clicking a bar will refresh the screen to reflect the data of the selected hour.

Under the bar charts are security and performance alarms grouped into five general categories respectively.

The Security IDS/IPS policies are divided into the following five general categories:

- Configuration Vulnerabilities
- IDS – Denial-of-Service Attack
- IDS – Security Penetration
- Rogue AP and Station
- User Authentication & Encryption

The Performance Intrusion policies are divided into five general categories:

- Channel or Device Overload
- Deployment & Operation Error
- IEEE 802.11g Issues
- Problematic Traffic Pattern
- RF Management

For information about AirMagnet Enterprise's Security IDS/IPS and Performance Intrusion policies, see [Chapter 12, "Managing Policy Profiles"](#), or refer to the "AirMagnet Enterprise Policy Reference Guide" on the AirMagnet Enterprise software CD.

The number for each general policy category indicates the number of alarms that have occurred in that category.

If you mouse over a general policy category with a total number of alarms, a tool tip screen will pop up, showing the number of alarms at each of the four severity levels, i.e., Critical, Urgent, Warning, and Informational. See Figure 5-5.

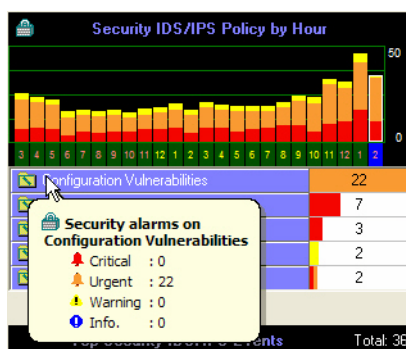


Figure 5-5: Tool tip screen showing alarm statistics

The bottom part of the Alarm Overview displays the top events for the selected general alarm category. It breaks the alarms into four severity-based categories (i.e., Critical, Urgent, Warning, and Informational) and shows the specific number of alarms for each category.

AP Information by Hour

The AP Information section displays the data of all access points detected at the selected segment of the WLAN in the last 24 hours. See Figure 5-6.

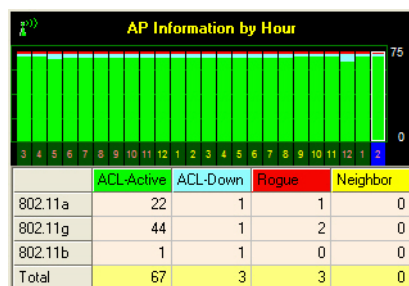


Figure 5-6: AP Information by Hour

The top part of this section is a color-coded bar chart, each column of the bar chart representing AP information at a specific hour. Clicking a column will refresh the screen to display the AP information of that hour. The bottom part of this section provides detailed information about the APs by media type and status, as described in Table 5-1.

Table 5-1: AP Information

Field	Description
ACL – Active	The AP is in the WLAN access control list and is working properly. (Green)
ACL – Down	The AP is in the WLAN access control list, but is down (not working). (Light Blue)
Rogue	The AP is a rogue device. (Red)
Neighbor	The AP belongs to a neighboring business. (Yellow)

Double-clicking the data shown in any of the ACL columns will open the Infrastructure screen.

STA Information by Hour

The STA Information by Hour section displays the data of all stations detected at the selected segment of the WLAN in the last 24 hours. See Figure 5-7.

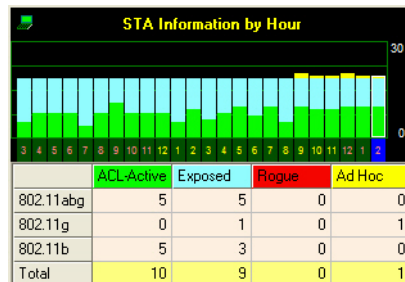


Figure 5-7: STA Information by Hour

The top part of this section is a color-coded bar chart, each column of the bar chart representing STA information at a specific hour. Clicking a column will refresh the screen to display the STA information of that hour. The bottom part of this section provides detailed information about the STAs by media type and status, as described in Table 5-2.

Table 5-2: Station Information

Field	Description
ACL – Active	The station is in the WLAN access control list (ACL) and is working properly. (Green)
Exposed	The station is in the ACL but with open WLAN connection, thus running the risk of exposing the corporate network to the outside world. (Light Blue)
Rogue	The station is a rogue device. (Red)
Ad Hoc	The station is part of an ad hoc network, where wireless stations communicate directly to one another without using an access point (AP) or connection to a wired network. (Yellow)

Most Events per AP/STA/AdHoc

The top section of the right column of the Start screen is used to show the APs, STAs, or AdHocs that have experienced the most events during the selected time frame. See Figure 5-8.

Most Events per AP	# Events
tech:1100	2
Proxim:53:8E:73	2
QA_VoFL_3	1
QA_VoFL_3	1
192.168.12.1	1
Proxim:52:8F:65	1
Belkin:2E:D7:C0	1

Figure 5-8: Most Events per AP by # Events

The left column displays the MAC addresses or the combination of Names and MAC addresses of the devices, while the right column shows the number of alarms that have been triggered by each of the devices. You can display any category of the devices by clicking the down arrow and selecting an option from the drop-down list.

If you mouse over any field in the # Events column, a tip screen will appear showing the numbers of alarms at each severity level.

Most Active APs/SSIDs

The middle section of the right column of the Start screen is used to display the most active APs or SSIDs by the number of stations that were associated with them (APs or SSIDs). See Figure 5-9.

Most Active APs	# STAs
QA_VoFi_3	4
QA_VoFi_3	2
10.1.8.1	1
ea-eng-local	1
Cisco_1200_G_3	1
QA_VoFi_3	1
Cisco:AF:3A:7C	1
Proxim:53:8E:72	1
QA-1200-7	1
QA-1200-7	1

Figure 5-9: Most Active APs by # STAs

The left column displays the names, MAC addresses, or name-MAC address combinations of the APs or the names of the SSIDs. The right column shows the number of stations associated with each AP or SSID.

Placing the cursor over any field will display a tip screen showing the breakdown of the number of stations connected to the AP or SSID. The colors of the STAs indicates the types of media the stations use. Double-clicking any field will open the Infrastructure screen.

New AP/STA/AdHoc

The bottom section is used to display the new APs, STAs, or AdHocs, if any, that are added to the network. There are two filters on top of the screen: one for selecting a device category and the other for setting the time frame. See Figures 5-10 and 5-11.

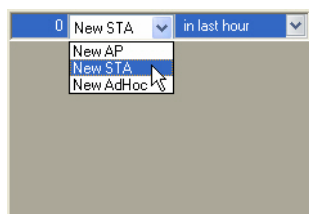


Figure 5-10: Selecting a device category

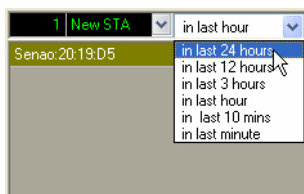


Figure 5-11: Selecting a time frame

MAC Address	Time
Senao:20:19:D5	14:59:12
Intel:CC:50:17	14:00:58
00:0D:02:3B:0B:4A	13:13:50
00:19:7E:46:63:1A	12:45:41
Cisco:A1:9C:63	11:38:01
00:1B:77:B0:7E:A7	11:35:19
00:0F:B5:35:09:48	10:51:04
00:1B:77:C4:A1:00	02:26:57
00:1C:B3:C0:13:79	17:21:28
Cisco:B8:BC:21	16:32:48

Figure 5-12: List of newly detected stations

Using the AirMagnet Alert Window

The AirMagnet Enterprise Console comes with an Alert Window that displays alarm data captured by the selected AirMagnet SmartEdge Sensor(s) as well as the working status of all the Sensors deployed on the network.

Note that the Alert Window is not available in the Start screen's Overall View. If users have the Overall View active, the Alert Window cannot be accessed from any screen.

The Alert Window can be activated from all major screens of the AirMagnet Enterprise Console by selecting **Manage>AirMagnet Alert Window**.

The Alert Window appears different on the screen, depending on the size and/or resolution of your screen. It may float on top of the screen, if the screen is of a smaller size or a lower resolution, and become docked at the bottom of the screen, if the screen is of a larger size and/or a higher resolution. Figure 5-13 shows the Alert Window docked at the bottom of the Start screen, whereas Figure 5-14 shows the Alert Window floating on top of the screen.

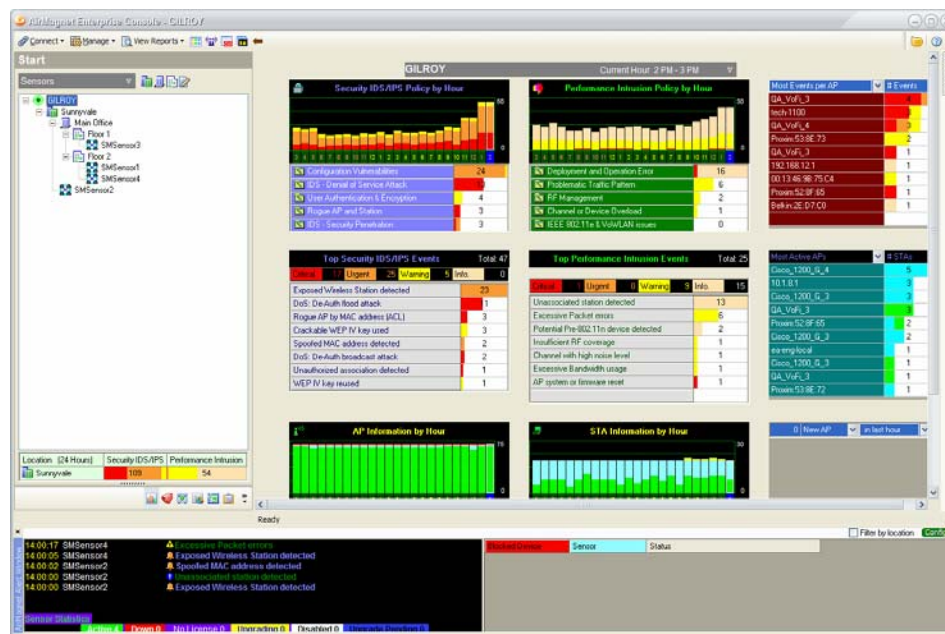


Figure 5-13: Alert Window docked at bottom of Start screen

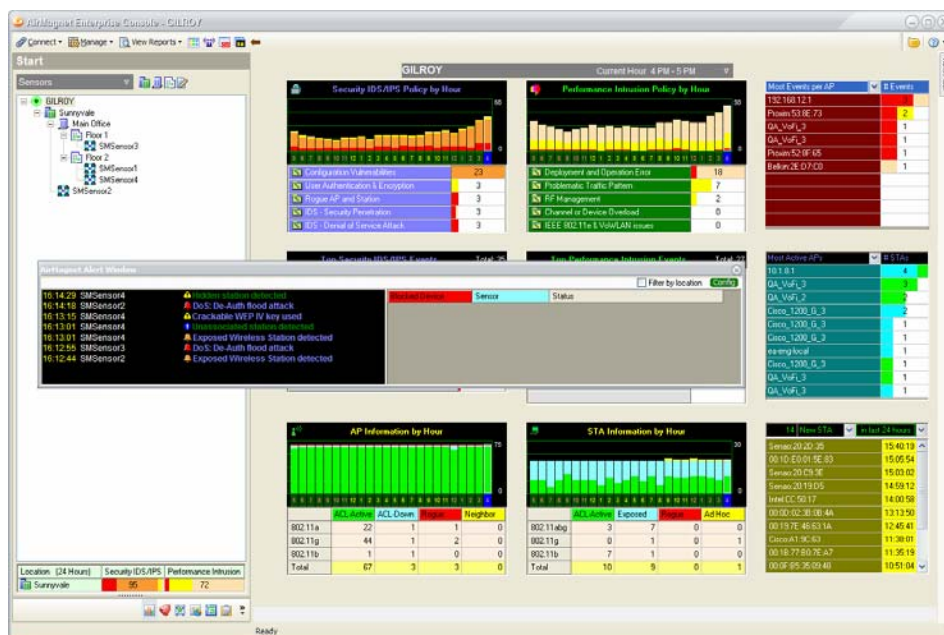


Figure 5-14: Alert Window floating on top of Start screen

Whether it is floating on top of a major screen or docked at the bottom of it, the Alert Window is a narrow scrolling window when it first appears on the screen, as shown in Figure 5-13 or 5-14. Because of this, you may not be able to see all the contents inside the window at a glance. If you want to view all the contents at once, you must stretch the Alert Window vertically by dragging either the top or the bottom edge of the window until all its contents is shown. This can be done only when the Alert Window is in a floating state. Therefore, if the Alert Window is docked at the bottom of the screen, you need to make it float first in order to stretch it. To do this, simply click the title bar of the docked Alert Window and drag it away from the bottom of the screen.

Figure 5-15 offers a close-up look at the controls contained in the Alert Window. These controls are described further in “Controls on the Alert Window” on page 135.

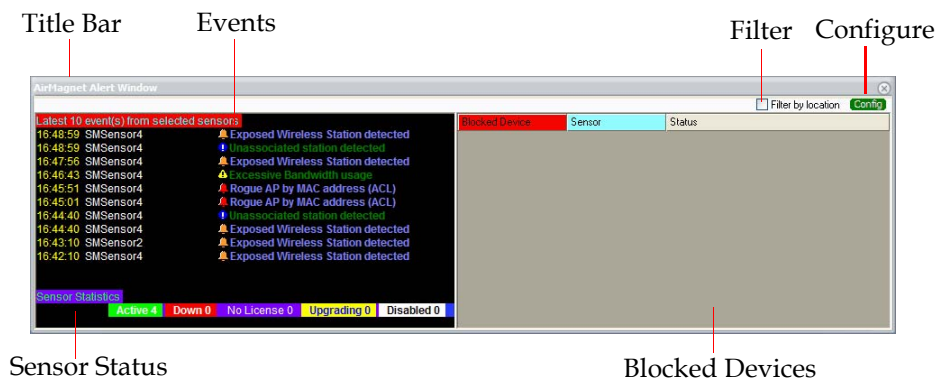


Figure 5-15: Alert Window Fields


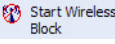
Controls on the Alert Window

As shown in Figure 5-15, the AirMagnet Alert Window contains the following components:

- **Events**—This section displays the specified number of the latest events, i.e., alarms, that have occurred on the network and are captured by the selected sensor or sensors.
- **Sensor Status**—This section shows the number of sensors in each of the five categories as described in Table 5-3.

Table 5-3: Sensor Status Options

Status	Description
Active	Sensors that are functioning properly.
Down	Sensors that have shut down or are disconnected. If a sensor goes down unexpectedly, unplugging its power and plugging it back in after 5 seconds will often remedy the problem.
No License	Sensors that do not have a license granted <i>Note: Once the AirMagnet Enterprise Server is up and running, the Sensor will automatically contact the Server for a license. The Server may grant a license to the Sensor or reject its request. If rejected, the Sensor will keep asking the Server for a license. Any Sensor in this state falls into the No License category, and cannot send any data to the Server.</i>
Upgrading	Sensors that are in the process of upgrading. <i>Note: Sensor upgrade occurs automatically each time the AirMagnet Enterprise Server is being upgraded. Since a Sensor cannot send data to the Server when it is being upgraded, you have to wait until the upgrade is completed before you can see data from the Sensor.</i>
Disabled	Sensors that are disabled. You can disable a Sensor if you do not want it to send data to the Enterprise Server. This can be done simply by right-clicking the Sensor icon in the Network Tree and deselecting (unchecking) Approve from the pop-up menu.
Upgrade Pending	Sensors that are waiting to be upgraded. Networks that utilize large sensor deployments may often limit the number of sensors that can upgrade simultaneously; the sensors that are waiting to receive the upgrade are listed here.

- **Blocked Devices**—This section lists the devices that are currently being blocked on the network. It reflects the results of the rogue-blocking actions taken on the Infrastructure screen using the  and  buttons. It identifies the blocked devices by IP or MAC address and the Sensors that are used to execute the blocking action. It also provides brief descriptions of the blocking actions.

- **Config (Configuration)** – This button opens the Alert Configuration dialog box where you can customize the display options of the Alert Window. See “Customizing Alert Window Display” on page 136.
- **Filter by Location (Check Box)** – If checked, the Alert Window displays only the data captured by the Sensor or Sensors at the selected location in the Network. Otherwise, you will see data captured by all Sensors in the network.
- **Close Button** – This button allows you to close the Alert Window with a click of the button.
- **Title Bar** – It enables you to dock or float the Alert Window by dragging it to or away from the bottom of the screen. It also allows you to move the Alert Window around by dragging and dropping it to any location on the screen.

Customizing Alert Window Display

You can customize the information displayed in the Alert Window to focus on the types of data that are most important and of the greatest concern to you.

To customize the Alert Window display:

- 1) From the Alert Window, click **Config** (Configuration). The Alert Configuration dialog box appears. See Figure 5-16.

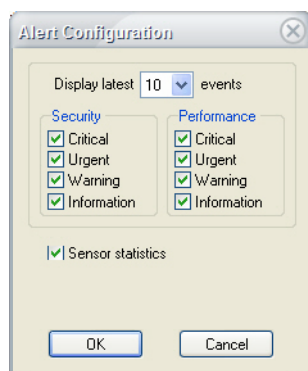


Figure 5-16: Configuring AirMagnet Alert Window

- 2) Make the selections as described in Table 5-4.

Table 5-4: Alert Window Display Options

Parameter	Description
Display latest # events	This allows you to set the number of the latest alarms that appear in the Alert Window. Click the down arrow to select a value from the drop-down list.

Table 5-4: Alert Window Display Options

Parameter	Description
Security	This allows you to specify the type or types of security alarms to be displayed in the Alert Window.
Performance	This section allows you to specify the type or types of performance alarms to be displayed in the Alert Window.
Sensor Statistics	If selected, this option allows you to have Sensor status data displayed in the Alert Window.

- 3) Click **OK**. The AirMagnet Alert Window refreshes to reflect the changes.

Chapter 6: Using the AirWISE Screen


Introduction

This chapter discusses the various sections of the AirMagnet Enterprise Console's AirWISE screen and shows how to use each of the sections to identify and solve various security and performance issues on your wireless network.

Uncontrolled and unplanned addition of wireless devices to a corporate network has always been a security concern for network administrators because such devices could inadvertently expose the entire network to external intrusions and attacks. The AirWISE expert analysis engine is a very important component of the AirMagnet WLAN Enterprise solution. It can automatically identify more than 120 security and performance violations on a WLAN and generate alarms in real time according to pre-defined policies. *See Chapter 11: "Managing Policy Profiles".*

As a wireless performance and security monitoring platform, AirWISE can help network administrators in the following ways:

- Automatically collecting network performance data;
- Identifying and tracking wireless devices and their distinguishing characteristics;
- Monitoring and analyzing the health of a WLAN;
- Providing context-driven advice for problem resolution;
- Allowing network administrators to manage the entire WLAN right from AirMagnet Enterprise Console.

You can navigate to the AirWISE screen from any of the other screens by clicking  on the Navigation Bar.

Major UI Components

The AirWISE screen has several major screen components, as indicated in Figure 6-1

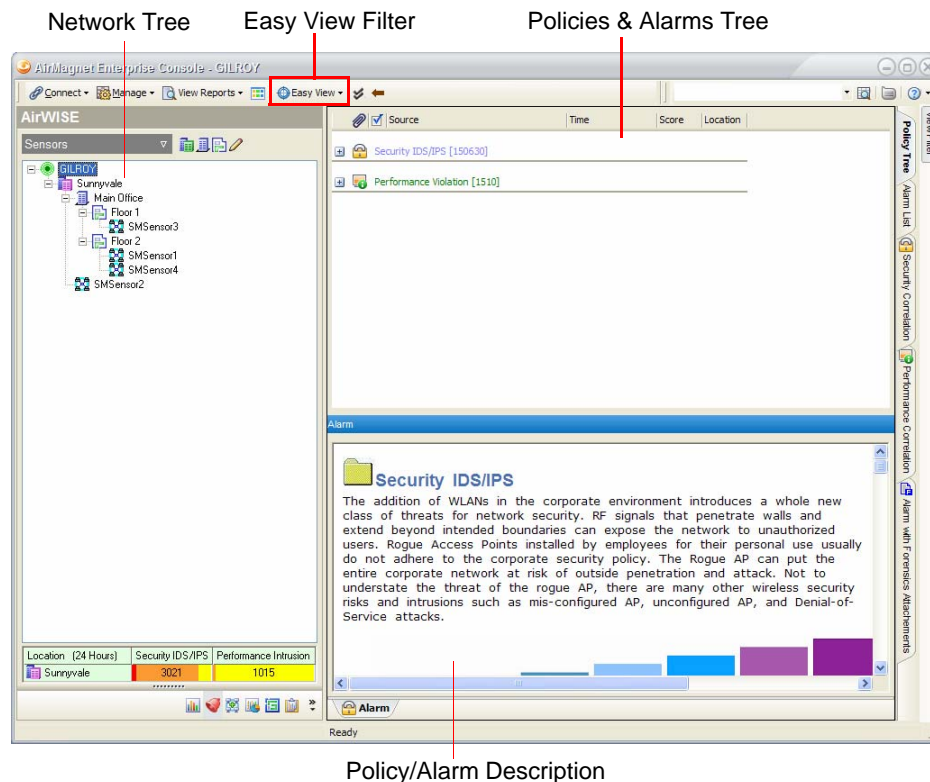


Figure 6-1: AirWISE Location-Policy screen


The Network Tree has been described in Chapter 4, but the remaining portions are unique to the AirWISE screen. Each portion of the screen is described in the following sections of this chapter.

Easy View Options

The Easy View filter located at the top of the screen allows the user to automatically filter the AirWISE display according to the present need.

Note that the tabs located on the right-hand side of the AirWISE screen match the options contained within the Easy View category currently selected. Thus, when a Security View is selected, the other Security Views are shown as tabs along the side.

To access Easy View options:

- 1) Click the  Easy View button in the Console's toolbar. The Easy View drop-down list appears. See Figure 6-2.

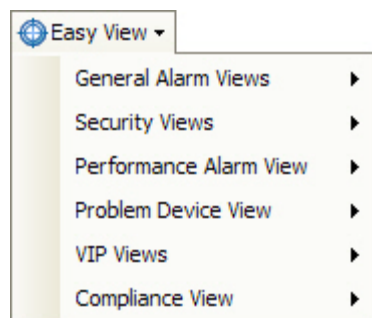


Figure 6-2: AirWISE Easy View Categories

- 2) Select the desired Easy View option. The AirWISE screen refreshes.

The following sections describe the different Easy View categories.

General Alarm Views

The General Alarm Views category contains options that correspond to the default view tabs located along the right-hand side of the AirWISE screen. These viewing options use the default View Filter selections, and therefore the most comprehensive view of alarm data among the various viewing options. Table 6-1 describes each General Alarm selection.

Table 6-1 General Alarm View Options

View	Description
Policy Tree	The default view upon navigating to the AirWISE screen. This option lists alarms by policy; expanding the tree reveals detailed information about each alarm. The sum of all alarm scores within each category is displayed in brackets alongside the category title.
Alarm List	Displays a list of all alarms currently detected on the enterprise network. This view allows users to easily display and sort alarms based on alarm score in order to remedy critical alarms immediately.
Security Correlation	Displays a list of all security violations on the enterprise network. These alarms are summed up in a bar chart that provides an easy view of the total score in each major category. As alarms are acknowledged, the chart refreshes with new totals.

Table 6-1 General Alarm View Options

View	Description
Performance Correlation	Displays a list of all performance violations on the enterprise network. These alarms are summed up in a bar chart that provides an easy view of the total score in each major category. As alarms are acknowledged, the chart refreshes with new totals.
Alarms with Forensics Attachments	Displays all alarms that have forensics (either 802.11 or spectrum) attachments.

Security Views

The Security Views list provides several different options that filter and display alarms specific to security violations on the network. These selections allow the user to easily focus on security issues related to specific categories, rather than having to sift through combined security and performance violations. Table 6-2 describes each Security View option.

Table 6-2 Security View Options

View	Description
Top Security Alarms	Displays all security alarms detected on the network, sorted from highest to lowest score.
VIP Security Alarms	Displays all security alarms related to VIP devices.
Top AP with Security Alarms	Displays all security alarms triggered by APs, sorted from highest to lowest score.
Critical Security Alarms	Displays all critical-level security alarms.
Urgent Security Alarms	Displays all urgent-level security alarms.
Security Alarms by Category	Displays all security alarms listed by their policy categories.
Top Floors with Security Alarms	Displays all security alarms by floor.

Performance Alarm Views

The Performance Alarm Views filter the display to show only performance alarms, sorted by various criteria. Each selection in the list allows the user to focus on performance-related issues, eliminating the need to manually sift out security alarms. Table 6-3 describes each Performance Alarm View.

Table 6-3 Performance Alarm View Options

View	Description
Top Performance Alarms	Displays all performance alarms detected on the network, sorted from highest to lowest score.
VIP Performance Alarms	Displays all performance alarms related to VIP devices.
Top APs with Performance Alarms	Displays all performance alarms triggered by APs, sorted from highest to lowest score.
Critical Performance Alarms	Displays all critical-level performance alarms.
Urgent Performance Alarms	Displays all urgent-level performance alarms.
Performance Alarms by Category	Displays all performance alarms listed by their policy categories.
Top Floors with Performance Alarms	Displays all performance alarms by floor.

Problem Device Views

The Problem Device Views filter the display to show only device-related alarms (excluding those that are channel-specific or have other sources). Each selection in the list allows the user to view device alarms sorted by different criteria. Table 6-4 describes each view.

Table 6-4 Problem Device View Options

View	Description
Alarms by Type	Displays a list of alarm types. Each entry can be expanded to reveal the devices triggering the alarm.
Top Problem Devices	Displays a list of all devices triggering alarms, sorted by score. Each entry can be expanded to reveal the alarms triggered by the device.

Table 6-4 Problem Device View Options

View	Description
Top Security Problem Devices	Displays a list of all devices triggering security alarms, sorted by score.
Top Performance Problem Devices	Displays a list of all devices triggering performance alarms, sorted by score.

VIP Views

The VIP Views filter the display to show information specifically about devices flagged as VIPs. This allows the user to focus primarily on devices of the utmost importance to the enterprise network; since these issues should be resolved as soon as possible, the VIP Views provide a means of quickly identifying and fixing problems with important devices. Table 6-5 describes each view.

Table 6-5 VIP View Options

View	Description
VIP Alarms	Displays all VIP devices with alarms detected.
VIP Security Alarms	Displays all VIP devices with security alarms.
VIP Performance Alarms	Displays all VIP devices with performance alarms.
VIP Devices with Security by Floor	Displays VIP devices with security alarms, sorted by floor.
VIP Devices with Performance by Floor	Displays VIP devices with performance alarms, sorted by floor.

Compliance Views

The Compliance Views filter the displayed alarms to allow the user to view only the alarms that affect the enterprise network's compliance with a specific standard. The compliance type can be specified using the Server tab in Enterprise Console's configuration (for more details, see "Server Settings" on page 252). Table 6-6 describes each view option.

Table 6-6 Compliance View Options

View	Description
Compliance Alarms by Section	Displays all compliance violations, arranged by section of the compliance regulation.

Table 6-6 Compliance View Options

View	Description
Compliance Alarms by Device	Displays all compliance violations, arranged by device.
Compliance Violating APs	Displays all compliance violations caused by APs.
Compliance Violating Stations	Displays all compliance violations caused by stations.

Policies & Alarms Tree

The Policies & Alarms Tree displays the various AirWISE policies and the alarms detected on the network. Users can easily navigate through the tree structure to find information on the specific policy in question. The alarm table structure provides detailed data for each alarm. See Figure 6-3.






Source	Time	Score	Location
Proxim:52:8F:64	10/11 08:36:26	1000	\GILROY\Sunnyvale\Main Office\Floor ...
Airespace:79:03:C0	10/11 08:42:55	1000	\GILROY\Sunnyvale\Main Office\Floor ...
Aruba:C2:34:F0	10/11 08:36:17	1000	\GILROY\Sunnyvale\Main Office\Floor ...
Aruba:C2:34:F1	10/11 08:40:11	1000	\GILROY\Sunnyvale\Main Office\Floor ...
Proxim:53:8E:72	10/11 08:18:42	1000	\GILROY\Sunnyvale\Main Office\Floor ...

Figure 6-3: Policy/Alarm Tree

You can expand all security or performance policies by right clicking the Security IDS/IPS or Performance Violation entry and then selecting Expand All from the pop-up menu. Or you may expand a specific policy by right-clicking the policy folder and then selecting Expand All from the pop-up menu. You can also collapse an expanded policy by right-clicking it and then selecting Collapse All from the pop-up menu.

As shown in Figure 6-2, the Policies & Alarms tree contains several descriptive columns that provide information about each alarm. Table 6-7 describes each column and its purpose.

Table 6-7 Policies & Alarms Tree Columns

Column	Description
Attachment	<p>This column displays a color-coded icon for alarms that have stored forensic information. These icons vary depending on the type of forensic data stored:  (blue) represents standard 802.11 data stored,  (pink) represents spectrum forensic data, and  (both) means that both 802.11 and spectrum forensic data are available.</p> <p>Users can double-click the icon to view the forensic data. Double-clicking any other column opens up a Remote Analyzer session with the sensor that detected the alarm.</p>
Acknowledge	<p>Check the box in this column to acknowledge the selected alarm. Acknowledged alarms will vanish from the list unless the “Show Acknowledged” option is checked in the View Filter tab.</p>
Alarm Description	<p>This column displays the title for the selected alarm. The alarm descriptions are color-coded depending on the type of alarm: Security IDS/IPS alarms are displayed in blue text whereas Performance Violations are displayed in green.</p> <p><i>Note: This column does not appear when the Policy Tree tab is selected.</i></p>
Source	<p>This column displays information about the device causing the alarm. The field is divided into two components:</p> <ul style="list-style-type: none"> The Device Type icon is color- and letter-coded to help users quickly recognize the device’s media type and band. Device icons display the media type letter (a, b, or g) on top of a color-coded icon. The icon is green () for devices utilizing the 2.4GHz band and blue () for the 5GHz band. The device name is displayed following the icon. This name generally consists of the device’s vendor name followed by the last three portions of its MAC address. <p><i>Note: If the source is a channel, the channel number is displayed.</i></p>
Time	<p>The Time field displays the time at which the alarm was generated. This field is color-coded according to the alarm’s severity: Light orange corresponds to Information alarms, yellow to warnings, orange to urgent, and red to critical-level alarms.</p>
Score	<p>This column displays the score associated with the alarm. Any alarm’s score can be customized using the Score Wizard in the Policy Manager.</p>
Location	<p>This column displays the location of the sensor that detected the selected alarm. If multiple sensors detected the device, the sensor with the strongest signal strength for the device triggering the alarm is displayed.</p>

Policy/Alarm Description

The Policy/ Alarm Description portion of the screen provides specific details for the selection made in the Policies & Alarms Tree. When a policy or policy category is selected, a detailed description of the selection is displayed in the Policy/ Alarm Description section. This information can help the user identify and repair problems on the enterprise network. See Figure 6-4.

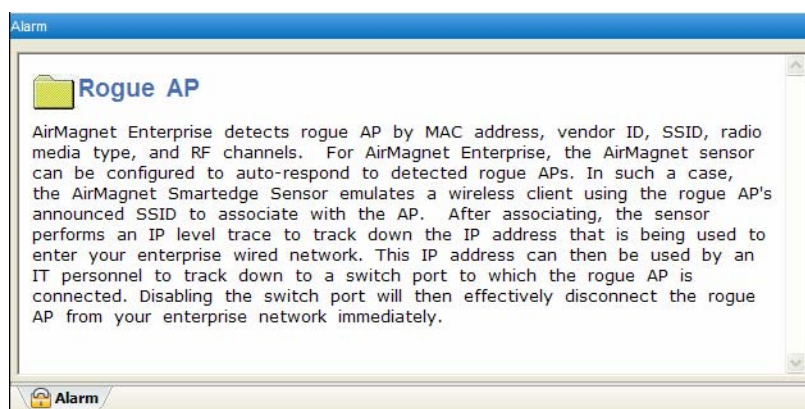


Figure 6-4: A Sample Policy Category Description

When a specific alarm is selected, this section provides a series of tabs that each contain detailed information for the device triggering the alarm. These tabs are described in greater detail in the following sections.

Alarm Tab

The Alarm Tab is the default tab when an alarm is selected. It provides details about the alarm itself, including the number of occurrences detected, notifications associated with it, and any forensics attachments. See Figure 6-5.

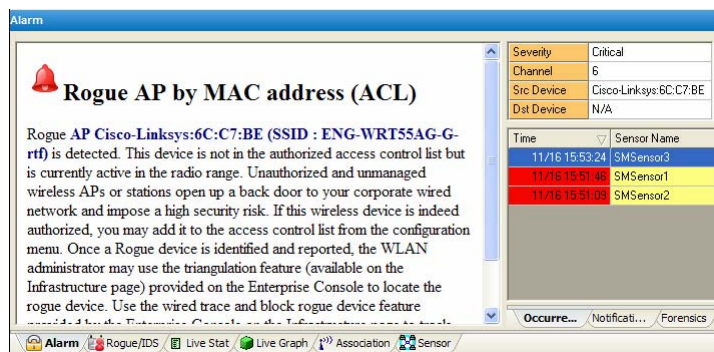


Figure 6-5: Alarm Tab Information

As shown in Figure 6-4, the Alarm tab is divided into two portions: the left-hand side contains a detailed description about the alarm selected. This provides information about the device that caused the alarm as well as recommended means of resolving the problem.

The right-hand side of the tab contains a table that shows the device's channel as well as the severity of the alarm. The information below the table is composed of three tabs, as described in Table 6-8.

Table 6-8 Alarm Information Tabs

Tab	Description
Occurrences	This tab lists all detected occurrences of the alarm associated with the device. The table provided shows the time of the alarm and the sensor that detected it.
Notifications	The Notifications tab lists all notifications that are triggered as a result of the selected alarm.
Forensics	The Forensics tab lists any forensics attachments for the selected alarm. Users can double-click forensic files to view the stored data.

Live Stats

The Live Stat Tab displays detailed information regarding the selected device in real time. These statistics can help users diagnose and troubleshoot the selected device. See Figure 6-6.

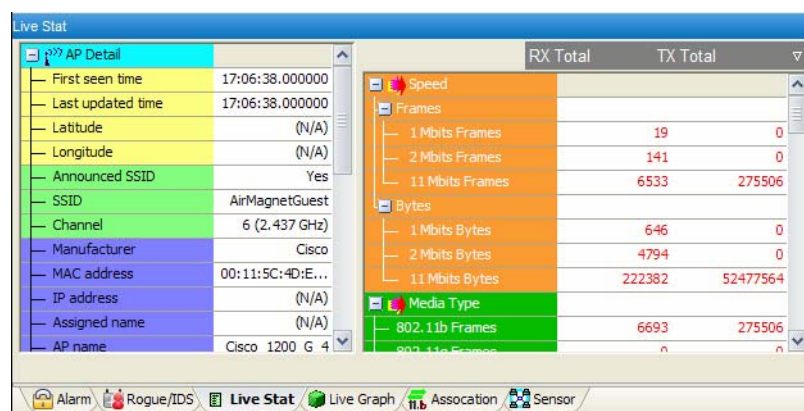


Figure 6-6: Live Statistic Information

As shown above, the Live Stat tab contains two major sections: AP/Station Details on the left and packet statistics on the right. These sections are briefly described in Tables 6-11 and 6-12, respectively.

Table 6-9 AP/Station Details

Field	Description
First Seen Time	The first time the device was detected.
Last Updated Time	The last time the device information was updated.

Table 6-9 AP/Station Details

Field	Description
Announced SSID	Displays “Yes” if the selected AP broadcasts its SSID. <i>This field does not appear when a station is selected.</i>
SSID	The SSID used by the device.
Channel	The channel and band that the device is operating on.
Manufacturer	The name of the device’s manufacturer.
MAC Address	The device’s MAC address.
IP Address	The IP address detected for the device (if available).
Assigned Name	The name assigned to the device (if available). This name can be specified using the Infrastructure screen.
AP/STA Name	The broadcast name of the AP or station selected.
WEP	Displays “Enabled” if the device is using WEP encryption.
WPA Type	Displays the type of WPA encryption (if any) in use by the device.
802.1X EAP Type	Displays “Enabled” or “Disabled”, depending on the status of 802.1X EAP on the selected device.
TKIP/MIC	Displays “Yes” if TKIP/MIC is enabled for the device.
VPN/Type	
Auth. Algorithm	Displays whether open or shared key authentication is used for the device. This field shows “unknown” if the algorithm cannot be determined.
PCF/DCF	Displays whether PCF (Point Coordination Function) or DCF (Distributed Coordination Function) is implemented on the device. PCF and DCF are collision avoidance algorithms designed to reduce unnecessary network traffic.
RTS/CTS	Displays “Yes” if the RTS/CTS (Request to Send/Clear to Send) function is enabled on the selected device. This function can help alleviate collisions and retransmissions.
Channel Agility	Displays “Yes” if channel agility is enabled on the selected AP. Channel Agility is a function on APs from certain vendors that can theoretically reduce adjacent channel interference. <i>This field does not appear if a station is selected.</i>
Rate Supported	Lists the transmission rates detected from the device. The rates are listed in terms of Mbps.
Ext. Rate Support	Lists the rates supported by the device that have not been detected thus far.
Network Mode	The network mode enabled on the selected device (Infrastructure, Ad-Hoc).

Table 6-9 AP/Station Details

Field	Description
Preamble Mode	Displays whether a “long” or “short” preamble mode is active on the device.
# STA	Displays the number of stations associated to the selected AP. <i>This field does not appear if a station is selected.</i>
Beacon Missed %	The percentage of missed beacons recorded by the AP. <i>This field does not appear if a station is selected.</i>
Cell Power, dBm	The power of the AP listed in dBm. <i>This field does not appear if a station is selected.</i>

Table 6-10 Packet Statistics

Field	Description
Speed	The sections listed in the Speed tree display statistics about the number of frames or bytes detected at various speeds from the selected device.
Media Type	The Media Type sections display statistics about the number of frames or bytes detected in each media type supported by the device.
Alert	The Alert section displays all alert packets detected. These packets include transmission errors, reassociation failures, and timeouts.
Frames	The Frames tree displays the types and number of frames detected from the selected device. These frames are grouped into Control Frames, Management Frames, Data Frames, and Other Frames.

Live Graphs

The Live Graph tab can display various graphs that allow the user to gain a visual idea of the selected device's performance. By default, the graph displays Signal/Noise data for the selected device. See Figure 6-7.

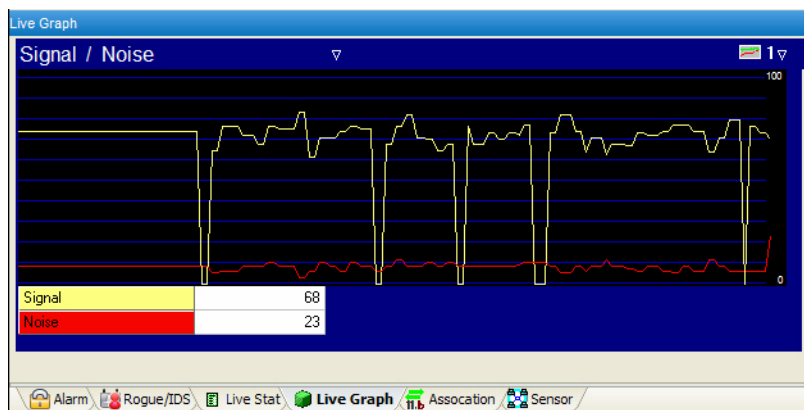


Figure 6-7: Live Graph Tab

The user can adjust the graph display to show different statistics using the drop-down menu located at the top-left. See Figure 6-8.

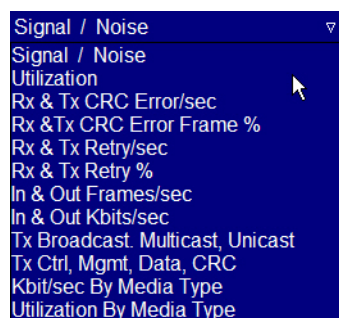


Figure 6-8: Graph Options

Additionally, users can display up to four different graphs at the same time by using the drop-down located at the top-right.

Association Tab


The Association tab displays the association history for the selected device. Consequently, its contents will vary depending on whether an AP or a station is selected. For a station, the tab displays information about any APs the device has attempted to associate to in the past. For an AP (shown in Figure 6-9), the tab shows any stations that have attempted an association with the device selected.

90:27:E4:0D:6E:03	WEP	02/25/2011 17:59:54	02/25/2011 17:59:54
90:27:E4:0D:6E:03	WPA2-P	02/25/2011 17:54:27	02/25/2011 17:56:54
90:27:E4:0D:6E:03	WPA2-P	02/25/2011 17:58:25	02/25/2011 17:59:06
90:27:E4:0D:6E:03	WPA2-P	02/25/2011 17:53:04	02/25/2011 17:58:18
90:27:E4:0D:6E:03	WPA2-P	02/25/2011 17:49:27	02/25/2011 17:54:01
90:27:E4:0D:6E:03	WPA2-P	02/25/2011 17:56:34	02/25/2011 17:57:21
90:27:E4:0D:6E:03	?	02/25/2011 17:56:49	02/25/2011 17:56:49

Figure 6-9: AP Association History

The Association tab contains several informative columns to provide details about each association attempt. These columns are described in Table 6-13.

Table 6-11 Association History Columns

Column	Description
Device Display Name	The name of the device (generally the device's vendor ID followed by the end of its MAC Address).
 (Encryption)	The method of encryption used by the device.
Start Time	The time when the association was started.
End Time	The time when the association was ended.
Location	The location of ...

Sensor Tab

The Sensor tab lists all sensors that have detected the selected device, as well as their locations, last time the device was detected, and signal strength detected from the device. See Figure 6-10.

Sensor Name	Signal Strength	Last Signal Time	Location
SMSensor2	-68	11/16 15:52:54	\\GILROY\Sunnyvale\SMSensor2
SMSensor4	-66	11/16 16:00:53	\\GILROY\Sunnyvale\\Main Office\\Floor 2\\SMSensor4
SMSensor3	-59	11/16 15:54:54	\\GILROY\Sunnyvale\\Main Office\\Floor 1\\SMSensor3
SMSensor1	-65	11/16 15:53:07	\\GILROY\Sunnyvale\\Main Office\\Floor 2\\SMSensor1

Figure 6-10: Sensor Tab Information

Table 6-12 Sensor Tab Columns

Columns	Description
Sensor Name	The name of the sensor (generally the device's vendor followed by the end of its MAC Address).
Signal Strength	Displays the signal strength in dBm
Last Signal Time	Displays the last signal time recorded for the sensor.
Location	MAC address of sensor or starts with server MAC address, name of sensor, city, building etc.
Device Distance to Sensor	Displays approximate distance of sensor to AP device using signal strength.

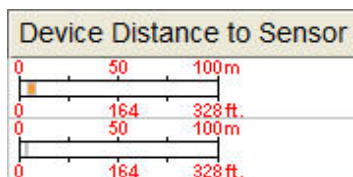


Figure 6-11: Device Distance to Sensor

Using Forensics Information

AirMagnet's built-in forensics system creates a trace file on the server that stores information regarding specific violations that have come up. Thus, you can use these data to analyze past events and compare them with current ones, or simply review what has happened on your network. You can access your stored forensics data by clicking **Easy View>General Alarm Views>Alarms with Forensics Attachments**.


Activating Forensic Logging

Before AirMagnet Enterprise will log any forensics data, you must activate forensics notifications in your policies list. This process consists of two steps, as described in the following sections.

Adding Forensics Notifications

The user must first activate forensics notifications on the Enterprise Server before the notifications can be applied to specific alarms.

To add forensics notifications:

- 1) From the Enterprise Console, click **Manage>Server Options....** The Manage Server Configuration window appears.
- 2) Click the Notifications tab to view the notifications currently on the server.
- 3) Click  (Add New Notification) to bring up the Notification Type Selection dialog box.
- 4) Select Forensics and click OK. Follow the instructions under "Configuring Forensics Notifications" on page 273 to finish setting up the notification.

It is recommended that users configure standard (802.11) forensic notifications for Security-related alarms and Spectrum forensics for Performance alarms.

Configuring Forensics Notifications on Specific Alarms

Now that the forensic notification option has been added to the Enterprise Server, the user must select the specific alarms that will trigger a forensics notification.

To configure forensics notifications:

- 1) From the console, click **Manage>Policy Profiles....**
- 2) Double-click the policy on which forensics notifications will be configured. The Policy Management window appears.
- 3) Click the Notification Wizard button to access the Notification selection page.
- 4) Check Forensics Notification and click Next.
- 5) Browse through the policy selection page and check the alarms you wish to save as forensic files.
- 6) Use the severity drop-down list to specify the notification severity that the forensic notification should apply to. In general, forensics notifications are considered critical, as they should usually be restricted to alarms that threaten network security.

Important: Be aware that storing forensics files will utilize system resources (CPU and memory) extensively. To avoid consuming the server's processing capacity, you must limit the number of total forensic alarms for the system. The ideal total forensic alarms count should not exceed five.

- 7) Click Next, and then Finish.

Viewing Forensics Data

Users can easily view forensics attachments by navigating to the Alarms with Forensics Attachments option from the Easy View. A list of all forensics files currently saved on the server is displayed. See Figure 6-12.

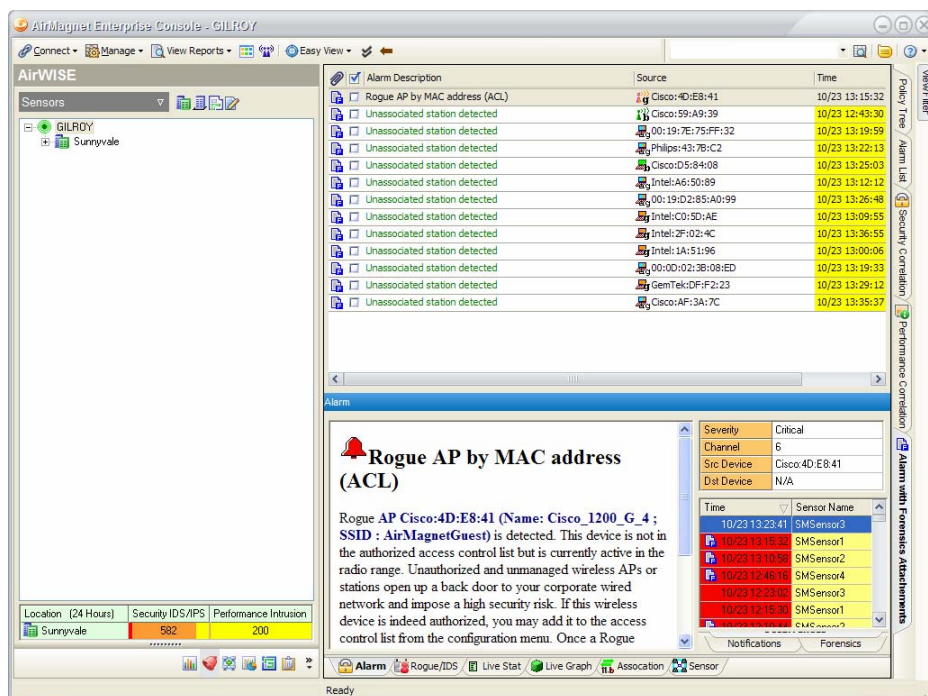


Figure 6-12: AirWISE Forensics screen

To view forensics data:

- 1) From the Alarms with Forensics Attachments view, double-click the  (Forensic File) icon beside the file to be opened.

Note that the forensic file can be opened from the icon located in the Policy/Alarm Description area as well as the icon in the Policies & Alarms tree.

- 2) The forensics log appears. See Figure 6-13.

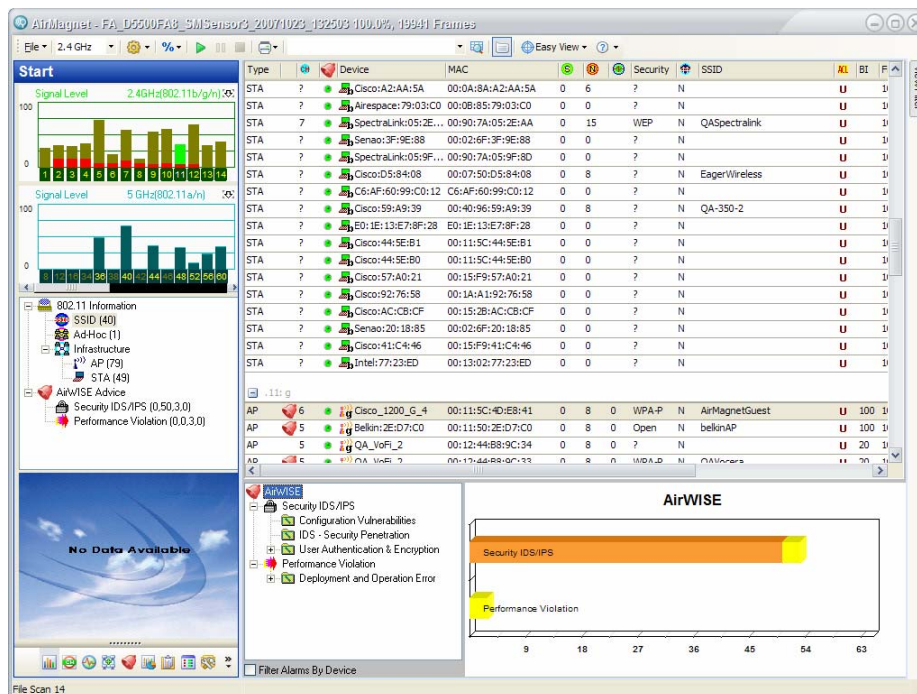



Figure 6-13: Forensics Evidence File

- 3) You can now browse through the detailed information using the Remote Analyzer interface.

Chapter 7: Using the Infrastructure Screen

Introduction

The AirMagnet Enterprise Console's Infrastructure screen shows detailed information about all the wireless real estate on your network, such as APs, STAs, and SSIDs. You can view your wireless assets at any location of your WLAN. Not only does it show what assets you have, but also tells where they are deployed. You can even check against a policy to see who is violating it and where.

You can navigate to the Infrastructure screen from any of the other screens by clicking  **Infrastructure** on the Navigation Bar.

Major Components of the Infrastructure Screen

The Infrastructure screen has several major screen components, as indicated in Figure 7-1.

Network Tree Easy View Filter Device Management Tools Device List

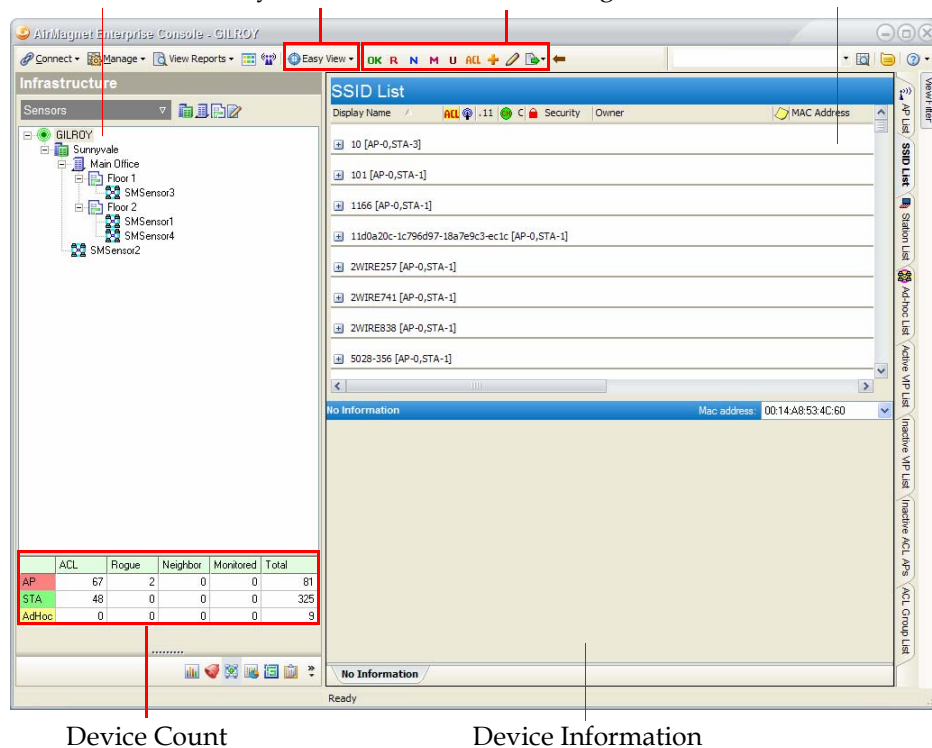


Figure 7-1: Infrastructure location tree screen

The Infrastructure screen can be divided into three major sections: the Network Tree, the Device List, and Device Information.

The Infrastructure screen delivers a whole wealth of information in great detail about your wireless assets and various options for viewing and managing data. The following sections discuss the major portions of the Infrastructure screen and their functions.

Network Tree

The Network Tree portion of the Infrastructure screen works in the same manner as it does on other screens. However, it also contains a brief summary of the devices currently detected on the network, as indicated in Figure 7-1. See Figure 7-2 for a more detailed image.

	ACL	Rogue	Neighbor	Monitored	Total
AP	150	1	0	0	199
STA	55	0	0	18	370
AdHoc	0	0	0	0	15

Figure 7-2: Device Summary


As shown above, the device summary simply lists the total number of APs, Stations, and Ad-Hoc devices in each ACL category. This can provide the user with a quick reference to determine whether any problems have occurred on the network that require closer inspection.

Easy View Options

The Easy View filter located at the top of the screen allows the user to automatically filter the Infrastructure display according to the present need.

Note that the tabs located on the right-hand side of the Infrastructure screen match the options contained within the Easy View category currently selected. Thus, when a Rogue View is selected, the other Rogue Views are shown as tabs along the side.

To access Easy View Options:

- 1) Click the  Easy View button in the Console's toolbar. The Easy View drop-down list appears. See Figure 7-3.

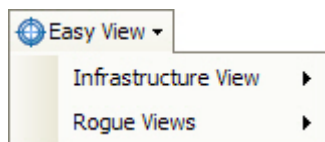


Figure 7-3: Infrastructure Easy View Categories

- 2) Select the desired Easy View option. The Infrastructure screen refreshes.

The following sections describe the different Easy View categories.

Infrastructure View

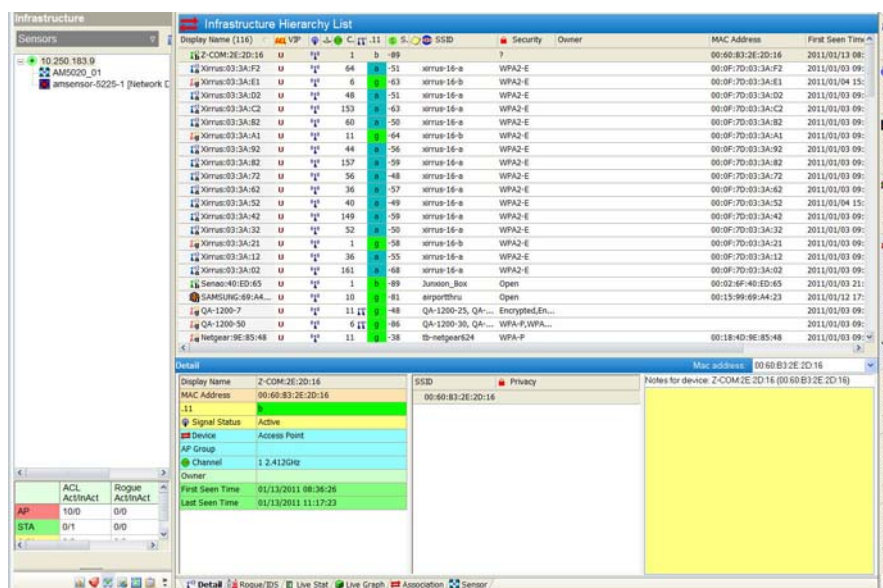
The Infrastructure Views provide quick access to device lists, allowing the user to filter the display to show only the devices of interest. Table 7-1 describes each Infrastructure View selection.

Table 7-1: Infrastructure View Options

View	Description
AP List	Displays a list of all APs detected on the network.
SSID List	Displays a list of all SSIDs detected on the network. Each SSID may be expanded to view the devices utilizing it.
Station List	Displays a list of all stations detected on the network.
Ad-Hoc List	Displays a list of all Ad-Hocs detected on the network.
Infrastructure Hierarchy List	Displays a list of all devices and their associated stations detected on the network.
Active VIP List	Displays a list of all VIP devices active on the network.
Inactive VIP List	Displays a list of all VIP devices inactive on the network.
Inactive ACL APs	Displays a list of all valid APs that are currently inactive.
ACL Group List	Displays a list of all ACL Groups in use on the network. Each group can be expanded to view the devices classified in it.

Infrastructure Hierarchy List Tab

The Infrastructure View Options now includes a new tab. It provides details on all devices and ethir associated stations. The usual ACL status Field which categorizes devices appears as well. All other fields which are present in other tabs are also available in this new tab.



Rogue View

The Rogue Views allow the user to filter the displayed devices to show only those marked as rogues on the enterprise network. This feature can help network administrators focus specifically on devices that are or may be hazards to network security without having to manually sort through valid known devices as well. Table 7-2 describes each Rogue View selection.

Table 7-2: Rogue View Options

View	Description
All Rogue Devices	Displays all rogue devices detected on the network.
Rogue APs	Displays all rogue APs detected on the network.
Rogue Stations	Displays all rogue stations detected on the network.
Rogue Ad-Hoc	Displays all rogue Ad-Hocs detected on the network.
Active Rogue Devices	Displays all rogue devices currently active on the network.
Traced or Blocked Devices	Displays all devices that have been traced or blocked.

Table 7-2: Rogue View Options

View	Description
Monitored Devices	Displays all devices currently marked to be monitored.

Note that although Monitored devices are not actually rogues, they do appear when the Rogue View options are selected.

Device Management Tools

The Infrastructure screen's toolbar contains some very useful buttons for managing the network's wireless assets. This section describes each button and its purpose for assisting network administrators manage the devices found on the network. Note that this section describes those buttons unique to the Infrastructure screen; for the tools common to all screens, see [“The Toolbar” on page 76](#). Figure 7-4 displays the Infrastructure tools.

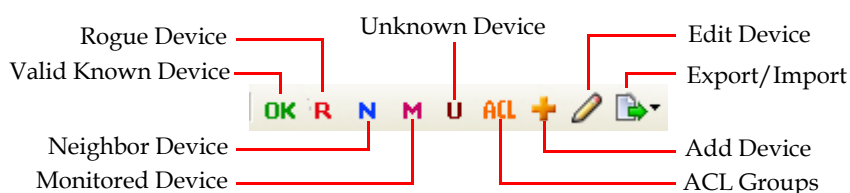








Figure 7-4: Managing tools on Infrastructure screen

These buttons allow you to properly categorize and tag the devices detected by AirMagnet Enterprise on your enterprise network. Table 7-3 briefly describes these tools and how to use them to effectively manage wireless devices.


Table 7-3: Infrastructure Screen Tools

Tool	Description
OK (Set as Valid Known Device)	Sets the selected device as a valid known device. Valid devices are those that are known and permitted on the enterprise network.
R (Set as Rogue Device)	Sets the selected device as a rogue. Rogue devices are those that may be malicious, and therefore must be watched closely.
N (Set as Neighbor Device)	Sets the selected device as a neighbor. Neighbor devices are those that are known to exist in a neighboring environment, such as an adjacent business/network.


Table 7-3: Infrastructure Screen Tools

Tool	Description
 (Set as Monitored Device)	Sets the selected device as a monitored device. Monitored devices are those that should be watched but are not known to be threatening enough to be considered rogues. This flag is also useful for users who wish to track down a device that appears sporadically on the network.
 (Set as Unknown Device)	Sets the selected device as unknown. By default, all new devices are considered unknown until the network administrator adjusts them or a device classification rule is applied.
 (ACL Groups)	Opens the Manage ACL Groups dialog box, which allows the user to add, remove, or modify ACL groups on the Enterprise Server. See “ Managing ACL Groups ” on page 87 for more information.
 (Add Device)	Opens the Add New Device dialog box, which allows the user to manually add a new device to the network. This is useful for users who wish to apply an ACL group and device classification for a device that has not been deployed on the network yet.
 (Edit Device)	Opens the Edit Device dialog box, which allows the user to adjust properties of an existing device.
 (Export/Import)	Allows the user to export or import an ACL for backup purposes.


Importing and Exporting ACL Data


The  (Export/Import) button allows you to easily import or export ACL files for your enterprise network. This helps you to share or back up your ACL data.

The ACL files you import or export must be in text format (.txt).


If you have an ACL file stored on a local machine or your enterprise network, you can easily import it to AirMagnet using the  (Export\Import) button on the AirMagnet Enterprise Console’s Infrastructure screen. This not only enables you to make full use of your existing resources, but also saves your the time and effort you would otherwise have to spend creating ACLs from scratch.

To import an ACL file:

- 1) From the AirMagnet Enterprise Console’s Infrastructure screen, click  (Export\Import) and select Import. The Import ACL dialog box appears.
- 2) Locate the ACL file on a local machine or on your enterprise network and click Open.

If you want to share your current ACL file or have a back-up copy of it just in case something unexpected happens that may cause the loss of the data, you can export the file using the  (Export\Import) button.

To export an ACL file:

- 1) From the AirMagnet Enterprise Console's Infrastructure screen, click  (Export\Import) and click Export. The Export ACL dialog box appears.
- 2) Select a destination, name the file, and click Save.

The file saved can be opened with a text editor and has nine columns of data. They are, from left to right:

- MAC address - Media Type
- SSID
- Node Type (0 = Unknown; 1 = in ACL; 2 = rogue; 4 = neighbor; 8 = monitored device)
- Alias
- Device name
- ACL expiration time
- Owner
- Notes
- ACL Group Name

Device List

The Device List contains a brief table describing the devices detected within the enterprise network. The display varies depending on the view selected in the Easy View drop-down. Figure 7-5 shows a sample AP List view.



















AP List							
Display Name (162)	ACL	VIP			.11	S	SSID
 Xirrus:09:EE:F1	U		9	g	-68		xirrus-b
 Xirrus:09:EE:E0	U		48	n	-52		xirrus-a
 Xirrus:09:EE:D1	U		11	g	-48		xirrus-b
 Xirrus:09:EE:C0	U		56	a	-52		xirrus-a
 Xirrus:09:EE:B1	U		6	g	-28		xirrus-b
 Xirrus:09:EE:A0	U		?	g	-46		xirrus-a
 Xirrus:09:EE:A0	U		161	a	-53		xirrus-a
 Xirrus:09:EE:91	U		1	g	-44		xirrus-b
 Xirrus:09:EE:80	U		64	a	-54		xirrus-a

Figure 7-5: AP List View

As shown above, the Device List generally contains a number of informative columns that summarize information about each device. These columns are described in Table 7-4.

Table 7-4: Device List Columns


















Column	Description
Display Name	This column displays the names of the WLAN components, i.e., SSIDs, access points, stations, or Ad-hoc stations detected by AirMagnet SmartEdge Sensors.
 (ACL Status)	This column indicates the ACL status of the WLAN devices: <ul style="list-style-type: none">  – Valid Known Device  – Neighbor Device  – Monitored Device  – Rogue Device  – Unknown Device
VIP	This column indicates displays a  for devices flagged as VIPs.
 (RF Signal)	This column indicates the operating status of the WLAN devices, i.e., access points, stations, and ad-hoc stations. <ul style="list-style-type: none">  – The device is active.  – The device is inactive.
 (In Network)	This column indicates whether or not the device has been traced within the enterprise network. This will only display information if tracing is configured. If the device has been located within the network, a  (In Network) icon is displayed.
 AHC Results	Indicates that AHC (Automated Health Check) has run for this AP and there are results available.
 (Channel)	This column shows the RF channels the devices are using as indicated by the channel numbers.
.11	This column indicates the 802.11 media type the device is using, i.e., 802.11a/b/g. The field is color-coded to show the device's band: 2.4GHz devices are displayed with a green background and 5GHz devices are shown with blue.
 (Notes)	This column allows you to add notes about the devices. Double-clicking in this column will bring up a note screen where you can enter a short note about a device. Right-clicking the note screen will open a pop-up screen that allows you to manage the note in a number of ways.
 (SSID)	This column shows the names of the SSIDs to which the network devices belong. It appears only when AP, STA, or Ad hoc Lists are selected in the primary filter.
 (Security)	This column displays the security mechanism employed by the device, i.e., Open, WEP, 802.1x, or WPA/WPA2 (Enterprise or Personal).



Table 7-4: Device List Columns

Column	Description
Owner	This field shows the names of the owners of the network devices, if such information is configured. It helps keep track of all devices in the enterprise network. You can specify the owner of a device by right-clicking the device and selecting Edit Device... or Add New Device... from the pop-up menu, and then entering the owner's in dialog box.
MAC Address	This column displays the MAC address of the device.
AP Group	This column displays the AP Group that the device belongs to (if any).
First Seen Time	This column shows the time at which the device was first detected.
Last Seen Time	This column shows the most recent time at which the device was detected.


Device Information

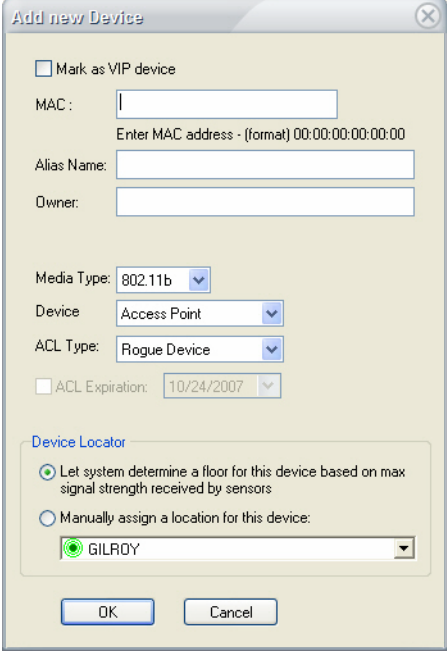
The Device Information section contains detailed information about the device selected in the Device List. As this area is nearly identical to the Policy/Alarm Description on the AirWISE screen, users can browse through these data in the same manner as described in the previous chapter. See [“Policy/Alarm Description” on page 147](#) for more details.

Adding Devices to the Device List

By default, AirMagnet Enterprise will mark all the devices it detects that are not defined in its access control list (ACL) as unknown devices. Unknown devices are indicated by a  in the  (In ACL) column on the Infrastructure screen. In order to maintain the most accurate list of network devices, it is recommended that users classify unknown devices as soon as a more accurate status is determined for them. For devices that are expected to be added to the network, users should add the device to the ACL manually before deploying it on the network.

To add a device to the device list:

- 1) From the Infrastructure screen, click  (Add New Device). The Add New Device dialog box appears. See Figure 7-6.



The "Add new Device" dialog box contains the following fields and options:

- ☐ Mark as VIP device
- MAC: (Placeholder: Enter MAC address - (format) 00:00:00:00:00:00)
- Alias Name:
- Owner:
- Media Type:
- Device:
- ACL Type:
- ☐ ACL Expiration:
- Device Locator**
 - ☒ Let system determine a floor for this device based on max signal strength received by sensors
 - ☐ Manually assign a location for this device:
 -
- OK Cancel

Figure 7-6: Adding a new device to device list

- 2) Make the entries and/or selections as described in Table 7-5.

Table 7-5: Add New Device Options

Option	Description
Mark as VIP Device	Check this box to flag the device as a VIP. VIP devices are those that are critical to the network, and must be monitored at all times.
MAC	Enter the MAC address of the new device.
Alias Name	Enter an alias for the device. The alias provides a means of identifying the device other than the MAC address.
Owner	Enter the name of the user who owns the device.

Table 7-5: Add New Device Options

Option	Description
Media Type	<p>Click the down arrow to select the device's media type as described below.</p> <ul style="list-style-type: none"> • 802.11a – A supplement to the IEEE 802.11 wireless LAN specification that describes transmission through the Physical layer (PHY) at a frequency of 5 GHz with data rates up to 54 Mbps. • 802.11b – A supplement to the IEEE 802.11 wireless LAN specification that describes transmission through the Physical layer (PHY) at a frequency of 2.4 GHz with data rates up to 11 Mbps. • 802.11g – A supplement to the IEEE 802.11 wireless LAN specification that describes transmission through the Physical layer (PHY) at a frequency of 2.4 GHz with data rates up to 54 Mbps. • 802.11a/b – A dual-mode device that supports both 802.11a and 802.11b. • 802.11a/g – A trio-mode device that supports 802.11a, 802.11b, and 802.11g.
Device	<p>Click the down arrow, and categorize the device using one of the choices:</p> <ul style="list-style-type: none"> • Access Point – Any device acting as a communication hub by connecting wireless mobile 802.11 stations such as PCs to a wired backbone network. Also known as AP. • Station – Any device with a MAC address and a Physical layer (PHY) interface to the wireless medium, both of which comply with the 802.11 standard. • Ad Hoc – A wireless station in a Ad Hoc network that communicates directly with other stations without using an AP or any connection to the wired network.
ACL Type	<p>Click the down arrow, and define the status of the device by selecting an option from the drop-down list:</p> <ul style="list-style-type: none"> • Rogue – Any device that is not authorized to operate within a wireless network. • Valid Known – Any device that is authorized to operate within the wireless network. If selected, the user may also need to specify the duration (i.e., the number of days) the device is to be in this status. • Neighbor – Any device that belongs to a neighboring business. • Monitored – Any device that may pose a potential threat to the enterprise network and, therefore, must be kept an eye on. For example, unreturned devices used by ex-employees, lost devices, and devices once used to attack the enterprise network. • Unknown – Any device that does not properly fit into the above categories should be flagged as unknown until further categorization can be performed.

Table 7-5: Add New Device Options

Option	Description
ACL Expiration	<p>Click in the check box and specify a date the device's status as a Valid Known Device is to expire.</p> <p><i>Note: This option is available ONLY when the device is defined as a Valid Known Device. The time is based on the system time of the AirMagnet Enterprise Server. You can only specify a future date, but NOT a past or present date. An error message will pop up if a present date is used. The time expires at mid-night on the date you specify.</i></p>
Device Locator	<p>Select to allow the system to automatically place a device or to place it manually. Each option is described below.</p> <ul style="list-style-type: none"> • Let the System... – If selected, AirMagnet Enterprise will automatically decide on which floor the device should be based on the maximum signal strengths received by the sensors that detected the device. This feature applies if the device is detected by more than one sensor • Manually Assign... – If selected, you will have to manually assign the device to a floor when it is detected by more than one sensor on different floors. In this case, you will have to click the down arrow and select a floor to which the device is to be assigned.


3) Click **OK**. The device will be added to the device list on the Infrastructure screen.

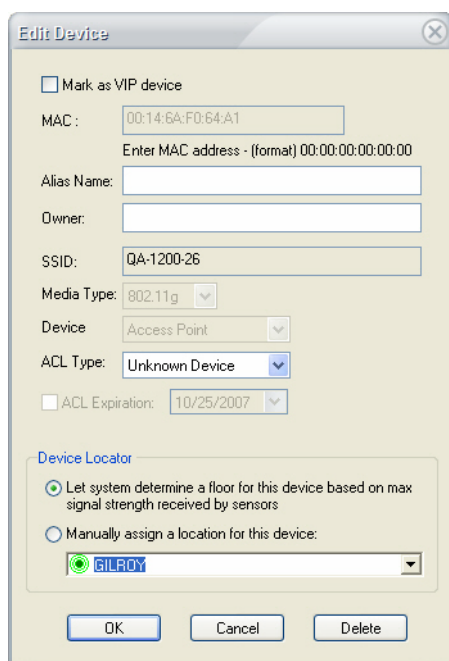
Re-categorizing Devices

As we have mentioned earlier, AirMagnet Enterprise automatically flag all new devices it detects as unknown devices and displays them in the **ACL** column on AirMagnet Enterprise Console's Infrastructure screen as **u**. However, in reality, not all devices marked this way are unknown devices. Therefore, it is up to the network administrator to look into all unknown devices the system has detected on the enterprise network to determine their true status and properly tag them in the ACL. As a result, some of the unknown devices may be re-categorized as valid known devices; some may turn out to be neighbor devices; some may need to be marked as monitored devices; and some as rogue devices that will be traced or blocked.

While the **+** (Add New Device) button allows you to add a new device to the device list with a properly defined ACL status (prior to plugging it into the network) to avoid false alarms, the **✎** (Edit Device) button lets you re-categorize those "unknown" devices to determine their true status upon further investigation. You may assign an unknown device to a specific ACL group, or even to several.

To re-categorize a device:

- 1) Highlight the device from the device list, and click  (Edit Device). The Edit Device dialog box appears. See Figure 7-7.

The image shows the 'Edit Device' dialog box. It has a title bar with 'Edit Device' and a close button. Inside, there's a checkbox 'Mark as VIP device'. Below it, the 'MAC' field is populated with '00:14:6A:F0:64:A1' and has a hint 'Enter MAC address - (format) 00:00:00:00:00:00'. The 'Alias Name' and 'Owner' fields are empty. The 'SSID' field is populated with 'QA-1200-26'. The 'Media Type' is a dropdown set to '802.11g'. The 'Device' is a dropdown set to 'Access Point'. The 'ACL Type' is a dropdown set to 'Unknown Device'. There's an 'ACL Expiration' checkbox and a date field set to '10/25/2007'. A 'Device Locator' section has two radio buttons: 'Let system determine a floor for this device based on max signal strength received by sensors' (selected) and 'Manually assign a location for this device:'. Below the second radio button is a location dropdown set to 'GILROY'. At the bottom are 'OK', 'Cancel', and 'Delete' buttons.**Figure 7-7: Editing a Device**

The Edit Device dialog box looks exactly the same as the Add New Device dialog box, but the main purpose of this dialog box is to let the user change the ACL status of any device from the device list. Notice that the fields for MAC address, Media Type, and Device Type are automatically interpolated by the system and cannot be modified.

- 2) In the Alias Name field, enter an alias (if it does not yet have one) or change the alias (if it already has one), if you wish to.
- 3) Add or modify the displayed Owner, if desired.
- 4) Use the ACL Type drop-down list to change the ACL Type into the proper category, if needed.

This information in the ACL Type field is identical to what is shown in the column on the Infrastructure screen. In other words, if the device is marked by **R** on the Infrastructure screen, the ACL Type field will show "Rogue Device" when the Edit Device dialog box opens. If you want to change a device's ACL Type to a Valid Known Device, you may also have to specify an ACL Expiration date. This feature is most useful in a situation where you have an outside contractor

come in to do some temporary work. You can mark the contractor's wireless station as Valid Known Device and use the last day of the contract as the ACL Expiration date.

- 5) Enter the name of the user who uses (owns) the device.
- 6) Click **OK** when done. You may remove the device from the network at any time by clicking **Delete**.

Chapter 8: Rogue Management View

Introduction

The Rogue Management view provides network administrators with a quick overview of rogue management information such as newly detected unknown devices, devices categorized as Rogue and blocked devices. It also provides quick links to rogue management functions.

This view is opened by clicking the IDS/Rogue icon on the navigation bar (see “[Navigation Bar](#)” on page 68).

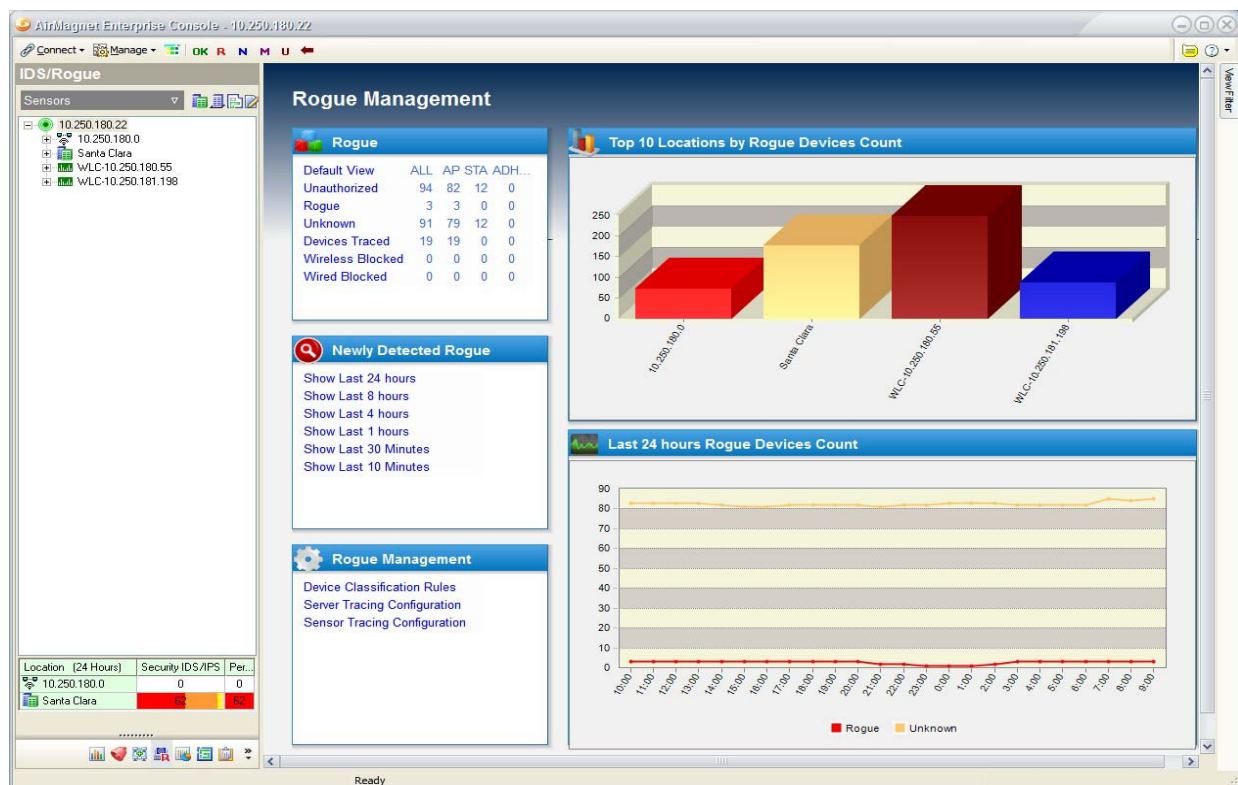


Figure 8-1: Rogue Management view

Rogue Definition: A rogue access point is defined as any unauthorized wireless access point connected to the enterprise’s internal wired network. This solution does not address rogue stations or peer-to-peer (ad hoc) wireless networks.

The AirMagnet Enterprise rogue management solution described herein works like this:

- 1) **Classify Known APs into ACL Groups:** When AirMagnet Enterprise is launched for the first time, it will classify all detected AP devices as “Unknown.” The network engineer can then create Access Control List Groups (ACLs) and classification rules that will

automatically classify APs as known devices. For information about ACL groups see [“Managing ACL Groups” on page 87](#) and [“Importing and Exporting ACL Data” on page 164](#).

- 2) **Establish Multi-layered Tracing to Identify Rogue APs:** Once the ACL Groups are established and all known APs have been automatically or manually classified as such, the network engineer can establish several methods of tracing to identify a rogue device. The types of tracing supported by Airmagnet Enterprise includes wireless tracing, switch tracing, wired Listening (Hub Correlation), Passive Detection (DHCP Fingerprinting), Enhanced Rogue on Wire (ARP Broadcasting) and Wireless Triangulation.
- 3) **Manage Rogue APs:** Policy profiles can be established within AirMagnet Enterprise that will determine system response to rogue APs. This includes implementing manual or automated rogue blocking along with various types of notification options such as system alarms, email notifications and text messaging alerts.

Rogue Management View Sections

Rogue

The Rogue section of the Rogue Management view provides some options for viewing information about unauthorized devices such as those categorized as Unknown and Rogue as well as those devices that have been traced and/or blocked. Click a link in this section to view the related information in the main area.

Table 8-1: Rogue Devices section of the Rogue Management view

Option	Description
Default View	<p>Top 10 Locations by Rogue Devices Count: The X axis lists up to 10 locations while the Y axis indicates the total number of unauthorized devices for each location.</p> <p>Last 24 hours Rogue Devices Count: The X axis indicates time intervals for the last 24 hours while the Y axis indicates the total number of Rogue and Unknown devices detected.</p>
Unauthorized	<p>Unauthorized (ALL): This table lists all devices categorized as Rogue or Unknown.</p> <p>Device Detail View: This table provides detailed information about the device selected in the All Unauthorized table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>

Table 8-1: Rogue Devices section of the Rogue Management view

Option	Description
Rogue	<p>Rogues (ALL): This table lists all devices categorized as Rogue.</p> <p>Device Detail View: This table provides detailed information about the device selected in the Rogues table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>
Unknown	<p>Unknown (ALL): This table lists all devices categorized as Unknown.</p> <p>Device Detail View: This table provides detailed information about the device selected in the Unknown table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>
Devices Traced	<p>Devices Traced (ALL): This table lists all devices that are being traced via the switch.</p> <p>Device Detail View: This table provides detailed information about the device selected in the Wired Traced table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>
Wireless Blocked	<p>Wireless Blocked (ALL): This table lists all devices that have been blocked via wireless blocking.</p> <p>Device Detail View: This table provides detailed information about the device selected in the Wireless Blocked table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>
Wired Blocked	<p>Wired Blocked (ALL): This table lists all devices that have been blocked via wired blocking.</p> <p>Device Detail View: This table provides detailed information about the device selected in the Wired Blocked table.</p> <p>Switch Trace History View: If a device was traced via a switch, the devices are listed here.</p> <p>Action History View: If a port block action was taken on a device, the devices are listed here.</p>

Newly Detected Rogue

This section of the Rogue Management view lists newly detected unauthorized devices for up to the last 24 hours. A device will be listed in this view if it was detected and categorized as Unknown or Rogue within the specified time interval.

A device may be categorized by three methods:

- When a device is newly detected, its default categorization is Unknown.
- The user may manually change the categorization of a device.
- A Policy or Device Classification rule may automatically change the category of a device based on the device's attributes such as vendor type, SSID, MAC address or other criteria.

Device Detail View: This table provides detailed information about the device selected in the time interval table.

Switch Trace History View: If a device was traced via a switch, the devices are listed here.

Action History View: If a port block action was taken on a device, the devices are listed here.

Rogue Management

The Rogue Management section of the Rogue Management view provides links to a few rogue management configuration dialogs.

Table 8-2: Rogue Management section of the Rogue Management view

Option	Description
Device Classification Configuration	This link opens the Auto Device Classification Rules. This enables the user to create rules that can automatically re-categorize a device based on rule application. “Device Classification” on page 283.
Server Tracing Configuration	See “To establish Server-based switch tracing” on page 180
Sensor Tracing Configuration	See “To establish Sensor-based switch tracing” on page 179

Establishing Multi-layered Tracing to Identify Rogue Devices

AirMagnet Enterprise Tracing informs the user that an unknown device is connected to the enterprise wired network. When this occurs, AirMagnet Enterprise may also be configured to automatically re-classify the target device, trigger alarms, send out notifications, and implement device blocking.

AirMagnet Enterprise enables the user to implement one, two or all tracing options to accomplish a customized multi-layered security approach.

The methods of tracing are as follows:

- Wireless Tracing
- Switch Tracing
- Wired Listening (Hub Correlation)
- Passive Detection
- Enhanced Rogue on Wire
- Wireless Triangulation (device locator) See [“Locating Rogue Devices” on page 199](#)
- Defining Policy Profiles to Detect Rogue Devices

Rogue Identification by Wireless Tracing

Wireless tracing is limited to tracing APs with open security using a DHCP IP assignment.

Wireless tracing can be summarized as comprising the following steps:

- 1) The AirMagnet SmartEdge sensor associates with the unknown AP.
- 2) The sensor sends a UDP packet through the unknown AP onto the wired network.
- 3) The destination address for the packet is the IP address of the sensor’s Ethernet port.
- 4) The packet collects the IP address of the wired interface of the unknown AP.
- 5) The device shows up as “traced” on the AirMagnet Enterprise IDS/Rogue view.

If the sensor receives the packet via its Ethernet interface, it can conclude that the AP is connected to the enterprise wired network. Rogue classification is therefore completed by the reception (or non-reception) of the UDP trace packet.

In terms of collecting rogue information, the SmartEdge sensor can determine if the rogue AP is performing NAT (Network Address Translation) from the source IP address of the received loop-back UDP packet. Rogue AP IP addresses can also be determined thereafter.

To establish wireless tracing:

- 1) Click the **IDS/Rogue** icon on the navigation bar.
- 2) Click **Sensor Tracing Configuration**. Double-click an existing profile.
- 3) Check **Auto wireless trace APs**.

- 4) Click **OK**.

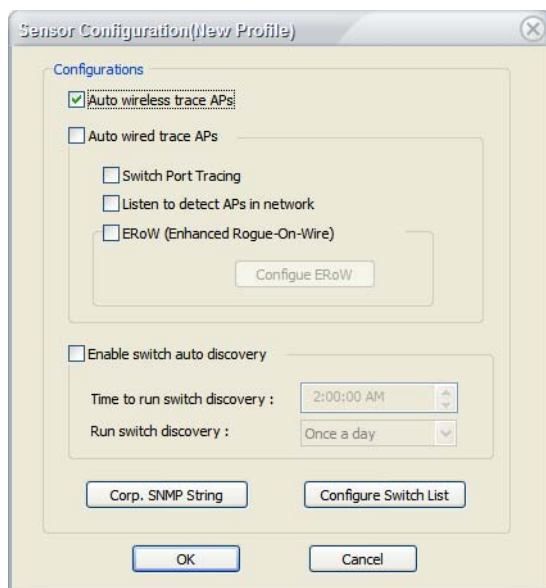


Figure 8-2: Sensor Configuration profile

Rogue Identification by Switch Tracing

AirMagnet Enterprise switch tracing queries the switch for MAC addresses and then correlates and compares the MAC addresses to identify a rogue AP.

Table 8-3: Switch Tracing by MAC Address

ab:cd:12:34:56:76
ab:cd:12:34:56:77
ab:cd:12:34:56:78 = Unknown wireless device
ab:cd:12:34:56:79
ab:cd:12:34:56:80
bb:cc:dd:ee:ff:11 = wireless client (STA)

It does this by using SNMP to query the CAM table of the switch. If the rogue is not connected to the target switch then, using CDP or LLDP, the neighboring switches are queried.

CDP is a data layer (a layer two protocol). It discovers any next hop device information. A CDP enabled device will broadcast its device information to a multicast address (limited to the same layer) and does not route device information to a higher level layer.

AirMagnet Enterprise supports Cisco Discovery Protocol (CDP) switch tracing as well as Link Layer Discovery Protocol (LLDP). It should be noted that some non-Cisco switches support CDP. Check the technical specifications for your switch to determine if it supports CDP.

AirMagnet Enterprise provides two methods of switch tracing (sensor-based and server-based) in order to meet the needs of the particular enterprise architecture:

Sensor-based switch tracing: Generally, this option is used when there are a large number of sensors organized in distributed networks. If the VLAN is not interconnected then the sensor and VLAN need to be in the same VLAN. If the VLAN is interconnected, it doesn't matter because the sensor can do cross VLAN connecting.

Server-based switch tracing: This option is centric to a particular server and where switch security is high with restricted access to the switch.

For both sensor and server switch tracing, there are two methods to discover the switches on the network:

- **Auto Switch Discovery:** All the corporate switches on the network use the same SNMP string. Air-Magnet Enterprise Auto discovery uses CDP protocol neighbor information to discover the switch information as well as SNMP with the CDP MIB to query the switch to find out the device information. There is no set limit to the number of devices AirMagnet Enterprise Auto Discovery will find, in fact it can traverse the whole network, however, auto discovery depends somewhat on how the network is structured, such as whether it is connected through layer two or three.
- **Switch List:** When different SNMP strings are used for different switches, then the different SNMP strings may be manually created into a switch list

Note: If you do not have a global SNMP read or read/write password, you cannot use AirMagnet Enterprise Auto Discovery, however, you can manually set tracing by using the manual switch list creation method. Also, SNMPv3 is not supported for sensor tracing.

Alarm: Rogue AP traced on enterprise wired network

To establish Sensor-based switch tracing

- 1) Click the **IDS/Rogue** icon on the navigation bar.
- 2) Click **Sensor Tracing Configuration**. Double-click an existing profile.
- 3) Check **Auto wired trace APs**.

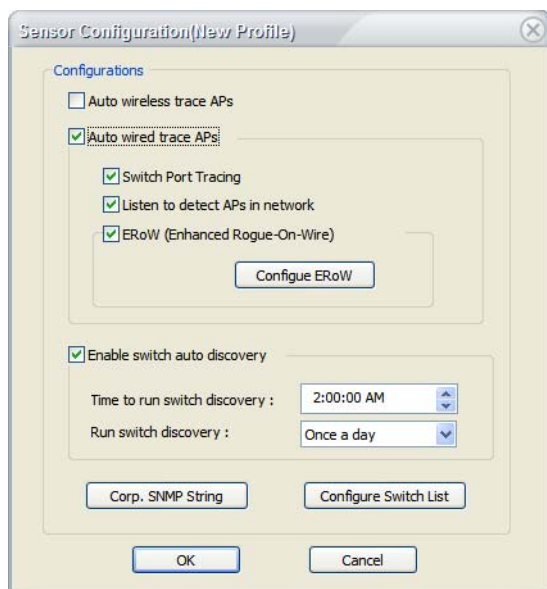




Figure 8-3: Sensor Configuration profile

- 4) **For auto switch discovery:** Check **Enable switch auto discovery**. Click **Corp SNMP String** and type the Read and Write strings. Click **OK**.
- 5) **To create a Switch List:** Click **Configure Switch List**.
- 6) Click  to add a switch to the list. Add the switch details. Click **OK**.

To establish Server-based switch tracing

- 1) Click the **IDS/Rogue** icon on the navigation bar.
- 2) Click **Server Tracing Configuration**.
- 3) Check **Auto trace APs from Server**. **Corp SNMP String** and **Configure Switch List** become active.
- 4) Click **Corp SNMP String** to set a single SNMP string for all switches that use the same SNMP string –and/or–
- 5) Click **Configure Switch List** to set an individual SNMP string per switch. Click  to add a switch to the list. Add the switch details. Click **OK**.

Rogue Identification by Wired Listening (hub correlation)

Wired Listening (hub correlation) builds upon a foundation of switch tracing by additionally listening to broadcast traffic on the same broadcast domain network to discover an out-of-sequence MAC address that may indicate a rogue AP. In other words, switch tracing may be “enhanced” in order to further enlarge the scope of rogue detection.

Alarm: Rogue AP traced on enterprise wired network

To establish Wired Listening:

- 1) First, follow the procedure for Switch Tracing to establish Switch Tracing.
- 2) Check **Listen to detect APs in network**.

Rogue Identification by Passive Detection

Each device on the network has a unique DHCP signature that AirMagnet Enterprise uses to identify whether a device may be unauthorized (rogue). With passive monitoring, any new DHCP packets that are injected into the network are identified and detected as a Rogue AP using the device unique DHCP signature.

***Note:** By establishing switch tracing and wired listening, passive detection is automatically established.*

Alarm: Rogue AP traced using passive detection

Rogue Identification by Enhanced Rogue on wire

When this option is enabled, AirMagnet Enterprise scans all the IPs in the sensor network range in order to detect any new IP that can indicate a rogue device by default. Since this option will generate ARP broadcasting traffic to the corporate network, the user has a choice to customize the sensor network range.

Alarm: Rogue AP traced on enterprise wired network

To establish Enhanced Rogue on Wire:

- 1) Follow the procedures for switch tracing and wired listening
- 2) Check **Enable Enhanced Rogue-On-Wire (ERoW)**.
- 3) Click **Configure ERoW**. This displays Enhanced Rogue-On-Wire Configuration
- 4) Choose the desired subnet mask option:
 - Sensor Subnet Mask
 - Use Configure Subnet Mask: Customize to a smaller subnet mask range
- 5) Set the time interval:
 - Per IP: How frequently to scan
 - Sleep timer: Time between scanning loops
- 6) Click **OK**.

Automatic Rogue Traffic Blocking

Real-time automated or manual rogue device containment is usually the first step to plug the rogue device security hole. AirMagnet Enterprise provides two distinct mechanisms for rogue containment – wire and wireless rogue blocking. The User can choose the suitable blocking methods according to the practical scenarios.

Device blocking may be established and canceled from the Rogue Management view, Rogues section.

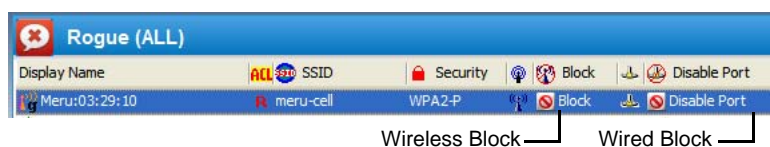


Figure 8-4: Rogue Management view blocking options

Wired Traffic Blocking

AirMagnet Enterprise supports a rogue policy that automatically blocks the rogue device from its directly connected switch by shutting down the switch port.

Some key AirMagnet advantages are:

- Both automated blocking and manual blocking are supported. For automated blocking action, a time period can be specified so that the switch port will be automatically unblocked making the switch port functional again. If the rogue device continues to be detected at the time when the blocking action expires, a rogue alarm will be regenerated to trigger the reinstated blocking action.
- When automated device blocking is used, the user needs to be aware that the notification action will work in combination with the device policy and classification rules. Once the rogue devices are detected according to the policy and classification rules, AirMagnet Enterprise will start device blocking either from the sensor or the server depending on the tracing configuration.

The AirMagnet SmartEdge sensor traces and blocks across VLANs on a switch. It also traverses down-stream to find the cascaded terminal switch to block the rogue port.

Enabling Wired Blocking

- 1) Click the **IDS/Rogue** icon on the navigation bar.
- 2) In the Rogue (ALL) section, click **Disable Port**. Select the desired method of disabling the port. See Figure 8-5.
- 3) Click **OK**.

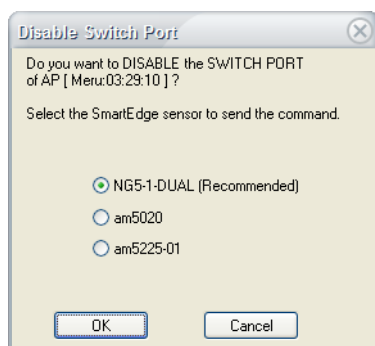


Figure 8-5: Disable Switch Port options

It may take several minutes for the port to be disabled. The status of the action may be viewed in the Action History section.

To re-enable the port, double-click **Disable Port** and click **OK**.

Wireless Traffic Blocking

Similar to the wired-side switch port blocking, AirMagnet Enterprise supports a rogue policy to automatically block the rogue device from the wireless side. Whether the rogue device is a client station, ad-hoc station or an AP, AirMagnet SmartEdge sensor can terminate its wireless communication.

The block is ingenious in that it blocks bi-directionally, spoofing the AP to the station and the station to the AP (or ad-hoc to ad-hoc) without interrupting normal (authorized) wireless traffic. This is true even of a blocked station attacking an AP.

The AirMagnet sensor will continue to scan as it blocks the devices and can adjust its blocking to “follow” a blocked device if it changes channels, SSIDs, Media bands etc. Additionally, the sensor will continue to generate alerts on other devices that may or may not be associated with the blocked device as normal with no interruption of service.

AirMagnet Management Server coordinates the blocking effort so that the closest sensor (sensor with the strongest rogue signal strength) does the tracing (if not already traced) and blocking. Each sensor can effectively block up to ten devices on the same channel.

Enabling wireless blocking

- 1) Click the **IDS/Rogue** icon on the navigation bar.
- 2) In the Rogue (ALL) section, click **Block**. Select the desired method of wireless blocking. See [Figure 8-6](#).
- 3) Click **OK**.

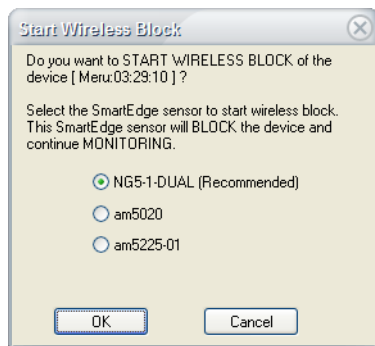


Figure 8-6: Start Wireless Blocking options

It may take several minutes for the wireless blocking to be enabled. The status of the action may be viewed in the Action History section.

To stop wireless blocking, double-click **Block** and click **OK**.

Defining Policy Profiles to Detect Rogue Devices

AirMagnet Enterprise can create a bullet-proof shield over your enterprise network by identifying and neutralizing in real time any threat as it arises. This is done through the integration of the industry's best intrusion detection system with a suite of proactive rogue tracing and blocking tools to respond to any intrusion automatically.

This section discusses the general procedures on how to set up the system to effectively detect, trace, block, and remove rogue devices that find their way into your enterprise network.

To manage rogue devices:

- 1) Create a network policy profile that specifically targets rogue devices. This can be done by selecting policies in the "Rogue AP and Station" category under "Security IDS/IPS" on

the AirMagnet Policy Management screen. See [Figure 8-7](#).

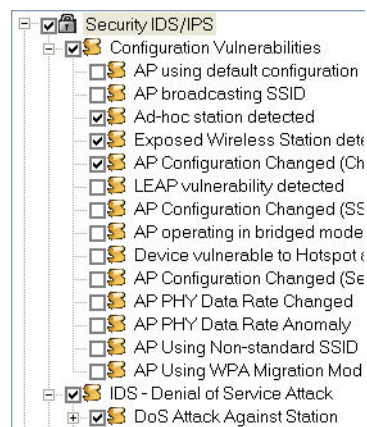


Figure 8-7: Setting rogue-control policies

As shown in Figure 7-8, you can set the system to automatically detect rogue APs or stations by the following criteria:

- **Channel** — This option enables the system to detect rogue devices by checking against the pre-assigned enterprise network’s radio channels for the 802.11a, 802.11b, or 802.11g standards. When an AP operating in a non-enterprise standardized radio channel is discovered, a “Rogue AP/Station Found” alarm will be generated.
- **IEEE ID (OUI)** — This option enables the system to detect rogue devices by checking against the enterprise network’s pre-configured authorized AP equipment vendor list. It will raise a rogue AP/station alarm whenever a device is discovered outside the vendor list.
- **MAC address (ACL)** — This option enables the system to detect rogue devices by checking against the enterprise networks’ list of pre-configured MAC addresses of the devices used on the network. The system will issue a rouge AP/station alarm upon discovering any device whose MAC address falls out of the pre-configured MAC address list.
- **SSID** — This option enables the system to detect rogue devices by checking against the enterprise network’s pre-configured authorized SSID list. The system will raise a rouge AP/station alarm when an AP from a foreign SSID is discovered on the network.
- **Wireless media type** — This option enables the system to detect rogue devices by checking against enterprise standardized operating radio media types, such as 802.11a, 802.11b, or 802.11g. Whenever an device operating outside of the enterprise standardized radio media is discovered, a rogue AP/station alarm will be generated.
- **Rogue AP detected inside** — This option enables the system to detect rogue APs inside a specific marked area, using the Device Locator.

- **Traced on Enterprise wired network (for rogue APs only)** – Once a rogue AP is identified, it can be successfully traced to the enterprise switch port using the AirMagnet Enterprise wired trace feature provided by the AirMagnet Enterprise Console on the Infrastructure page. This is used to track down the wired-side IP address of the rogue AP and then disable the switch port manually. AirMagnet Enterprise also provides the feature of wired auto-trace and blocking, in which the rogue AP will be traced and blocked automatically as soon as it is detected.

Once the rogue-detection policies are in place, the system will automatically generate alarms when rogue devices are discovered on the network. You can view the alarms from the AirMagnet Enterprise Console's AirWISE screen. For instructions on how to configure network policies, see [Chapter 12, "Managing Policy Profiles"](#).

- 2) Configure methods of notification and integrate them with the alarms. AirMagnet Enterprise can generate up to 11 notifications.

For instructions on how to configure notifications and integrate them with policy alarms, see [Chapter 12, "Managing Policy Profiles"](#) and ["Configuring Notification List" on page 257](#).

- 3) Configure the system's automatic rogue tracing and blocking feature. See the following sections for more details.

Note that Automatic tracing and blocking features work only with rogue APs. Rogue stations must be blocked manually when detected.

Rogue Management Examples

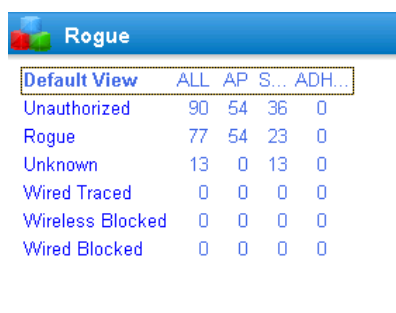
- 1) How can a WLAN administrator see the entire rogue devices status of my enterprise WLAN if the rogue devices are the main threat of enterprise WLAN network?

The Rogue view provides a very efficient way to view all the unauthorized devices within enterprise WLAN in a centralized place, including the status of rogue devices lately found in the enterprise WLAN.



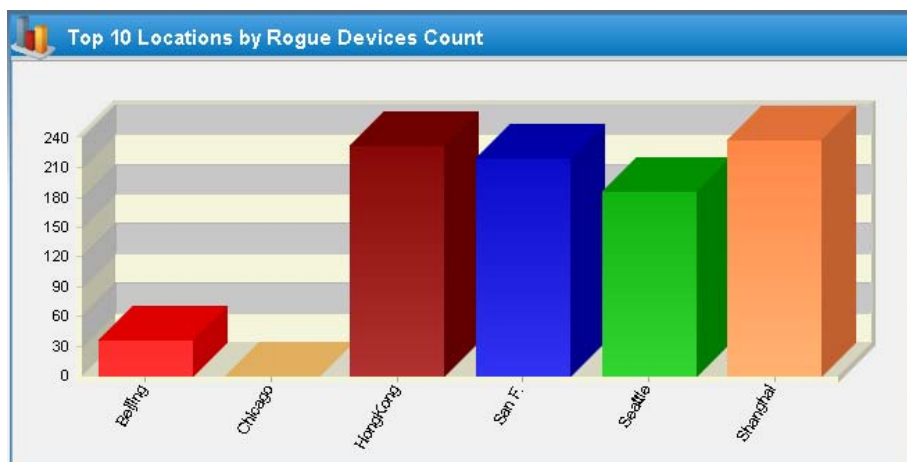
Location (24 Hours)	Security IDS/IPS	Per...
Beijing	0	0
Chicago	0	0
HongKong	0	0
San F.	0	0
Seattle	0	0
Shanghai	0	0

Statistic matrix dashboard of unauthorized devices classified shows a one glance of WLAN rogue devices status in number format.

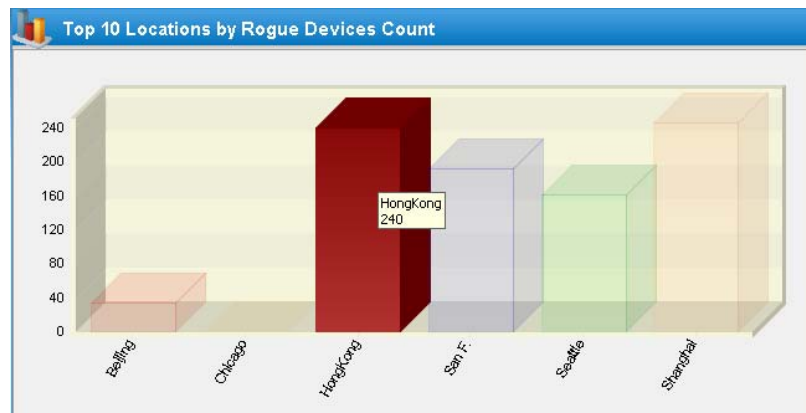


Default View	ALL	AP	S...	ADH...
Unauthorized	90	54	36	0
Rogue	77	54	23	0
Unknown	13	0	13	0
Wired Traced	0	0	0	0
Wireless Blocked	0	0	0	0
Wired Blocked	0	0	0	0

List top 10 locations with the most rogue devices for the large scale WLAN deployment enterprise.



Fast drill down on the location bar clicking to show rogue devices detected in the specific location.



Newly Detected Rogue panel provides a quick view of lately detected rogue devices by different time filter. IT administrator can take action on these new threatens appear on enterprise WLAN in time.

Rogue

Default View	ALL	AP	STA	ADH...
Unauthorized	440	314	125	1
Rogue	15	13	2	0
Unknown	425	301	123	1
Wired Traced	43	43	0	0
Wireless Blocked	0	0	0	0
Wired Blocked	0	0	0	0

Newly Detected Rogue

- Show Last 24 hours
- Show Last 8 hours
- Show Last 4 hours**
- Show Last 1 hours
- Show Last 30 Minutes
- Show Last 10 Minutes

Show Last 4 hours

Display Name	ALL	STA	SSID	Security	Block	Disable Port	C...	.11
INTEL:16:C7:28	R	galaxywind1	WEP	Block			11	g

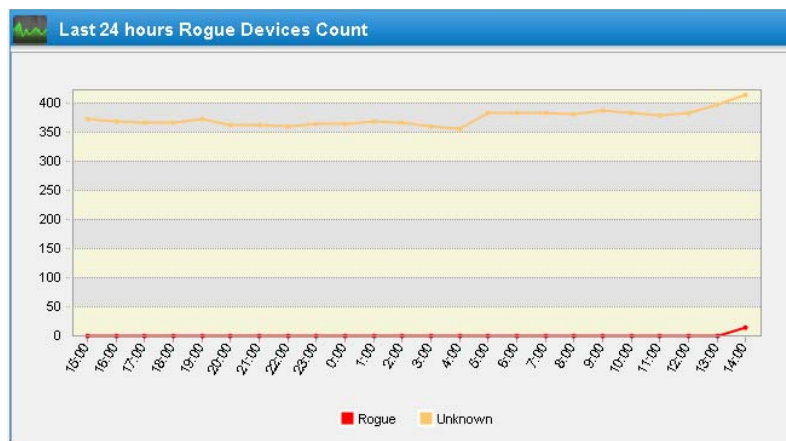
Device Detail View

Display Name	INTEL:16:C7:28
MAC Address	00:26:C7:16:C7:28
Channel	11 2.462GHz
First Seen Time	01/09/2012 13:38:39

Switch Trace History View

Time	Switch Name	Port	# D...	Uplink	Trace Mac
There are no items to show.					

Rogue devices trend of last 24 hours.



2) How could WLAN administrator manage the rogue devices once system identified?

User can view the details of rogues classified from rogue details panel on clicking the numbers of the rogue panel.

Rogue				
Default View	ALL	AP	STA	ADH...
Unauthorized	470	300	169	1
Rogue	0	0	0	0
Unknown	470	300	169	1
Wired Traced	43	43	0	0
Wireless Blocked	0	0	0	0
Wired Blocked	0	0	0	0

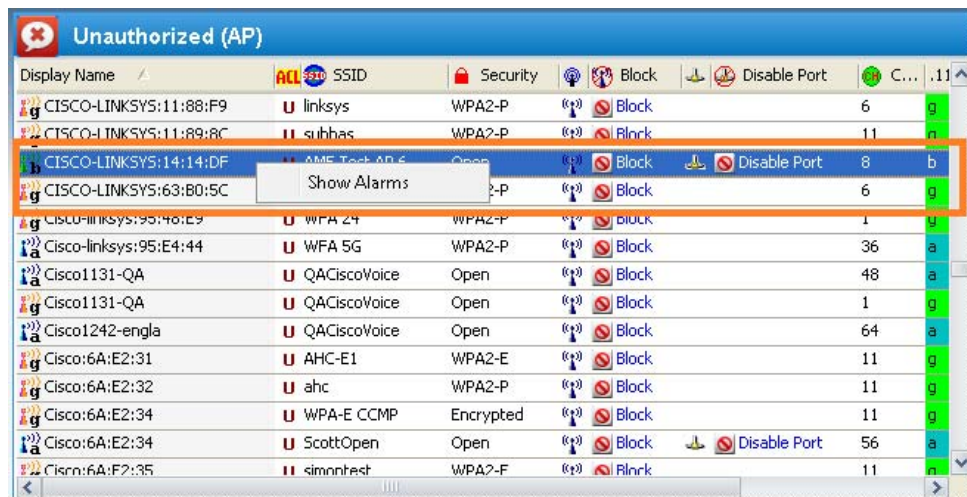
IT administrator can take wireless/wired blocking actions of the rogue devices conveniently on the same rogue detail panel.



Display Name	ACL	SSID	Security	Block	Disable Port	C...	.11
AME TEST AP 1	U	AHC-TKIP	WPA2-P	Block	Disable Port	5	g
AME TEST AP 1	U	AME TEST	WPA2-P	Block	Disable Port	5	g
AME TEST AP 2	U	WPA2-E TKIP	WPA2-E	Block	Disable Port	9	g
AME TEST AP 2	U	AHC-CCMP	WPA2-P	Block	Disable Port	9	g
AME TEST AP 2	U	AME TEST	WPA2-P	Block	Disable Port	9	g
Netgear:F7:29:87	U	AME Test AP 4	Open	Block	Disable Port	8	g
AME TEST AP 3	U	WPA-E CCMP	WPA-E	Block	Disable Port	10	g
AME TEST AP 3	U	WPA2-E TKIP	WPA2-E	Block	Disable Port	10	g
AME TEST AP 3	U	AHC-TKIP	WPA2-P	Block	Disable Port	10	g
AME TEST AP 3	U	AME TEST	WPA2-P	Block	Disable Port	10	g
Cisco:6A:E2:34	U	ScottOpen	Open	Block	Disable Port	56	a
AME-Test-AP5-9	U	Daisy_profile	WPA-E	Block	Disable Port	56	a
Cisco:6A:E2:3D	U	ahc	WPA2-P	Block	Disable Port	56	a
AMF-Test-AP5-9	U	AMF-TFST2	WFP	Block	Disable Port	56	a

- 3) How could WLAN administrator quickly find out reason of the specific device classified as rogue and also other rogue related alarms?

Show the rogue alarms of the specific rogue device on right-click.



Display Name	ACL	SSID	Security	Block	Disable Port	C...	.11
CISCO-LINKSYS:11:88:F9	U	linksys	WPA2-P	Block		6	g
CISCO-LINKSYS:11:89:8C	U	subhas	WPA2-P	Block		11	n
CISCO-LINKSYS:14:14:DF	U	AME Test AP 6	Open	Block	Disable Port	8	b
CISCO-LINKSYS:63:B0:5C	U		WPA2-P	Block		6	g
CISCO-LINKSYS:95:46:E9	U	WPA 24	WPA2-P	Block		1	g
Cisco-linksys:95:E4:44	U	WFA 5G	WPA2-P	Block		36	a
Cisco1131-QA	U	QACiscoVoice	Open	Block		48	a
Cisco1131-QA	U	QACiscoVoice	Open	Block		1	g
Cisco1242-engla	U	QACiscoVoice	Open	Block		64	a
Cisco:6A:E2:31	U	AHC-E1	WPA2-E	Block		11	g
Cisco:6A:E2:32	U	ahc	WPA2-P	Block		11	g
Cisco:6A:E2:34	U	WPA-E CCMP	Encrypted	Block		11	g
Cisco:6A:E2:34	U	ScottOpen	Open	Block	Disable Port	56	a
Cisco:6A:F2:35	U	simonnet	WPA2-F	Block		11	n

Only focus on the rogue alarms of the specific unauthorized device cares about.

Alarm Description	Source	Time	Score
Rogue AP traced on Enterprise wired network	CISCO-LINKSYS:14:14:DF	01/09/2012 14:35:26	1000

Rogue AP traced on Enterprise wired network

Rogue AP CISCO-LINKSYS:14:14:DF (SSID : AME Test AP 6) is traced to be connected to your enterprise wired network through switch 129.196.34.2 port Fa0/7. This device is not in the authorized access control list but is currently active in the radio range. Unauthorized and damaged wireless APs or stations open up a back door to your corporate wired network and impose a high security risk. If this wireless device is indeed authorized, you may add it to the access control list from the configuration menu.

Severity	Channel	Src Device	Dst Device
Critical	8 2.447GHz	68:7F:74:14:14:DF	68:7F:74:14:14:DF

Time	Sensor Name
1/09/2012 14:35:26	amism5020-34...
1/09/2012 14:32:41	amism5020-34...
1/09/2012 13:11:30	amism5020-34...
1/09/2012 13:05:37	amism5020-34...
1/09/2012 12:40:39	amism5020-34...
1/09/2012 12:32:52	amism5020-34...
1/09/2012 11:11:35	amism5020-34...

4) How could WLAN administrator configure the rogue management now?

User does not have to click around on different policies and find options to generate the rogue management strategy, the centralized management options of rogue screen provides WLAN administrator new interface to define all the related configurations.

Rogue Management

- Device Classification Rules
- Server Tracing Configuration
- Sensor Tracing Configuration

Now it takes 3 steps to define the rogue management strategy

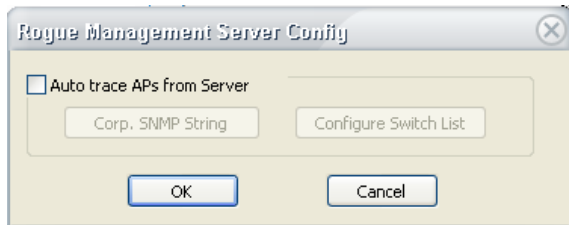
Classify the devices as rogue by device classification rules

Auto Device Classification Rules

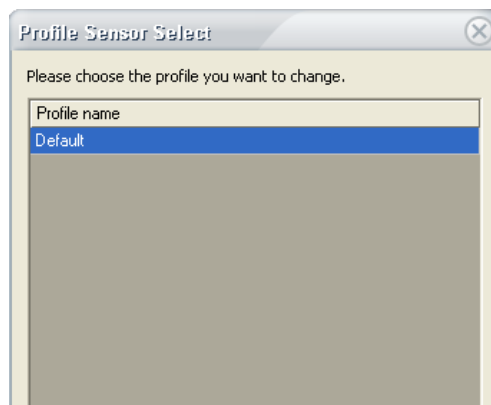
Name: New Rule ☒ Enable

Change the ACL status of all Devices to Rogue for which New Classification Type

Define the server trace options



Define the sensor trace option to profiles




Then done!

Chapter 9: Viewing Top Analyses

Introduction

This section discusses the various portions of AirMagnet Enterprise's Top Analysis screen as well as its major components and their basic functions.

Major UI Components

The Top Analysis screen allows you to display and analyze WLAN data using graphs. You can navigate to the Top Analysis screen from any of the other screens by clicking  on the Navigation Bar.

The Top Analysis screen consists of two major sections, as shown in Figure 9-1.

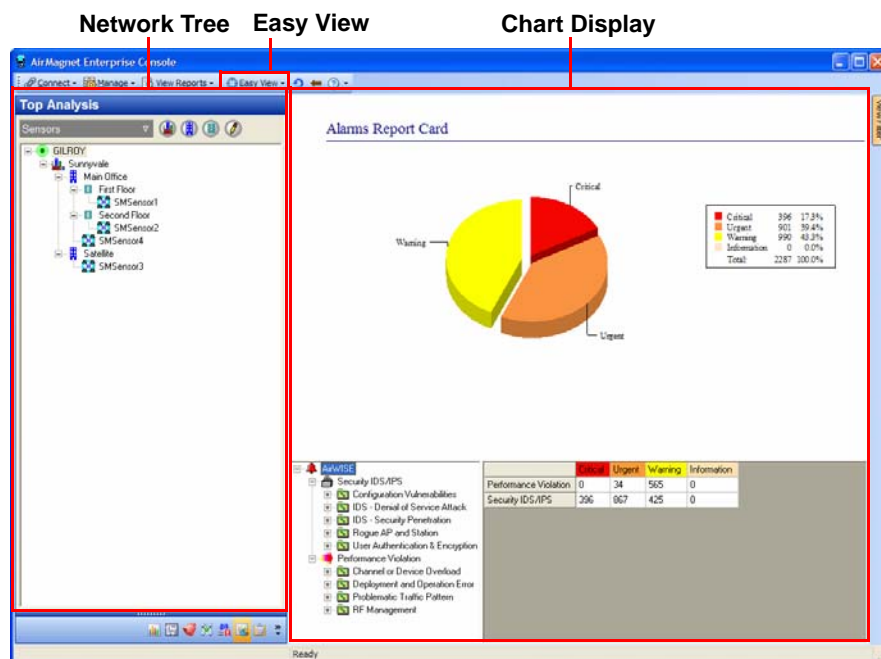



Figure 9-1: Top Analysis Screen UI Components

Using the Easy View

Users can view charts on a variety of different network data; different chart types are accessed by using the  **Easy View** button located at the top of the screen. Clicking this button displays a list of different charts that can be displayed. See [Figure 9-2](#).

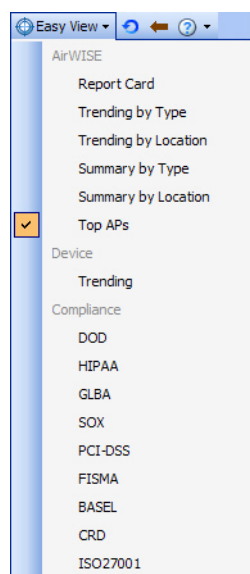


Figure 9-2: Easy View Options

The Top Analysis screen can display three types of data, which are represented by the three different categories shown by the Easy View:

- **AirWISE** – AirWISE charts give the user a basic idea of the alarms status at the selected location. These charts make it easy to identify alarm trends (both in frequency and alarm type) as well as which types of alarms are occurring at each location in the network tree.
- **Device** – Device charts provide a basic overview of the devices detected on the network. Users can easily narrow down the focus of the chart to view only rogue or monitored devices, or gain an overall view of all devices and media types in use. This information can be further defined by selecting only stations or APs to view, depending on the information required by the user.
- **Compliance** – Compliance charts provide a quick overview of how well the enterprise network complies with the selected regulation. Each compliance chart consists of a pie chart that displays the number of violations for the network under each regulation, and the lower portion displays the number of violating and compliant devices overall.

Chart Display

The main chart display consists of two sections, as shown in [Figure 9-3](#).

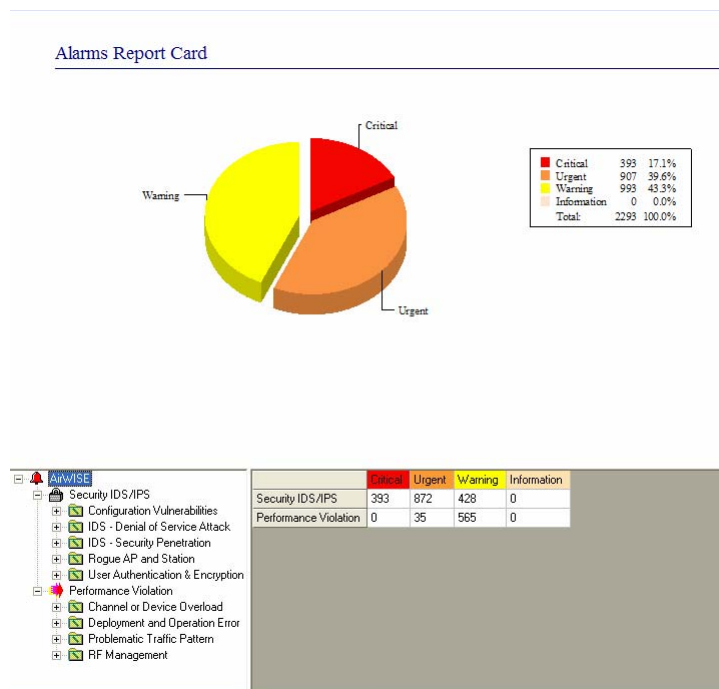



Figure 9-3: Main Chart Display

The upper portion of the screen simply displays the selected chart along with a descriptive legend to help users quickly view data of interest. The lower portion will vary depending on the type of chart selected and is divided into two portions. The left-hand portion provides a selection tree, which allows the user to narrow the focus of the displayed data. In [Figure 9-3](#), the AirWISE Report Card chart is shown and the policy tree is displayed in the bottom-left. Since the root of the tree is currently selected, the chart displays information regarding all alarms within the last 24 hours. Selecting a branch on the tree (such as the Configuration Vulnerabilities policy tree) will subsequently display data specific to that area.

The right-hand portion of the lower frame displays the actual numbers behind the chart above (in this case, the number of alarms in each severity level). With different chart type selections, this data can display the top 10 active devices, a list of devices based on their ACL status, or various other options.

Working in the Top Analysis Screen

To use the Top Analysis screen, you first need to select a node from the network tree on the left. It can be the AirMagnet Enterprise Server, which is the highest level in the network hierarchy, or a city, building, floor, or sensor, depending on how broad or specific you want the data to be. Once a node is selected, the next step is to decide what type of information you want to display in the charts, i.e., security and performance alarms, devices, or compliance. You can make a selection simply by clicking the  (Easy View) button and clicking your choice.

Sample Analysis Charts

Figure 9-4 and Figure 9-5 are sample chart selections from the Top Analysis screen.

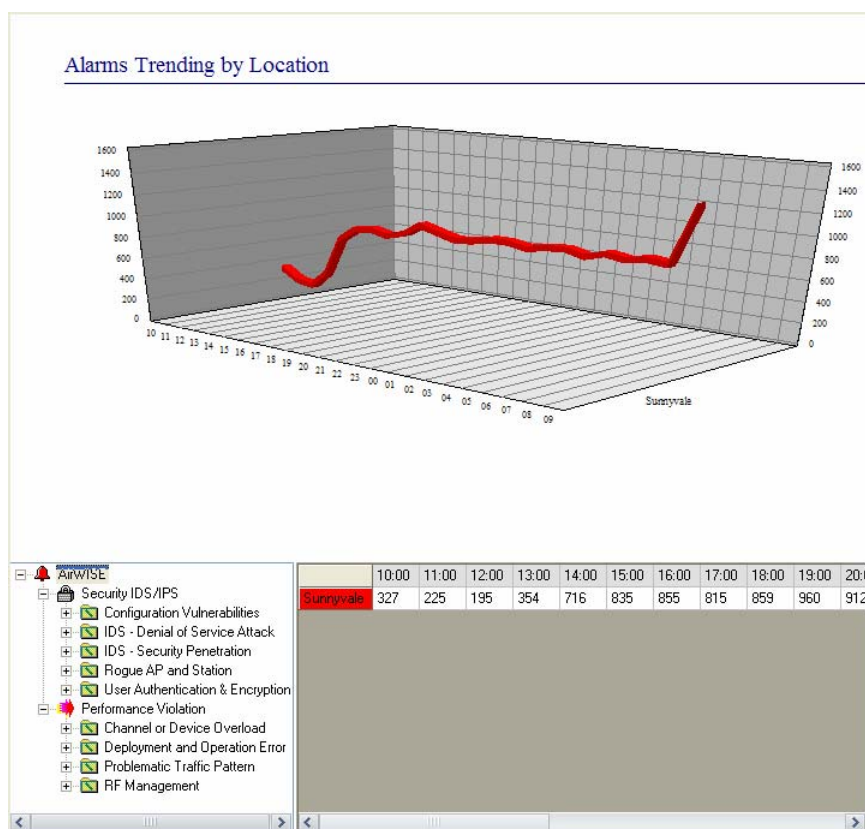


Figure 9-4: An Alarm Trending by Location chart

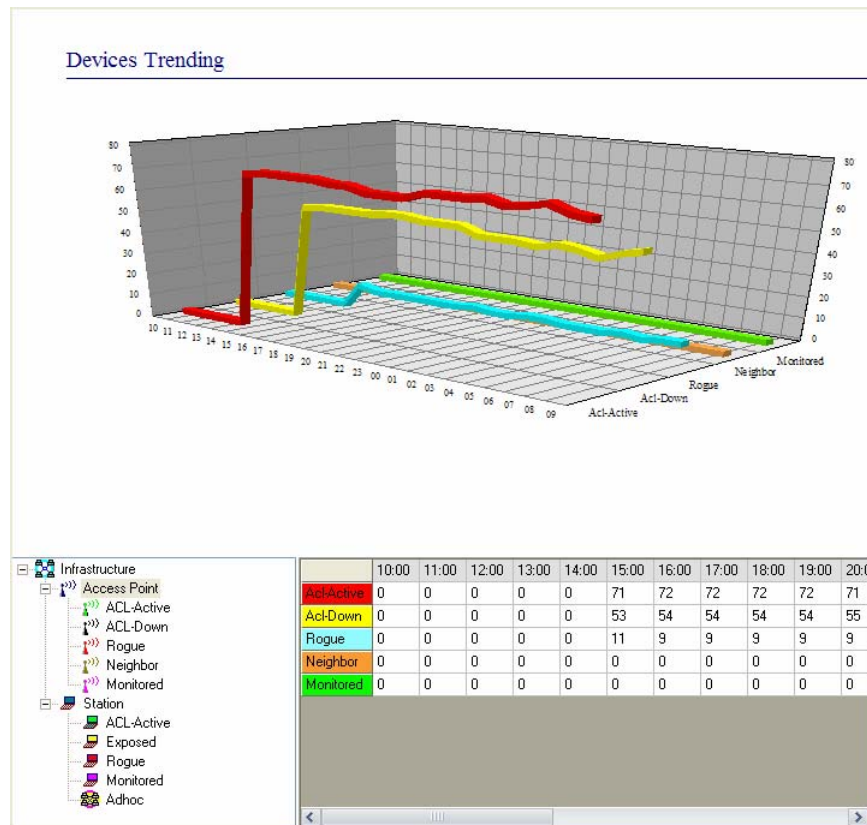


Figure 9-5: A Devices Trending chart

Chapter10: Locating Rogue Devices

Introduction

AirMagnet Enterprise's Device Locator is a powerful yet easy-to-use tool that enables WLAN administrators to easily and quickly locate any wireless device (i.e., APs, stations, and ad hoc stations) on a wireless network. You can identify the location of virtually any device of interest that AirMagnet has detected on the network or track down any device that has violated your wireless network security or performance policies, thus triggering the alarm or alarms.

It is important to note that this feature applies only to the floor level in the network tree structure. Therefore, the user must select the floor where the device or devices are or may be located. Also, in order to ensure the accuracy (or level of confidence) of the result of a device-locating operation, you must have at least three sensors deployed on the same floor and make sure that the sensors are deployed where they can have good FOV (field of view) and are about 60 to 90 feet apart from one another.

This chapter describes how to use AirMagnet Enterprise's Device Locator to identify the location of any wireless device that AirMagnet has detected on your wireless network. However, for illustration purposes, we focus our discussion on using the Device Locator to locate rogue devices even though the same procedures can be applied when locating all types of devices.

Enabling the Device Locator

Before users can access the Floor Plan screen, the Device Locator service must be enabled in the Enterprise configuration.

To enable Device Locator:

- 1) Click Manage>Server Options....
- 2) Select the **Server** tab.
- 3) Check **Enable Device Locator Service**. See Figure 10-1.

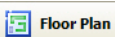


Figure 10-1: Enabling the Device Locator Service

- 4) Click **OK** to save the changes.

The following sections of this chapter assume that the Device Locator is enabled. If users attempt to navigate to the Floor Plan page before following these steps, an error message appears.

Major UI Components

To access the Device Locator, click  **Floor Plan** from the Navigation Bar. **Figure 10-2** highlights the main components of the Floor Plan screen.

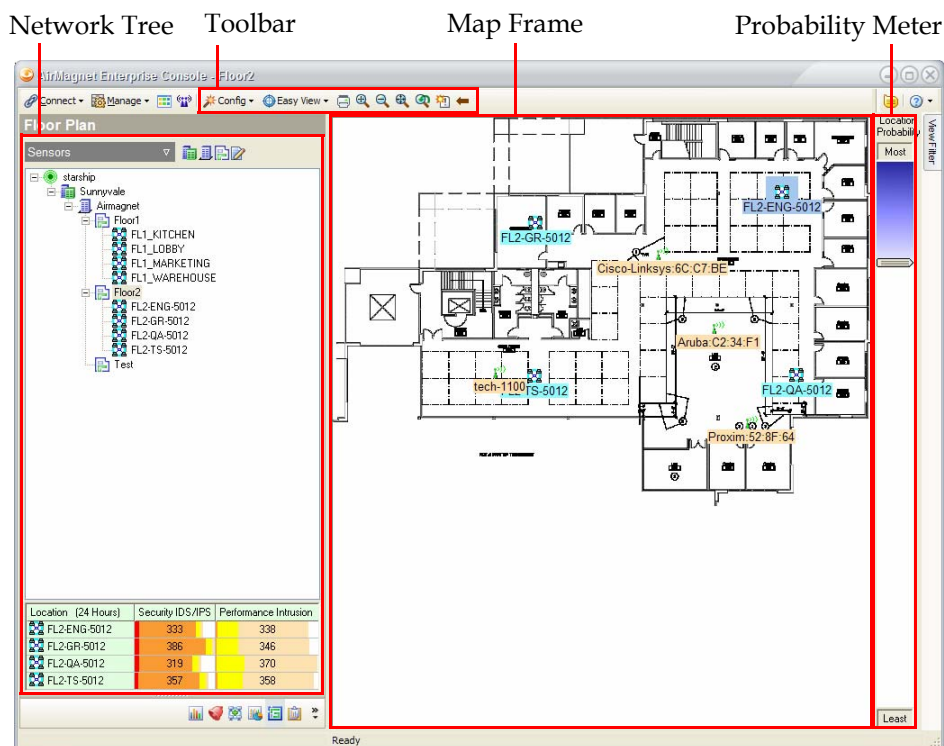


Figure 10-2: Floor Plan Components

Each portion highlighted above is covered in the following sections of this chapter.

Network Tree

The Floor Plan screen's Network Tree operates in the same manner as described in "Network Tree" on page 70. Users can select specific cities, buildings, floors, or sensors to view data from.

Note that in order to view a floor plan, a site image must be applied to the floor selected. Images can only be applied for floors in the network structure.

Toolbar

The Floor Plan screen contains several toolbar options that do not appear on the other screens. See [Figure 10-3](#).

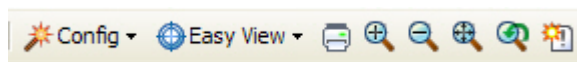


Figure 10-3: Floor Plan Toolbar

These buttons are described in [Table 10-1](#).

Table 10-1: Toolbar Buttons

Button	Description
Config	Allows the user to configure various aspects about the Floor Plan, including the site image used, amount of usable space, and site boundaries. See “Configuring the Floor Plan” on page 202 for more information.
Easy View	Allows the user to switch between the Device Locator and Survey Heatmap views.
Print	Prints the current site map.
Zoom In	Zooms in on the current image.
Zoom Out	Zooms out from the current image.
Zoom to Fit	Fits the image to fill the entire Map Frame.
Zoom Reset	Resets to the default zoom level.
Show Device Name	Toggles the device names on and off on the site map.

Map Frame

The Map Frame displays the map for the selected floor. All devices detected as well as the sensors deployed on the floor are displayed along with their names (unless the Show Device Name option is turned off).


Note that the devices displayed can be filtered or modified by using the View Filter tab. This can be useful for floors with large numbers of active devices cluttering the display.

Probability Meter

The Probability Meter allows the user to customize probable location of any given device. When a device is selected in the Map Frame, a blue “halo” should appear about the device, indicating the possible location(s) of the device. As the Device Locator service cannot be 100% accurate (due to varying wireless environment issues, such as site-specific interference), this

allows the user to customize the percentage of error to be built in to the device's location. By using the Probability Meter, users can customize the view to see the varying certainty of the device's location; as the slider bar is dragged downwards (towards the "Least" tag), a greater percentage of the area is shown.

Configuring the Floor Plan

As discussed earlier in this chapter, users must first configure a site map for the Floor Plan page before attempting to locate devices. This can be done using the  Config button in the Toolbar. See [Figure 10-4](#).

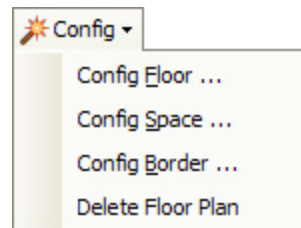


Figure 10-4: Configure Menu

As shown in the Figure above, the Config menu has several different options. These are described in the following sections.

The Delete Floor Plan option will delete any site map associated with the selected floor. Note that this also erases any areas or boundaries drawn on the plan.

Configuring a Floor Map

The Config Floor... option from the Config menu allows the user to import a site map for the floor selected from the Network Tree.

To apply a map to the current floor:

- 1) Click Config>Config Floor.... The Floor Plan Wizard appears. See Figure 10-5.

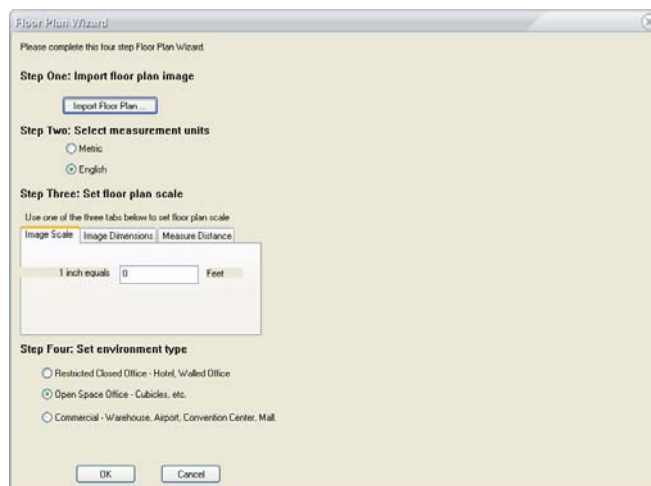


Figure 10-5: Floor Plan Wizard

- 2) Click Import Floor Plan... to import a site map. The Open Picture File window appears.
- 3) Browse to the desired floor plan image and click Open. The Floor Plan Wizard refreshes. See Figure 10-6.

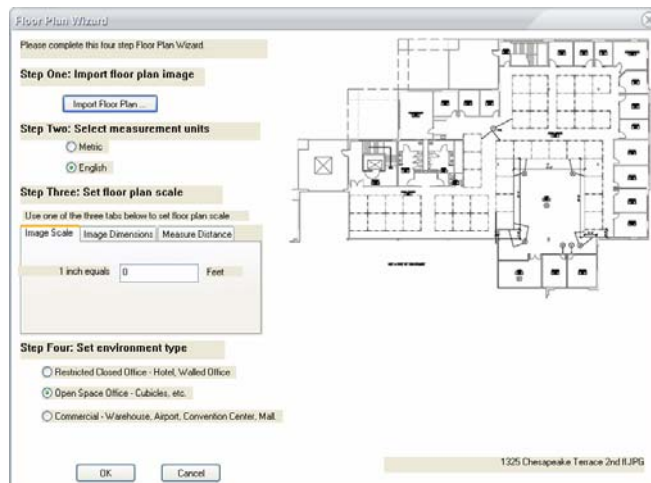


Figure 10-6: Imported Floor Plan

- 4) Select the measurement standard to be applied to the floor plan (Metric or Standard).
- 5) Enter the scale for the selected floor plan. This is easiest if the user knows that the image is drawn to a specific scale. Alternatively, users can use the Measure Distance tab to measure a small portion of the map that is a known length. For example, if a cubicle is known to be eight feet wide, this distance can be measured on the map and entered manually.

To measure a location manually, click and hold at the start location and drag the mouse cursor to the finish location.

- 6) Select the type of environment represented by the map from the options provided. This helps the Device Locator determine standard measurements for network impedance and interference based on the general location.
- 7) Click OK to save the new plan. The map is applied to the current floor.

Configuring the Network Space

After the site map has been imported for the selected floor, it is recommended that the user specify the actual portion of the map that is used for network traffic. This helps the Device Locator determine where devices are expected to be, limiting inaccurate results.

To configure the network space:

- 1) Click Config>Config Space.... Additional toolbar buttons appear to help users configure the different types of network space to be drawn. These buttons are color-coded, as

described in Table 10-2.

Table 10-2: Space Types

Color	Description
Red	Used to draw out walled office locations.
Yellow	Used to draw cubicle spaces.
Green	Used to draw warehouse areas.

- 2) Use the tools to draw the regions appropriate to the site map. See Figure 10-7.



Figure 10-7: Configured Network Space

- 3) Click Track Devices from the Toolbar to return to the Device Locator screen.

Configuring Site Boundaries

After the regions of the site have been designated properly, the user must draw out the site boundaries. This allows the Device Locator to determine the region that devices must be contained within.

To draw a site boundary:

- 1) Click the corner of the building or site from which the boundary should start.
- 2) Click a corner adjacent to the first. A red line will appear between the first point and the second. See Figure 10-8.

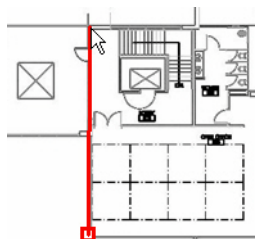


Figure 10-8: Red Boundary Line

- 3) Continue clicking the site corners until the building is completely outlined.

If a mistake is made in the drawing, the user can restart by right-clicking anywhere on the map. The drawing will restart when the user left-clicks the new starting point.

- 4) Click Track Devices from the Toolbar to return to the Device Locator screen

Placing Sensors on the Floor Plan

Unlike APs and stations, the sensors on the Floor Plan will not auto-place themselves, and thus the user must place each sensor by hand. To do so, simply drag the sensor image displayed on the plan to the appropriate location on the floor map. Sensors will automatically appear if they are placed on the floor in the Network Tree frame.

It is important that sensors are placed on the floor plan correctly. Misplaced sensors could cause discrepancies in the Device Location process, causing skewed results.

Locating Rogue APs

This section discusses the procedure used for identifying the location of rogue APs on a wireless network. Despite the heading of this section, the same procedure described here can be used for locating APs in any of the other categories as well, such as neighbor APs, monitored APs, guest APs, etc.

To show all rogue APs:

- 1) From the Floor Plan screen, open the View Filter tab.
- 2) Use the View Filter drop-down box to select Rogue APs. See Figure 10-9.

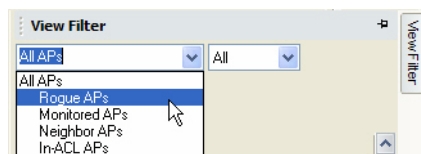


Figure 10-9: Filtering on Rogue APs

Note that the View Filter can also allow the user to manually filter results. By checking specific devices in the View Filter tab, the user can select precisely which devices should be displayed. Users can also “pin” devices by dragging them to the correct location on the map. A pushpin icon appears on the pinned device to show that it has been manually placed.

- 3) Click Apply. The Floor Plan screen refreshes, displaying only Rogue APs on the network. See Figure 10-10.

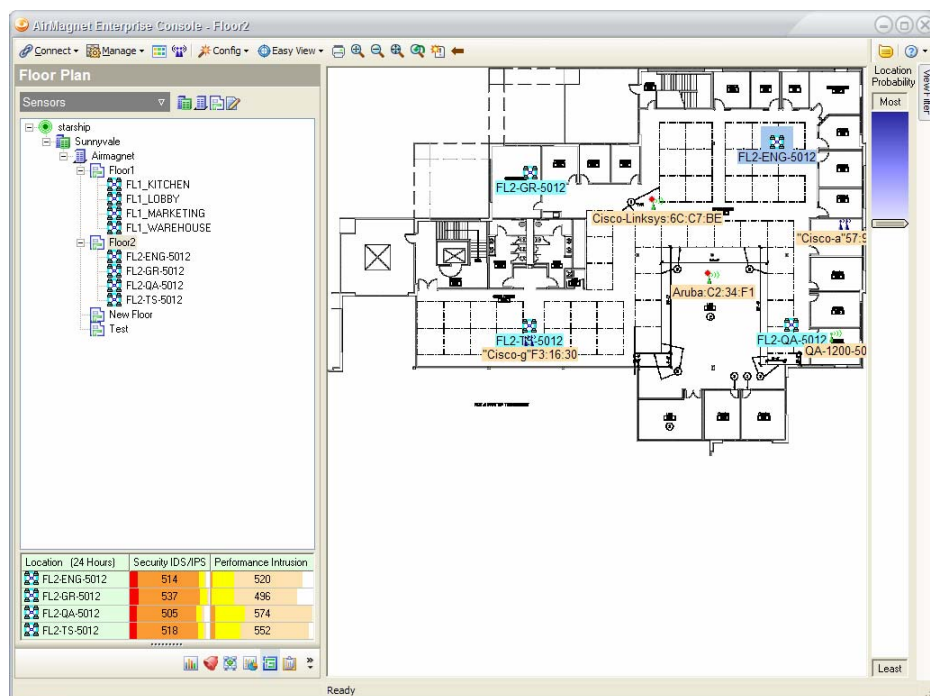


Figure 10-10: Rogue APs Displayed

In [Figure 10-10](#), two of the rogue APs displayed have a red dot on them. This indicates that the APs have triggered alarms on the Enterprise network.

Locating Rogue Stations

As shown in [Figure 10-9](#) earlier in this chapter, the Floor Plan's View Filter tab only allows filtering on APs. While the user can locate stations as well, the process is slightly different, and must be conducted from the Infrastructure screen.

To locate a rogue station:

- 1) From the Infrastructure screen, identify a rogue station that needs to be located.
- 2) Right-click the rogue station and select "Show location in Floor Plan". The Floor Plan screen appears with the selected station displayed. See [Figure 10-11](#).

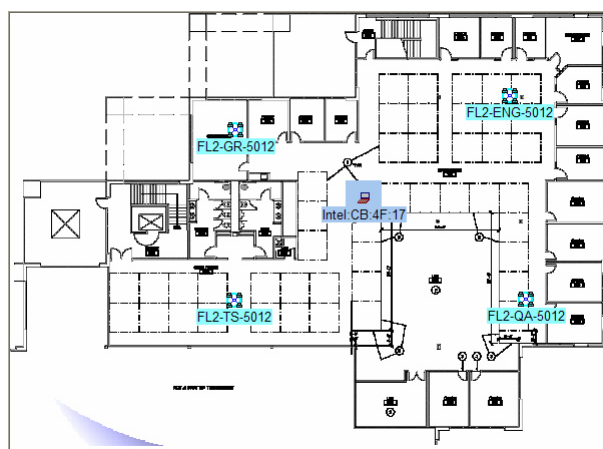



Figure 10-11: Rogue Station Shown

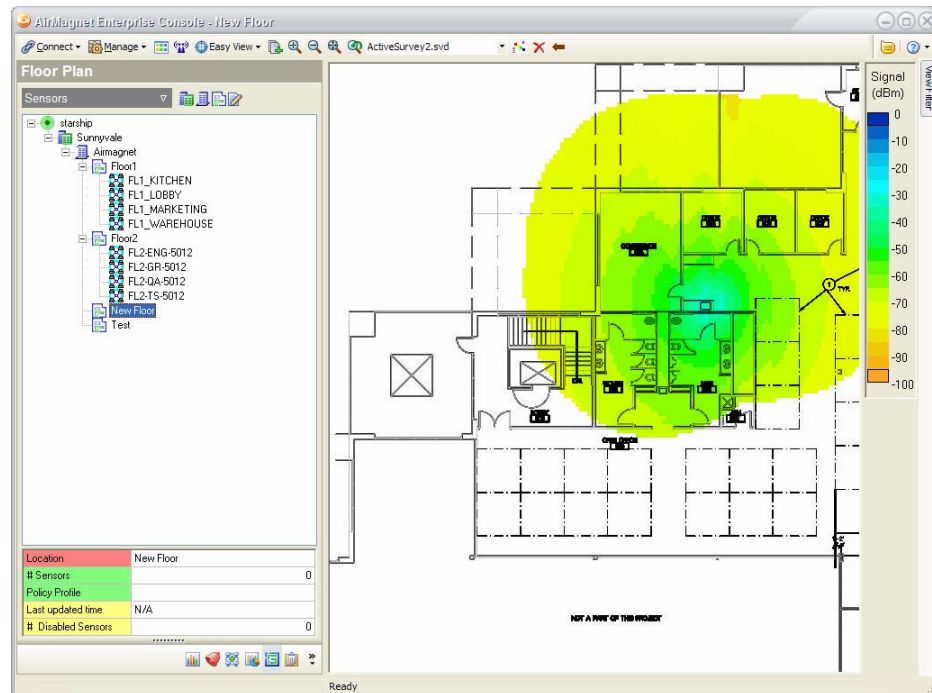
Note that the process outlined for locating rogue stations may also be applied to rogue APs or Ad-Hocs, if desired.

Displaying AirMagnet Survey Heat Maps

Enterprise users who have purchased AirMagnet Survey can import the heat map generated by a site survey to overlay onto the site plan. This can be useful for showing the actual wireless environment on the Floor Plan screen, which can help highlight discrepancies in the projected locations of devices.

To view a Survey heat map:

- 1) Click Easy View>Survey Heatmap. A new button appears on the toolbar, which allows the user to import a heat map.
- 2) Click  (Import SVD File). The Import SVD File window appears.
- 3) Browse to the .svd file of interest and click Open. The heat map appears in the Map Frame. See [Figure 10-12](#).



**Figure 10-12: Survey Heat Map Data**

Chapter 11: Using the Reports Screen

Introduction

The Reports screen provides a powerful reporting utility that automatically converts all sorts of WLAN data into professional reports and presents them in an organized, easy-to-understand fashion. Not only does it allow you to view and output various reports, but also lets you compile your own custom report books using selected individual reports.

Major UI Components

You can bring up AirMagnet Enterprise Reports from any of the major screens of the Enterprise Console by clicking  **Reports** from the Navigation Bar. Several screens also allow quick access to specific reports by clicking  **View Reports**, and then selecting a report option from the list menu. The image below displays the major UI components in the Reports screen. See [Figure 11-1](#).

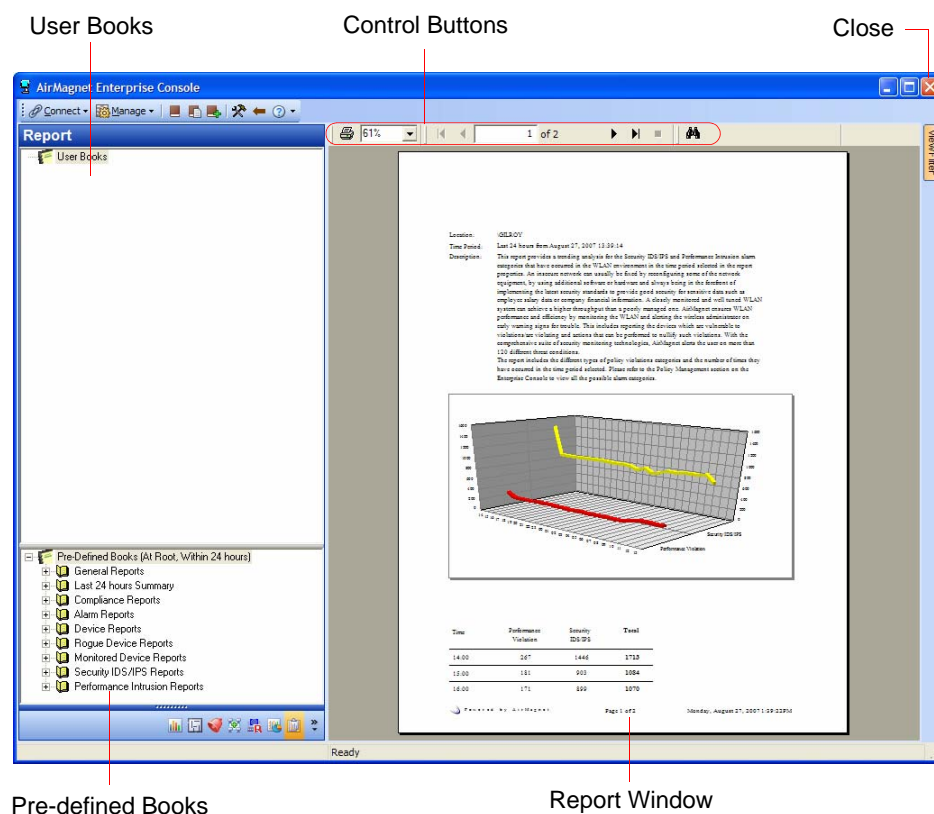



Figure 11-1: AirMagnet Enterprise Reports screen

Each entry in the View Report drop-down menu represents a specific type of report. The content of the drop-down menu varies depending on the Console screen you are on. Clicking an entry in the drop-down menu opens the Reports screen, which by default displays the report you have selected. The  View Reports button provides easy and quick access to reports that are specific to the Console screen you are currently on.

Managing Report Books

The Reports screen uses the book concept to enable users to compile report books, which are collections of selected reports. It provides a convenient way for organizing, sharing, and archiving your WLAN data. The Report Books portion of the screen contains two separate sections, as shown in [Figure 11-1](#).

- User Books— This part of the screen allows you to compile your own report book, which is a collection of reports selected from the Pre-defined Books section of the screen.
- Pre-defined Books— This part of the screen shows the collection of all the reports that the program has generated. The reports are grouped by the screen to which the data are related. Clicking an entry opens the report in the report window.

The words “At Root, Within 24 hours” in parentheses following Pre-defined Books in [Figure 11-1](#) indicate the location and time frame of the reports that AirMagnet Enterprise uses when generating the reports listed in the Pre-defined Books section. The word “root” refers to the segment or location of the network tree structure which the reports are all about. It could be an Enterprise Server, a city/campus, a building, a floor, or a Sensor that you select from the network tree. To this extent, the words in parentheses simply tells you that those pre-defined reports are based on data collected at the selected location during the specified time frame.

Creating a Report Book

To create a report book:

- 1) Right-click **User Books** and select **New Book...** from the drop-down menu. The AirMagnet Report Book Detail dialog box appears. See [Figure 11-2](#).

Figure 11-2: Creating a new report book

- 2) Make the following entries and/or selections as described in [Table 11-1](#).


Table 11-1: Parameters for a Report Book

Entry	Description
Book Name	Enter a title for the report book. This title will appear on the highest level in the report book structure on the left-hand side of the Reports screen.
Main Title	Enter a main title for the book. This title will appear on the top of the book's cover page.
Subtitle	Enter a subtitle for the book. It should help explain the main title.
Author Info	Enter some information about the person who compiles the book, e.g., name, title, etc.
Company Info	Enter some information about the entity which the report is all about.


- 3) Click **OK**. The newly created book will be added in the User Books section.

You can view the cover page of any book by clicking the Book Title or Cover. The table of contents for new books start out empty since no reports have been added yet.

Adding Reports to a Book

The Reports screen provides two ways for creating custom report books: using  (Add to Book) or dragging and dropping reports from the Pre-Defined Books section to a new book created in the User Books section. The following discussion covers both scenarios.

Adding Reports with the Add-to-Book Button:

- 1) From the User Books section, highlight the title of the newly created book.
- 2) From the Pre-defined Books section, click to select a report.
- 3) Click  (Add to Book). The report will be added to the user book, and the title of the report will be added to the table of contents.
- 4) Repeat Steps 2 and 3 to add more reports to the report book.

Adding Reports by Drag-and-Drop

- 1) From the Pre-Defined Books section, select the report of interest and drag it to the newly created report book in the User Books section.
- 2) Release the mouse button when the title of the book or any chapter of book becomes highlighted. The report will appear in the book.
- 3) Repeat Steps 1 and 2 to add the other reports.

Deleting Reports from a Book

You can delete any part of a report book, including the cover page, table of contents, and individual chapters.


To remove a part from a report book:

- 1) From the User Books section, right-click the part of the book to be deleted.
- 2) From the pop-up menu, click **Delete....** A confirmation message appears.
- 3) Click **Yes**. The selected item will be deleted from the report book when the screen refreshes.

Searching Text through a Report

You can conduct text-based searches through a report using the Reports screen's **Search Text** tool, which allow you to find any alphanumeric characters or string of characters.

To search text in a report:

- 1) Open a report from the Report screen.
- 2) Click  (Search Text). The Search dialog box appears.
- 3) Enter the text you want to find, and click **Find Next**.
- 4) The program will find the text, if it exists, and highlight it in the report window.
- 5) Keep clicking **Find Next** until you reach the end of the report.

Modifying Book Properties

You can modify a report book by changing the book title, cover page, and the title of the reports inside the book. You can also add or delete reports to or from the book. All these operations can be carried out using the pop-up menu that appears when you right-click any component of a book in the User Books section. Book properties refer to all the information you entered in the AirMagnet Report Book Detail dialog box at the time a report was created. They include the book title, cover page, table of contents, etc.

To modify the properties of a book:

- 1) From the Custom Books section, right-click the book title and select **Properties...** from the pop-up menu. The AirMagnet Report Book Detail dialog box appears, showing the information that was entered when the report book was created.
- 2) Make the desired changes by highlighting the text and overwriting it with new information.
- 3) Click **OK** when completed.

Modifying Report Contents

This feature allows you to modify the content of the chapters (or reports) in a report book.

To modify the contents of a report:

- 1) Right-click the chapter of interest in a report book, and select Properties from the drop-down list. The AirMagnet Report Detail dialog box appears. See [Figure 11-3](#).

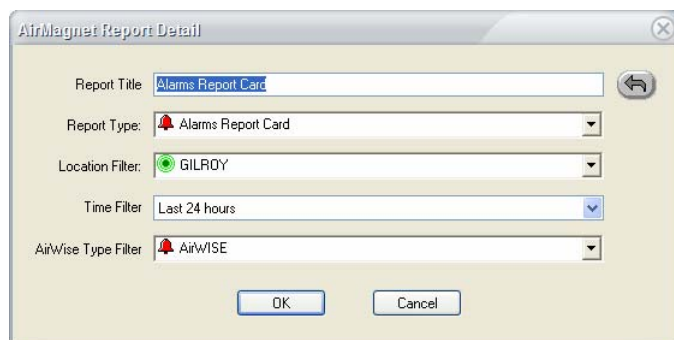




Figure 11-3: Modifying contents of a report

You can also open the AirMagnet Report Detail dialog box by selecting a report and then clicking the  (Report Properties) button.

- 2) Make the desired changes as described in Table 11-2.

Table 11-2: Report Detail Options


Field	Description
Report Title	Overwrite the report's current title with a title of your choice. This title can also be automatically created using the  (Generate report title from filters) button.
Report Type	This drop-down allows the user to change the type of report selected. Adjusting this field works in a similar manner to simply selecting a different report from the pre-defined books.
Location Filter	This drop-down allows the user to specify that the report display data only from a specific building, floor, etc.
Time Filter	This drop-down allows the user to narrow the report's data to within a specific time frame. Users can select from a list of pre-determined time intervals or select a custom one by selecting Custom Times. <i>This field will not appear if the Report Type currently selected is Sensors or Policy Profile.</i>
Policy Profile	This drop-down allows the user to specify the policy profile to be used in the report. <i>This field only appears when the Policy Profile Report Type is selected.</i>
AirWISE Type Filter	This drop-down allows the user to select a specific policy or policy tree to view report data on. <i>This field only appears if one of the Alarms Reports is selected.</i>
Device Filter	This drop-down allows the user to select certain types of devices to view, based on their status in the ACL (Monitored, Rogue, etc.) <i>This field only appears if one of the Devices Reports is selected.</i>
Generate report title from filters	This button generates a descriptive title for the report based on the filters selected.

- 3) Click **OK**. The selected chapter will be modified based on the entries or selections you have made.

Printing Data Reports

You can print any report or report book by right-clicking the corresponding entry in the User Books section and then selecting **Print** from the pop-up menu.

To print a report or report book:

- 1) From the User Books section, right-click the report or report book and select Print (you may also print a report by selecting it and then clicking the  button). The **Print** dialog

box appears. See Figure 11-4.

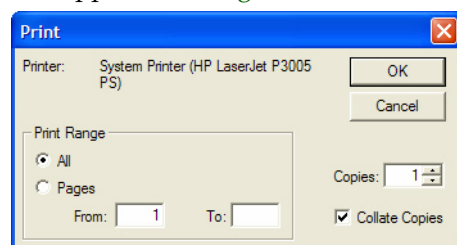


Figure 11-4: Print dialog box

- 2) Make the desired selections and click **OK**.

Exporting a Report or Report Book

You can export a report or report book directly from the Reports screen. You can save the reports to a disk using any of the file formats that AirMagnet supports.

To export a report or report book:

- 1) From the Reports screen, right-click the report or report book of interest, and click **Export** from the pop-up menu. The Report(s) Export dialog box appears. See Figure 11-5.

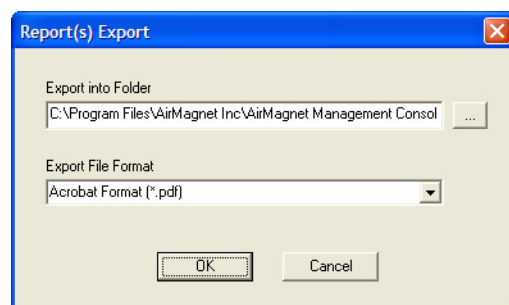


Figure 11-5: Report(s) Export dialog box

- 2) Select a destination to which the report(s) will be exported, if it is different from the default.
- 3) Click the down arrow and select a file format from the drop-down list.

AirMagnet reports can be exported in .pdf, .html, .xml, .doc, .rtf, and .xls formats.

- 4) Click **OK**.

Automatic Report Generation

Report scheduling lets users configure Enterprise to automatically generate a specific report book (or books) at regular intervals in order to maintain records of company data. These reports may then be automatically emailed to any number of users who require this information.

Automatic report generation requires that the user create a report book and configure the Report Email Server before scheduling the process. The following sections describe these steps.

Configuring the Report Email Server

The Report Email Server settings provide Enterprise with the email account information to be used when automatically sending generated reports and report books to selected users/email addresses. Users must provide this information before automatic report generation can be used to send reports to other users.

To configure the report email server:

- 1) From the Console, click **Manage>Auto Report Task....** The Schedule Auto Report Task window appears.
- 2) Click the **Mail Server...** button located at the lower-right portion of the window. See [Figure 11-6](#).

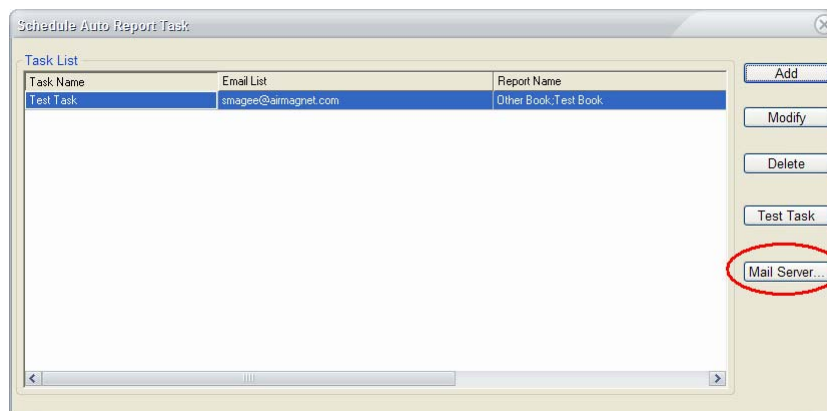


Figure 11-6: Mail Server Button

- 3) The Email Notification Configure for AUTO Report dialog box appears. See [Figure 11-7](#).

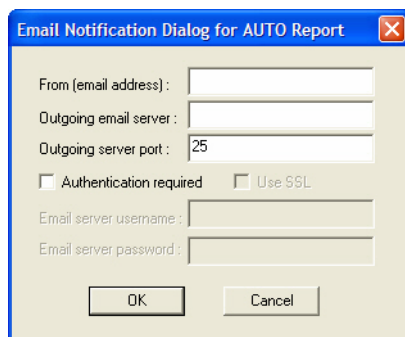


Figure 11-7: Mail Server Info

- 4) Enter the required information as described below.

Table 11-3: Mail Server Configuration

Field	Description
From (email address)	Enter the email address that will be used to send the reports (e.g., AutoReports@airmagnet.com)
Outgoing email server	Enter the outgoing email server for the email address entered in the From field (e.g., mail.airmagnet.com).
Outgoing server port	Enter the port used by the outgoing email server. As shown above, this value defaults to 25.
Authentication Required	Check this box if the email server requires authentication information.
Use SSL	This box will only be available if the Authentication required box has been checked. Check this box if the email server uses the Secure Sockets Layer (SSL) protocol for sending secure email.
Email server Username	This field will only be available if the Authentication required box has been checked. Enter the username required to log into the email server.
Email server Password	This field will only be available if the Authentication required box has been checked. Enter the password required to log into the email server.

- 5) Click OK to save the changes.

Scheduling a New Auto Report Task

After configuring the Report Email Server, the user can schedule a new automatic report task.

To schedule auto report generation:

- 1) From the Console, click **Manage>Auto Report Task....** The Schedule Auto Report Task window appears. See [Figure 11-8](#).

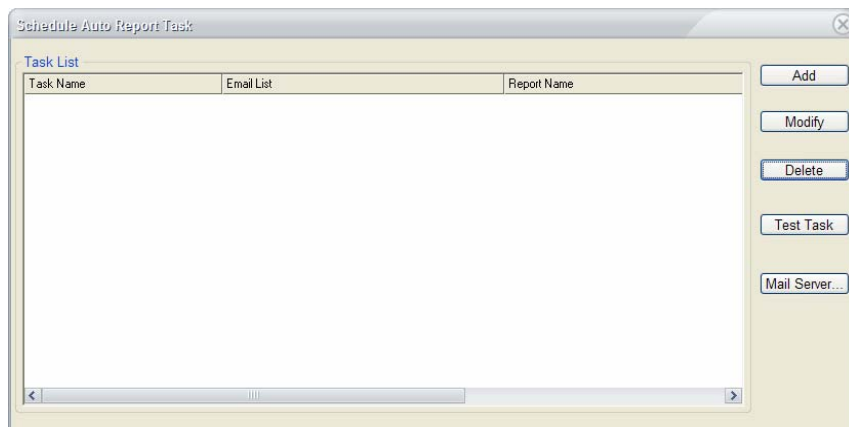


Figure 11-8: Auto Report Task List

- 2) Click **Add** to bring up the Add a New Auto Report Task dialog box. See [Figure 11-9](#).

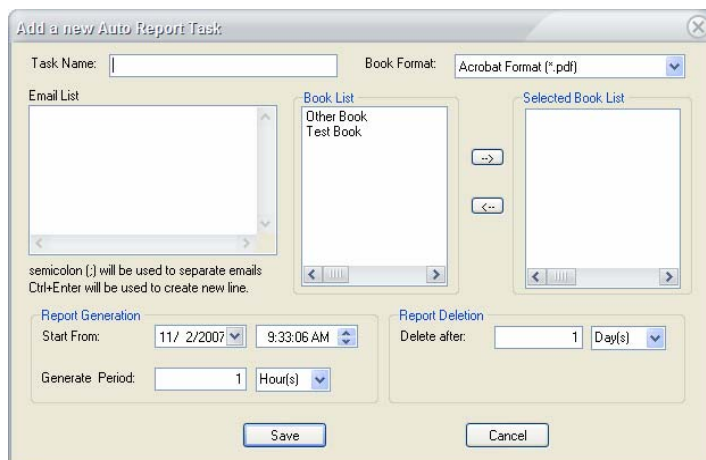




Figure 11-9: Add New Auto Report Task

- 3) Enter the required task information as described in [Table 11-4](#).

Table 11-4: New Report Task Options

Field	Description
Task Name	Enter a unique name for this report task. This name will be used to identify the task in the Schedule Auto Report Task window displayed above.
Book Format	Use this drop-down to select a format for the book(s) to be sent in.

Table 11-4: New Report Task Options

Field	Description
Email List	Enter the email addresses that the book(s) should be sent to. As described in the dialog box, separate multiple email addresses with semicolons (;). Press Ctrl+Enter to start a new line.
Book List	This area allows the user to select the report book(s) to be emailed. Simply click each book that should be scheduled; after all required books are selected, click  to add them to the Selected Book List. To remove books from the list, simply select them and click  .
Start From	Specify the date and time that this auto report task will first be performed.
Generate Period	Specify the frequency with which the task should be repeated. By default, the task will be run once every hour.
Delete After	Specify how long the Enterprise Server should retain a copy of the book(s) generated. The book(s) are stored on the server so that users can download them. This field lets the server administrator specify when old report data will be eliminated.

- 4) Click **Save** to save the new Report Task and return to the Schedule Auto Report Task window.
- 5) The user can test the new task by clicking **Test Task**. A message appears describing whether the task passed or failed the task. If a failure message appears, the Report Email Server configuration may be incorrect.

Compliance Reports

Compliance reports provide you with an easy-to-view summary of your network's compliance with various industry standards. The following sections briefly describe some of the compliance reports provided by AirMagnet.

Department of Defense Directive 8100.2

The Department of Defense (DoD) Directive Number 8100.2 (the Directive hereafter) stipulates the key policy sections regarding the use of commercial wireless devices, services, and technologies in the DoD. Its purpose is to safeguard the DoD networks from the security vulnerabilities inherent with wireless networks, making security a prerequisite for the deployment and use of commercial wireless technologies in the DoD.

Health Insurance Portability and Accountability Act

HIPAA was passed to improve the efficiency and effectiveness of the nation's health care system and promote the use of EDI (Electronic Data Interchange) in health care. To accomplish its purpose, regulations were issued by HHS (Department of Health and Human Services) to safeguard the privacy and security of the PHI (Protected Health Information). PHI is any health information that identifies an individual and relates to his or her physical or mental health.

Gramm-Leach Bliley Act

The "Gramm-Leach Bliley Act" (GLBA), also known as the Financial Services Modernization Act of 1999, mandates that financial institutions protect the security and confidentiality of their customers' personally identifiable financial information.

Sarbanes-Oxley Act

The Sarbanes-Oxley (SOX) Act, also known as the Public Company Accounting Reform and Investor Protection Act, was passed by the US Congress in 2002 as a comprehensive legislation to reform the accounting practices, financial disclosures, and corporate governance of public companies.

Payment Card Industry Data Security Standard

The PCI Data Security Standard was developed by Visa and MasterCard to prevent identity theft and credit card fraud. It is a standard required of Visa and MasterCard Members, service providers, and merchants and one voluntarily adopted by other card associations like American Express and Discover Card as a condition for participation. Participating businesses must comply with 12 "best practice" requirements for wireline and wireless networks and validate their compliance periodically. AirMagnet Enterprise supports PCI v2 reports.

Basel II

The Basel II Accord promotes greater consistency in the way banks and banking regulators approach risk management. It is designed to establish minimum levels of capital for internationally active banks. In specific regard to AirMagnet, Basel II incorporates an explicit capital charge for operational risk. Operational risk includes the security risks in operating a wireless network. Basel II succeeds the Basel I Accord. Both were developed by the Basel Committee on Banking Supervision (hereinafter, the Committee). The Committee is made up of bank supervisors and central bankers from the Group of Ten (G10) countries. The G10 countries include: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States. International banks can use AirMagnet products and Compliance Reports™ to identify and mitigate the operational risks of maintaining a wireless network.

EU CRD/CAD3

The European Union (EU) Capital Requirements Directive, popularly known as CAD3 (Capital Adequacy Directive), implements the Basel II Accord and introduces new capital requirements for internationally active banks, credit institutions, and investment firms in the EU. It succeeds earlier directives that implemented the capital requirements found in the Basel I Accord. AirMagnet System- and Device-level Compliance Reports™ will identify the operational risks in wireless networks that may lead to system disruptions or failures and external fraud.

ISO 27001

ISO/IEC 27001:2005 (hereinafter ISO 27001) is an International Standard designed for all sizes and types of organizations (government and non-government). At base, the International Standard should be used as a model to build an Information Security Management System (ISMS). An ISMS is part of an organization's system that manages networks and systems. It is premised on business risks and aims to “establish, implement, operate, monitor, review, maintain, and improve information security.” Going beyond the model, organizations can attain an ISO 27001 certification from independent auditors. A certification can show an organizations commitment to security and instill trust with partners and customers. It can also be used as evidence in compliance with legal requirements, but it will not, in itself, satisfy legal requirements. Independent auditors like ISOQAR and Lloyd's Registered Quality Assurance (LRQA) certify an organization's compliance with ISO 27001. Note that the American National Accreditation Body (ANAB) in the United States and the United Kingdom Accreditation Service in the United Kingdom regulate ISO 27001 auditors. AirMagnet Enterprise can satisfy ISO 27001 and 17799 requirements for wireless networks and devices with System Level, Policy Level, and Device-Specific Compliance Reports. Using the ISO 27001 Plan-Do-Check-Act model, AirMagnet solutions can help an organization PLAN, CHECK, and ACT to improve an ISMS.

FISMA

FISMA (Federal Information Security Management Act) mandates that Federal agencies like the Department of Health and Human Services, the FCC (Federal Communication Commission), and the FTC (Federal Trade Commission) develop, document, and implement an information security program to provide security for the information and information systems that support the operations and assets of the agencies. This includes the information and information systems provided to the agency from another agency or from a contractor.

FISMA applies to the following:

- All information in the Federal government except information marked as classified.
- All information systems except those operating as national security systems.
- Any organization that is a government agency, sells hardware and/or software to a government agency, or supports the information or information systems of a government agency.

Compliance Reports Disclaimer

AirMagnet DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley, and Payment Card Industry Data Security Standard (PCI DSS) Compliance Reports provide a security framework to comply with regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on wireless network security and aim to guide network administrators in documenting their security policies and responding to security threats and incidents in compliance with industry best practice and government regulations.

AirMagnet Policy Compliance Reports provide information about the law and are designed to help users satisfy government regulations. This information, however, is not legal advice. AirMagnet has gone to great lengths to ensure the information contained in the Policy Compliance Reports is accurate and useful. AirMagnet, Inc. recommends you consult legal counsel if you want legal advice on whether our information and software is interpreted and implemented to fully comply with industry regulations.

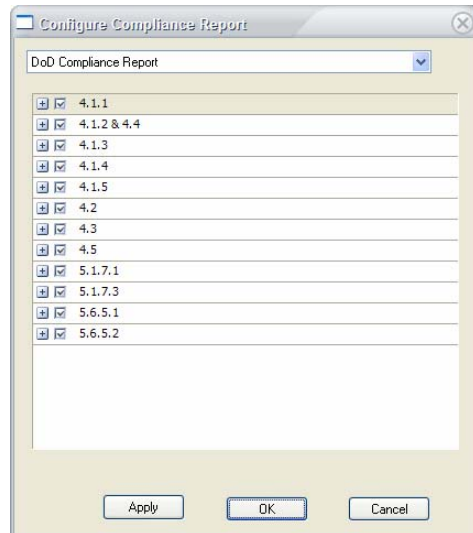
The information contained in the Policy Compliance Reports is furnished under and subject to the terms of the Software License Agreement ("License"). The Policy Compliance Reports do not create a binding business, legal, or professional services relationship between you and AirMagnet, Inc. Because business practice, technology, and governing laws and regulations vary by location, full compliance with regulations will depend on your particular circumstances.

Customizing Compliance Reports

If the data reported by the existing compliance reports provided by AirMagnet Enterprise don't match the requirements of the user's corporate network, users may customize the information used by each type of compliance report. The ability to configure specific report information can help users to tailor Enterprise's reporting abilities to the needs of the company.

To customize compliance report data:

- 1) From the Console's Reports screen, click  (Config Compliance Report). The Configure Compliance Report dialog box appears. See [Figure 11-10](#).

**Figure 11-10: Compliance Report Customization**

- 2) Use the drop-down box at the top of the window to select the compliance report to be customized. The lower pane displays all the sections in the selected report.
- 3) Use the '+' buttons to expand each section. This will reveal the alarms reported on a section-by-section basis.
- 4) Uncheck the alarms that should not be included in the report.
- 5) Click **Apply** to save the changes, and click **OK** to close the dialog box.

Chapter 12: Managing Policy Profiles

Introduction

This chapter discusses the ways to create and modify security and performance policy profiles and assign them to various locations on your WLAN network. From our discussions in the preceding chapters, it is apparent that WLAN policies play an important role in the AirMagnet Enterprise solution. Therefore, the ability to create and manage policies to address the specific needs of your network is essential to successful implementation of the AirMagnet Enterprise technology solution.

Network administrators must keep the following important questions in mind when configuring a policy profile:

- Which part of the WLAN do you want to monitor (location and Sensor)?
- What policy or policies do you want to implement (Security IDS/IPS vs. Performance Intrusion, general policies vs. specific policies within a policy category)?
- Which WLANs (i.e., SSIDs) do you care most (e.g., VoWLAN, corporate WLAN, neighboring WLAN, Guest WLAN, etc.)?
- Who should be notified in case of policy violations?
- How should the person be notified (e.g., via email, sound, SNMP, etc.)?

The comprehensive security IDS/IPS and Performance Intrusion alarms generated by AirMagnet's AirWISE expert engine have proved powerful in WLAN intrusion detection & prevention and performance monitoring. This patent-pending intelligent network management technology is a major component of the AirMagnet Enterprise, especially for managing large-scale enterprise Wireless networks. The AirMagnet Enterprise uses a layered policy structure that greatly facilitates WLAN event management and analysis. Understanding this structured policy configuration not only helps WLAN administrators characterize and interpret the nature of various policy violations, but also enables them to take the right course of action when needed.

Policy Profile Creation Procedures

You can manage your network policies by selecting **Policy Profiles...** under the Manage menu. Managing network policies involves creating new policy profiles and modifying or removing existing ones. You can do this by configuring or modifying alarm notifications, policy settings, and sensor options.

The procedure for managing network policies is as follows:

- 1) Select a location on your WLAN (i.e., city>building>floor).
- 2) Select the AirMagnet SmartEdge Sensor that covers the location.
- 3) Determine what policy you want to manage:
 - Security IDS/IPS
 - Performance Intrusion

- 4) Select a policy category, its subcategory, and then a specific policy within the category.
- 5) Configure the following policy settings:
 - Threshold
 - SSID
 - Notification
 - Severity

The AirMagnet Enterprise system allows you to configure multiple Threshold, SSID, Notification, and Severity settings. See the sections later in this chapter for more information.

Creating Network Policy Profiles

AirMagnet Enterprise provides a number of ways to streamline and simplify policy configuration. Depending on the user's experience with the system or preference, new policy profiles can be created by:

- Starting from scratch;
- Adapting a default policy profile; or
- Importing a policy profile.

Creating a Policy Profile from Scratch

This method is used for creating new policy profiles without using any pre-configured policy profile as a reference. It is often used by advanced users of AirMagnet Enterprise who are familiar with all the intricacies involved in policy configuration.

To create a policy profile from scratch:

- 1) From the AirMagnet Enterprise Console screen, click **Manage>Policy Profiles....** The Manage Policy Profiles screen appears. See [Figure 12-1](#).

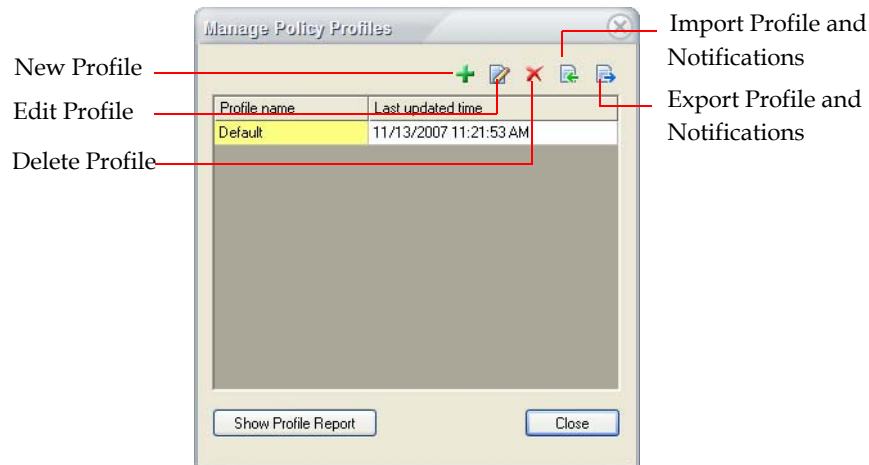


Figure 12-1: Manage policy profiles screen

- 2) Click **+** (New Profile). The New Profile Name screen appears. See [Figure 12-2](#).

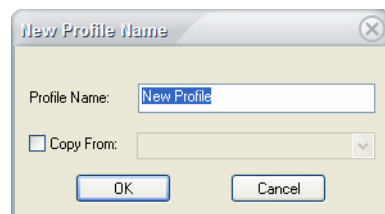


Figure 12-2: New Profile Name screen

- 3) Enter a name for the new policy profile, and click **OK**. The AirMagnet Policy Management screen appears, which allows you to modify the policy settings. See

Figure 12-3.

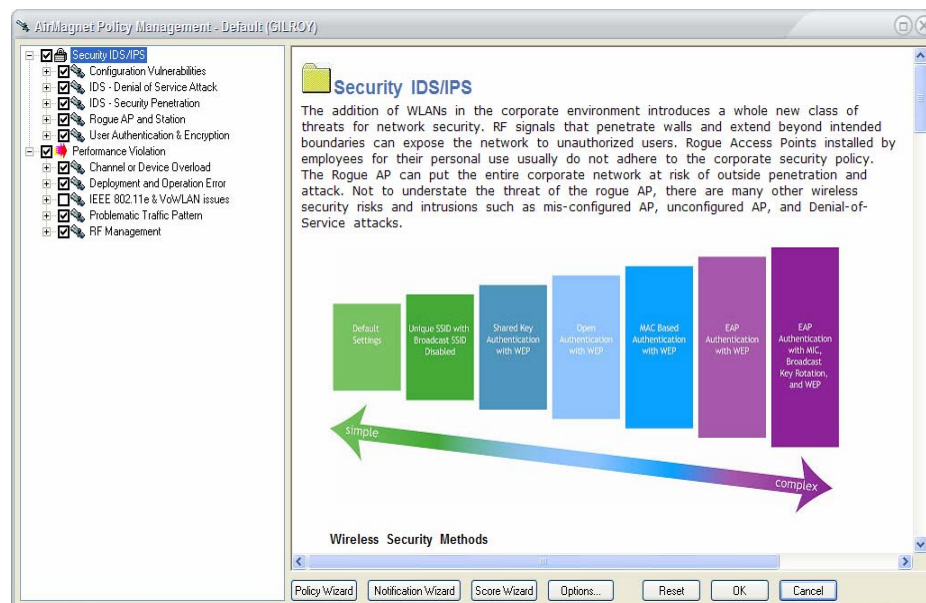


Figure 12-3: AirMagnet Policy Management screen

Using a Pre-Configured Policy Profile

This is perhaps the easiest and quickest way to create a new policy profile. All you need to do is to copy a pre-configured policy profile and adapt it to the needs of your network environment.

To adapt a policy profile:

- 1) From the AirMagnet Enterprise Console screen, select **Manage>Policy Profiles....** The Manage Policy Profiles screen appears. See Figure 12-4.

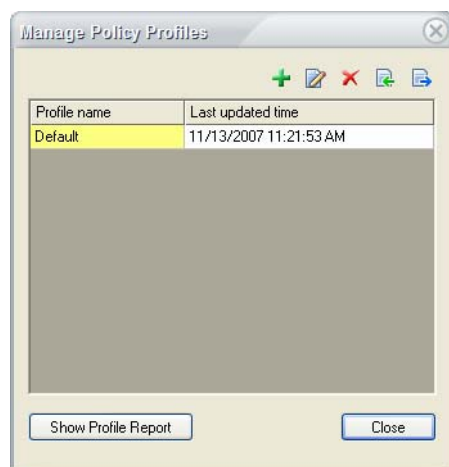



Figure 12-4: Manage Policy Profiles screen

- 2) Click  (New Profile). The New Profile Name screen appears. See Figure 12-5.

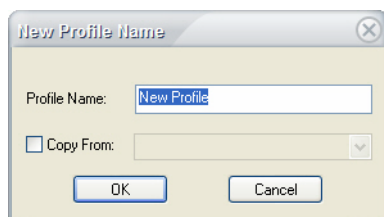


Figure 12-5: New Profile Name screen

- 3) Enter a name for the new policy profile, check the **Copy From** check box, click the down arrow to select a pre-configure policy profile from the drop-down list. See Figure 12-6.

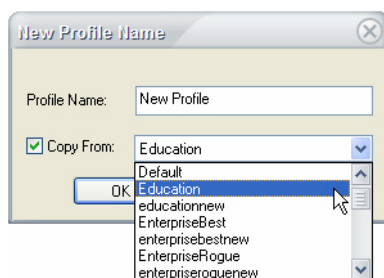


Figure 12-6: Selecting a pre-configured policy profile

- 4) Click **OK**. The AirMagnet Policy Management screen appears, which allows you to modify the policy settings. See Figure 12-3.


Exporting and Importing Policy Profiles

Any policy profile can be exported (saved) from one AirMagnet Enterprise Server and then imported into another AirMagnet Enterprise Server. This makes it easier to share policy profiles between AirMagnet Enterprise Servers on a large enterprise network. In this sense, new policy profiles can also be created by importing and adapting existing policy profiles.

It is important to note that, since policy profiles are associated with notifications, AirMagnet Enterprise makes the export and import of notifications an integral part of policy profile export or import.

Exporting Policy Profiles and Notifications

To export a policy profile:

- 1) From the AirMagnet Enterprise Console screen, click **Manage>Policy Profiles....** The Manage Policy Profiles screen appears.
- 2) Click  (Export Profile and Notification). The Export Profile dialog box appears. See Figure 12-7 and Figure 12-8.

Each AirMagnet Enterprise policy profile consists of two types of files: Profile Files (.aci) and Notification Files (.ali). Then exporting a policy profile, you are required to export both the profile (i.e., .aci file) and the notification list (i.e., .ali file) that is used in the profile. For this reason, you will see two different dialog boxes that appear one after the other as shown in Figure 12-7 and Figure 12-8.

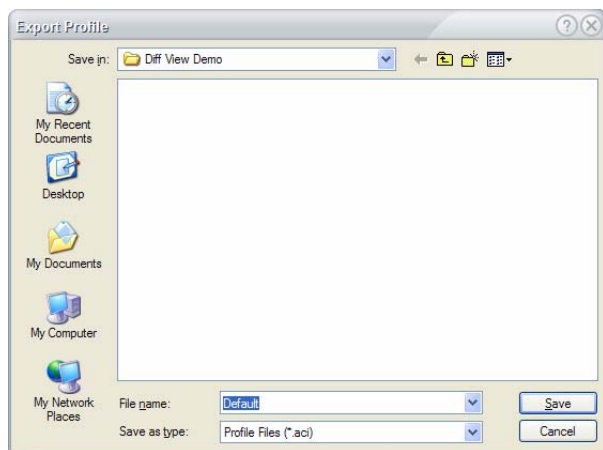


Figure 12-7: Exporting a profile

- 3) Specify the export destination and click **Save**. The Export Profile dialog box closes and the Export Notifications dialog box appears. See Figure 12-8.

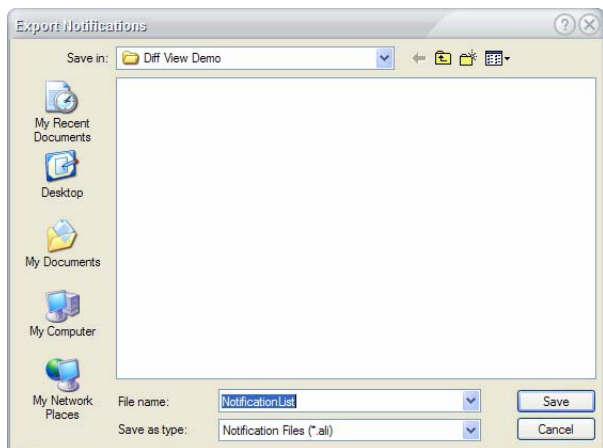



Figure 12-8: Exporting a list of notifications

- 4) Click **Save**.

As shown in [Figure 12-7](#) and [Figure 12-8](#), Profile Files use the .aci file extension while Notification Files use the .ali file extension. The two files are related and, therefore, should be stored in the same location. This will make importing the policy profiles much easier.

Importing Profiles and Notifications

To import a profile and notifications:

- 1) From the AirMagnet Enterprise Console screen, click **Manage>Policy Profiles....** The Manage Policy Profile screen appears.
- 2) Click  (Import Profile and Notification). A confirmation message appears. See [Figure 12-9](#).

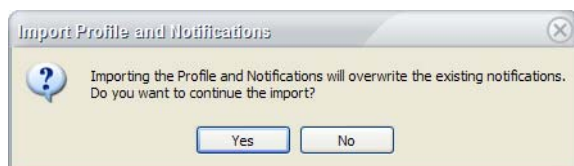


Figure 12-9: A warning message

Each AirMagnet Enterprise Server can only have one notification file (i.e., Actionlist.ali). Therefore, when you import an policy profile, you are overwriting the .ali file with the one that comes with the profile you are importing. The confirmation message is to tell the user what's going to happen to the existing .ali file.

- 3) Click **OK**. The Import Profile dialog box appears. See [Figure 12-10](#).

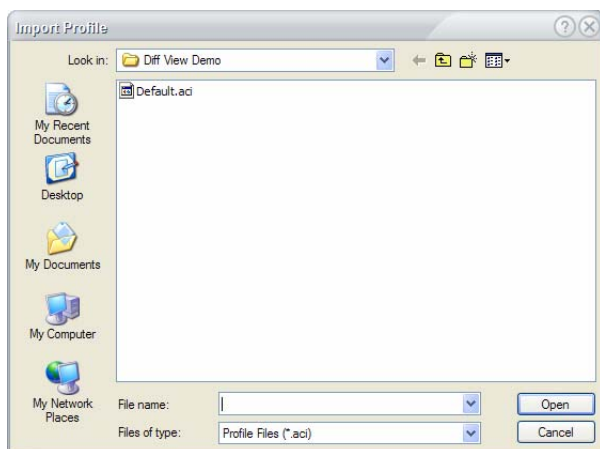


Figure 12-10: Importing a profile

- 4) Highlight the name of the profile and click Open. The Import Profile dialog box closes and the Import Notifications dialog box appears. See Figure 12-11.

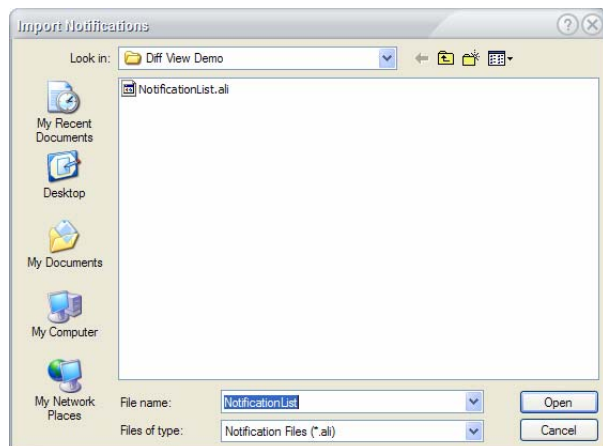


Figure 12-11: Importing notifications

- 5) Highlight the name of the file and click Open.

Managing Network Policies

After a policy profile has been created, users can set up which policies should be activated within that profile using the AirMagnet Policy Management window. This window appears automatically after a policy is created or is double-clicked from the Manage Policy Profiles dialog box.

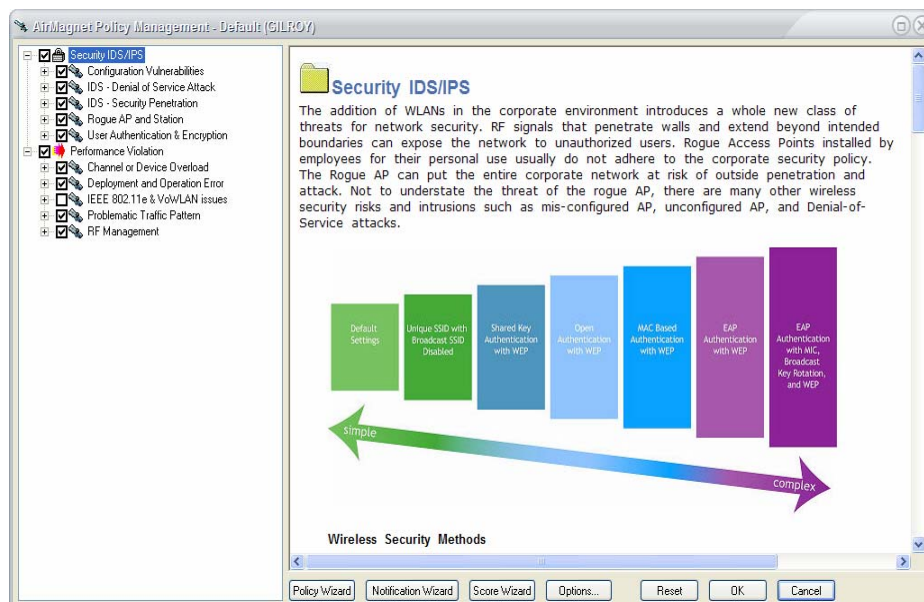


Figure 12-12: AirMagnet Policy Management Window

The left-hand side of the AirMagnet Policy Management screen displays all the policy violations that could happen to a WLAN. The events are divided into 10 major categories which fall evenly under two groups: Security IDS/IPS and Performance Intrusion. The user must fully expand each event category to see all the specific policy violations within that category. By default, all policy violations are enabled (checked) when the AirMagnet Policy Management screen opens (i.e., when you create a new policy profile).


To modify activated policies in the current profile:

- 1) From the left-hand side of the screen, deselect (uncheck) the policy violations that are irrelevant or unimportant to your network.

When a specific policy violation is selected, a list of policy rules will appear at the bottom of the right-hand side of the screen. In the upper right-hand corner of the screen are three control buttons. The policy rules are numbered, each row representing a specific network policy rule. While most policy violations can have multiple policy rules, certain violations can have only one policy rule. For this reason, you may get the error message "Multiple policy rules are not allowed for this alarm," when you try to add a new policy rule to certain alarms.

- 2) To modify the notification(s) associated with a specific alarm, select the alarm in the policy tree and select the notification of interest in the bottom right.

You may use either the buttons (Edit/Add/Delete Notifications) or the Wizards (Policy/Notification Wizard, and Options...) or a combination of the two to change the settings of the notification associated with a policy violation. While the buttons limit the changes only to a selected policy violation, the wizards allow you to apply the changes to any level of the policy violation event structure.

- 3) To edit the notification, highlight it from the list of notifications and click  (Edit Notification), or simply double-click the notification. The AirMagnet Policy Notification

screen appears. See Figure 12-13.

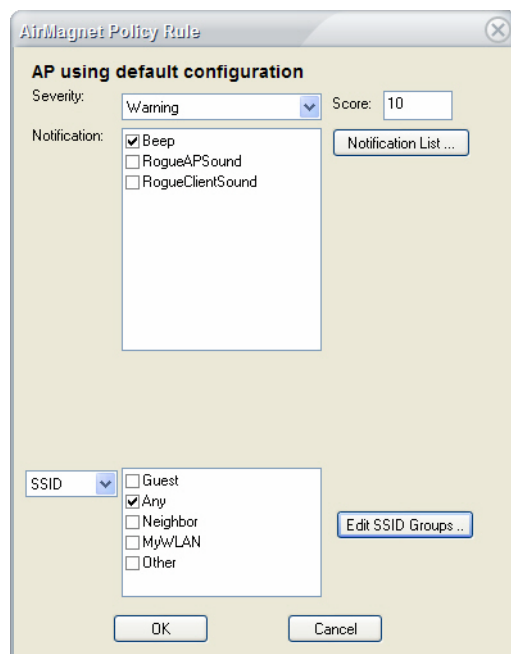



Figure 12-13: Editing alarm notification

- 4) Make the desired changes as described below.

Table 12-1: Configuring Policy Notification Settings

Parameter	Description
Severity	Adjust the level of severity of policy violation at which the alarm is to be triggered.
Notification	<p>Change the method by which the notification is to be sent in case the alarm is triggered.</p> <ul style="list-style-type: none"> • This part of the screen displays all the available ways of notification that can be used with the alarm. You can link a method of notification with the alarm by checking the corresponding check box. • You can modify the list of notification using the Notification List.... See “Configuring Notification List” on page 257 for more information. • An alarm can have multiple ways of notification.
Thresholds	<p>Adjust the value of the threshold used to trigger the alarm, if necessary.</p> <p>The parameters used as thresholds may differ, depending on the type or nature of the policy violation. Also, not all the events have thresholds.</p>

- 5) Click OK to close the AirMagnet Policy Notification screen when all notification changes have been performed.

- 6) To delete a notification from the screen, highlight it and click  (Delete). The notification will disappear from the list of notifications.

Each policy violation MUST have at least one notification associated with it. Therefore, you will get the error message "Must have one notification" if you are trying to delete a notification which is the only one for the alarm.

- 7) From the AirMagnet Policy Management screen, click OK to implement the policy profile, or click Cancel to void it, or click Reset to restore the manufacturer setting.

Working with the Policy Wizard

The Policy Wizard provides an simple, intuitive, and easy-to-follow approach for configuring WLAN security and performance policies. Users can quickly and effectively configure their WLAN policies based on their knowledge of their own networks. This is especially helpful for first-time users of the AirMagnet Enterprise, who do not have much experience with the product but would like to get up and running in no time. The Policy Wizard walks the user through the policy configuration process in three easy-to-follow steps:

- a) Configuring SSID groups
- b) Specifying method of authentication
- c) Specifying vendor list

To configure a policy profile using the Policy Wizard:

- 1) From the AirMagnet Policy Management screen, click **Policy Wizard**. The Setup SSIDs screen appears. See [Figure 12-14](#).

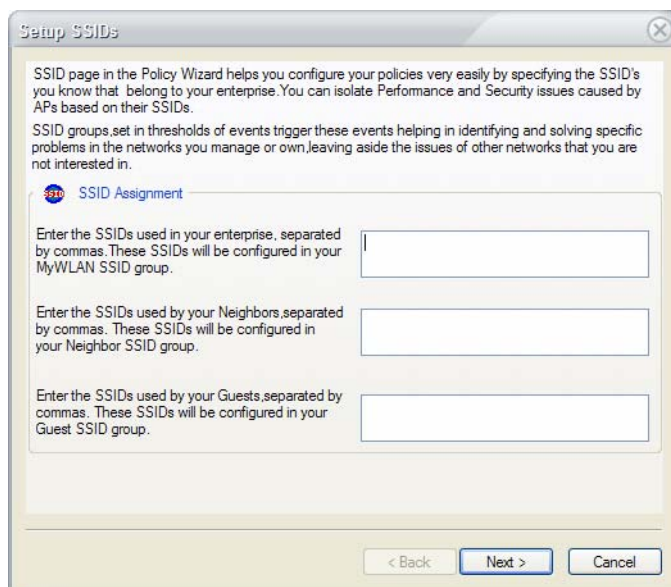


Figure 12-14: Configuring SSID groups

- 2) Enter the SSIDs for the following networks:
 - MyWLAN SSID group – Enter the SSIDs used for your own enterprise network.
 - Neighbor SSID group – Enter the SSIDs used on the networks of your neighboring businesses.
 - Guests SSID group – Enter the SSIDs used by visitors to your business.
- 3) Click **Next**. The Setup Authentication Types dialog box appears. See [Figure 12-15](#).

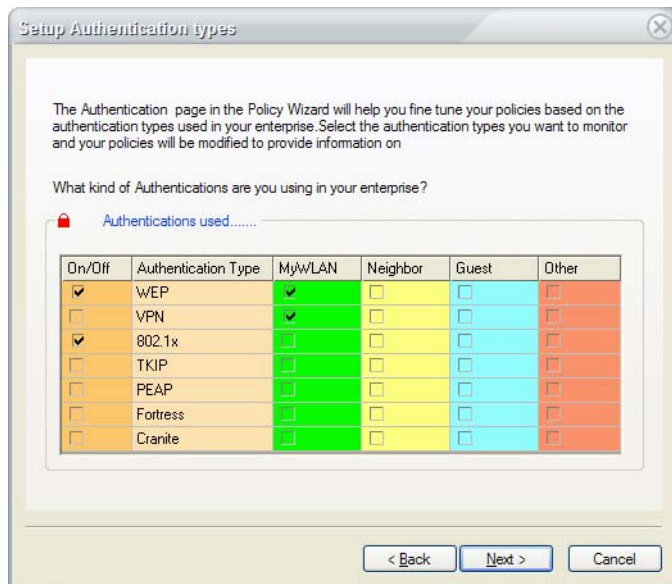


Figure 12-15: Selecting authentication methods

- 4) Select the types of authentication for each of the SSID groups.

Be sure to check the On/Off check boxes corresponding to the Authentication Types you have configured. Otherwise, the authentication types will not be implemented.

- 5) Click **Next**. The Setup Vendor List appears. See [Figure 12-16](#).

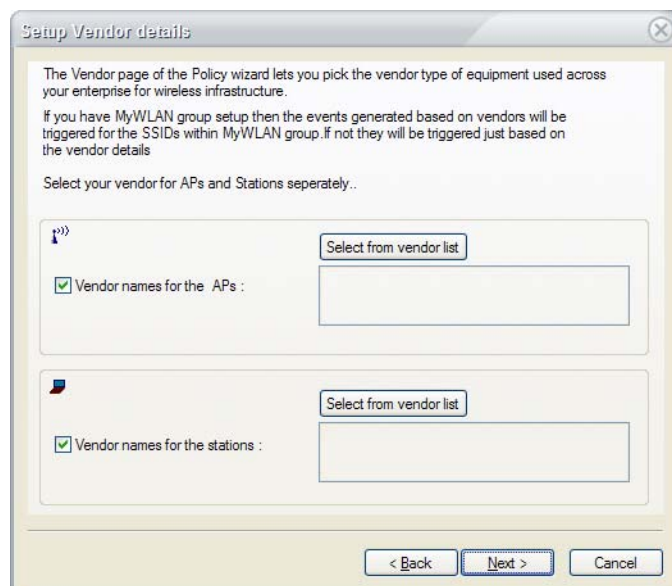


Figure 12-16: Configuring WLAN card vendor lists

- 6) To specify vendors for the APs in use, click **Select from vendor list**. The Vendor List dialog box appears. See [Figure 12-17](#).

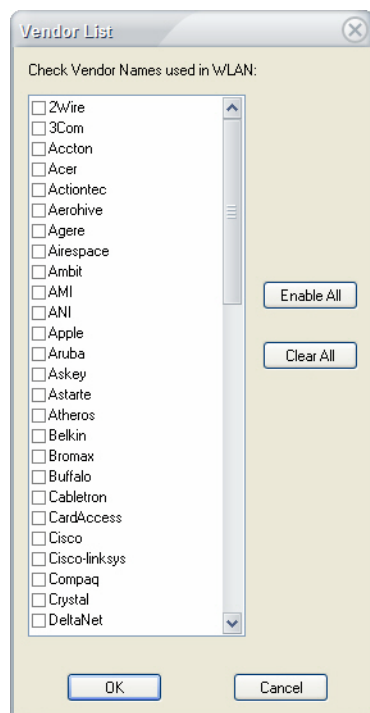


Figure 12-17: Selecting device vendors

- 7) Check off the vendors that are in use on the network and click OK to save the selections.
- 8) Repeat steps 6 and 7 for the stations on the network as well. Click Next to continue.
- 9) The Confirmation page appears. Click **Finish** to save the changes to the policy.

Working with the Notification Wizard

The Notification Wizard lets you assign notifications to policies so that AirMagnet Enterprise can automatically notify the responsible party of the policy violations that occur on the enterprise network.

AirMagnet Enterprise can generate up to 13 types of notifications. For instructions on how to add or change notification options, see the following section “Configuring Alarm Notification Options”.

Assigning Notifications to Alarms

To assign a notification to an alarm:

- 1) From the AirMagnet Policy Management screen, click **Notification Wizard**. The Notification Selection Page appears. See [Figure 12-18](#).

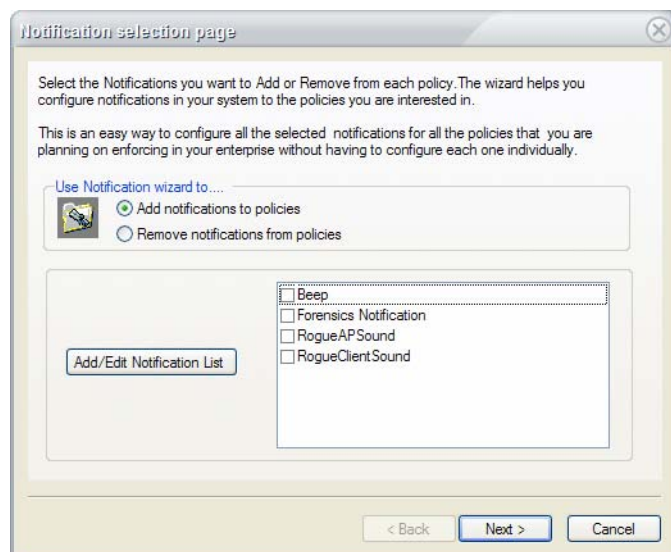


Figure 12-18: Notification Selection page

[Figure 12-18](#) shows the default notifications that are available with AirMagnet Enterprise. The user can modify the list by adding more options or changing the existing ones using the Add/Edit Notification List button. All notifications that are added will end up in this table. For more instructions on how to add or change notification options, see the section “Adding Notification Options”. To link notifications with a policy profile, you need to select (check) the notifications

from this screen and then assign them to policies (See Step 2 below). Furthermore, you must check the **Add notification to policies** radio button to activate notifications that you configure.

- 2) Check the **Add notifications to policies** radio button (if not already clicked), select the notification(s) to which you want to link to the policy profile, and click **Next**. The Policy Selection Page appears. See Figure 12-19.

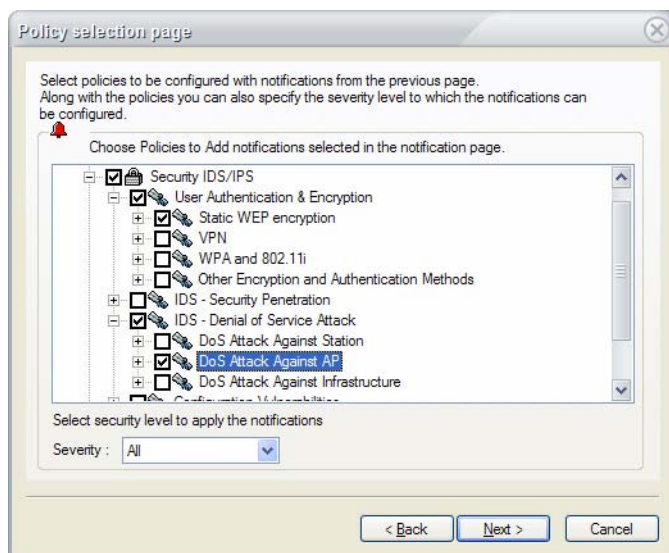


Figure 12-19: Assigning notifications to alarms

- 3) Select the alarms to which you want to assign the notifications, click the down arrow to select a level of severity from the drop-down list, and click **Next**. The Confirmation Page appears.
- 4) Click **Finish**. The selected notifications will be assigned to the policies or alarms.

Adding Notification Options

By default, each alarm is associated with only one notification option. For most alarms, the default is a beep, whereas for rogue APs and stations, the default is a voice message "Rogue AP/Client Found". However, the user can also add, change, or delete notifications as needed.

To add a notification:

- 1) From the Notification Selection Page (Figure 12-19), click **Add/Edit Notification List**. The AirMagnet Policy Notification List screen appears. See Figure 12-20.

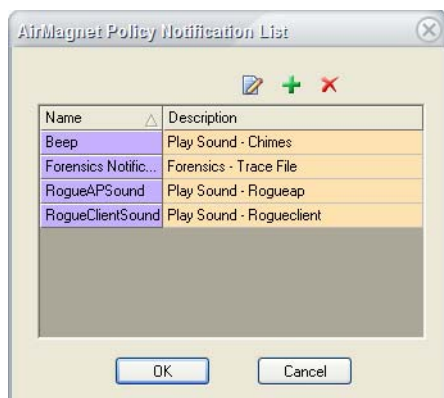


Figure 12-20: AirMagnet Policy Notification List screen

- 2) Click **+** (Add New Notification). The Notification Type Selection Dialog screen appears.
- 3) Select a notification, configure it, and click **OK**. See “[Configuring Notification List](#)” on page 257 for more information on setting up individual notification types.

Modifying Existing Notification Settings

You can also modify existing notifications by making changes to their settings as necessary.

To modify an existing notification:

- 1) From the AirMagnet Policy Notification List (Figure 12-20), highlight the notification and click **E** (Edit Notification), or simply double-click the notification. The configuration dialog box for the notification appears.
- 2) Make the desired changes to the settings of the notification, and click **OK**.

Deleting a Notification

Notifications that are no longer needed for a policy profile can be removed from the policy.

To delete a notification:

- 1) From the AirMagnet Policy Notification List screen (Figure 12-20), highlight the notification, and click **D** (Delete Notification).

Working with the Score Wizard

The Score Wizard allows users to customize the scores associated with various alarms. These scores help to classify different alarms beyond the standard levels of Critical, Urgent, Warning, and Informational. This can be useful for two alarms that are both Critical in nature but present very different threats to the network. For example, an Access Point Down alarm is labeled Critical, but a Rogue AP Traced on Enterprise Wired Network alarm is generally far more dangerous to network security.

Using the Score Wizard, users can tailor the scores of each alarm to distinguish sub-categories within the different levels of urgency.

To modify alarm scores:

- 1) From the AirMagnet Policy Management window, click **Score Wizard**. The Score Wizard dialog box appears. See Figure 12-21.

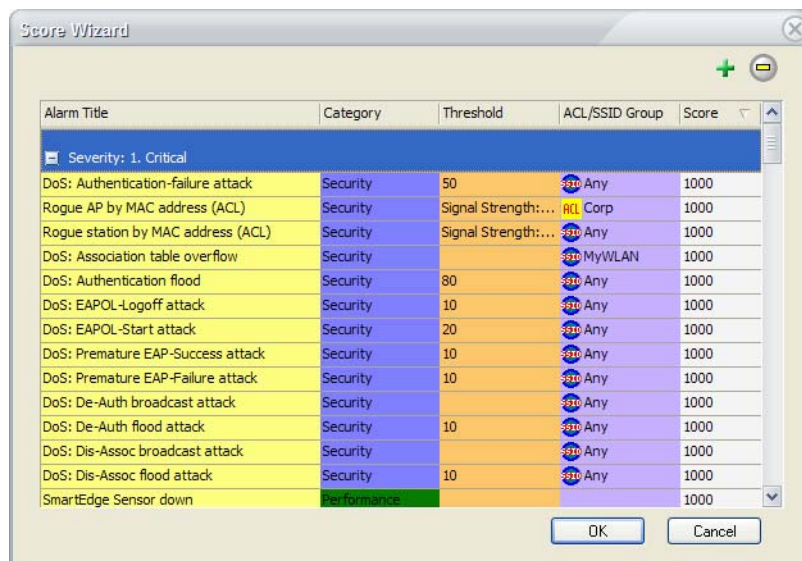




Figure 12-21: Score Wizard

- 2) Select the alarm to be adjusted from the list. By default, the alarms are sorted by their scores, from highest to lowest.
- 3) Use the  and  buttons to add to or subtract from the selected alarm's current score.

*To adjust an alarm's score by a large amount quickly, double-click the alarm to open the AirMagnet Policy Rule dialog box. The score can be entered by keyboard in the **Score:** text field.*

- 4) Click OK to save the changes.

Configuring Policy Options

The **Option...** button allow you to customize the settings of a network. You can tailor the settings of a network's 802.11 settings or rogue management mechanisms.

802.11 Settings

The 802.11 tab manages various transmit and receive settings for the sensors using the current policy profile. Users can use this tab to configure authentication settings for SSIDs known to exist in the current enterprise network.

To customize your WLAN/LAN options:

- 1) From the AirMagnet Policy Management window, click the Options... button. The WLAN/LAN Option box appears, with the 802.11 tab selected by default. See Figure 12-22.

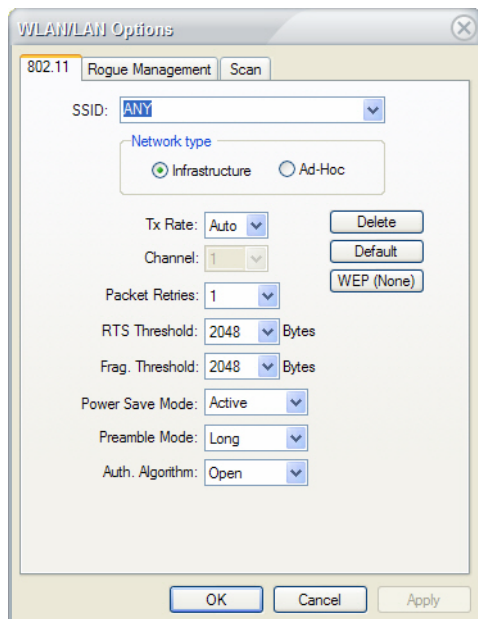


Figure 12-22: Configuring 802.11 settings

- 2) Make the selections as described in Table 12-2.

Table 12-2: Configuring 802.11 Settings

Option	Description
SSID	Select ANY or specify a SSID group (i.e., My WLAN, Guest, Neighbor, Other). If ANY is selected, the configured parameters will be applied to all the SSIDs names above.
Network Type	Select the type of network to which the selected SSID belongs. <ul style="list-style-type: none"> • Infrastructure – This mode bridges a WLAN with a wired Ethernet LAN. • Ad-Hoc – This is a method for wireless devices to directly communicate with each other, i.e., all wireless devices within reach of each other are able to communicate in a peer-to-peer fashion without involving any access point.
Tx Rate	Select a transmission speed at which your AirMagnet Enterprise is to be operated. <i>Keep in mind that the higher the speed, the more bandwidth you will consume. The default setting is Auto, which allows the system to select whatever speed that is appropriate.</i>

Table 12-2: Configuring 802.11 Settings

Option	Description
Channel	Select a channel. <i>The option applies only for an Ad-Hoc network.</i>
Packet Retries	Specify the maximum number of transmission retries at the 802.11 protocol level.
RTS Threshold	Specify the maximum packet length to trigger the use of the 802.11 RTS/CTS mechanism.
Frag. Threshold	Specify maximum value of the 802.11 frame fragmentation.
Power Save Mode	Choose Active or Power Save. The former will keep the system active all the time whereas the latter will switch the system to an energy-saving mode when it is left idle for some time.
Preamble Mode	Choose Long or Short (for 802.11 preamble).
Auth. Algorithm	Select Open if you do NOT wish to use a secret key; choose Shared Key if you require the use of a shared secret key for authentication.
Delete	Click this button to delete the selected SSID.
Default	Click this button to restore the 802.11 settings to the manufacturer's configuration.
WEP	Click this button to open the WEP configuration dialog box where you can configure the WEP settings of your system.

3) Click **OK**.

These 802.11 settings are used only when the AirMagnet Remote Analyzer is used with the AirMagnet SmartEdge Sensor and active tools such as Ping, DHCP, etc.

Configuring WEP Authentication

Security is a big concern for wireless LAN administrators. AirMagnet supports the latest wireless network security technologies to ensure your network security. Currently, AirMagnet supports the following WEP authentication:

By default, your AirMagnet Enterprise comes without any authentication mechanism pre-configured. You can configure WEP security settings based on the needs of your wireless network.

To configure WEP authentication:

- 1) Click the **WEP (None)** button. The Wireless Authentication dialog box appears. See [Figure 12-23](#).



Figure 12-23: Configuring WEP

- 2) Make the desired selections and click **Apply**.

Rogue Management

The Rogue Management tab functions in a similar manner to the same tab found in the IDS/Rogue section. However, configuring settings from the IDS/Rogue area applies globally to the entire Enterprise system, whereas any changes made from the policy page will affect only sensors utilizing the policy profile in which this configuration takes place. This is useful for systems that need to configure rogue management settings specific to a given city or building, but do not wish the settings to apply to an entire network of sensors.

Channel Scan

The scan tab allows you to select the channels you wish to scan. By default, you have all standard channels selected for scanning. However, in order to successfully detect rogue APs in all channels supported by the 802.11 standard, you may wish to click on the Extended... button in order to expand your search.

To configure channel scan settings:

- 1) From the AirMagnet Policy Management window, click the Options... button and select the Scan tab. See Figure 12-24.

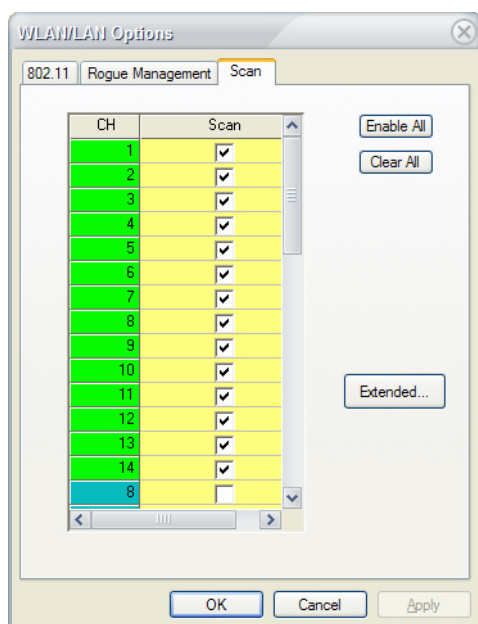


Figure 12-24: Channel Scan Tab

- 2) Check or uncheck the channels as required by the enterprise network configuration.
- 3) Optionally, click the Extended... button to check and uncheck channels in the extended spectrum.
- 4) Click OK to save the changes. The channels selected will be applied to the sensors on which the current policy is active. Those sensors will consequently focus scanning on the selected channels in order to provide more specialized rogue detection capabilities.


Scanning Extended 802.11a Channels

Extended channels refer to the 802.11a channels not normally used by most businesses or countries. Since attacks from outside sources may not always choose to attack from the usual channels, you may scan the extended ones that are normally unused by clicking the Extended... button. Scanning extended channels takes longer than the standard ones, so they are scanned separately from the basic set. You may alter the scan time and scan window to your liking.

Implementing Policy Profiles

A policy profile will not go to effect until it is assigned to the AirMagnet SmartEdge Sensors that are deployed on an enterprise network.

To implement a policy profile:

- 1) From your network Location Tree on the AirMagnet Enterprise Console UI, highlight the network node (e.g., AirMagnet Enterprise Server, city, building, floor, AirMagnet SmartEdge Sensor), and click  (Properties) from the top of the screen. Or right-click the node and select **Properties** from the pop-up menu. See [Figure 12-25](#).

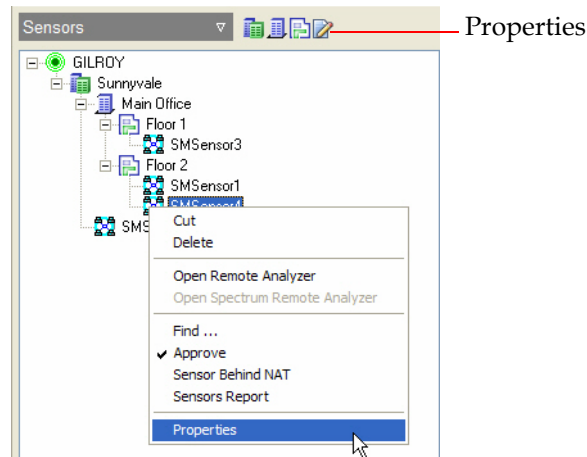


Figure 12-25: SmartEdge Sensor right-click menu

Once you click Properties, a dialog box pops up from which you can choose and assign a policy profile. Depending on the level of the node in the network structure selected, the dialog box that pops up may differ, as sensors will have more properties to configure than buildings or floors.

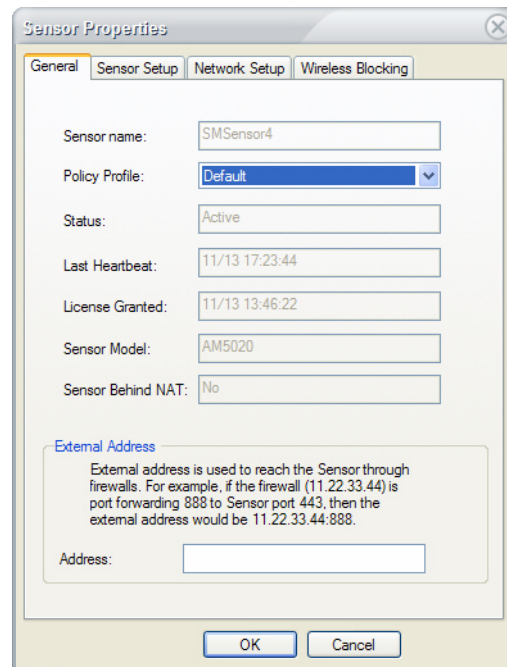


Figure 12-26: Assigning policy profile to Sensor

- 2) Click the Policy Profile drop-down list and select the policy to be applied.

Note that a policy profile can be applied to multiple sensors on the same floor by applying that policy to the floor itself in the Network Tree.

- 3) Click OK to save the changes.

Chapter 13: Configuring System Settings

Introduction

The AirMagnet Enterprise system allows WLAN administrators to quickly and easily configure or modify the system settings for their AirMagnet Enterprise Console, Server, Sensor, shared secret key, and notification list right from the AirMagnet Enterprise Console user interface. This section describes each of the tabs within the main configuration menu of AirMagnet Enterprise.

To access the AirMagnet Enterprise Configuration menu, click **Manage>Server Options....**

Console Settings

The Console tab allows users to customize the display and operation of the Enterprise Console. These options do not apply to the Enterprise Server, and so are specific to the computer that the Enterprise Console is installed on.

To configure Console settings:

- 1) From the Enterprise Console, click **Manage>Server Options....** The Manage Server Configuration screen appears. By default, the Console tab is selected. See [Figure 13-1](#).

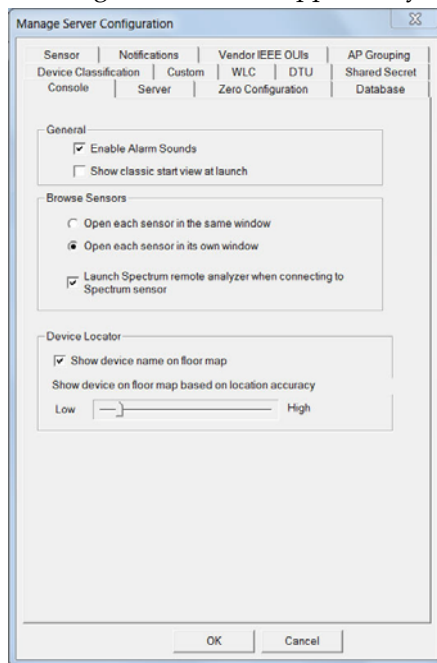


Figure 13-1: Configuring Console settings

Managing system configuration involves several tasks as indicated by the tabs across the top of the Manage Server Configuration screen. Each task is carried out in a separate screen. You need to use the tab to bring up the screen for the task you want to perform. [Figure 13-1](#) shows the default

Manage Server Configuration screen, where you can configure or change Management Console settings.

- 2) Make the selections as described in [Table 13-1](#).

Table 13-1: Console Settings

Parameter	Description
Enable Alarm Sounds	Check this check box if you want AirMagnet Enterprise Console to send out sounds to alert you when alarms are generated.
Show Classic Start View at Launch	Check this box if you would prefer to view AirMagnet Enterprise's "Classic" start page upon launching the Console.
Open each sensor in the same window	If selected, all AirMagnet SmartEdge Sensors will use the same AirMagnet Remote Analyzer window. In this case, you can view the Remote Analyzer UI of only one Sensor at a time. In other words, opening the AirMagnet Remote Analyzer of one Sensor will automatically close the screen of another Sensor.
Open each sensor in its own window	If selected, each AirMagnet SmartEdge Sensor will be displayed in its own AirMagnet Remote Analyzer window.
Launch Spectrum XT when connecting to Spectrum Sensor	If checked, the Spectrum XT will be activated when the Console is connected to an AirMagnet Spectrum Sensor.
Show device name on floor map	Check this box to have device names displayed beneath the icons on the Floor Plan screen.
Show device on floor map based on location accuracy	This slider allows the user to specify how accurate a device's location must be before it is placed on the Floor Plan screen. Increasing the required accuracy will help reduce the clutter of devices on the page, making it easier to see devices that have static locations.

- 3) Click OK.

Server Settings

The Server tab allows users to customize various AirMagnet Enterprise Server settings, providing many different options for rogue and alarm management.

To configure Server settings:

- 1) From the Manage Server Configuration screen, click the **Server** tab. The Manage Server Configuration screen refreshes. See Figure 13-2.

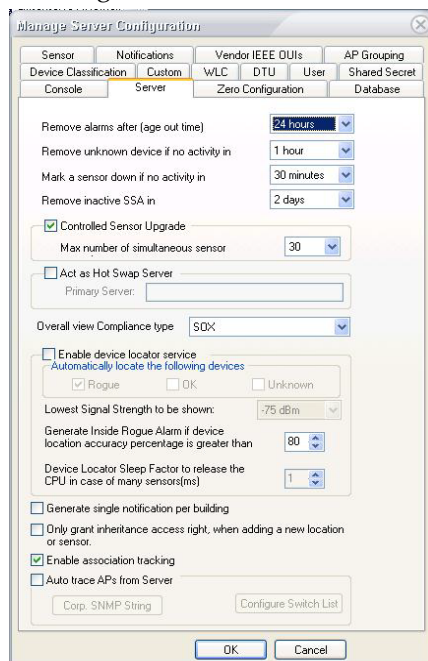


Figure 13-2: Configuring Server settings

- 2) Make the selections as described in Table 13-2.

Table 13-2: Server Settings

Parameter	Description
Remove alarms after (age out time)	Select the maximum time alarms will be kept in the system. The AirMagnet Enterprise Server will remove the alarms from the system once the time expires.
Reclaim license for device not active in	Specify the maximum idle time a device is allowed. The AirMagnet Enterprise Server will reclaim the license from the device once the idle time is exceeded.
Remove unknown device if no activity in	Specify the maximum time unknown devices are allowed to stay idle. The AirMagnet Enterprise Server will remove such devices off the system once the time is exceeded.
Mark a sensor down if no activity in	Specify the maximum number of hours allowed for a sensor to be inactive before the system marks it as down (not functioning).
Controlled Sensor Upgrade	Check this box if you want to specify the maximum number of sensors that may upgrade from the server at one time.

Table 13-2: Server Settings

Parameter	Description
Act as a Hot Swap Server	IMPORTANT: Check this check box <u>ONLY</u> if the AirMagnet Enterprise Server is configured as a backup server. See “Configuring a Hot-Swap Server” on page 255 for more information.
Overall view Compliance type	Use this drop-down list to select the compliance type to be used on the CIO view and AirWISE screens.
Enable device locator service	When Enable Device Locator Service is checked, you will be able to use the Floor Plan screen to identify the location of any device detected by a Sensor or Sensors. Checkbox options indicate ACL status of the devices that will be located on the floor plan.
Lowest Signal Strength to be shown	Devices below the signal strength will not be shown on the floor plan when Enable Device Locator is enabled.
Generate Inside Rogue Alarm if device location accuracy is greater than	AirMagnet Enterprise is capable of finding devices within a specific area of the network. This option will cause AirMagnet Enterprise to generate an Inside Rogue alarm if a device is detected and located within the boundaries defined on the Floor Plan screen. Click the up or down arrow to set a level of confidence for AirMagnet to generate rogue inside alarms. The value can range from 0% to 100%. The higher the value, the greater the accuracy.
Device locator sleep factor...	Enables the user to set CPU sleep timer in milliseconds. A higher number will release the CPU longer for other activities. This may be useful in environments with a large volume of sensors.
Generate single notification per building	When this box is checked, if multiple sensors all detect a single event, their alerts will be consolidated into one notification.
Only grant inheritance access right when adding new location or sensor	This option is useful for systems that manage multiple different areas or businesses that each have custom access privileges to the network tree. With this option checked, new buildings, floors, and sensors added to the tree will only be visible to users who have access to that particular city in the tree.
Enable association tracking	When this option is checked (enabled), the server will track STAs that are associated with the selected AP. This information will be reflected in the Infrastructure view when the Association tab is selected
Auto trace APs from server	When this option is checked (enabled), the server will be enabled to perform wire tracing on the network against any Unknown or Rogue device.

- 3) Click OK.

Configuring a Hot-Swap Server

Sometimes, the AirMagnet Enterprise Server may be down for one reason or another. If this happens, you may lose valuable WLAN data due to the interruption of communication between the Sensor and the Server. To prevent this from happening, AirMagnet Enterprise has the hot swap server feature that allows users to set up a backup server so that the Sensors can automatically connect to it in case the primary server is down.

Keep in mind that the hot-swap (backup) server and the primary server must be installed on two different machines and that the hot-swap server option should be selected ONLY if the Server is configured as a backup server.

To set up a backup server:

- 1) From the Enterprise Server Configuration screen, check the **Act as Hot Swap Server** check box. See [Figure 13-3](#).

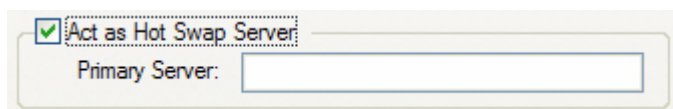


Figure 13-3: Configuring hot swap Server

- 2) Enter the name or IP address of the primary server.
- 3) Click **OK** to save the changes.

Each AirMagnet Enterprise system has two sets of serial numbers and serial keys: one for the primary server and the other for the hot-swap (backup) server. Make sure that they are used correctly.

Sensor Settings

The Sensor tab allows the user to manage the settings for all sensors connected to the AirMagnet Enterprise Server.

To configure Sensor settings:

- 1) From the Manage Server Configuration screen, click the **Sensor** tab. The Manage Server Configuration screen refreshes. See Figure 13-4.

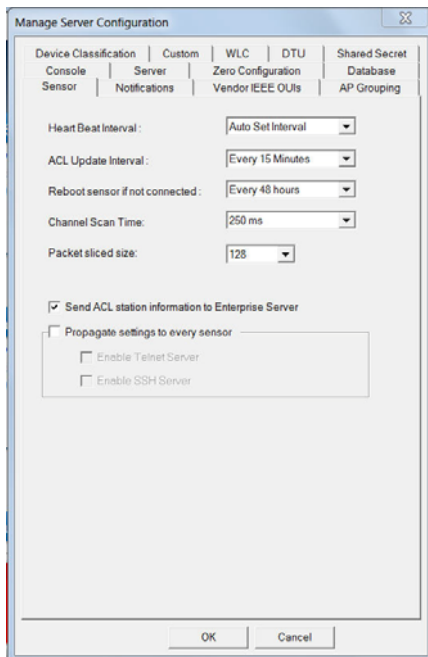


Figure 13-4: Configuring Sensor settings

- 2) Make the selections as described in Table 13-3.

Table 13-3: Sensor Settings

Parameter	Description
Heart Beat Interval	Use the drop-down field to adjust the heart beat interval for sensors. The heart beat is a signal that the sensor sends to the server periodically to confirm that the sensor is still active.
ACL Update Interval	Use the drop-down field to adjust the frequency with which sensors will download ACL information from the server. If ACL information on the network changes frequently, sensors will need to download the updates often in order to prevent false rogue alarms.
Reboot Sensor if not connected	Use the drop-down field to specify how long a sensor should wait after being disconnected from the server before rebooting.
Channel Scan Time	Use the drop-down field to specify how long sensors should focus on a channel at any given time. By default, sensors will scan each channel for 250ms before moving on to the next channel.

Table 13-3: Sensor Settings

Parameter	Description
Packet Sliced Size	Specify the size at which you want AirMagnet to truncate the packets it captures for analysis. The smaller the size, the shorter the processing time.
Send ACL station information to Enterprise Server	Check this box if you want the sensors to send ACL station information to the server. On large deployments, sensors that send both station and AP information can quickly overload the server with data. This option allows the user to focus specifically on ACL AP data.
Propagate settings to every sensor	This box allows the user to enable Telnet and SSH connections to sensors.

- 3) Click OK.

Configuring Notification List

The Notifications tab allows users to customize the types of notifications that will be sent upon various events as configured in the server policy. The notification list can include a variety of different types of alerts, as described in the following sections.

To configure Notification List:

- 1) From the Manage Server Configuration screen, click the Notifications tab. The Manage Server Configuration screen refreshes. See [Figure 13-5](#).

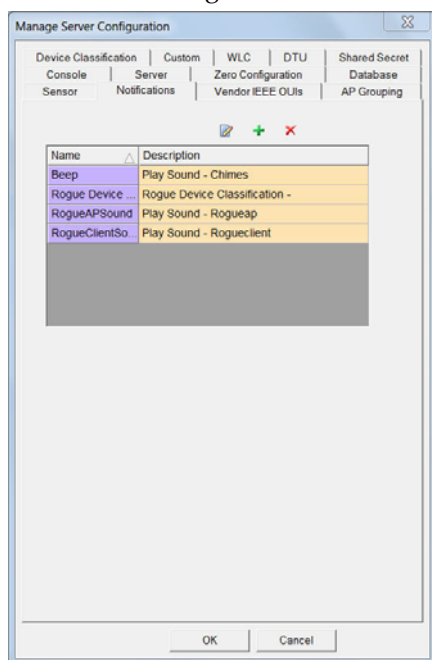


Figure 13-5: Configuring notification list

- 2) Click **+** (Add New Notification). The Notification Type Selection Dialog appears. See Figure 13-6.

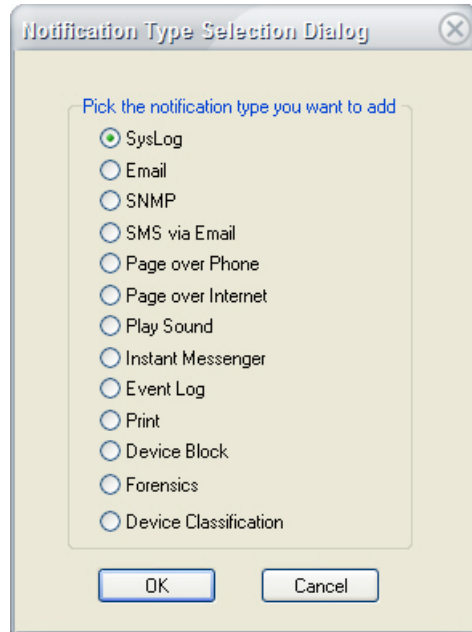


Figure 13-6: Notification Type Selection dialog box

- 3) Select a type of notification, and click **OK**. This will open the dialog box for configuring the notification.

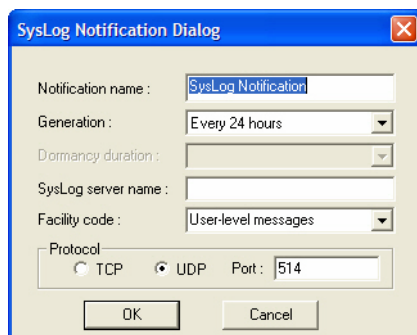
Each of the notifications must be configured separately using a specific screen. The following subsections discuss in detail how to configure each of these notifications.

Configuring SysLog Notification

This option allows AirMagnet Enterprise to send notifications to the Syslog server when alarms are triggered.

To configure SysLog notification:

- 1) From the AirMagnet Policy Notification List (Figure 13-6), check the SysLog radio button. The SysLog Notification Dialog box appears. See Figure 13-7.

**Figure 13-7: Configuring SysLog notification**

- 2) Make the entries or selections as described in Table 13-4.

Table 13-4: Configuring a Syslog Notification

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
SysLog Server Name	Enter the name of the SysLog server.
Facility Code	Select a facility code from the drop-down list.
Protocol	Select the protocol and the port number to be used.

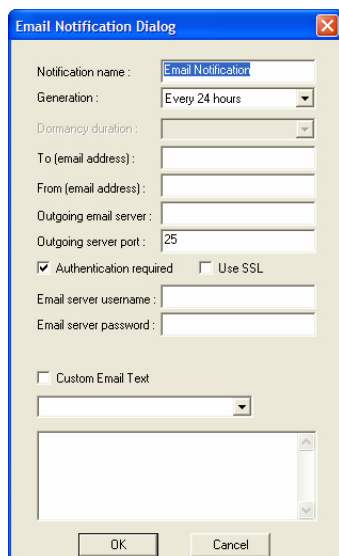
- 3) Click OK.

Configuring Email Notification

This option allows AirMagnet Enterprise to send email messages to the specified email account when alarms are generated.

To configure email notification:

- 1) From the AirMagnet Policy Notification List, check the Email radio button. The Email Notification dialog box appears. See [Figure 13-8](#).



The image shows the 'Email Notification Dialog' box. It contains the following fields and options:

- Notification name:** A text box containing 'Email Notification'.
- Generation:** A dropdown menu set to 'Every 24 hours'.
- Dormancy duration:** A dropdown menu.
- To (email address):** A text box.
- From (email address):** A text box.
- Outgoing email server:** A text box.
- Outgoing server port:** A text box containing '25'.
- ☒ **Authentication required** and ☐ **Use SSL**
- Email server username:** A text box.
- Email server password:** A text box.
- ☐ **Custom Email Text** with a dropdown menu and a large text area below it.
- Buttons:** 'OK' and 'Cancel' at the bottom.

Figure 13-8: Configuring Email notification

- 2) Make the entries or selections as described in [Table 13-5](#).

Table 13-5: Configuring Email Notification

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
To (email address)	Enter the email address of the account to which the email message is to be sent when an alarm is generated.
From (email address)	Enter the email address of the account from which the email message is to be sent.

Table 13-5: Configuring Email Notification

Parameter	Description
Outgoing email server	Enter the name of the outgoing email server.
Outgoing server port	Specify the communication port used by the outgoing email server.
Authentication required	Check this check box if you want to add authentication to the email communication.
Use SSL	Check this check box if you want to use SSL.
Email server username	Enter the user name of the email server.
Email server password	Enter the password of the email server.
Custom Email Text	Check this box if you wish to customize the text included in the email. Use the drop-down and the text field provided to enter the text to describe the alarm message.

- 3) Click OK.

Configuring SNMP Notification

If configured, AirMagnet Enterprise will send SNMP traps to the SNMP server when alarms are generated.

To configure SNMP notification:

- 1) From the AirMagnet Policy Notification List, check the SNMP radio button. The SNMP Notification dialog box appears. See [Figure 13-9](#).

The image shows the 'SNMP Notification Dialog' window. It has two main sections: 'Common SNMP parameters' and 'SNMP v3 parameters'. In the 'Common' section, 'Notification name' is 'SNMP Notification', 'Generation' is 'Every 24 hours', 'Dormancy duration' is empty, 'SNMP Version' is 'SNMP v1', 'MIB Type' is '1', 'SNMP Manager' is empty, 'Port' is '162', and 'Community String' is empty. In the 'v3 parameters' section, 'Context String' is empty, and there are checkboxes for 'Authentication' and 'Privacy', each with 'Protocol' and 'Password' fields. At the bottom, there is a checked checkbox 'Include event description as part of SNMP trap' and 'OK' and 'Cancel' buttons.

Figure 13-9: Configuring SNMP notification

- 2) Make the entries or selections as described in [Table 13-6](#).

Table 13-6: Configuring SNMP Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
SNMP Version	Select the version of the SNMP server application.
MIB Type	Select Type 1 or Type 2 MIB. <ul style="list-style-type: none"> • Type 1 traps are the standard types of SNMP traps, and contain basic information about the trap. • Type 2 transmits more data fields but truncates extended descriptions. This selection is useful for SNMP trap receivers that require a limited message length.

Table 13-6: Configuring SNMP Notifications

Parameter	Description
SNMP Manager	Enter the name of the SNMP Manager (server).
Port	Enter the port (number) of the SNMP server.
Community String/User Name	Enter the Community String used by the SNMP. When SNMP v3 is selected, this field will change to User Name and you must to enter that information.
SNMP v3 Parameters	The parameters described here only apply to SNMP version 3. <ul style="list-style-type: none">• Context String – Enter the context string for the SNMP.• Authentication – If selected, specify the type of authentication to be used.• Privacy – If selected, specify the type if privacy to be used.
Include event description as part of SNMP trap	This check box is checked as default setting where all information defined from the MIB will be reported on the trap message. When the check box is unchecked, the SNMP trap that is sent out to the SNMP manager from the AirMagnet Management server will not include the description of the alarm. This is created to avoid information getting truncated at the trap receiver such as KIWI Daemon, or some other trap receiver.

3) Click OK.

When configuring the SNMP notification, make sure that the parameters match those used in the SNMP trap collector.

Configuring SMS-via-Email Notification

This option allows AirMagnet Enterprise to send SMS messages via email to the recipient when alarms are generated.

To configure SMS-via-Email Notifications:

- 1) From the AirMagnet Policy Notification List, check the SMS via Email radio button. The SMS via Email Notification dialog box appears. See [Figure 13-10](#).

Figure 13-10: Configuring SMS notification

- 2) Make the entries and selections as described in [Table 13-7](#).

Table 13-7: Configuring SMS-via-Email Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Phone/Pager number	Enter the phone or pager number of the party to whom the SMS message is to be sent when an alarm is generated.
SMS server	Enter the name of the SMS application server.

Table 13-7: Configuring SMS-via-Email Notifications

Parameter	Description
SNPP Server Port	The Simple Network Paging Protocol (SNPP) port is hard-coded as 444. This value cannot be changed.
My email address	Enter the email address of the party to whom the message is to be sent.
Outgoing email server	Specify the name of the outgoing email server.
Outgoing email server port	Enter the port (number) of the outgoing email server.
Email server username	Enter the user name of the email server.
Email server password	Enter the password of the email server.

- 3) Click OK.

Configuring Page-Over-Phone Notification

This option allows AirMagnet Enterprise to page the responsible party over the phone when alarms are generated.

To configure Page-over-Phone notifications:

- 1) From the AirMagnet Policy Notification List, check the Page over Phone radio button. The Page over Phone Notification dialog box appears. See [Figure 13-11](#).

Figure 13-11: Configuring Page-over-Phone notification

- 2) Make the entries or selections as described [Table 13-8](#).

Table 13-8: Configuring Page-Over-Phone Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Phone/Pager number	Enter the phone or pager number of the party to whom the SMS message is to be sent when an alarm is generated.
TAP Server Number	Enter the number of the TAP server.

- 3) Click OK.

Configuring Page-over-Internet Notification

This option allows AirMagnet Enterprise to page the responsible party over the Internet when alarms are generated.

To configure Page-over-Internet notifications:

- 1) From the AirMagnet Policy Notification List, check the Page over Internet radio button. The Page over Internet Notification dialog box appears. See [Figure 13-12](#).

The image shows a 'Page Over Internet Notification Dialog' window. It has a title bar with a close button. Inside, there are several input fields and dropdown menus. The 'Notification name' field is pre-filled with 'Page Over Internet Notification'. The 'Generation' dropdown is set to 'Every 24 hours'. The 'Dormancy duration' dropdown is empty. The 'Phone/Pager number', 'SNPP Server', 'My email address', 'Outgoing email server', 'Email server username', and 'Email server password' fields are empty. The 'SNPP Server Port' field is pre-filled with '444'. The 'Outgoing email server port' field is pre-filled with '25'. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 13-12: Configuring Page-over-Internet notification

- 2) Make the entries or selections as described in [Table 13-9](#).

Table 13-9: Configuring Page-Over-Internet Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Phone/Pager number	Enter the number of the Internet phone or pager.
SNPP Server	Enter the name of the SNPP server.
SNPP Server Port	Enter the SNPP Server Port number.

- 3) Click OK.

Configuring Sound Notification

This option allows AirMagnet Enterprise to send out the specified sound to alert the responsible party when alarms are generated.

To configure a sound notification:

- 1) From the AirMagnet Policy Notification List, check the Play Sound radio button. The Sound Notification dialog box appears. See [Figure 13-13](#).

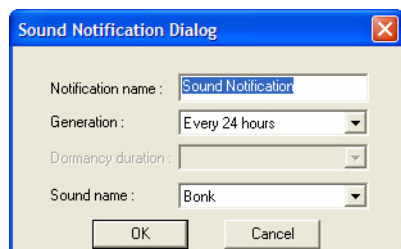


Figure 13-13: Configuring sound notification

- 2) Make the entries or selections as described in [Table 13-10](#).

Table 13-10: Configuring Sound Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Sound name	Select a sound option from the drop-down list. You may either select from the included sound files or select (browse...) from the drop-down list to choose your own.

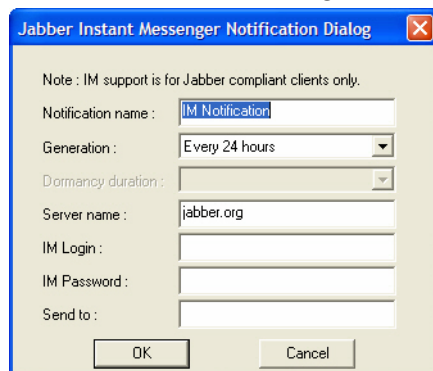
- 3) Click OK.

Configuring Instant Messenger Notification

This option allows AirMagnet Enterprise to send messages to the responsible party through the Instant Messenger application when alarms are generated.

To configure Instant Messenger Notification:

- 1) From the AirMagnet Policy Notification List, check the Instant Messenger radio button. The Jabber Instant Messenger Notification dialog box appears. See [Figure 13-14](#).

**Figure 13-14: Configuring Instant Messenger notification**

- 2) Make the entries and selections as described in [Table 13-11](#).

Table 13-11: Configuring Instant Messenger Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Server name	Enter the name of the Jabber Instant Messenger server.
IM Login	Enter the login name of the Jabber Instant Messenger account.
IM Password	Enter the password of the Jabber Instant Messenger account.
Send to	Enter the destination information of the Instant Messenger notification.

- 3) Click **OK**.

Configuring Event Log Notification

This option allows AirMagnet Enterprise to log events in the Event Log server when alarms are generated.

To configure Event Log notification:

- 1) From the AirMagnet Policy Notification List, check the Event Log radio button. The Event Log Notification dialog box appears. See [Figure 13-15](#).

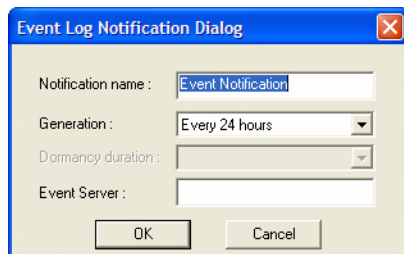


Figure 13-15: Configuring Event Log notification

- 2) Make the entries and selections as described in [Table 13-12](#).

Table 13-12: Configuring Event Log Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Event Server	Enter the name of the event server to which the notification is to be sent and logged.

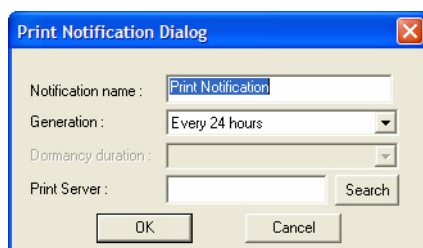
- 3) Click OK.

Configuring Print Notification

This option allows AirMagnet Enterprise to print out notification messages when alarms are generated.

To configure a print notification:

- 1) From the AirMagnet Policy Notification List, check the Print radio button. The Print Notification dialog box appears. See [Figure 13-16](#).

**Figure 13-16: Configuring print notification**

- 2) Make the entries or selections as described in [Table 13-13](#).

Table 13-13: Configuring Print Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.
Print Server	Click the Search button to locate the print server and configure the printer settings.

- 3) Click **OK**.

Configuring Device Block Notification

This option allows AirMagnet Enterprise to automatically block rogue APs when they are detected.

To configure rogue device blocking:

- 1) From the AirMagnet Policy Notification List, check the AP Block radio button. The Device Block Notification dialog box appears. See [Figure 13-17](#).

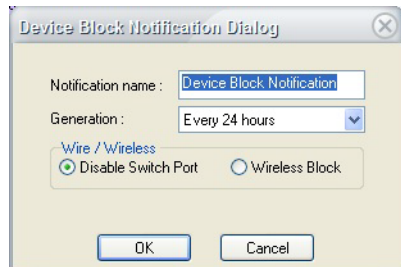


Figure 13-17: Configuring automatic rogue AP blocking

- 2) Make the entries and selections as described in [Table 13-14](#).

Table 13-14: Configuring Automatic Rogue AP Blocking

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising you to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Wire/Wireless	Select a method for blocking rogue APs: <ul style="list-style-type: none"> • Disable Switch Port—This option allows AirMagnet Enterprise to disable the switch port of rogue APs when they are detected. • Wireless Block—This option allows AirMagnet Enterprise to block rogue devices wirelessly when they are detected.

- 3) Click **OK**.

Configuring Forensics Notifications

This option allows you to log specific policy violations for future reference.

- 1) From the AirMagnet Policy Notification List, check the Forensics radio button. The Forensics Notification dialog box appears. See [Figure 13-18](#).

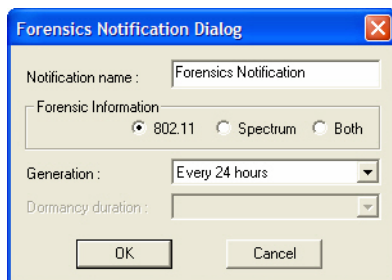


Figure 13-18: Configuring forensics notification

- 2) Make the entries and selections as described in [Table 13-15](#).

Table 13-15: Configuring Forensics Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	<p>This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.</p>
Forensic Information	<p>Select the type of forensic information to be saved. Users can choose to save standard 802.11 information, Spectrum information, or both.</p> <ul style="list-style-type: none"> • 802.11 Forensic files contain data relating to the alarm that triggered the notification. This helps users establish if a specific device is triggering repeated alarms. • Spectrum Forensic files contain a brief snapshot of the RF spectrum, which helps identify sources of non-802.11 problems (such as bluetooth devices, cordless phones, etc). <p><i>Note: Spectrum Forensics data can only be captured by spectrum-enabled (A5120 and A5123) sensor models.</i></p>

- 3) Click OK to save the changes.

Note: Forensics notifications consume a large amount of network bandwidth. Consequently, they are not intended to be continuously active on the network. It is recommended that users activate forensic notifications for specific recurring problems, and disable the notification once the problem is resolved.

Configuring Device Classification Notification

This option allows you to set AirMagnet Enterprise to automatically flag a device as a Rogue upon triggering a specific alarm. As certain alarms tend to be generated by malicious devices, those alarms can be configured with a Device Classification notification to ensure that the responsible devices are marked as rogues on the network.

To configure Device Classification Notifications:

- 1) From the AirMagnet Policy Notification List, check the Device Classification radio button. The Rogue Device Classification Notification dialog box appears.

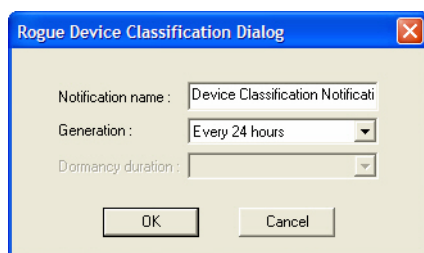


Figure 13-19: Device Classification Notification Dialog Box

- 2) Make the entries or selections as described in [Table 13-16](#).

Table 13-16: Configuring Device Classification Notifications

Parameter	Description
Notification Name	Replace the default with a unique notification name. Otherwise, an error message will pop up, advising to rename it.
Generation	Select one of the time intervals at which the notification is to be generated.
Dormancy Duration	This field is only available if the New or After Dormancy option is selected in the Generation field (above). The Dormancy Duration allows users to specify that an alarm shall trigger only if the same alarm hasn't triggered within a specified time interval. For example, if the Dormancy Duration selected is 90 minutes, the alarm will trigger only once every 90 minutes, even if a rogue device is detected multiple times. This option can be useful for users who have alarms trigger in clusters, and wish to only be alerted once.

- 3) Click OK to save the changes.

Configuring the Shared Secret Key

The Shared Secret tab allows the user to modify the shared secret key used by the sensors connected to the Enterprise server.

To configure a shared secret key:

- 1) From the Manage Server Configuration screen, click the Shared Secret Key tab. The Manage Server Configuration screen refreshes. See Figure 12-24.

The screenshot shows a window titled "Manage Server Configuration" with a close button in the top right. It features a tabbed interface with the following tabs: Sensor, Notifications, Vendor IEEE OUIs, AP Grouping, Console, Server, Zero Configuration, Database, Device Classification, Custom, WLC, DTU, and Shared Secret. The "Shared Secret" tab is selected. The main content area contains the text: "The Sensor Shared Secret Key is used by SmartEdge Sensors to validate with the AirMagnet Enterprise Server." Below this are two text input fields labeled "Sensor Shared Secret Key:" and "Confirm Sensor Shared Secret Key:". A checkbox labeled "Provide all the approved sensors with the updated Sensor Shared Secret" is checked. A note at the bottom states: "NOTE: When the above check box is NOT turned on or 'Zero Configuration' is NOT turned on, ALL Sensors must have their configuration updated. Open a web browser to <https://Sensor> and then click on 'Sensor Setup' menu for all the Sensors." At the bottom of the window are "OK" and "Cancel" buttons.

Figure 13-20: Configuring a shared secret key

- 2) Enter and confirm the Sensor Shared Secret Key.
- 3) Check **Provide all the approved sensors with the updated Sensor Shared Secret** check box. (*Highly recommended.*) This should remain unchecked in FIPS-approved mode.
- 4) Click **OK**.

Be sure to update the configuration for all the AirMagnet SmartEdge Sensors each time the Sensor Shared Secret Key is changed.

Database Settings

The Database tab allows you to schedule some routine database management tasks that AirMagnet Enterprise Server can perform automatically.

To set your database management schedule:

- 1) Click the Database tab. The AirMagnet Server Configuration screen refreshes. See [Figure 13-21](#).

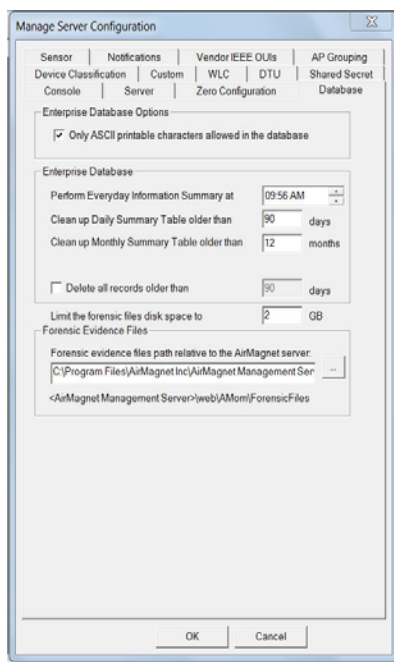


Figure 13-21: Scheduling database management

- 2) Make the desired entries or selections as described in [Table 13-17](#).

Table 13-17: Database Settings

Parameter	Description
Only ASCII printable characters allowed in the database	Check this box if you wish to limit the database input to standard characters.
Perform Everyday Information Summary at	Set a time (hour) at which AirMagnet automatically consolidates the total number of captured alarms in each of the four categories (i.e., Critical, Urgent, Warning, Informational). The data are categorized by policy and device and consolidated on a daily or monthly basis.
Clean up Daily Summary Table older than	Specify the number of days captured alarms are to be kept in the daily summary table of the database. Any alarm that has been in the daily summary table longer than the specified number of days will be automatically deleted from the table.

Table 13-17: Database Settings

Parameter	Description
Clean up Monthly Summary Table older than	Specify the number of months captured alarms are to be kept in the monthly summary table of the database. Any alarm that has been in the monthly summary table longer than the specified number of months will be automatically deleted from the table.
Delete all records older than	Check the check box to enable this field, and then specify the number of days all the alarms can be kept in the database. Data that have been in the database longer than the specified number of days will be automatically deleted.
Limit the forensic files disk space to	Input the amount of free space you wish to allocate towards storing backlogged forensic data.
Forensic evidence files path	Enter or browse (...) to the location where you would like to store the forensic data.

- 3) Click OK.

Enabling Sensor Zero Configuration

This feature must be disabled in FIPS-Approved mode.

The zero configuration feature in AirMagnet Enterprise 7.5 release is designed to obviate the cumbersome procedures of configuring and managing AirMagnet SmartEdge Sensors in WLAN deployment and to reduce the overhead during regular maintenance cycles.

This feature spans across various components/modules of the AirMagnet Enterprise system, which include, but are not limited to, the AirMagnet Enterprise Console, the AirMagnet Enterprise Server, and the AirMagnet SmartEdge Sensor. This AirMagnet SmartEdge Sensor Zero Configuration feature functions in two operating models:

Pre-Installation Model

In this scenario, the user knows the exact locations of the Sensors in the WLAN and has mapped them out accordingly in the Network Tree on the AirMagnet Enterprise Console user interface. Once plugged into the actual network, the Sensors will automatically contact the AirMagnet Enterprise Server to get the needed network settings such as user name, password, shared secret key, etc. that are required for secure Sensor-Server communication. In this case, the Sensors only report to the governing Enterprise Server to which they are assigned, as shown in the Network Tree on the Enterprise Console. This model works best for large-scale Sensor deployment involving hundreds of Sensors.

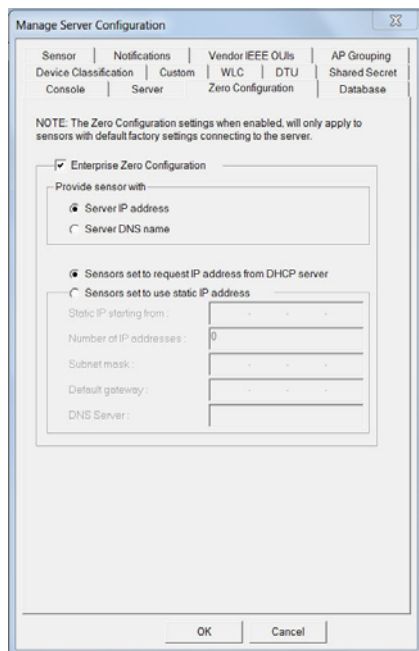
Post-Installation Model

In this scenario, the Sensors are plugged into the network after the Enterprise Server is deployed. In other words, the locations of the Sensors are NOT mapped out in the Network Tree on Enterprise Console user interface. Once plugged into the actual network, the Sensors will automatically contact the AirMagnet Enterprise Server to get the needed network settings such as user name, password, shared secret key, etc. that are required for secure Sensor-Server communication. Unlike the pre-installation model, once the Sensor-Server connection is established, the Sensors will show up as Not Approved under the Server on the Console screen, and the Enterprise Server keeps getting heart beats from the Sensors which indicate that they (the Sensors) are up and running. These pending-approval Sensors do not send any alarm or ACL to the Enterprise Server. To enable these Sensors, the user needs to right-click and approve them in the pop-up menu. The model is ideal for small-scale Sensor deployment in a lab setting or for an evaluator who wants to test-drive the AirMagnet Enterprise system.

***Note:** The network on which the AirMagnet SmartEdge Sensor(s) and the AirMagnet Enterprise Server reside must have either a DHCP server or a DNS server with an entry for the AirMagnet Enterprise Server (by default, the Sensor's DNS Entry is "AirMagnetEnterprise"). In case there is no DNS server with a DNS entry for the AirMagnet Enterprise Server, they (Sensor and Server) must be on a network where the broadcast messages can be sent and received between the Sensor and the Server.*

To Enable sensor zero configuration:

- 1) Click the Zero Configuration tab. The AirMagnet Server Configuration screen refreshes. See [Figure 13-22](#).

**Figure 13-22: Enabling Sensor zero configuration**

- 2) Check the Enterprise Zero Configuration check box.
- 3) Make the required selections and entries that are applicable.
- 4) Click OK.

Vendor IEEE OUIs

The Vendor IEEE OUIs tab allows the user to customize the vendor OUIs for the authorized devices in use on the network. OUIs are assigned by the IEEE to vendors of network components, and AirMagnet Enterprise comes with several common vendors automatically built-in. If your network utilizes vendors that are not included already, this feature will allow you to ensure that Enterprise doesn't generate an alarm because your network vendor is not recognized.

The Vendor IEEE OUI list is updated daily and synced up to all sensors (instead of updating on the server only). With this feature, any new network vendor will be recognized by both servers and sensors faster and device display names will be consistent on both servers and sensors. If your network utilizes vendors that are not included already, this feature ensures that AirMagnet Enterprise does not generate an alarm simply because a network vendor is not recognized.

Note: For customers who do not provide internet access to their server farm VLANs and thus AirMagnet Enterprise servers are not able to retrieve OUI updates, the customer security team may create targeted firewall rules allowing the specific server access to the specific sites to pull the OUI update information. OUI gets its list from here: <http://standards.ieee.org/develop/regauth/oui/oui.txt> (140.98.193.16).

To configure the Vendor ID:

- 1) From the Manage Server Configuration screen, click the Vendor IEEE OUI(s) tab. The Manage Server Configuration screen refreshes. See Figure 12-23.

Manage Server Configuration

Device Classification Custom WLC DTU User Shared Secret

Console Server Zero Configuration Database

Sensor Notifications Vendor IEEE OUIs AP Grouping

+ X ↺ ↻

Please enter vendor MAC address and name

MAC Address	Vendor Name

Note:

1. Please enter only the first three bytes of the MAC address in the format: FF:FF:FF
2. Please visit the 'Rogue AP/Station by IEEE ID (OUI)' Policy Profile to authorize the newly added Vendors

The last update time of OUI: 18:07 01-11-2012

☒ Auto Download OUI

Figure 13-23: Configuring Vendor IEEE OUI(s)

- 2) Click to add a new vendor to the list.
- 3) Enter the first three bytes (six digits – FF:FF:FF) of the MAC address, and then enter the Vendor's name on the right.
- 4) Click OK.

AP Grouping

AirMagnet Enterprise's AP Grouping feature allows users to create labels for APs that utilize multiple SSIDs under different BSSIDs (or MAC addresses). Infrastructure vendors provide multiple BSSIDs to allow a single AP to support multiple security configurations. These BSSIDs can each implement a different SSID, which would each display as a separate device

entry in AirMagnet Enterprise's Infrastructure screen. With AP Grouping active, all BSSIDs that belong to a single device will be grouped as a single device entry. For example, if a given AP utilizes five different SSIDs under different MAC addresses, the user can create an AP group classification for them so that they are grouped together when viewing the data.

To configure AP Grouping settings:

- 1) From the Manage Server Configuration window, click the AP Grouping tab. See [Figure 13-24](#).

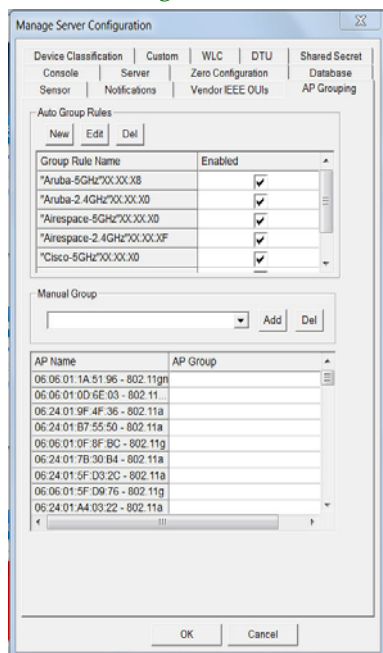


Figure 13-24: AP Grouping Tab

This tab provides two different types of rules for grouping APs. See the sections below for instructions on configuring each type.

Auto Group Rules

AirMagnet Enterprise comes with several built-in “automatic” AP Group rules. If you enable them, they will automatically clump all devices meeting the criteria specified in the rule under a single AP Group. This is helpful if your company uses devices from a specific vendor; Enterprise will recognize those devices and group them accordingly. To see the criteria that the auto group rules use, select one and click the “edit” button. See [Figure 13-25](#).

Figure 13-25: Auto Group Rule Configuration

The table below describes the various configuration fields for auto group rules.

Table 13-18: Auto Group Rule Configuration

Field	Description
Vendor ID	This field allows you to specify the vendor name that the rule will apply to.
Media Type	This field specifies what device media type the rule is intended to classify.
MAC address last hex-digit starting	Select the hex digit you wish the grouping to start from.
Number of contiguous MAC address	Select the number of consecutive devices you wish to classify in the group.
MAC address order	This determines whether your rule will count up or down towards your specified maximum.

Manual Group Rules

The lower half of the AP Grouping tab allows you to set up manual groups for your devices. Using this feature, you can create your own AP Group name and then select exactly which devices you wish to be classified under it. To create a new group, simply click the “Add” button.

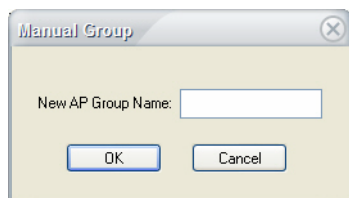


Figure 13-26: Manual Group Configuration

After entering your new AP Group name, click OK, and then simply click the devices you wish to add to it. Whenever you select a device, a drop-down box will appear to the right of its name, allowing you to select which group it belongs to. See [Figure 13-27](#).

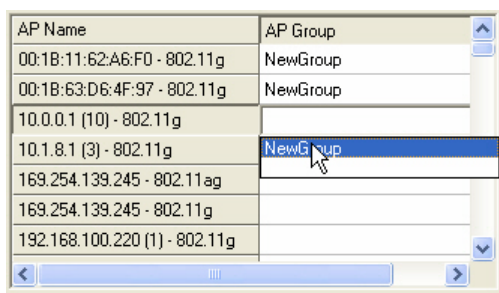


Figure 13-27: Applying Manual Groups

Device Classification

The Device Classification tab allows users to set up various "rules" that can be used to automatically classify new devices as they are detected. By setting up and activating classification rules, new devices can be automatically tagged to their appropriate ACL categories based on device vendor, SSID, or minimum signal strength.

To set up automatic device classification:

- 1) From the Manage Server Configuration window, click the Device Classification tab. The AirMagnet Server Configuration screen refreshes.

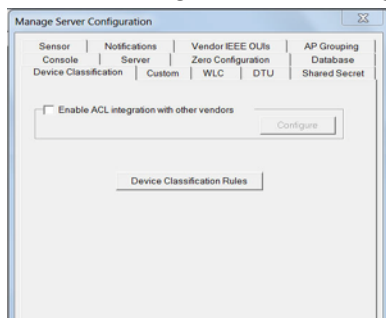


Figure 13-28: Device Classification Tab

- 2) Click Device Classification Rules to open up the Auto Device Classification Rules dialog box. See [Figure 13-29](#).

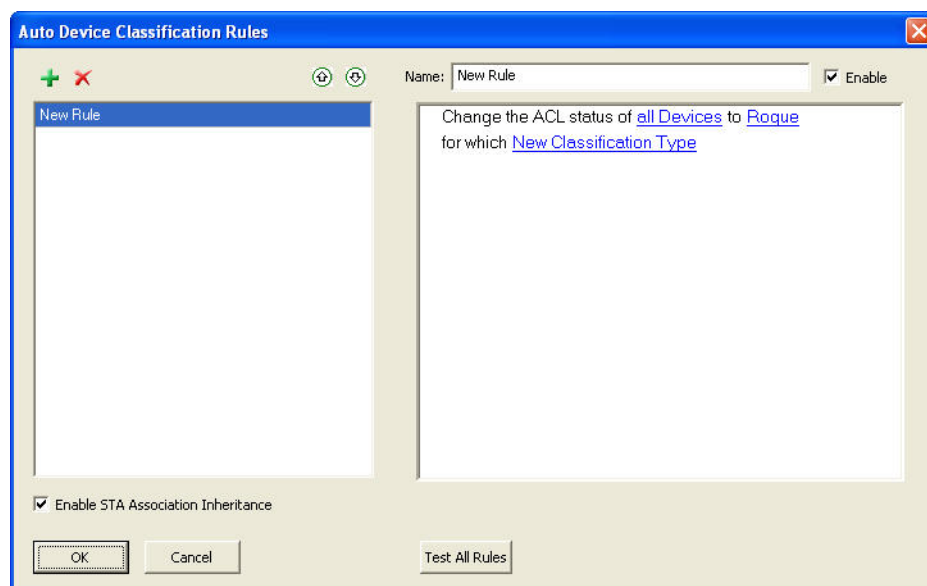



Figure 13-29: Device Classification Settings

- 3) Click  (Add new Classification Rule) to create a new rule to be customized.
- 4) Use the right-hand pane to customize the rule's function. The rule may be modified by clicking on the hyperlinks in the rule description; for example, the user can click on "all Devices" and modify the rule to only apply to APs, stations, or Ad-Hocs as needed.
- 5) If more than one criteria is needed, click on the Add... hyperlink to create additional specifications.

When multiple criteria are specified for a rule, the entries will be chained together using “and” or “or” operators. The user can remove criteria by clicking on the and/or operator and selecting Delete Statement.

- 6) Click OK when finished to save the rule. It will automatically be applied within 15 minutes.

Importing ACL from Other Vendors

AirMagnet Enterprise also allows you to import ACL from other vendors. This feature lets the user import ACL data collected by comparable products by other device vendors.

To import ACL from another vendor’s device:

- 1) Check the **Enable ACL integration with other vendors** check box. See [Figure 13-30](#).

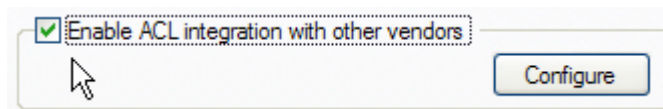


Figure 13-30: Importing ACL from other vendors

- 2) Click **Configure**. The ACL Integration screen appears. See [Figure 13-31](#).

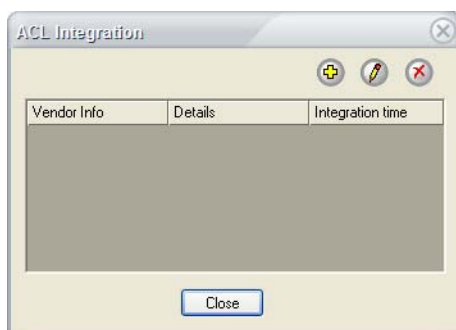


Figure 13-31: Configuring AirWave Server information

- 3) Click **+** (Add Info). The ACL Integration Information dialog box appears. See [Figure 13-32](#).

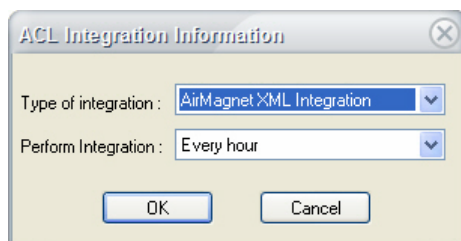


Figure 13-32: Importing an ACL

- 4) Click the down arrow and select an option from the Type of Integration drop-down list.
- 5) Select the integration frequency using the Perform Integration drop-down list. This specifies how often the system will attempt to import ACL information from the device.
- 6) Click OK to save the new settings, and click Close to close the ACL Integration dialog.
- 7) Click OK to save the settings.

Figure 13-33 shows all the ACL options that AirMagnet Enterprise supports. If you import from ACL File Integration, you input the name of the file you wish to import. Use the format below for the XML file: For the other options, you will need to enter the server name and username/password.

Sample of XML file for AirMagnet XML Integration:

```
<Device Type="AP">
  <MACAddress>06:24:01:C0:C6:FC-a</MACAddress>
  <SSID>meru-eng</SSID>
  <ACLStatus>0</ACLStatus>
  <AliasName></AliasName>
  <NodeName></NodeName>
  <ACLToRogueTime></ACLToRogueTime>
  <Owner></Owner>
  <Note></Note>
  <ACLGroupName></ACLGroupName>
  <VIP>0</VIP>
</Device>
```

Table 13-19: Description of codes for XML Integration

Code	Description
<Device Type="AP">	Specify type of device. There are three types: AP (Access Point), STA (Station), ADHOC (AD-HOC).
<MACAddress>06:24:01:C0:C6:FC-a</MACAddress>	Specify the MAC address and media type of the current device, media type could be a, b, g, n.

Table 13-19: Description of codes for XML Integration

Code	Description
<SSID>meru-eng</SSID>	The current SSID the device is using.
<ACLStatus>0</ACLStatus>	Specify the ACL Status including Valid Known Device (In ACL "1"), Rogue Device (illegitimate, malicious "2"), Neighbor Device (belonging to a neighboring network "4"), Unknown Device "0".
<AliasName></AliasName>	An alias name in text format (optional).
<NodeName></NodeName>	Another name for the device.
<ACLToRogueTime></ACLToRogueTime>	A time in the following format: yyyy/mm/dd, used to record when the device becomes a rogue.
<Owner></Owner>	Used to specify the owner of the device (optional).
<Note></Note>	Provides more information about this device (optional).
<ACLGroupName></ACLGroupName>	The ACL Group Name in text format, users can add devices in different ACL groups (optional).
<VIP>0</VIP>	Specifying whether a device is a VIP or not. 0 means it is not a VIP device, while 1 means it is a VIP device

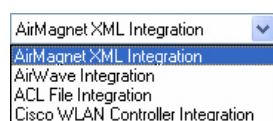


Figure 13-33: Supported ACL Integration

Custom Settings

The Custom tab allows users to customize the appearance of the Enterprise Console interface. Any changes made to the Custom tab are saved and applied any time Console is loaded after making the alterations.

The Custom tab contains several different options to modify the user interface. See [Figure 13-34](#).

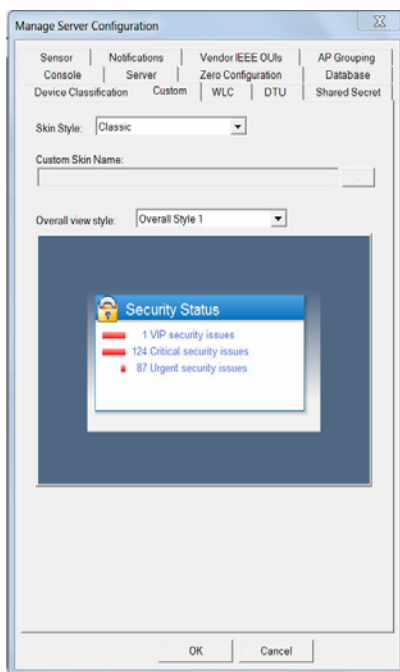


Figure 13-34: Custom Tab


[Table 13-20](#) describes the use of each option.

Table 13-20: Custom Tab Modifications

Field	Description
Skin Style	This drop-down allows the user to select a skin style to apply to the interface. The Enterprise Console comes with three built-in skins, but users can download additional skins from the Internet if desired. <i>Skins use a standard .msstyles file for custom styles.</i>
Custom Skin Name	This field can only be used if the user has selected "Custom..." from the Skin Style drop-down. Users can browse to the directory of their custom skins in order to apply them to the Console interface.
Overall View Style	This drop-down adjusts the appearance of the Overall View on the Start screen. Enterprise comes with three different styles for the Overall View.

WLC Settings

The WLC tab allows collection of RSSI data from an AP's near device of interest, used as input to AirMagnet Enterprise devices locator/floor plan mapping. It allows IT staff access to real-time spectrum analysis remotely over any routed network-expanding cases where IT can reach, running full Spectrum XT interface to troubleshoot interference problems. Users will benefit from expanded flexibility for sensor designs (without min. 3 sensors per floor) and more aggressive position on device location, enabling low cost options and saving time.

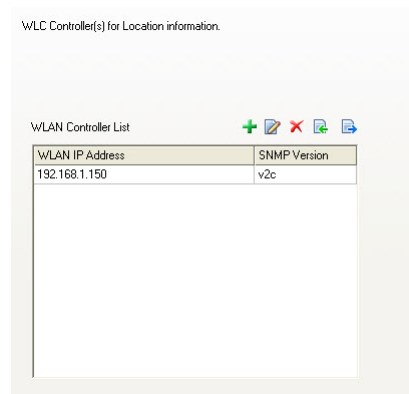
- Adding Cisco WLAN Controllers
 - 1) Click on the  icon to begin adding your Cisco WLAN Controller.
 - 2) In the IP address/Hostname field, enter in your Cisco WLAN Controllers IP or Hostname.
 - 3) Enter in the Community String that you have setup on your Cisco WLAN Controller (A Read-Only community string is all that's needed).
 - 4) Select your SNMP version and Port. Click Ok when done.



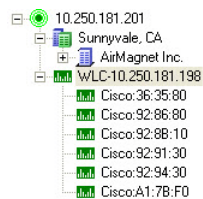
The image shows a dialog box titled "WLAN Controller Details". It contains two sections: "Common SNMP parameters" and "SNMP V3 Parameters". In the "Common SNMP parameters" section, the "IP Address/Hostname" field has radio buttons for "ip Address" (selected) and "Hostname". The "Community String" field is empty. The "SNMP Version" dropdown is set to "v2c". The "Port" field is set to "161". The "SNMP V3 Parameters" section has a "Context Name" checkbox (unchecked), a "User Name" field, an "Auth Algorithm" dropdown set to "NO_AUTH", an "Auth Password" field, a "Privacy Algorithm" dropdown set to "NO_PRIV", and a "Privacy Password" field. At the bottom are "OK" and "Cancel" buttons.

Figure 13-35: SNMP Configuration window

Your WLC Controller list should look like the following:

**Figure 13-36: WLC List**

After about a minute you should see a new item appear in the sensor tree. It will contain the WLC, labeled using its IP address and all of the Cisco AP's that are connected to that WLAN Controller.

**Figure 13-37: Sensor Tree**

- Moving the Cisco AP's into place:
 - 1) In order to utilize the RSSI information from the Cisco AP's to help determine location, you will first need to drag and drop them onto the correct floor that they are currently located on. Right click on the floor that you are working on and select 'Move Sensors'.

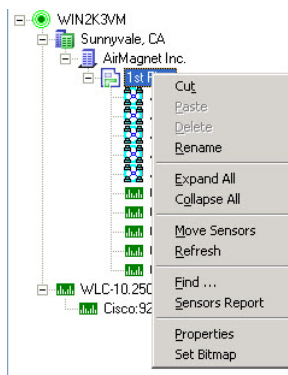


Figure 13-38: Cisco AP Floorplan

- 2) Once you are done moving the Cisco AP's into place, Right Click again on the floor and select 'Refresh'.

By Default, all of the Cisco AP's that have been moved onto the floor will be located up in the left corner of your floor map. You will now need to move them to their correct location. Again, just drag and drop them on the floor map page. When complete, you should have your AirMagnet sensors + your Cisco AP's placed correctly on the floor map.

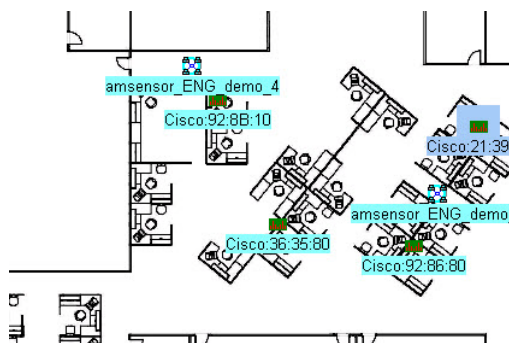


Figure 13-39: Cisco AP Floorplan

The WLC tab includes icons which allow the user to add a new controller, edit it, remove it or export/import a controller list. The WLC Update Interval option enables you to set how frequently to perform a WLC update.

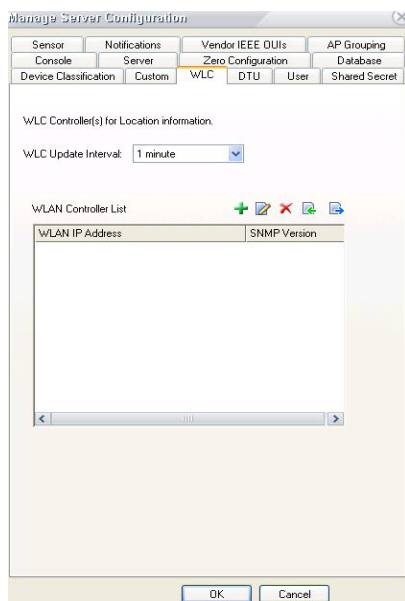


Figure 13-40: WLC Tab

DTU Settings

Dynamic Threat Update (DTU) is the next generation answer for users to address new threats to their wireless networks between major releases of AirMagnet Enterprise. Through the user of custom signature files, new alarms can be added to a Policy on the fly. These new alarms will be indistinguishable from alarms that AirMagnet Enterprise ships with in both form and function. This interface is handled through the DTU tab on the Server Configuration screen, as seen below in Figure 13-41.

Note: For customers who do not provide internet access to their server farm VLANs and thus AirMagnet Enterprise servers are not able to retrieve DTU updates, the customer security team may create targeted firewall rules allowing the specific server access to the specific sites to pull the DTU update information. DTU gets its signatures from here: airmagnet.flukenetworks.com (209.220.161.135 and 209.220.161.140).

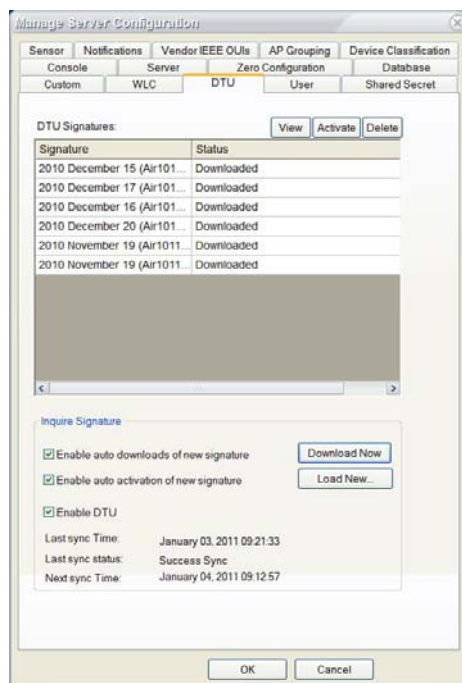


Figure 13-41: DTU tab

Table 13-21: DTU Feature Components

Component	Function
Signature	This field has information on the signature files on the server. The data includes the date of their creation as well as the filename.
Status	This field shows which signature file is currently active.
View	This button will show information about the alarms contained within the signature file.
Activate	This button will activate the selected signature file and turn on its contained alarms in all profiles.
Delete	Delete the selected signature file.
Download Now	Initiates a download of signature files(s) from the AirMagnet server.

Table 13-21: DTU Feature Components

Component	Function
Load New	Allows the user to select a signature file manually to be loaded into the server.
Enable auto-download of new signature	Causes the server to automatically query the AirMagnet signature server for new signature files.
Enable DTU	Allows the DTU feature to be turned on or off.
Last Sync Time	Records the last time the Enterprise server successfully queried the AirMagnet signature server.
Last Sync Status	Reports the outcome of the last sync to take place.
Next Sync Time	Holds a record of when the next signature server sync will take place automatically.

Chapter 14: Automated Health Check (AHC)

Introduction

The Automated Health Check (AHC) feature verifies availability and connectivity of the network from the perspective of a wireless real user, from the AP connection all the way to application services or the internet. It does this by simulating an actual client connection, fully authenticating to the enterprise network, then running various availability and performance tests against multiple network resources. Tests can be configured to connect to a specific Access Point (AP) or SSID in the wireless network environment, and can be run either manually or on a scheduled basis. The device that is used for the Automated Health Check must be in the ACL with OK status. The results and analysis can be viewed from the AirMagnet Enterprise Console UI.

In order to enable the AHC feature, an additional license is required. For more information, please contact your AirMagnet/Fluke Networks sales representative.

The AHC feature may be enabled in the following two types of sensors:

- AirMagnet 52xx sensor models (hardware sensor)
- Software Sensor Agent (SSA – software sensor)

Enabling AHC mode on a sensor

To enable a AHC in a sensor: Right-click on the hardware sensor or software sensor in the sensor tree. Select **AHC mode**. On the AHC tab, check the box **Enable AHC Mode**.

Notes regarding hardware sensors in AHC mode:

- The color of the sensor in the tree view will change to purple, indicating that it is set to AHC mode.
- The hardware sensor will no longer perform passive scanning and will only perform the AHC jobs. Thus, it is a best practice to have another hardware sensor (in non-AHC mode) in the area.
- Enabling a hardware sensor in AHC mode will reboot the sensor.

Notes regarding software sensors:

- When AHC mode is enabled on software sensor, the software sensor does not need to be rebooted.

Configuring AHC in the AME console

From the Menu bar, select **Manage > AHC Jobs**. Under the AHC Jobs tab, click + to add new entry which will bring up the AHC Configurations screen.

Note: The time filter selected in View Filter tab, does not apply to the list in the SSID (ACL=OK) drop down box and in the AP (ACL=OK) drop down box when configuring an AHC Job.

Table 14-1: AHC Configuration dialog

Option	Description
Audit Name	The SSID of the target AP is auto-filled. However, any alpha-numeric text string may be typed here to identify this profile.
SSID	Choose this radio button to create a profile based on an SSID. In the case of a roaming SSID (multiple APs), the sensor will associate with the AP having the strongest signal.
AP	Choose this radio button to create a profile for a specific AP. This will auto-fill with the SSID of the AP. Note that the status of an AP must be OK in order for the AP to show up in this drop-down list.
Security Profile	<p>A security profile will need to be established that corresponds to the security set-up of the target AP in order for the sensor to establish a connection when running the test. Click New to create a security profile. Once one or more security profiles have been created, a profile may be selected from the drop-down. With a profile selected, click Edit in order to edit an existing profile.</p> <p>A hardware sensor uses the AHC Security Profile as configured. SSA uses the security profile configured in Windows Zero Config on the machine where SSA client is installed on. The contents in the AHC Security Profile do not apply to SSA</p>

Table 14-1: AHC Configuration dialog

Option	Description
Action Profile	<p>The action profile establishes the type of test to run and the schedule for running the tests. Click New to create an action profile. Once one or more action profiles have been created, a profile may be selected from the drop-down. With a profile selected, click Edit in order to edit an existing profile.</p> <p>When using any of these special characters (% , / , + , ? , # , = , &) in the download path tests in AHC Action Profile, the download test might fail.</p> <p>The download file size is limited to 2MB for both hardware sensor and SSA regardless of the large size file configured by user.</p> <p>Examples:</p> <p>Ping Host: airmagnet.flukenetworks.com</p> <p>FTP Server: ftp://<ftp-server-IP>/testdocument.txt (Make sure to supply the credential to access the FTP server)</p> <p>Https server: https://<AME-server-IP>/Doc/Enterprise_User_Guide.pdf (Make sure to supply the credential to access the AME server)</p> <p>Http server: http://www.wireshark.org/download/docs/user-guide-us.pdf</p> <p>Trace Route: airmagnet.flukenetworks.com</p>
Signal Strength Threshold	If the signal strength of the target AP falls below this threshold, the test will not be run.
Enable Quiet Mode	If the connection with the AP is established, the AHC job will skip the connection step and run the tests without attempting to re-connect first.
Manual Test	Once a profile is configured, click Manual Test to perform an ad hoc test. There must be at least one sensor enabled in AHC mode to run a test. This test only applies to hardware sensors. The test will run and a pop-up notification will open that indicates whether the test succeeded or failed. To end the test before completion, click Cancel Test .
OK	Click Okay to save the profile. Click Cancel to close the AHC Configuration dialog without saving the profile.

Table 14-2: AHC Security Config dialog

Option	Description
Security Profile	Any alpha-numeric text string to name and identify this profile
Security Type	Choose the APs established authentication type from the drop-down menu.

Table 14-2: AHC Security Config dialog

Option	Description
Security Login Detail	Depending on the Security Type selected, the login details will reflect authentication options for that security type. Key: The security code for the Security Type selected. Check Show Characters to display actual characters rather than asterisks.

Table 14-3: AHC Action Profile Config

Option	Description
Action Profile	Any alpha-numeric text string to name and identify this profile
Audit Schedule	Use the radio buttons and calendar drop-down options to set up the schedule to run the AHC. Time Out: Specify the number of minutes the AHC will run before it is canceled. Repeat: Specify the number of times to repeat the schedule.
Ping Host	Type an IP address or URL to ping
FTP Server Https server Http server	Type (or copy and paste) the path and file name. For example: ftp://IPaddress/ftpfile.txt Use the supplied text boxes to include the user name and password if required.
Trace Route	Only used for SSA performance test. Type the IP address or URL.

Table 14-4: Supported AHC Security Types

Security Type	Authentication	Data encryption
OPEN		
WEP(64 bits)	OPEN	

Table 14-4: Supported AHC Security Types

Security Type	Authentication	Data encryption
WEP (64 bits)	Shared	
WEP (128 bits)	OPEN	
WEP (128 bits)	Shared	
WPA-P/WPA2-P		TKIP/ AES-CCMP
WPA-E/WPA2-E	EAP-TLS	TKIP/ AES-CCMP
WPA-E/WPA2-E	LEAP	TKIP/ AES-CCMP
WPA-E/WPA2-E	PEAP	TKIP/ AES-CCMP
WPA-E/WPA2-E	EAP-TTLS	TKIP/ AES-CCMP

Note: The security types in Table 14-4 are only supported for hardware sensors. Software Sensor Agent (SSA) uses the security profile configured in Windows Zero Config on the SSA machine.

Assigning AHC jobs to a sensor

Note: Up to five AHC jobs may be assigned to one sensor. This limit applies to both the hardware sensor and the SSA in AHC mode.

AHC jobs may be assigned to sensors using the AME console by two methods:

- In the Infrastructure screen, right-click the desired sensor, select **AHC mode** (If AHC mode is already checked, select **Properties**). Under the AHC tab, check the desired AHC Job. This will assign it to that particular sensor.

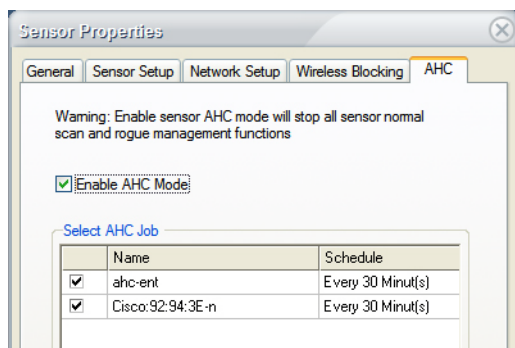


Figure 14-1: Sensor Properties AHC tab

- From the Menu bar, select **Manage > AHC Jobs**. Under the AHC Jobs tab > AHC Job Assignment, click the Sensor list link for each job to assign it to one or more sensors.

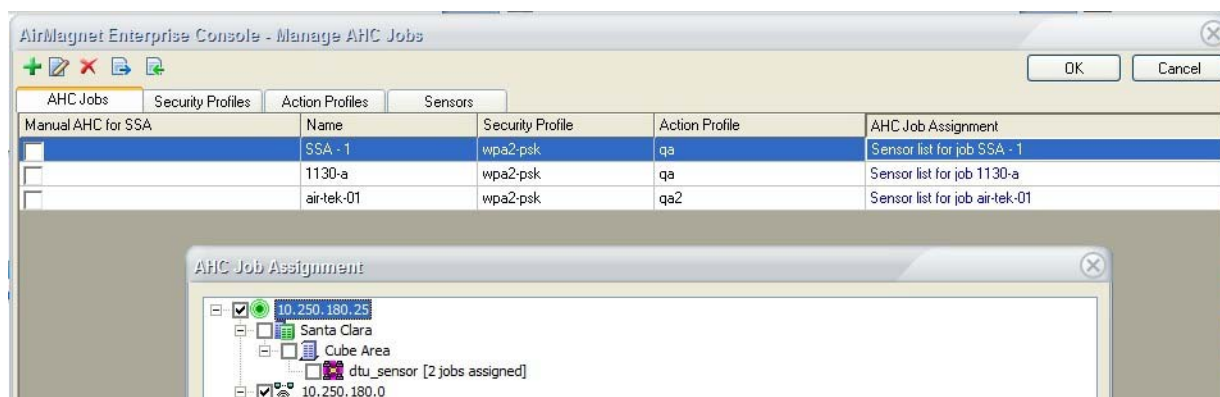


Figure 14-2: AHC job assignment

Viewing AHC Results

Once any scheduled AHC Jobs have completed running, the Infrastructure view will display a check mark in the AHC Status column for the associated AP.

- In Infrastructure screen, highlight an AP showing the AHC Result icon and click the Automated Health Check tab in the Details panel at the bottom.
- Use the drop-down menu on the left to view jobs and trends:
 - Manual AHC Audit (manual jobs)
 - Schedule AHC Audit (scheduled jobs)
 - Trends (trends data can be exported to Microsoft Excel)

If the machine running AirMagnet Enterprise Console does not have Excel 2007 or Excel 2010 installed, the AHC result will not be able to export to Excel successfully.

When viewing the averaged AHC result for the particular SSID in the SSID List tab, the user can select the floor level or the sensor level in the sensor tree. There is no AHC result available at Campus/City level or the Building level in sensor tree.

Only the last month of AHC results are retained in the AirMagnet Enterprise system (30 days before the current day).

Note: AHC results pertaining to a particular Software Sensor Agent (SSA) may also be viewed on the SSA host machine. Right-click the SSA icon in the system tray and select "Show SSA Agent" – or – Start>Programs>AirMagnet Enterprise SSA>SSA.

Trends

The Trends option plots all the AHC results records for the selected AP over the time frame specified in the X axis. The Y axis plots the job completion time in milliseconds. If the job failed, zero milliseconds will be plotted for that job.

You may view data by selecting an option from the Trends drop-down:

With a Trend option selected, you may click Export to open the data in Microsoft Excel. Microsoft Excel (version 2007 or 2010) must be installed on the machine hosting the AirMagnet Console to use this feature.

Part III: AirMagnet Remote Analyzer

Chapter 15: Introducing Remote Analyzer

Chapter Summary

AirMagnet Remote Analyzer (the Remote Analyzer hereafter) is part of the AirMagnet Enterprise network management system. Although it presents pretty much the same types of data as AirMagnet Enterprise Console does, the Remote Analyzer focuses exclusively on data captured by the specific AirMagnet SmartEdge Sensor that is being selected. In this sense, the data shown on the AirMagnet Remote Analyzer user interface are sensor-specific. You can launch a separate Remote Analyzer session for each Sensor from AirMagnet Enterprise Console; you can also open multiple Remote Analyzer sessions at the same time.

This section provides a brief overview of the Remote Analyzer. It covers the following topics:

- Launching Remote Analyzer
- Major UI Components
- Major Screen Options
- Common Menu Options
- Applying View Filters
- Accessing Remote Spectrum Analyzer User Documentation
- Device Detection

Launching Remote Analyzer

There are a number of ways to launch the AirMagnet Remote Analyzer from the AirMagnet Enterprise Console:

- From a major screen of the Console, click **Connect>Sensor....**
- Select and click a Sensor icon from the location tree.
- From the AirWISE screen, double-click an alarm.

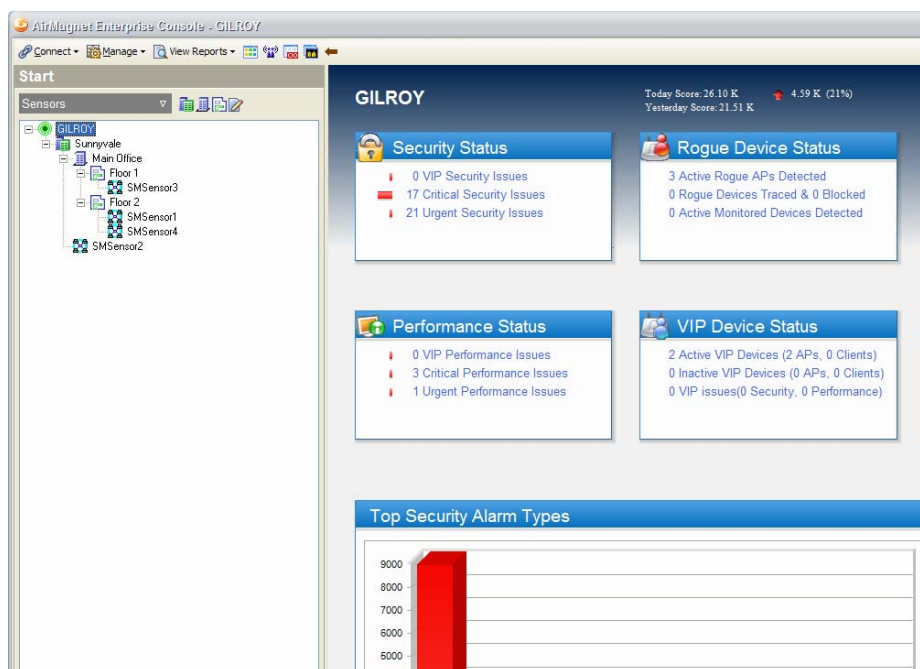


Figure 15-1: Start screen

Navigation Bar

At the bottom left of the Remote Analyzer screen is the program's navigation bar, which contains navigation buttons for accessing different screens and tools. You can navigate from one screen to another using these buttons. See [Figure 15-2](#).












Figure 15-2: Navigation Bar

You can expand the navigation bar for easier viewing by clicking and dragging the dotted line across the top of the buttons upwards. Depending on your computer's screen size and resolution, this may cause the pie chart above the navigation bar to vanish.

Table 15-1 contains brief descriptions of each of these buttons.

Table 15-1: Navigation Bar and Buttons

Button	Description
 Start	Start button opens the Start screen, which shows the overall health of the wireless LAN environment.
 Channel	Channel button opens the Channel screen, which allows you to visualize 802.11 traffic by channel.
 Interference	Interference button opens the Interference screen, which allows you to view the levels of interference each channel on your network is experiencing.
 Infrastructure	Infrastructure button opens the Infrastructure screen, which displays the WLAN's structure and components.
 AirWISE	AirWISE button opens the AirWISE screen, which lists the performance and security alarms detected by AirWISE.
 Top Traffic Analysis	Top Traffic Analysis button displays the top 10 bandwidth consumers in the wireless LAN, and allows you to view many other common charts.
 Reports	Reports button allows you to view custom and default reports, including compliance and alarm detail pre-generated reports.
 Decodes	Decodes button opens the Decode screen, which displays the 802.11 packet summary in real time.
 WiFi Tools	WiFi Tools button opens the Tools screen, which contains more than a dozen easy-to-use WLAN tools for you to choose from.

View Filter

The View Filter tab located in the top right portion of Remote Analyzer user interface provides the user with an easily accessible means of filtering the data displayed. To access the different filter options, simply move the mouse cursor over the tab and the View Filter pane will expand. See [Figure 15-3](#).

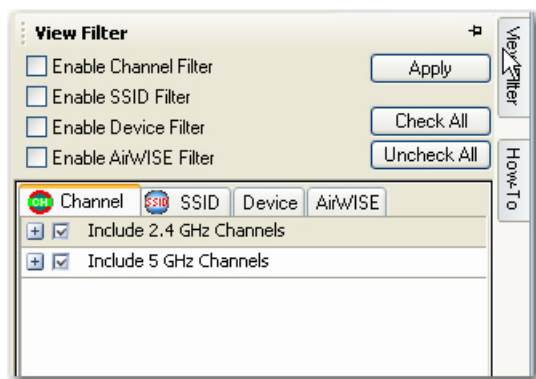


Figure 15-3: View Filter Pane

The View Filter pane automatically collapses when you click an area outside of it. You can anchor the pane to keep it visible by clicking the thumbtack icon in its upper-right corner.

Applying Filters

As shown in [Figure 15-3](#), the View Filter pane contains four tabs: Channel, SSID, Device, and AirWISE, each representing a specific type of filters. You may filter on any or any combination of the four categories. By default, all filters are turned off. If you wish to enable a given filter category, you must first check the corresponding check box in the top portion of this pane. Then you need to click to open the corresponding filter tab below to select the entries to be filtered, i.e., channels, SSIDs, devices, or AirWISE alarms. You then need to make your desired selections individually or use the Check All button. Finally, you need to click the Apply button to activate your filters.

Channel Tab

The Channel filter allows you to define the channels whose data are shown on the screen. It differs from changing the channel scan settings (see [“Configuring SmartEdge Sensor’s 802.11 Settings” on page 399](#)) in that by using the View Filter, you are simply altering the data that will be displayed, not the data that are actually processed. In other words, Remote Analyzer will continue to monitor the unchecked channels, but it will not display data from them until you disable the filter.

SSID Tab

The SSID filter allows you to display data regarding specific SSIDs of interest. As with the channel filter, it affects the data display only. Once you disable the filter, data detected from other SSIDs will appear onscreen as well.

Device Tab

The Device filter allows you to define the devices of interest to be shown on the screen. For example, you can filter out devices that have been inactive for a certain period of time or those whose signal strength fall below a certain value.

AirWISE Tab

The AirWISE filter allows you to specify alarms to be shown onscreen based on the level of severity you specify. This way, you can focus your attention more on alarms that are of great interest to you.

How-To Guide

The tab located below the View Filter opens up an interactive guide that helps the user troubleshoot problems or configuration issues for the wireless environment. The guide contains links that allow the user to select from a variety of common wireless network scenarios. The major categories are:

- Device Monitoring Issues
- Remote Analyzer Configuration
- Troubleshooting WLAN Networks
- Security Auditing
- Performance Auditing
- 802.11n Troubleshooting

After selecting the desired option, the user is presented with a step-by-step process for analyzing and repairing the issue at hand. Links contained within the steps help the user easily navigate to the necessary screens within Remote Analyzer itself. You can activate the How-To guide from any major Remote Analyzer screen by clicking the tool button along the right edge of the user interface, as shown in [Figure 15-4](#).

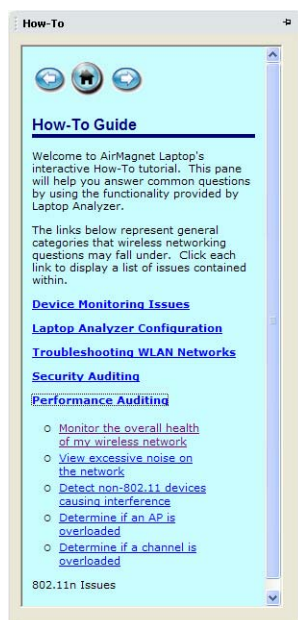


Figure 15-4: How-To guide main page

Toolbar

Across the top of Remote Analyzer is a toolbar that contains a collection of buttons and drop-downs that provide tools for using the program. While some contents of the toolbar may be available only on certain screens, the major options remain the same on all major screens.

Figure 15-5 shows the common options on the toolbar.



Figure 15-5: Common tools

Table 15-2 describes the common tool options on the toolbar and their functions.

Table 15-2: Common Toolbar Options










Tool	Description
	<p>The File menu provides the following command options:</p> <ul style="list-style-type: none"> Open. . . —brings up the Open dialog box which allows you to browse for and open a file in a .amc, .ecp, or .cap format. Close—closes the file currently opened on the screen. Save—saves the data the application has captured as a file using any of the supported formats. See Open above. Save As. . . —saves the file currently opened on the screen using a different file name or format. Configure. . . —Opens the AirMagnet Configure dialog box which allows you to set or change the settings of the application. Recent Files—Shows a list of recently opened files. Reset—This option erases all collected data from the buffer, effectively restarting Remote Analyzer. Exit—Closes the application.
	<p>The Band button allows you to select one of the following 802.11 bands you wish to scan:</p> <ul style="list-style-type: none"> 2.4 GHz (for 802.11b/g/n channels) 5 GHz (for 802.11a/n channels) 2.4/5 GHz (for 802.11a/b/g/n)
	<p>The Configure button contains two options in its drop-down menu: Configure. . . and Policy Management. . .</p> <p>Note: <i>Policy Management is not available in the Remote Analyzer interface. Policies for AirMagnet Enterprise sensors must be applied using the Enterprise Console. See Chapter 12, “Managing Policy Profiles” for more details.</i></p>
	<p>This button allows you to show data on screen either by percentage or by dBm.</p>
	<p>These buttons allow you to control the application’s live capture mode. They are from left to right, Start Live Capture, Pause Live Capture, and Stop Live Capture.</p> <p>Note: <i>Pause Live Capture applies only to the Decodes screen.</i></p>
	<p>The View Reports button allows you to view reports based on data on the current screen and to set up your printer settings.</p>
	<p>The Import-Export button allows you to import or export an ACL as well as some important data captured by the application.</p>

Table 15-2: Common Toolbar Options

Tool	Description
	<p>The Help button contains three options in its drop-down menu:</p> <ul style="list-style-type: none"> Contents . . . — opens Remote Analyzer’s online Help. About . . . — opens the About AirMagnet dialog box which contains important information about this product. Check Update — allows to check the availability of software update.

Working on Start Screen

Remote Analyzer’s Start screen serves as a dashboard of your WLAN and is loaded with comprehensive, summarized information about RF signal quality, network infrastructure, security and performance status, and frame communication in your wireless LAN environment. You can get to the Start screen when you launch the program or by clicking  from the Navigation Bar if you are on another screen.

By default, Remote Analyzer starts in live capture mode, as indicated by Live Capture on its title bar. (Refer to [Figure 15-1](#).) From the Start screen, one can easily drill down to a specific channel, a WLAN component (e.g., an AP or client station), or a security or performance alarm for further information or analysis.

Start Screen UI Components

As shown in [Figure 15-1](#), Remote Analyzer’s Start screen can be divided into the following sections as indicated by the boxed areas, each showing a specific type of information of the wireless network. On the left, from top to bottom, are the RF Signal Meter, 802.11 Information and Alarm Summary, and Frame Address Type Table. On the right, from top to bottom, are Device Data and Alarm Details.


Toolbar Options

The Start screen’s toolbar contains several tools that are available only on this screen: the text-search tool, the Easy View button, and OK/Rogue buttons. See [Figure 15-6](#).



Figure 15-6: Start Screen Toolbar

Text-Search Tool

The text-search tool allows you to easily find a node based on device name, AP Group, MAC address, or SSID on the Device Data section of the Start screen. Simply enter your search criteria into the box and click the  (Find in this view) button. Click the button repeatedly to continue finding the next device that meets your criteria.

Easy View Button

The Easy View button allows you to open a drop-down menu that contains the pre-configured viewing options for you to choose from:

- **View by SSID** – This option allows you to sort all devices in the Device Data section by SSID.
- **View by Device** – This option groups all devices by device name. It is especially useful if you have multiple devices using the same name.
- **View by Media Type** – Devices will be grouped based on their media types: 802.11a devices show up first, then 11b, 11g, and 11n. If your devices use a different media type (such as FCC 4.9GHz), they show up only if your card supports that mode.
- **View by Channel** – This option sorts devices based on the channel on which they are detected.
- **View by Node Type** – This (default) option allows you to sort all devices by device type (i.e., AP, STA, or Ad-Hoc).
- **View by 802.11n** – This option allows the user to view only 802.11n devices currently active. Note that this option only appears if a supported 802.11n adapter is in use.
- **Advanced** – This option allows you to customize the way devices are sorted. After it is selected, a new grey field will appear above the Device Data pane. You can drag and drop column headings into this field to define your sorting tree structure. For example, if you wish to sort based on Type first, then channel, and then device name, drag the Type column heading into the grey area first, followed by the Channel heading, and finally the Device heading. The devices will be sorted accordingly. To remove a heading from your tree, simply drag it back into the column headings below.

OK/R(ogue) Buttons

The OK and R buttons next to the Easy View drop-down menu allow you to mark a selected device as authorized or rogue device with a click of the button. Simply select the device of interest in the Device Data pane and click the status option (OK or R) you wish to use. The changes will be immediately reflected in the ACL column of the Device Data pane.

RF Signal Meter

The upper-left part of the Start screen is the RF signal meter, which provides an overview of RF signal quality on all available channels, each represented by a bar. The bars implement a high watermark feature that shows the highest point each channel has reached within a user-specified interval (configurable via the General tab of the Configure menu). See [Figure 15-7](#).

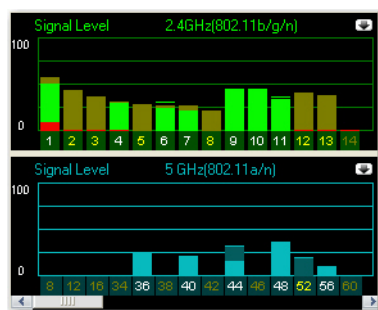


Figure 15-7: Signal meter

RF Signal Quality Codes

As seen from the screen, the channel bars are color-coded, and the colors change dynamically to reflect the changes in RF signal quality. Also note that the color coding schemes for 802.11a and 802.11b/g differ slightly, as shown in Figure 15-7.


For 2.4-GHz (802.11b/g/n) channels, RF signal quality is color-coded as follows: (Refer to the upper part of Figure 15-7):

- **Green** — means that access points (APs) and/or stations (STs) are being detected on the channel. If an unassigned channel shows bright green, it may indicate that there are RF signals coming from APs of a neighboring business or from some other unknown sources, possibly rogue APs. In this case, actions should be taken to look into the sources of all unidentified RF signals.
- **Brown** — denotes cross-channel interference or station probing are being detected on the channel. Cross-channel interference is common in an 802.11 network because 802.11 channels tend to overlap each other. Therefore, an AP transmitting RF signals on Channel 2 will inevitably cause noticeable interference on Channels 1 and 3. This is why APs should be assigned to non-overlapping channels. For example, if you have three APs and Channels 1 through 11 available, you may want to assign the APs to Channels 1, 6, and 11, respectively, to minimize the chances of cross-channel interference.
- **Red** — indicates that noise is being detected on the channel. If you have 2.4-GHz cordless phones, Web cameras, microwave ovens, or similar devices operating in the same frequency spectrum, you may see a noise level (red bar) above 10% or 75 dBm. Channel noise could cause high packet error rates and disrupt wireless transmission, resulting in poor network performance or unstable network connectivity.

For the 5-GHz 802.11a/g/n channels, RF signal quality is color-coded as follows:

- **Light Blue** — indicates that access points (APs) and/or stations (STs) are being detected on the channel.
- **Dark Blue** — indicates that cross-channel interference or station probing is being detected on the channel.
- **Red** — indicates that noise is being detected on the channel.

Expanded RF Graphs

You can expand the channel view by clicking  (Expand) in the upper-right corner of the signal meter. This allows you to view signal level (Green/Brown), noise level (Red), signal/noise ratio (Yellow), and interference score (Off-white) in separate graphs. See [Figure 15-8](#).

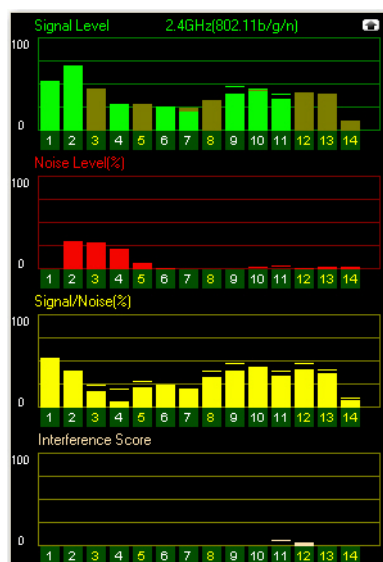



Figure 15-8: Expanded signal meter

The interference score graph gives you a quick view of the interference currently seen on each channel. For a more detailed view, click the channel of interest and you will be taken to the Interference page with that channel selected.

You can customize the channel scan list by eliminating unused channels and changing the scan frequency (see [“Configuring System Settings” on page 251](#)). This allows you to focus your attention on capturing traffic on known active channels while still keeping an eye on the other channels for rogue APs and stations.

You can restore the signal meter to its original state by clicking  (Collapse) in the upper-right corner of the expanded signal meter screen. Refer to [Figure 15-7](#).

Tip: Double-clicking a channel in the signal meter will take you directly to the Channel screen.

802.11n 20-/40-MHz Channels

With an AirMagnet-supported 802.11n wireless network adapter, Remote Analyzer is also able to scan 802.11n data traffic on the 20- and 40-MHz channels. The 40-MHz wide band is denoted by a wide bar in the RF Signal Meter section on the Start screen. See [Figure 15-9](#).

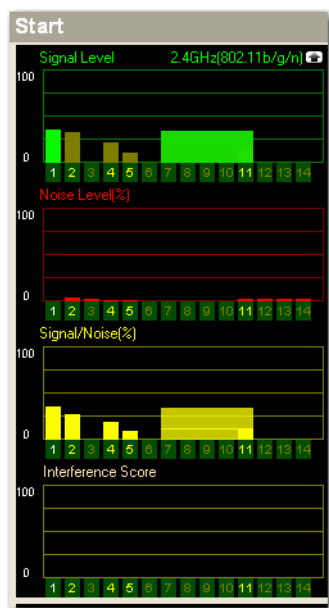


Figure 15-9: 20-/40-MHz channels

802.11 Information

The **802.11 Information** is an visual summary of your wireless LAN infrastructure. It categorizes all the components or devices detected on your wireless network and shows the total number of components or devices in each category. See [Figure 15-10](#).

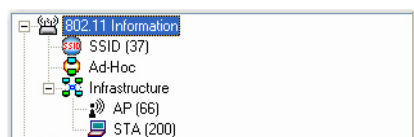


Figure 15-10: 802.11 information

Tip: Highlighting a node such as SSID, Ad-Hoc, AP, or STA allows you to display the network infrastructure information in the pie chart below; double-clicking an entry takes you directly to the Infrastructure screen.

AirWISE Advice

Below the 802.11 Information is a section entitled AirWISE Advice, which categorizes all the alarms detected on your WLAN into security and performance. There are four sets of digits for each category, representing different levels of severity. The digits, from left to right, represent alarms that are Critical, Urgent, Warning, or Informational. See [Figure 15-11](#).

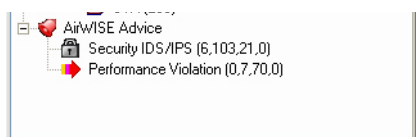


Figure 15-11: AirWISE advice

Highlighting an alarm category allows you to display in the pie chart the percentage of alarms of different severity levels; double-clicking an alarm category takes you directly to the AirWISE screen.

Pie Chart

This section summarizes the RF data in the form of a pie chart. It provides an easy visual display of the selected RF data. See [Figure 15-12](#).

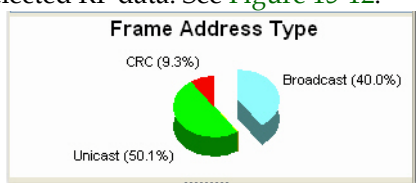


Figure 15-12: Pie chart

The content of the pie chart depends on the item selected from the 802.11 Information and AirWISE Advice sections of the Start screen.

Tip: To display the pie chart, you may need to maximize the size and/or resolution of your screen. You may also need to have the signal meter in a collapsed state.

Packet Frames Summary

In the lower-left corner of the Start screen is a tabulation of packet frames Remote Analyzer has detected. The frames are categorized into four categories: broadcast, multicast, unicast, and CRC. See [Figure 15-13](#).

Broadcast	184004	Multicast	2547
Unicast	226917	CRC	43486
Total Frames	456954	CRC	9.52%

Figure 15-13: Packet frames summary

*By default, the packet frames summary pane is hidden from view. The user has to enable it by clicking **File>Configuration...>General>Show Frame Statistics>OK**.*

[Table 15-3](#) briefly describes each of these frames.

Table 15-3: Summary of Packet Frames Transmission

Frame Type	Description
Broadcast	Broadcast is a term used to describe communication where data are sent for one point to all other points. In other words, there is just one sender, but the information is sent to all connected receivers.
Multicast	Multicast is a communication pattern in which a source host sends a message to a group of destination hosts simultaneously.
Unicast	Unicast is a term used to describe communication where data are sent from one point to another point. There are only one sender and one receiver.
CRC	Cyclic Redundancy Checks are used to verify packet information and reduce the potential for errors.

The Total Frames field displays the total number of frames that have been detected on the network so far. The field to its right allows you to view how much (the percentage) each frame type accounts for in the total number of frames. Simply click the down arrow and select from the drop-down menu the frame type you wish to view.

Device Data

The upper right-hand side of the Start screen is the Device Data section which summarizes the data about all the wireless devices detected on your WLAN. See [Figure 15-14](#).

	Device	MAC	.11	Security	SSID	ACL	BI
1	QA_VoFL_2	00:14:A8:44:13:20	g	2	Encrypted N	QACiscoVoice	R 100
1	Edimax:0B:8C:C4	00:1F:1F:0B:8C:C4	n	2	Encrypted N	anygate	R 100
1	QA_VoFL_2	00:0F:34:A7:78:13	g	0	Encrypted N	QAVocera	OK 100
1	AP-10(BG)	00:14:69:F3:16:31	g	34	2 WPA-P	N AirMagnetGuest	R 100
1	QA_VoFL_2	00:0F:34:A7:78:12	g	0	0 WPA2-P	N QAVOFI	OK 100
1	AP-10(BG)	00:14:69:F3:16:30	g	35	2 WPA2-E	N Air2	R 100
1	QA_VoFL_2	00:0F:34:A7:78:11	g	0	0 WPA-P	N QASpectralink	R 100
1	QA_VoFL_2	00:0F:34:A7:78:10	g	0	0 Encrypted N	QACiscoVoice	R 100
1	D-Link:EC:5D:CB	00:1B:11:EC:5D:CB	g	0	2 WPA2-P	N Amicus_G1	R 100
1	DeltaNet:15:C4:E9	00:30:AB:15:C4:E9	b	0	0 Open	N Wireless	R 100
3	Netgear:9E:85:48	00:1B:4D:9E:85:48	g	31	2 WPA-P	N chopper	R 100
4	Cisco-linksys:DB:88:81	00:12:17:DB:88:81	g	35	3 WPA-P	N QA-linksys-WRT54G-LAB	R 100
4	Symbol:9E:A7:29	00:A0:F8:9E:A7:29	b	27	3 Open	N qa_symbol@QA_lab_in_s...	R 100
4	AP-12(BG)	00:11:5C:4D:E8:F1	g	15	3 WPA-P	N AirMagnetGuest	R 100
4	AP-12(BG)	00:11:5C:4D:E8:F0	g	10	3 WPA2-E	N Air2	R 100
5	00:11:22:33:44:55	00:11:22:33:44:55	g	0	0 802.1x	N wIPS_Attack	R 1
5	00:11:22:33:44:66	00:11:22:33:44:66	g	0	0 Open	N wIPS_Attack	R 69
6	Cisco-Linksys:95:48:E9	00:1D:7E:95:48:E9	n	36	3 Open	N linksys	R 100
6	Cisco-Linksys:0F:BB:F0	00:1D:7E:0F:BB:F0	g	27	3 Open	N linksys-g-tv	R 100
6	1200-Calibratio	00:14:A8:53:66:40	g	0	0 Encrypted N	1200-calibration	R 20
7	AP-11(BG)	00:11:5C:44:5E:B1	g	16	2 WPA-P	N AirMagnetGuest	R 100
7	AP-11(BG)	00:11:5C:44:5E:B0	g	17	2 WPA2-E	N Air2	R 100
7	AP-13(BG)	00:11:5C:4D:E9:11	g	6	2 WPA-P	N AirMagnetGuest	R 100
7	AP-13(BG)	00:11:5C:4D:E9:10	g	0	0 WPA2-E	N Air2	R 100

Figure 15-14: Device data

The devices are organized into three categories, as indicated by the collapsible sections: APs, Ad-Hocs, and STAs. You can choose to display a certain category of devices by clicking the '-' button on the fields that you wish to omit to collapse them (for example, to view stations only, collapse the AP and Ad-Hoc sections). The table contains 30 data fields, including Channel, Device/MAC Address, Display 802.11, Signal Strength, Noise Level, Signal-to-Noise Ratio, Security Mechanisms, TKIP & MIC, Bridge Mode, SSID, ACL Status, Rogue in Network, Beacon Interval, Number of Stations, Preamble, PCF/DCF, Latitude, Longitude, Altitude, Distance, First Seen Time, and Last Updated Time.

You can sort the data by any category simply by clicking the title of that column, e.g., SSID. Use the scroll bar at the bottom of the table to view all the data contained in the table. You can also customize the number of columns of data to be displayed.

In [Figure 15-14](#), "n" in the .11 column denotes an 802.11n device. An 802.11n wireless network adapter is required in order for Remote Analyzer to detect 802.11n devices on the network.

To add/remove display columns:

- 1) Right-click anywhere in the data display field and select “Set Display Columns” from the menu. The Field Chooser dialog will appear.
- 2) Drag-and-drop the column headings from the dialog box into the columns in the table. The heading you dragged in will be added to the Start page.
- 3) Reverse Step 2 to remove a heading from the table.

Tip: Double-clicking a field in the alarm column takes to the AirWISE screen, which shows all alarms detected from that device; double-clicking in any other column takes you directly to the Infrastructure screen.

Table 15-4 briefly describes the data shown in Figure 15-14.

Table 15-4: WLAN RF Data Summary Table Entries

Icon	Description
Type	Shows the category of the device which can be one of the following: <ul style="list-style-type: none"> • AP • STA • Ad-Hoc
Alarms	Displays alarms involving the device. An alarm (bell) icon appears in this column if the device has triggered alarms.
Channel	All available channels detected on the WLAN: <ul style="list-style-type: none"> • Red = Alarms are detected on the channel. • Yellow = No alarm is detected on the channel.
Active Time for Device	Displays the current status of the device. The icon is color-coded to display how long the device has been active: <ul style="list-style-type: none"> • Green = Device has been active within the last 5s. • Yellow = Inactive within the last 5-60s. • Red = Inactive within 60-300s. • Grey = Inactive for more than 300s.
AP Group	Shows AP group names if you have set up the AP Grouping feature. See “ AP Grouping ” on page 280 for more information

Table 15-4: WLAN RF Data Summary Table Entries

Icon	Description
Device	<p>Displays the name of the device. Often, the name will default to the device's MAC address. This field (and the MAC Address field below) is color-coded to display the activity status of the device:</p> <ul style="list-style-type: none"> Green = The device has been active within the last 5 seconds. Yellow = The device has been inactive between the last 5~60 seconds. Red = The device has been inactive between the last 60~300 seconds. Grey = The device has been inactive for more 300 seconds.
MAC Address	Displays the device's MAC Address. This field uses the same color-coding conventions as the Device field (above).
802.11	<p>Type of 802.11 media, i.e., 802.11b or 802.11g, the device is using.</p> <ul style="list-style-type: none"> Green = 802.11b Orange = 802.11g Blue = 802.11a Green/Blue = 2.4 GHz 802.11n/5 GHz 802.11n
Signal	Displays the signal strength in % or dBm.
Noise	Displays the noise level in % or dBm.
Signal-to-Noise Ratio	Displays signal-to-noise ratio measured in % or dBm.
Interference Score	Displays the interference score of the channel.
Security Mechanisms	<p>Indicates the security mechanisms used on the device:</p> <ul style="list-style-type: none"> WPA-P = WPA-Personal WPA-E = WPA-Enterprise WPA2-P = WPA2-Personal WPA2-E = WPA2-Enterprise VPN = PPTP, IPsec, Secure Shell, etc. Open = no security mechanism in place Encrypted = packets are encrypted, but the specific encryption mechanism is not known ? = Security mechanism is unknown <p>Devices utilizing multiple SSIDs will display the security settings for each SSID implemented, separated by commas.</p>

Table 15-4: WLAN RF Data Summary Table Entries

Icon	Description
TKIP/MIC	Shows TKIP/MIC security settings: <ul style="list-style-type: none"> Y = Enabled; N = Disabled; U = Unknown. Devices utilizing multiple SSIDs will display the security settings for each SSID implemented, separated by commas.
Bridge Mode	<ul style="list-style-type: none"> Y = Bridge Mode; N = Non-Bridge Mode.
SSID	Displays the SSID of the device.
ACL Status	Shows the ACL status of the device. <i>Note: When Remote Analyzer is launched for the first time upon installation, all devices detected are shown as U (Unknown). The user has to change the ACL status of all the devices one by one. This can be done by right-clicking a device and then selecting Rogue Device if it is a rogue device or Valid Device and then a specific ACL group from the submenu if it is a known, valid device on the network. All valid devices are marked by OK. Once a device's ACL status is marked, it will show up on the Start screen with same ACL status the next time you launch the application if the same device is detected. However, if you all devices are marked R (Rogue), all devices will show up as U (Unknown) if you restart the application after exiting it.</i>
Rogue in Network	Shows rogue devices traced inside the enterprise network.
BI	Shows Beacon Interval (in milliseconds)
Associated AP	Displays the name of the AP that the device is associated with.
#STA	Shows the number of stations associated.
Preamble	Shows the preamble value which can be either of the following: <ul style="list-style-type: none"> Long Short
PCE/DCF	Displays whether Point Coordination Function or Distributed Coordination Function is being used.
Latitude	Shows the latitude of the device (GPS only).
Longitude	Shows the longitude of the device (GPS only).
Altitude	Shows the altitude of the device (GPS only).
Distance	Shows the distance of the device (GPS only).
First	Displays the time the first packet was received.


Table 15-4: WLAN RF Data Summary Table Entries


Icon	Description
Last	Displays the time the last packet was received.
Cell Power	Shows the power level at which the AP is transmitting in dBm.
Note:	<i>The following are applicable to View by 802.11n only.</i>
Tx Ch Width	Shows supported Tx channel width.
Rx Ch Width	Defines the channel width that may be used to transmit to the AP or STA.
PCO	Shows the PCO status which can be either of the following: <ul style="list-style-type: none"> • PCO active in the BSS • PCO inactive
Greenfield Supported	Indicates whether Greenfield transmission is supported, which can be either of the following: <ul style="list-style-type: none"> • Y = Yes • N = No
SGI	(Short Guard Interval) Shows the Short Guard Interval for 20-MHz and 40-MHz.
2nd Channel	(Secondary Channel Offset) Indicates the offset of the secondary channel relative to the primary channel.
Operating Mode	Indicates the operating mode of the BSS from which protection requirements of HT transmissions are determined.
Non-Greenfield STA Present	Indicates whether non-Greenfield stations are present, which can be either of the following: <ul style="list-style-type: none"> • N = All stations are greenfield-capable. • Y = One or more HT stations associated are not Greenfield-capable.
Non-HT OBSS	(OBSS Non-HT STAs Present) <ul style="list-style-type: none"> • Y = Use protection due to OBSS • N = No protection due to OBSS
40 GHz Intolerant	For APs, this indicates whether BSSs within the range are required to prohibit 40-MHz transmissions; for STAs, it indicates to its associated AP that it is required to prohibit all 40-MHz transmissions within the BSS.
RIFS Mode	Displays FIFS mode.
Tx STBC	(Tx STBC Supported) Indicates whether Tx STBC is supported, which can be either of the following: <ul style="list-style-type: none"> • Y = Supported • N = Not supported.

Table 15-4: WLAN RF Data Summary Table Entries

Icon	Description
Rx STBC	(Rx STBC Supported) Indicates the state of Rx STBC support, which can be one of the following: <ul style="list-style-type: none"> • 0 = Not supported • 1 = 1 stream • 2 = 2 one and two streams • 3 = One, two, and three streams
LDPC	Shows LDPC Coding Capability which cab either of the following: <ul style="list-style-type: none"> • Y = Yes • N = No
SM Power Save	Displays SM Power Save.
Dual Beacon	Indicates whether Dual Beacon is used: <ul style="list-style-type: none"> • Y = Secondary beacon is transmitted by AP. • N = No secondary beacon is used.
Dual CTS Protection	Indicates wether Dual CTS Protection is required: <ul style="list-style-type: none"> • Y = Required. • N = Not required.
L-SIG TxOP Full Support	Indicates whether L-SIG TxOP is supported: <ul style="list-style-type: none"> • Y = All HT STAs support LSIG TxOP Protection. • N = One or more HT STAs do not support LSIG TxOP Protection.

Using Bubble Help

The  (Show/Hide Bubble Help) button allows you to enable or disable the bubble help, which is a context-sensitive tip screen that is only available for the Signal Meter, 802.11 Information and AirWISE Advice, and Device Data sections of the Start screen. It provides helpful information these parts of the screen where text labeling is impossible to implement due to space constraints.

To use the bubble help, click  and then mouse over an object in any of the those sections. Refer to [Figure 15-15](#).

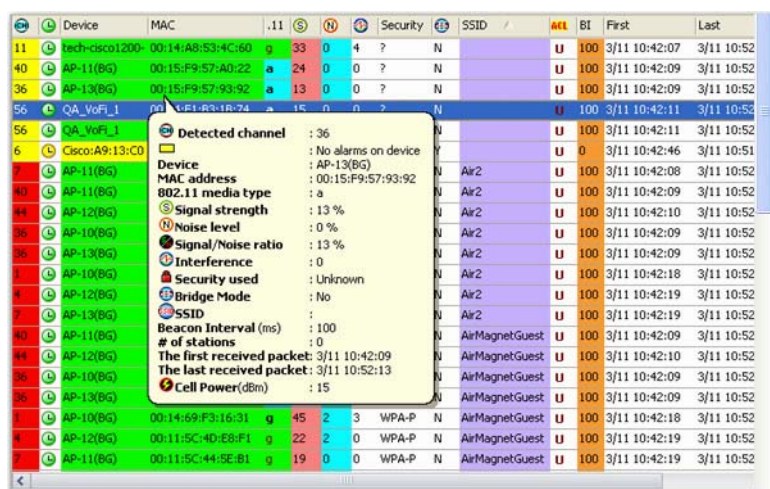


Figure 15-15: Using Bubble Help

AirWISE Details

Below the Device Data section is the AirWISE section, which shows alarms data in two major categories, i.e., Security IDS/IPS v.s. Performance Violation. See Figure 15-16.

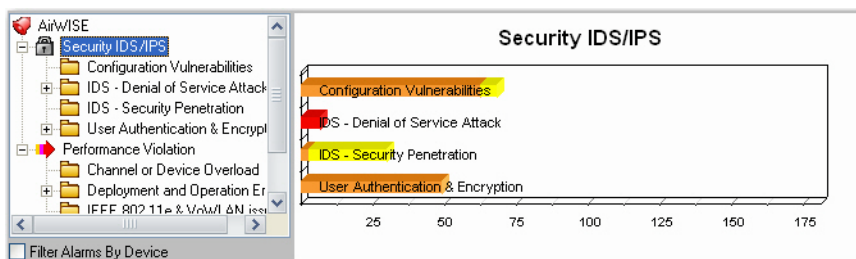


Figure 15-16: AirWISE

On the left are various types of alarms in each category; on the right is a bar chart that displays the total number of alarms contained in each category that you have selected.

In the lower left-hand corner of this section is the **Filter Alarms by Device** check box. Normally, the Alarm Summary section displays the alarms that have been generated by all the devices (i.e., APs, STAs, or Ad Hoc). However, if this check box is checked, the Alarm Summary section will only display alarms about the device, whether it is an AP, station, or ad hoc station, you select from the Device Data section.

Changing Operating Frequency

Wireless devices can use different radio operating frequencies to transmit and receive packets on a wireless network, depending on the 802.11 wireless networking protocol being used. Remote Analyzer supports all 802.11 protocols, i.e., 802.11a/b/g/n. Since wireless devices built on different 802.11 standards use different operating frequencies, selecting or changing the operating frequency on Remote Analyzer forces the application to gather packets that are

generated only by devices using a specific radio operating frequency. In so doing, it allows you to focus on network traffic involving wireless devices that are using a specific 802.11 protocol. The Operating Frequency drop-down menu lists all the operating frequencies supported by the wireless network card currently used on Remote Analyzer. [Figure 15-17](#) shows the options that are available when an 802.11a/b/g/n wireless network card is used.

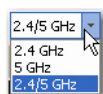


Figure 15-17: Operating Frequency Drop-Down Box

Changing operating frequency is just like physically changing the wireless network card. Remote Analyzer will empty all the packets captured in the buffer and then start capturing data using the new operating frequency. Any change in operating frequency is reflected in other parts of the UI that are affected. If you are on a screen other than the Start screen, selecting another band will take you directly to the Start screen.

802.11 Protocols and Operating Frequencies

[Table 15-5](#) briefly describes the operating frequencies used by different 802.11 wireless networking standards.

Table 15-5: 802.11 Protocols and Operating Frequencies

Protocol	Operating Frequency (GHz)	Typical Throughput (Mbps)	Maximum Data Rate (Mbps)	(Indoor) Range (Feet)	(Outdoor) Range (Feet)
80211a	5.15~5.25 5.25~5.35 5.745~5.825	23	54	~90	~300
80211b	2.4~2.5	4	11	~105	~330
80211g	2.4~2.5	19	54	~105	~330
80211n	2.4 and/or 5	74	248	~210	~480

Changing RF Signal Unit of Measurement

By default, channel RF signal strength, noise level, and signal-to-noise ratio are displayed in percentage (%). However, you can change to dBm by clicking the %/dBm drop-down menu next to the media type button. See [Figure 15-18](#).



Figure 15-18: dBm/% Drop-Down Box

Notice the changes in the Signal, noise, and signal-to-noise ratio fields in the Device Data section as you toggle between % and dBm.

Worldwide 802.11 a/b/g/n Radio Channel Allocation



Since regulatory rules dictate the radio frequencies (channels) and emission powers for 802.11 standards in various parts of the world, the number of channels available depends on the geographical location and the media band (2.4 GHz vs. 5 GHz) you select. [Table 15-6](#) shows channel allocation for all both 2.4 GHz and 5 GHz media bands in major parts of the world.

Table 15-6: Worldwide Radio Channel Assignment

Region/Country	2.4 GHz	5 GHz
Americas	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 149, 153, 157, 161, 165
Most part of Europe and Australia	1 ~ 13	36, 40, 44, 48, 52, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
France	10 ~ 14	36, 40, 44, 48, 52, 56, 60, 64
Spain	10 ~ 11	36, 40, 44, 48, 52, 56, 60, 64
Japan	1 ~ 14	36, 40, 44, 48, 52, 56, 60, 64,
Pacific Rim (China, Taiwan, Hong Kong, Singapore, Korea, etc.)	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161


The Start screen displays the top-level information of your WLAN's RF environment. It is especially useful if you want to have a quick grasp of what is going on in or around your WLAN. However, keep in mind that the data on this screen are real-time and dynamic. Old data get erased as new data come in. It is for this reason that Remote Analyzer comes with a live capture feature that allows you to record (save) data so that they can be replayed at a later time for analysis. The data can be exported as well.

Accessing Data Reports

The integrated AirMagnet Reporter automatically converts all on-screen data into reports. The content of the reports are screen-specific, making them easy to view, analyze, share, and archive. You can access the reports by clicking  Reports from the Navigation Bar or  (View Reports).

Detailed instructions on how to use the Reporter can be found in [Chapter 11, "Using the Reports Screen"](#).

Working on Channel Screen

You can drill down to the Channel screen by clicking any of the channel bars on the signal meter from the Start screen or by clicking  Channel from the Navigation Bar. The Channel screen lets you focus on a specific channel for detailed analysis. See [Figure 15-19](#).

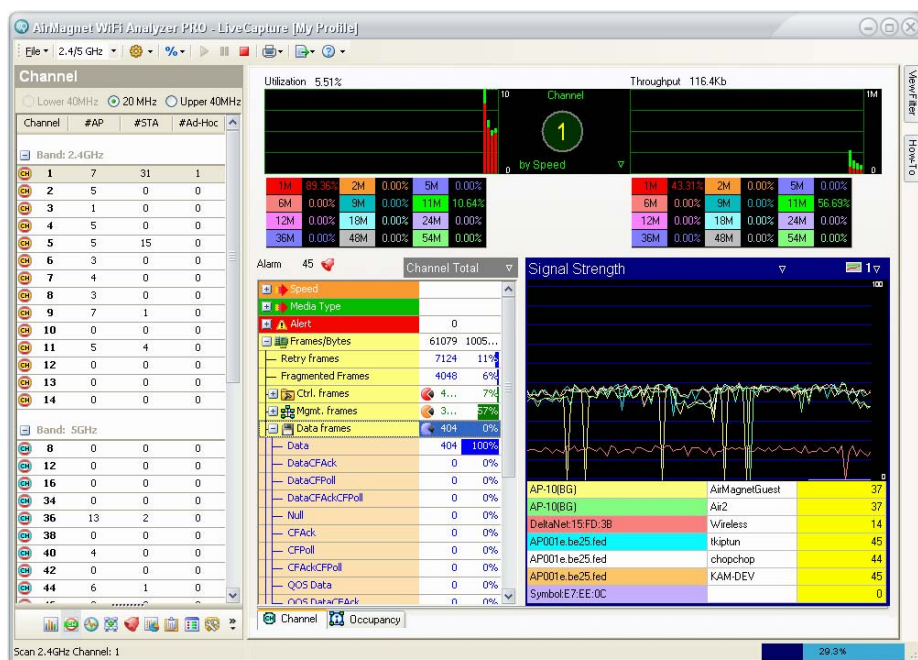


Figure 15-19: Channel screen

Channel Utilization and Throughput

The top part of the screen consists of two signal meters: one for channel utilization and the other channel throughput. As a rule of thumb, 60% of utilization or 6 Mbps of throughput is a realistic upper limit for an 802.11b network. Constant high channel utilization with most traffic in 11 Mbps and low packet error rates may indicate that the 802.11b network may not have enough capacity to meet the needs of all its users. One possible solution would be to reduce the cell size and to add access points at strategic locations.

Channel Selection Pane

The left-hand side of the screen contains the channel selection pane. Its contents vary depending on the media type you select. There are four columns in the channel selection pane: Channel, #AP, #STA, and #Ad-Hoc. These columns display the channel numbers and the number of APs, Stations, and Ad-Hoc devices on each channel.

Across the top of this part of the Channel screen are three radio buttons that represent the mode of the network. The buttons are:

- **Lower 40 MHz** — If selected, the 40-MHz lower channel is shown. Both the legacy and HT packets can be transmitted in lower 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.
- **20 MHz** — If selected, only shows 20-MHz channel. This mode focuses on the 20-MHz channel. According to the 802.11n Draft 2 standard, this mode is mandatory.
- **Upper 40 MHz** — If selected, the 40-MHz upper channel is shown. Both the legacy and HT packets can be transmitted in upper 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.

You can know whether any or all of these three modes are supported on a certain channel simply by clicking the channel number below. The mode will be automatically greyed out if it is not supported on that channel.

You can switch from one channel to another simply by selecting a from the list. Once a channel is selected, Remote Analyzer will lock on that channel until another channel is selected. The selected channel is indicated by the number inside the circle in the middle of the upper part of the screen. See [Figure 15-20](#).

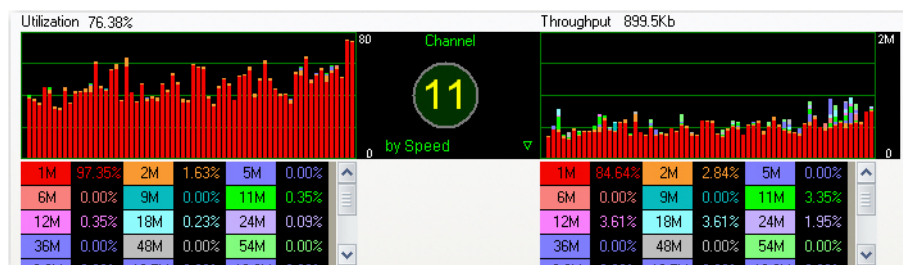


Figure 15-20: Focusing on one channel

The number “11” inside circle in [Figure 15-20](#) indicates that the channel you are focusing on is a 20-MHz channel. However, a left arrow will appear below the channel number when a lower 40-MHz channel is selected and a right arrow will appear below the channel number when a upper 40-MHz channel is selected. Both arrows indicate that the channel you are focusing on is the primary channel in a 40-MHz channel. Furthermore, the left arrow indicates that the secondary channel is below the primary channel whereas the right arrow indicates that the secondary channel is above the primary channel.


The lower portion of the graph displays the speed at which packets are being transmitted on the selected channel. These fields are color-coded and correspond with the graphs above. If the entire graph is red (as shown in [Figure 13-20](#)), virtually all packets on your network are being transmitted at 1 Mbps.

Link Speed and Media Type

When you are using 802.11g, a/g, or a/b/g/n for your media type, a filter appears below the channel number, allowing you to toggle the data display between link speed and media type. Both link speed and media type are color-coded. Selecting by **Speed** will display the different rates at which data are being transmitted in the fields below the graphs; selecting by **Media** will display the media types that packets are being sent using.

Channel Data Summary

The middle-left part of the Channel screen summarizes various critical information about the selected channel.

On the top is a channel alarm summary. It shows the number of alarms triggered on the channel. Clicking  will take you to the AirWISE screen, where a detailed explanation about the alarm(s) and expert advice are available.

Below the alarm summary is a list of RF data summary for the selected channel. All the data are displayed in frames or bytes. Each type of data is represented by an icon. You can choose to view the details of any of these data or hide them by clicking the plus or a minus sign next to the corresponding icon. You can also filter the data display either by Channel Rate or by Channel Total using the options from the drop-down menu in the top-right corner of the summary pane. See [Figure 15-21](#).

Category	Value 1	Value 2
Speed		
Media Type		
Alert	0	
Frames/Bytes	2059	1909157
Retry frames	0	0%
Fragmented Frames	345	16%
Ctrl. frames	1158	56%
Mgmt. frames	2	0%
Data frames	1	0%
CRC frames	898	43
Ctrl. Bytes	40272	2%
Mgmt. Bytes	354	0%
Data Bytes	50	0%
CRC error Bytes	1868481	97%

Figure 15-21: Viewing channel data summary

[Table 15-7](#) describes the screen information as shown in [Figure 15-21](#).

Table 15-7: Channel Screen Control Buttons








Button	Description
	<ul style="list-style-type: none"> Summarizes link speed of the channel.
	<ul style="list-style-type: none"> Summarizes the types of media discovered on the channel.
	<ul style="list-style-type: none"> Lists frame error code information.

Table 15-7: Channel Screen Control Buttons

Button	Description
 Frames/Bytes	<ul style="list-style-type: none"> Divides frame and byte counts into retry frames, fragmented frames, control frames, management frames, data frames, and CRC error frames, etc.
 Ctrl. frames	<ul style="list-style-type: none"> Summarizes control frames/bytes.
 Mgmt. frames	<ul style="list-style-type: none"> Summarizes management frames/bytes.
 Data frames	<ul style="list-style-type: none"> Summarizes data frames/bytes.

The Channel screen makes it easy to detect low link speeds, excessive retries, and cyclic redundancy check (CRC) errors.

Device Data Graph

The part of the Channel screen displays the various types of network data in the form of line chart. Across the top this screen are two filters: the one on the left provides up to a dozen types of data for you to choose from for the graph and the one on the right allows you to choose the number of graphs (from 1 to 6) to display at one time. See [Figure 15-22](#).

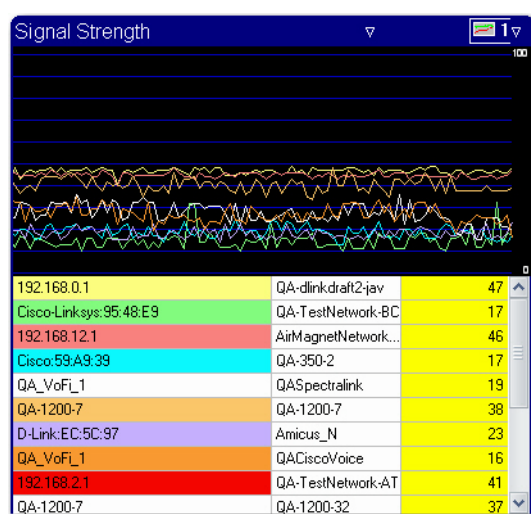


Figure 15-22: Device Data Graph for Selected Channel

[Figure 15-22](#) shows the device data on the selected channel in the lower-right part of the Channel screen. Across the top are two filters: the Data Selector on the left allows you to select the type of data to display and the Graph Options on the right lets you choose to display the data in up to six individual mini screens.

From [Figure 15-23](#) above, we can make the following observations about the first 5 devices listed:

- 1) They are operating on 2.4-GHz Channel 1.
- 2) The 5th device has the weakest signal strength of the 5.
- 3) All 5 devices contribute modulated interference on Channels 2 and 3.
- 4) All 5 devices contribute (at least some) un-modulated interference on Channels 4 through 7.

We may also make the following observations about the 7th and 8th devices listed:

- 1) These devices are operating on 40 MHz (Lower), Channel 11.
- 2) The modulated interference extends two additional cells on either side of the center frequency, as compared to the 20 MHz devices discussed above.
- 3) However little, the un-modulated interference extends all the way to Channel 1.
- 4) We can see the 10-MHz shift in center frequency for the device (as indicated by the fact that the center channel is under Channel column 9, instead of 11).

It should be noted that the 2.4-GHz and 5-GHz channel occupancy differs from each other, in the fact that the 5-GHz channels are spaced 20 MHz apart, as compared to 5 MHz for the 2.4-GHz channels. Thus, devices will take up less cells in the 5-GHz view than the 2.4-GHz view.

Working on Interference Screen

The Interference screen allows you to view the amount of signal interference that currently exists on a given channel. The selected channel's interference score is displayed numerically as well as graphed on the right of the device listing. The interference score indicates the extent to which signal interference impacts your network's performance. The larger the value, the severe the impact. See [Figure 15-24](#).

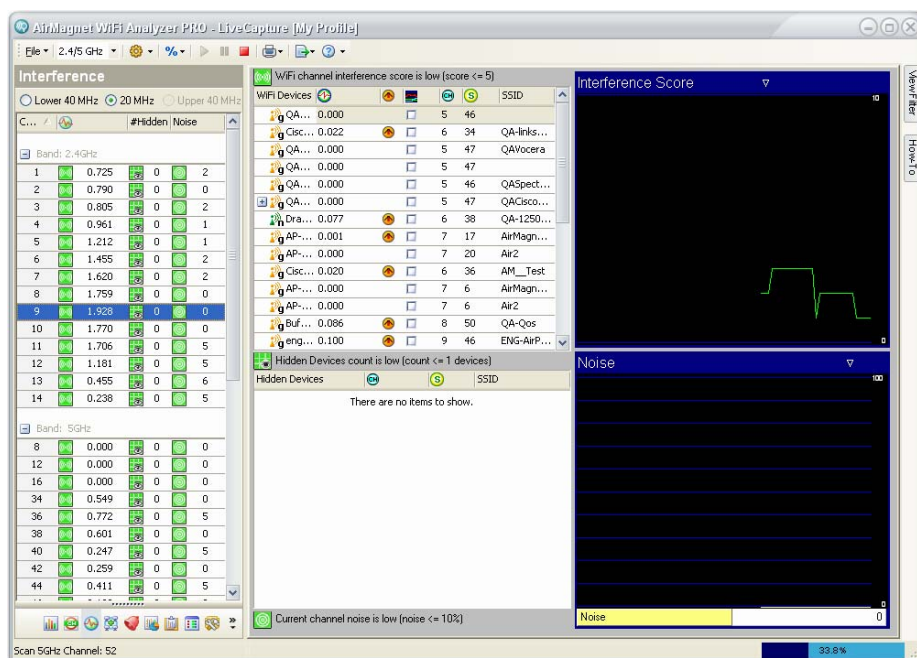


Figure 15-24: The RF Interference Page

A channel's interference score is calculated based entirely on standard WiFi devices. Each device operating on the selected channel or on adjacent channels will generate interference on the channel you are focusing on. The displayed interference score adds up the interference from these devices and shows how much interference the channel is experiencing as a result. Each separate channel may have widely varying interference scores due to different numbers of devices operating in the adjacent channels.

The displayed interference score represents the total of all standard interference generated on the selected channel by 802.11 devices, i.e., APs, wireless stations, etc. Any non-802.11 interference will simply show up as noise, which you can view by selecting the Noise option in the graph below.

Interference Score

A channel's interference score is calculated based entirely on standard WiFi devices. Each device operating on the selected channel or on adjacent channels will generate interference on the channel you are focusing on. The displayed interference score adds up the interference caused by all these devices and shows you how much interference the channel is experiencing as a result. The interference scores may vary widely among channels due to the difference in the number of devices operating on their adjacent channels.

If you are using Remote Analyzer by itself (without Remote Spectrum Analyzer integration), the displayed interference represents the total of all standard interference generated on the selected channel by 802.11 devices, i.e., APs, stations, etc. Any non-802.11 interference will simply show up as noise, which you can view by selecting the Noise graph option in the lower right-hand corner of the screen. To identify the sources of noise (i.e., objects or devices that are causing this noise), you may purchase AirMagnet Spectrum Analyzer and integrate it with Remote Analyzer.

Channel Interference Calculation

802.11 defines RF transmit spectrum mask requirements for each of the modulation types supported by the standard. These requirements are used to limit the amount of interference an 802.11 device contributes to channels which are adjacent to the channel on which it is operating. As RF channels do not have exact edges, it is prudent that 802.11 devices employ filtering and/or other techniques to minimize the amount of RF energy they emit outside their operating channel when they transmit. While this “out-of-channel” interference is minimized, it can't be zero.

The following transmit spectrum masks are defined in the 802.11 standard (and/or its amendments):

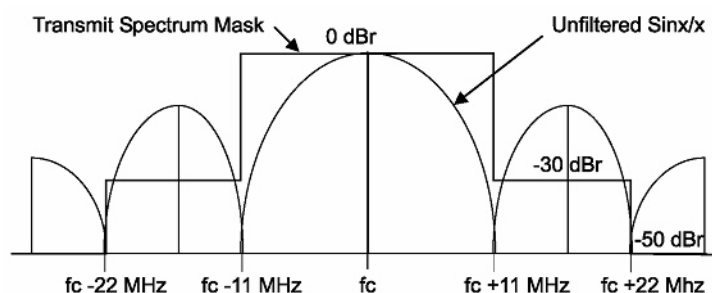


Figure 15-25: Transmit Spectrum Mask for 802.11b

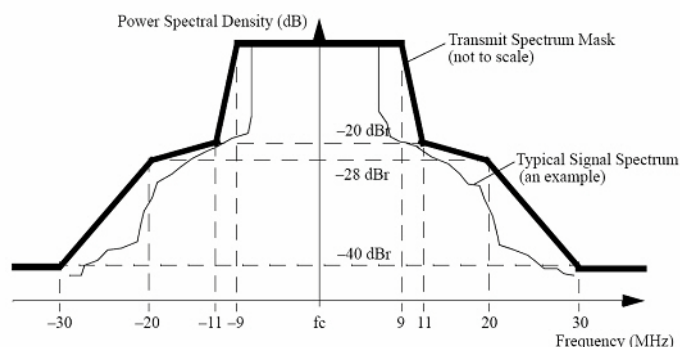


Figure 15-26: Transmit Spectrum Mask for 802.11a/g (20 MHz)

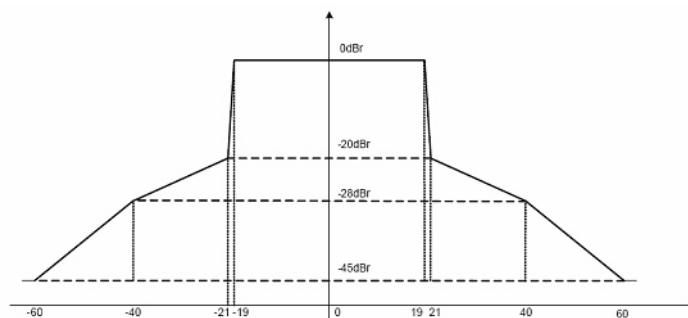


Figure 15-27: Transmit Spectrum Mask for 802.11n (40 MHz)

As illustrated in [Figure 15-25](#) through [Figure 15-27](#), an 802.11 device is allowed to contribute as much as -28 to -50 dBm (decibels relative to peak) on adjacent channels when they transmit. For 40 MHz transmissions in the 2.4 GHz band, RF energy may be present as far away as 11 channels from the center frequency.

Remote Analyzer uses these spectral properties of 802.11 devices to determine the amount of interference a particular device contributes to a particular (logical) channel.

In calculating an interference score, the following details are taken into consideration:

- 1) The “spectral distance” between the channel of interest and a device’s operating channel (including each of the channel’s widths).
- 2) Whether or not the interference from a device (to a channel) is caused by modulated spectrum (i.e., within the device’s operating channel width), or by the “bleed over” outside the modulated portion of the transmission(s).
- 3) The RSSI (signal strength) of the device.
- 4) The current “bandwidth utilization” of the device; that is, how often it is currently transmitting.

After performing calculations based upon the above, the interference score is normalized, scaled (and potentially capped) for each device in order to provide some consistency with previous versions of the product.

It should be noted that, in this way, a “busy” AP on Channel 6, with very strong signal strength, may contribute more interference to Channel 1, than a less busy AP on Channel 3, with a weaker signal strength (from the capture vantage point).

The list of interfering devices shown on the Interference screen distinguishes between modulated (🔴) and un-modulated (🟡) interference contributions.

Channel Interference Summary

The left-hand side of the Interference screen allows you to specify which channel you wish to view. The channel listings are divided by media type, with 802.11g channels listed first, and 802.11a channels below. You may collapse list by simply clicking the '+' sign next to the heading. See [Figure 15-28](#).

The screenshot shows the 'Interference' window with three radio buttons at the top: 'Lower 40 MHz' (unselected), '20 MHz' (selected), and 'Upper 40 MHz' (unselected). Below the buttons are three tabs: 'Channel' (selected), '#Hidden', and 'Noise'. The window displays two sections of data, one for 'Band: 2.4GHz' and one for 'Band: 5GHz'. Each section contains a table with four columns: Channel, Frequency (MHz), #Hidden, and Noise (dBm). The 2.4GHz band shows 14 channels, and the 5GHz band shows 3 channels.

Channel	Frequency (MHz)	#Hidden	Noise (dBm)
Band: 2.4GHz			
1	0.000	21	0
2	208.802	21	28
3	214.994	22	28
4	239.875	22	28
5	278.203	11	27
6	285.257	11	27
7	333.241	49	26
8	367.294	65	26
9	307.067	65	26
10	388.379	64	25
11	368.349	64	0
12	325.095	64	0
13	281.069	64	28
14	198.463	26	28
Band: 5GHz			
8	100.253	0	23
12	4.052	0	0
16	2.834	0	23

Figure 15-28: Channel Interference Summary

The channels you have available for selection vary depending on the media type you select and geographical location you reside. Different 802.11 media type and countries or regions of the world utilize different channels.

You can filter the content of the channel interference summary by using the radio buttons across the top of this section (Figure 15-28):

- **Lower 40 MHz** — Only the 40-MHz lower channel is shown. Both the legacy and HT packets can be transmitted in lower 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.
- **20 MHz** — Only 20-MHz channel is shown. This mode is similar to 802.11a/g because the bandwidth required is 20 MHz and the devices present in this network are similar to the legacy devices. Per 802.11n Draft 2 standard, this mode is mandatory.
- **Upper 40 MHz** — Only the 40-MHz upper channel is shown. Both the legacy and HT packets can be transmitted in upper 40-MHz mode. Per 802.11n Draft 2 standard, this mode is optional.

The channel interference summary contains four data columns which are intended to provide a brief overview of data on each channel. The columns (from left to right) are as follows:

- **The first column** - lists all available channels by 802.11 media band (2.4 GHz vs. 5 GHz). You may show or hide the media bands simply by clicking the '+' or '-' signs at the top of each section.

The channels you have available for selection will vary based on the media band you have selected and the country or region Remote Analyzer is used; channel allocation may differ from country to country.

- **The second column** - displays the interference scores on the channels in real time.

The icons next to interference scores are color-coded: green for interference scores that aren't considered outside of normal levels (0-4.999); yellow for interference scores that are considered 'warning' signs (5-19.999); and red for severe interference (20 and above) that requires immediate attention. Table 15-8 below provides a list of the color thresholds for each column.

Table 15-8: Channel Pane Color Codes

	Green	Yellow	Red
Interference	0-5	5.01-20	20.01 or greater
#Hidden	0-1	2-5	6 or greater
#Interferers	0-1	2-5	6 or greater

- **The third column** - displays the number of hidden devices detected on the corresponding channels. Hidden devices can cause interference and traffic collisions within your network, thereby slowing down general network operations (for more details regarding hidden devices, see Hidden Station Detected).
- **The fourth column** - displays the noise level detected on each of the listed devices. It can be in dBm or percentage, depending on the unit of measurement you use from the menu bar.

However, the fourth column will display the number of non-802.11 interfering devices detected on each of the channels if you have integrated AirMagnet Spectrum Analyzer and are using a Spectrum Analyzer card.

When a particular channel is selected, all areas in the right-hand side of the Interference screen will be updated to show interference- or noise-causing devices that are detected on that channel.

Interfering Devices

The interfering devices pane is made up of two parts. The left part is a table that shows all devices detected on the selected channel as well as the channel, interference score, modulated (📶)/un-modulated (📶), channel, signal strength, and SSID of each of the devices; the right part is that Interference Score graph that displays the interference scores of selected devices in the form of line charts. The message across the top of the table tells you about the overall state of RF interference on the channel. See [Figure 15-29](#).

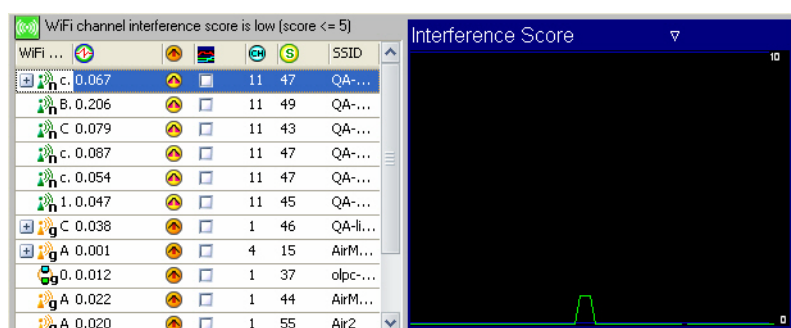


Figure 15-29: Devices and Interference Graph

You can use the check boxes in the middle column of the table to select the devices to be graphed on the Interference Score graph. You may select as many devices as you wish (each selected device is represented by a line chart of a unique color). You can also right-click anywhere in the table and select “Enable All” from the pop-up menu to all devices in the list. However, having too many devices selected at one time may result in a cluttered graph that could be difficult to read. For this reason, you may want to select only the devices of interest to you.

Even when you are focusing on a specific channel, devices from other channels will often appear on the RF Interference screen. This is because these devices are also causing interference on the selected channel. Devices on adjacent channels can cause cross-channel interference.

Hidden Devices

The hidden devices pane is located right below the interfering devices pane. It displays all hidden devices, if any, that are detected on your network. It provides information such as device name, channel, signal strength, and SSID of each hidden devices being detected. The message across the top of this section tells about the total number of hidden devices detected on the channel. See [Figure 15-30](#).

Hidden Devices: count is medium (1 < count <= 5 devices)			
Hidden Devices			SSID
GemTek:BD:FC:7F	1	43	Air2
GemTek:BD:FC:7F	1	0	Air2
Senao:22:78:AB	1	41	ShawnXiong_AP, p...
Intel:63:8B:0A	1	8	
Intel:63:9A:C0	1	15	<No current ssid>,...

Figure 15-30: Hidden devices on a channel

Hidden devices represent a problem where two different devices (stations, for example) cannot see each other directly (often due to distance between them). Since the two devices are unaware of each other, they may try to access an AP between them at the same time, causing network collisions. This would result in both stations needing to re-transmit their packets, thus creating a delay in your network traffic. For more information on hidden devices, refer to the “Hidden Station Detected” alarm in the AirMagnet Remote Analyzer Policy Reference Guide.

Graph Pane

As shown in the preceding screen shots, the interference score graph charts the interference score of the selected channel and devices over time. The bottom portion of the graph pane, however, is more flexible. It graphs data involving the specific device you have selected in the interfering devices pane. See [Figure 15-31](#).

*Note that the lower graph does not chart the devices you have **checked**, but rather the one you have **selected** at any given time. Selecting a new device will cause the graph to refresh.*

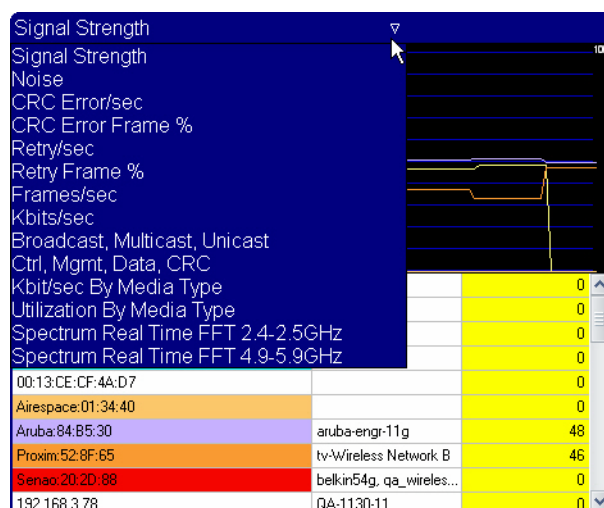



Figure 15-31: Lower graph field

Figure 15-31 displays the graph with no device selected. It charts statistics based on all the devices in the channel. The graph options change, however, when you actually select a device to view. Since this graph is based on the selected device (as opposed to a range of devices you have checked), it provides a wider variety of graph types to view.

Working on the Infrastructure Screen

You can drill down directly to the Infrastructure screen by clicking a node (e.g., an SSID, Ad-Hoc, AP, or STA) from the Start screen. You may also access the Infrastructure screen by tapping  **Infrastructure** on the Navigation Bar. See Figure 15-32.

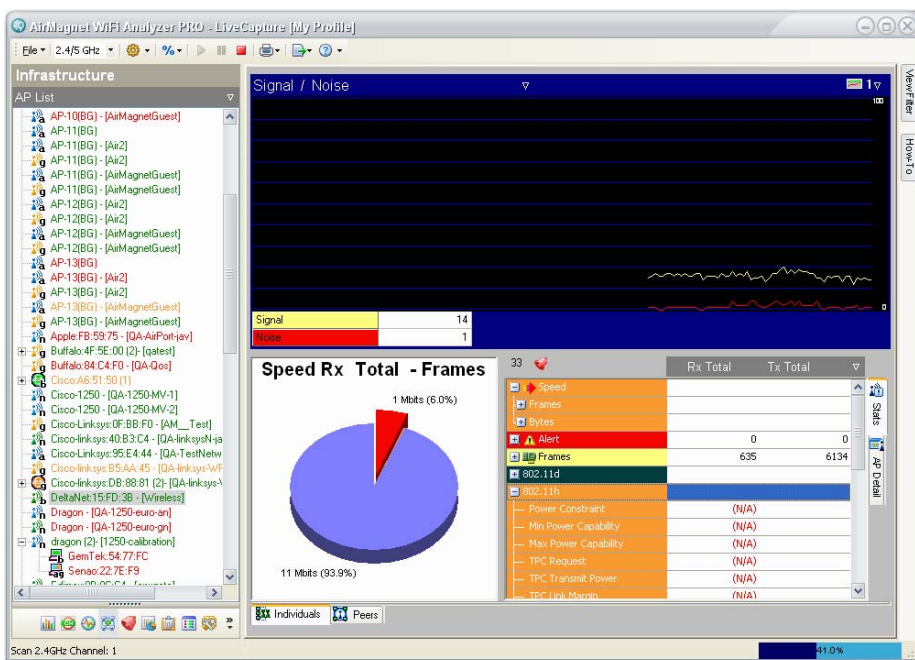


Figure 15-32: Infrastructure screen

Network Tree Structure

The left part of the Infrastructure screen displays in an organized form all nodes detected on your WLAN. You can use the filter at the top of this field to display the network infrastructure by SSID, channel, access point, station, ad-hoc network, 802.1x user, or media type. Selecting an access point will have all associated stations shown under the access point, identified by MAC or IP address. See Figure 15-33.

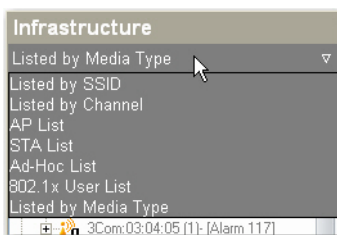


Figure 15-33: Infrastructure screen filters

Network Infrastructure Color Codes

As seen from [Figure 15-32](#), SSIDs, APs, and stations on the network tree structure are color-coded. Each color represents a specific RF signal status as described in [Table 15-9](#).

Table 15-9: Infrastructure RF Signal Color Codes

Color	Description
Green	The device has been active for the last 5 seconds.
Orange	The device has been inactive for the last 5 to 60 seconds.
Red	The device has been inactive for the last 60 to 300 seconds.
Grey	The device has been inactive for more 300 seconds.

Analyzing Data of Individual Devices

The right-hand side of the Infrastructure screen displays the data for the selected node on the network tree structure. Selecting an AP or station from the network infrastructure allows you to display various detailed information about the selected device.

The Infrastructure Data Graphs

The top of the right-hand side of the Infrastructure screen is a graphical display of data for the selected node on the network tree. You can use the Data Selector at the top left of this pane to choose the data to display and the Graph Options at the top right to select a viewing option. This allows you to view up to six graphs simultaneously. The default graph displays the selected device's signal and noise levels, but you may choose from a variety of graphs similar to the options in the RF Interference page. See [Figure 15-34](#) and [Figure 15-35](#).

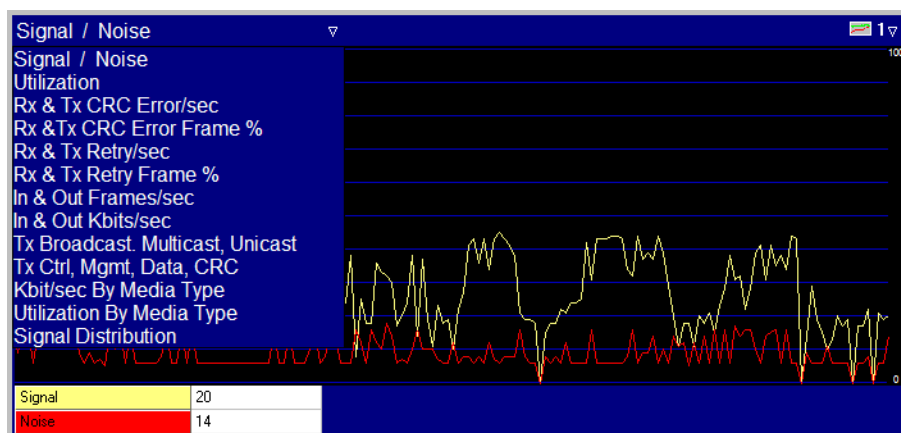


Figure 15-34: Viewing a single data graph

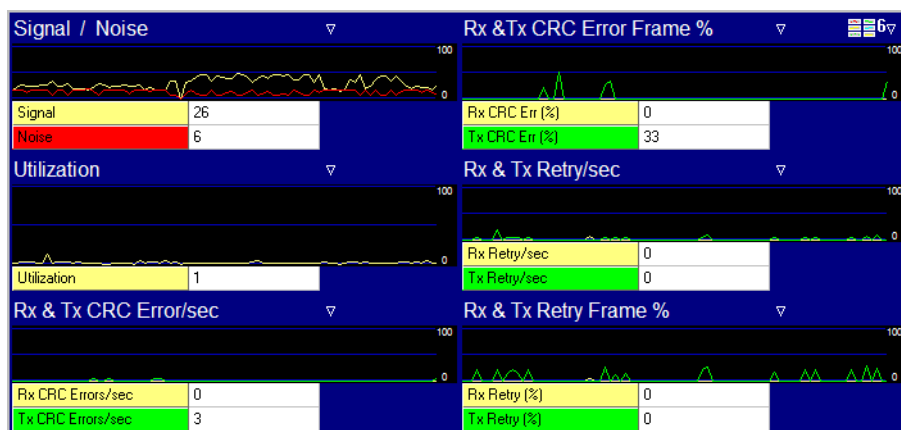


Figure 15-35: Viewing multiple data graphs

Infrastructure Data Summary

The lower part of the screen looks almost the same as what is shown on the Channel screen, but the Infrastructure screen focuses more on the WLAN structural components (i.e., SSIDs, access points, stations, etc.). Therefore, the section at the far right could be AP Detail or Station Detail, depending on the selection made on the network infrastructure.

The AP/Station Detail section shows the authentication mechanisms enabled on the selected device. If a particular device utilizes multiple SSIDs, this section will be repeated for each SSID used.

You can click a plus sign to show detailed data in that category. The selected data are also graphed in the pie chart. You can also customize the data display using the filter in the upper-right corner of the pane. See Figure 15-36.

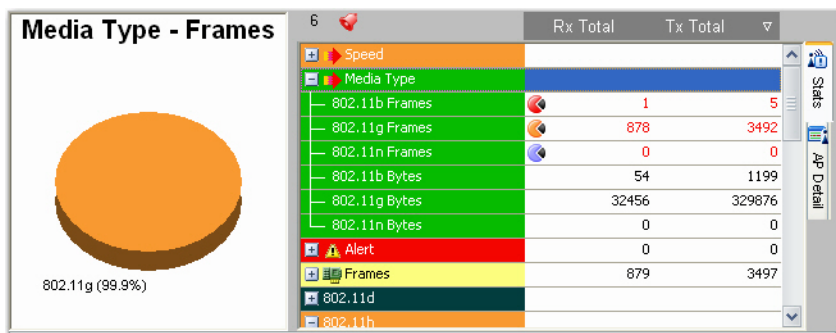


Figure 15-36: Infrastructure data summary


Figure 15-36 shows the AP Detail field on the far right of the screen, but your view may vary depending on your computer's resolution. A laptop PC with a screen resolution below 1600 x 1200

dpi may show the AP/Station Detail field listed below the other ones to the immediate right of the pie chart.

Infrastructure Data Pie Chart

The pie chart displays data for the selected AP or station from the network tree. You can display the data by Speed, Alert, Frames, Control Frames, Management Frames, or Data Frames by clicking the corresponding icon on the right. The chart is color-coded and each slice is labeled with its data type and percentage of the overall chart.

Alarm Status

The alarm status above the data summary field shows the number of alarms that have been logged involving the selected network nodes (i.e., SSID, AP, or station). Clicking  will take you to the AirWISE screen where you can view detailed information about the alarm(s).

802.11d/h Information

Two additional fields that aren't found in the Channel screen provide information regarding any 802.11d or 11h packets detected. The 802.11d specification is much like 802.11b except that 802.11d allows its configuration to be modified at the MAC layer in order to ensure that a network complies with any local rules or regulations. Systems that utilize 802.11d may adjust frequency settings, power levels, and a number of other specifications; this ensures that 802.11d is ideal for systems that will be used in multiple different areas across the world because it can be adapted to suit almost any standard. AirMagnet Remote Analyzer will allow you to view the settings of any device utilizing 802.11d so that you may ensure that all of your devices use the same settings.

802.11h addresses restrictions placed on the 5-GHz frequency currently used by 802.11a devices. The International Telecommunication Union created this set of standards in order to prevent potential interference between 802.11a devices and satellite communications systems. AirMagnet Remote Analyzer provides an easy view of all the information contained in any 802.11h packets detected on your network.

Viewing Connections between Devices

Clicking the Peers tab at the bottom of the Infrastructure screen changes the Infrastructure screen display to peer-to-peer mapping. It allows the user to visualize the relationship between wireless stations at Layers 2 and 3 when they are associating with each other. There are two scenarios as indicated by the drop-down menu in the upper-left corner of the graph screen: Peer-to-Peer and Peer-AP-Peer.

Peer-to-Peer Connections

The Peer-to-Peer graph shows two wireless stations directly associating with each other, without the aid of an AP. All stations are marked in white; the lines joining the stations are of different colors which are assigned randomly for the sole purpose of easy differentiation. See [Figure 15-37](#).

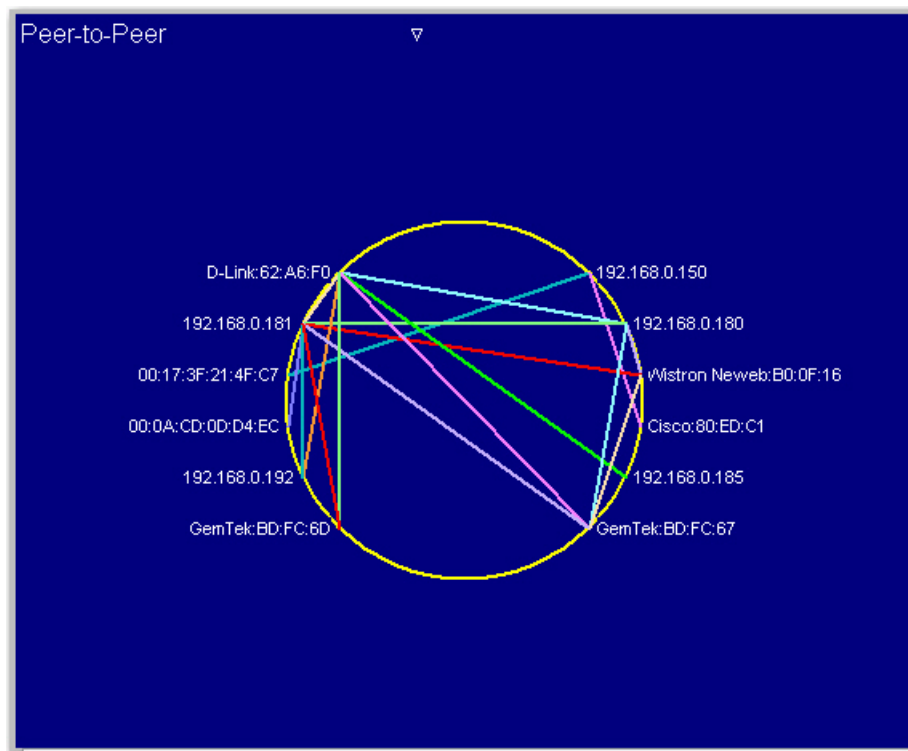


Figure 15-37: Peer-to-Peer connections

Peer-AP-Peer Connections

The Peer-AP-Peer view shows that stations are associating with each other through an AP. See [Figure 15-38](#).

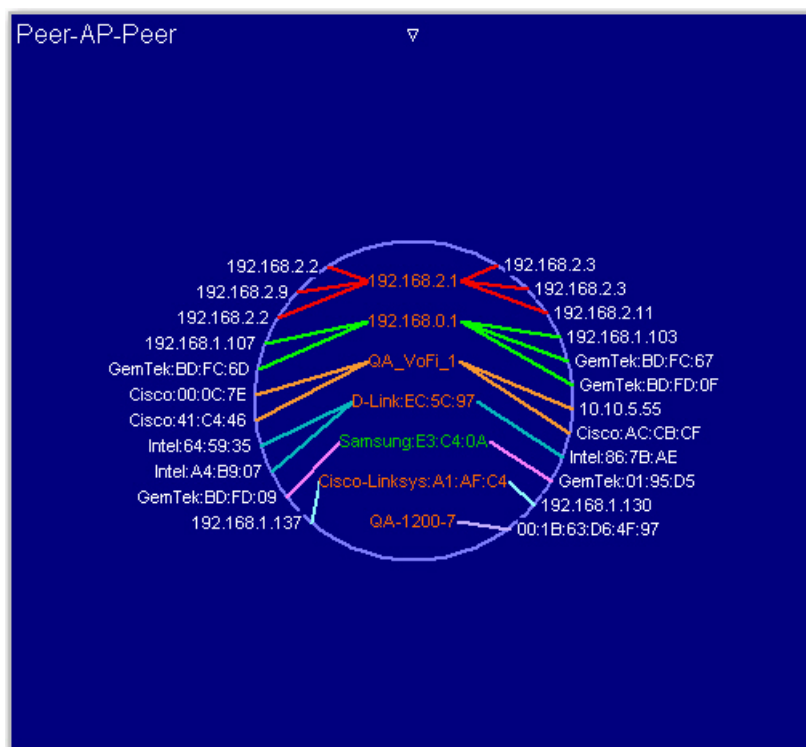


Figure 15-38: Viewing connections between devices



As shown in [Figure 15-38](#), the APs and stations shown in the Peer-AP-Peer connection map are identified by device name, MAC address, vendor name, or a combination of vendor name and MAC address, etc. The entries inside the circle are APs while those outside the circle are stations. The APs are color-coded, reflecting the 802.11 protocols that are used on them:

- Blue—802.11a
- Green—802.11b
- Orange—802.11g
- Green (for 2.4 GHz) and Blue (for 5 GHz) — 802.11n

The lines between APs and stations are also of different colors. However, unlike the color scheme used for APs, the colors for the lines are randomly assigned and merely indicate the order in which the connections are established.

Working on AirWISE Screen

AirMagnet's alarm feature is driven by AirWISE—AirMagnet's patent-pending intelligence analytical engine that helps network professionals monitoring network security and performance status, pinpoint problems, and assist in problem resolution.

You can drill down directly to the AirWISE screen by double-clicking **Security** or **Performance** under AirWISE Advice from the Start screen, by clicking  on any of the screens, or selecting  on the Navigation Bar. See [Figure 15-39](#).

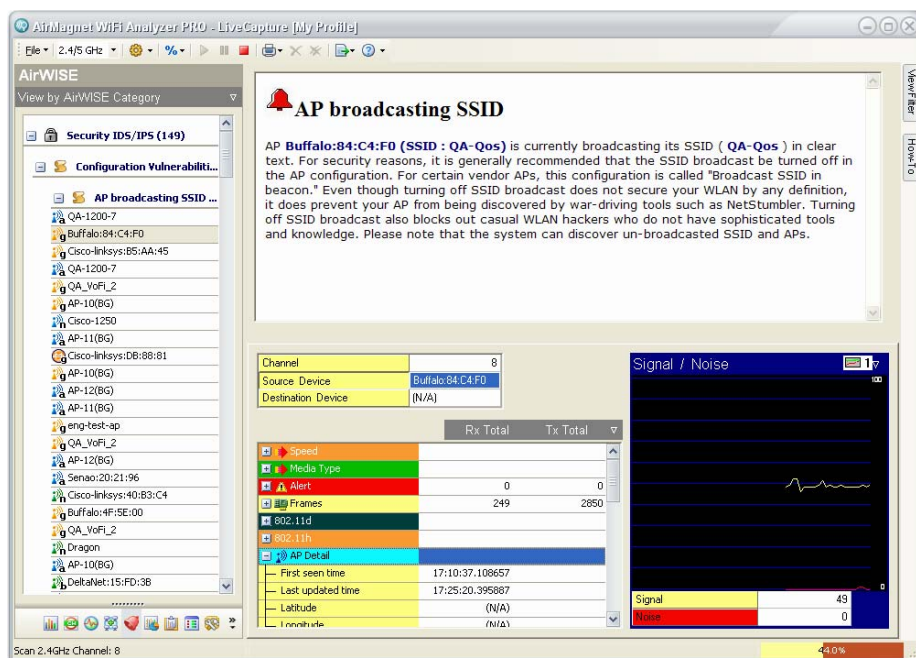


Figure 15-39: AirWISE screen

AirWISE Screen Viewing Options

The left-hand side of the AirWISE screen displays network alarms that have been captured by Remote Analyzer since the beginning of the session. The alarms are listed according to the viewing option the user selects. You can select an option using the filter across the top of the screen. Simply click the down arrow and select an option from the drop down list. See [Figure 15-40](#).

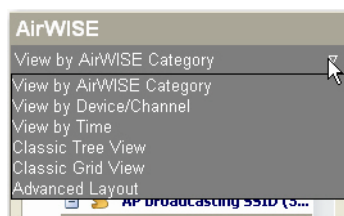


Figure 15-40: AirWISE screen viewing options

As shown in [Figure 15-40](#), the AirWISE screen offers the following viewing options:

- **View by AirWISE Category** - This option displays alarms by the structure of the AirMagnet AirWISE network policy.
- **View by Device/Channel** - This option displays alarms by channel or by device.
- **View by Time** - This option displays alarms by the time they are captured: alarms that are captured within a certain time frame are grouped together; alarms in the same time frame are then further divided by the structure of the AirWISE network policy.
- **Classic Tree View** - This option displays alarms using the classic AirMagnet tree structure which is based on the structure of the AirWISE network policy. All alarms belong to the same policy category are grouped together. It also shows the level of severity of each alarm. In this view, the severity of an alarm is indicated by the icon in front of it, as explained in [Table 15-10](#):



Table 15-10: Alarm Icon and Alarm Severity

Icon	Severity
	Critical
	Urgent
	Warning
	Informational

Managing Alarm List

AirMagnet displays all alarms as they occur. Normally, the alarms are listed in the order they were generated, with the oldest one appearing on top of the list.

The alarms, especially those that have been taken care of, can be removed from the Alarm List using the following options:

-  — Delete the selected alarm or the one on top of the list.
-  — Delete all alarms at once.

You may also right-click any alarm and select “Delete Alarm” from the resulting menu.

Analyzing Network Policy Alarms

The right hand-side of the AirWISE screen is the Expert Advice screen. It provides event-driven explanations and detailed analysis of the policy or policy violation selected from the Alarm Tree.

Tip: The policy hierarchy on the left-hand side of the AirWISE screen governs the way data are displayed on the Expert Advice screen. As you drill down deeper into the policy structure, the information becomes more specific. See [Figure 15-41](#).

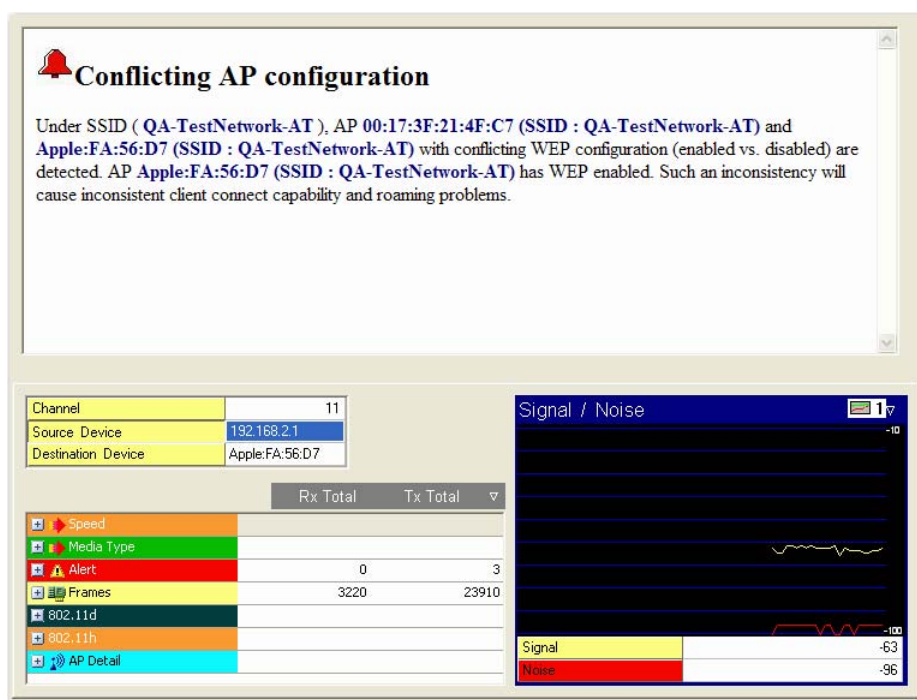


Figure 15-41: AirWISE alarm selected

As shown above, when you have a specific alarm selected, the top pane will display exactly which device caused the alarm and how it did so. The lower pane contains a summary of packet information from the device in question, much like the summary panes in the Infrastructure screen. To find advice regarding how to resolve the alarm, select the alarm subcategory in the AirWISE tree pane on the left.

Expert Advice

The Expert Advice provides detailed explanation of the selected policy, event, or alarm. It warns of the potential risk of the policy breach and offers solutions for the identified issues or problems. The user may need to use the scroll bar or arrow along the right edge of the screen to access the complete advice.

Data Analysis

The Data Analysis section shows the channel where the alarm has occurred, as well as the source and destination node of the link. It allows you to conduct detailed analysis of the selected alarm. The screen provides two display options: Details and Graph. The former is a tabulated summary of data in terms of Speed, Alert, Frames, Control frames, Management Frames, Data Frames, and AP Details or Station Detail; the latter provide a graphical display of data in six different viewing options. You can toggle between the two options using the tabs along the right edge of the screen. Figure 15-42 shows the Data Analysis screen when the Graph tab is selected. If the screen resolution is high enough or if the screen itself is wide enough, the contents for each tab will be displayed in a separate screen.

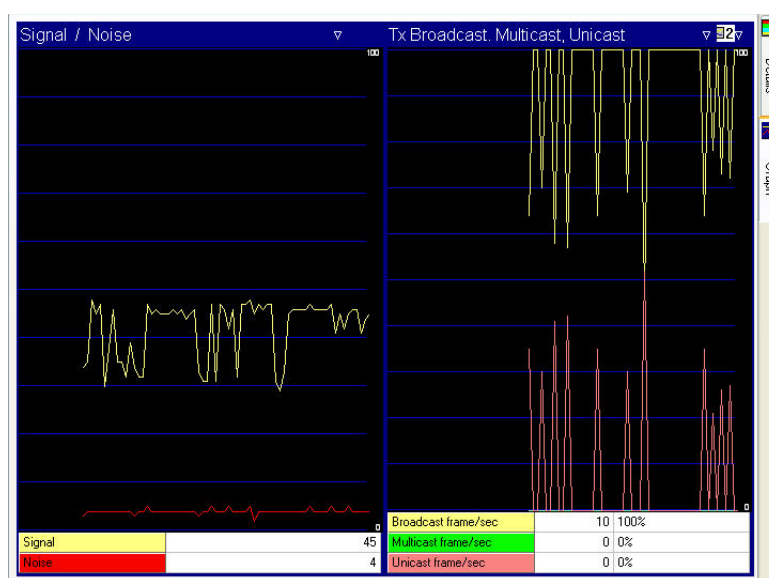


Figure 15-42: Infrastructure screen data graphs

Notice that the data tabulation and graphs are the same as those shown on the Infrastructure screen.

Viewing All Alarms Generated by a Specific Device

This feature allows you to view all alarms generated by a specific device on the same screen. It provides a way for you to organize and view alarms by device, making alarm analysis device-centric.

To display all alarms triggered by a specific device:

- 1) From the Network Policy Hierarchy section, select a policy category and expand it to the alarm level.
- 2) Right-click an alarm, and select **View Device Alarms** from the pop-up menu. See [Figure 15-43](#).

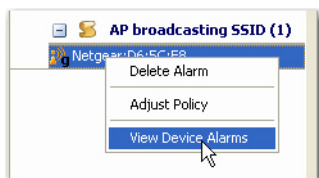


Figure 15-43: The right-click menu

Once you click *View Device Alarms*, the AirWISE screen will refresh and it will focus on all alarms generated by the same device. See [Figure 15-44](#).

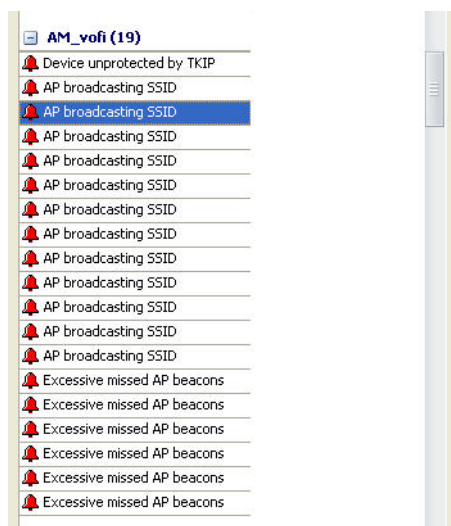


Figure 15-44: Viewing device-specific alarms

- 3) Click each alarm to view the information about the device and alarm description.
- 4) To return to the general AirWISE screen, click the filter down arrow above the Network Policy Hierarchy and select **View by AirWISE Category** from the drop-down list. Refer to [Figure 15-44](#).

Working on Top Traffic Analysis Screen

The Top Traffic Analysis screen allows you to view and analyze data in the form of charts. There are several options for the screen: most show data about the wireless devices (including 802.11n devices) detected on your WLAN, but the compliance section presents data about your network's compliance with government and industry regulations regarding information security.

To access the **Top Traffic Analysis** screen, click  **Top Traffic Analysis** on the **Navigation Bar**. By default, the screen displays device data when it opens. See [Figure 15-45](#).

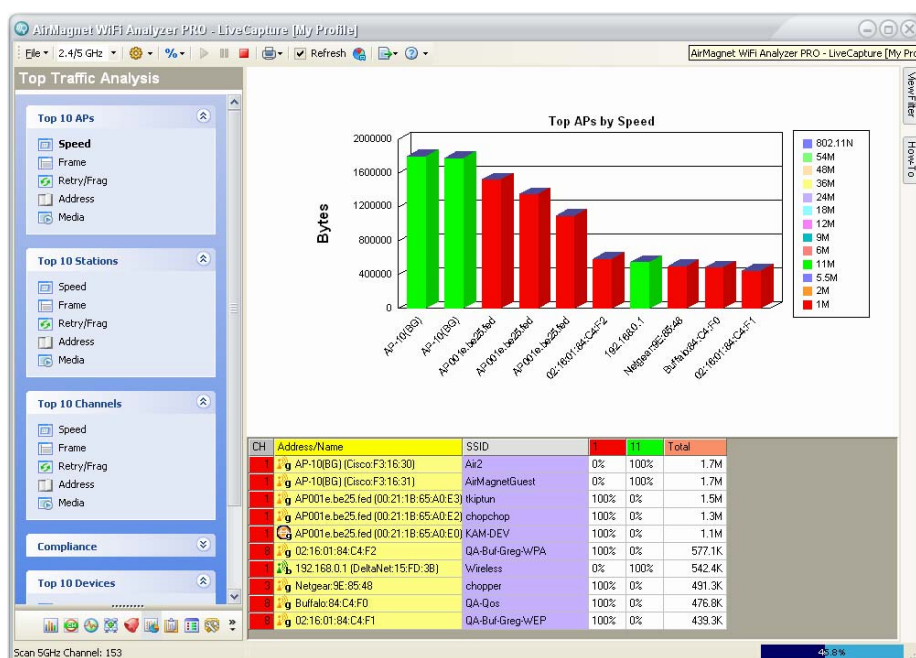


Figure 15-45: Top Traffic Analysis screen

The Top Traffic Analysis Screen refreshes frequently, which may cause a flickering effect on your screen. You may uncheck the refresh box in the tool bar to prevent this.

Top Traffic Analysis Screen UI Components

As shown in [Figure 15-45](#), the Top Traffic Analysis screen has three different panes:

- The charts navigation pane on the left allows you to select the type of data you wish to view a chart regarding.
- The main display pane in the top right displays the currently selected chart.
- The devices pane on the bottom right displays specific statistics regarding the devices shown in the chart above.

Viewing Device Charts

By default, all the channels and SSIDs are selected when the Top Traffic Analysis screen opens. And the screen can provide graphical display of the top 10 devices in the following categories as indicated in [Figure 15-46](#). The Compliance section below displays the various compliance charts, giving you a detailed summary of how well your network complies with regulatory security standards.

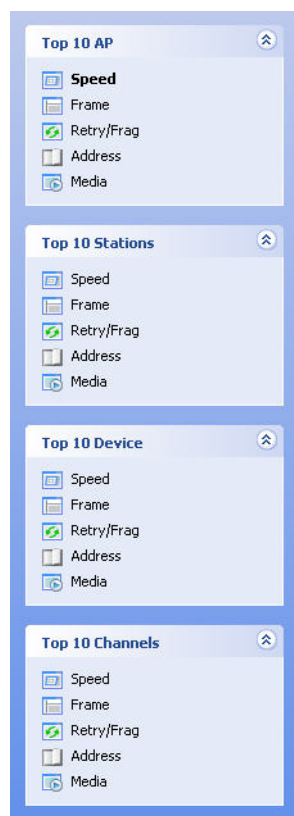


Figure 15-46: Selecting a top 10

Each top 10 category can then be further divided by data type as shown in the Data Type drop-down list displayed under each section heading.

Normally, you can view a device chart by selecting a top 10 category and then choosing a data type. The screen will then display the top 10 most active devices in the selected category. However, if you want to view the most active devices in certain SSIDs or on certain channels, you can do so by using the View Filter tab to select only the SSIDs or channels in which you are interested. In this case, the device chart may still be capable to display data of up to 10 devices, but the actual number of devices displayed depends on the number of devices that are active in the SSIDs or on the channels. [Figure 15-47](#) shows a device chart for only 6 devices on a single SSID.

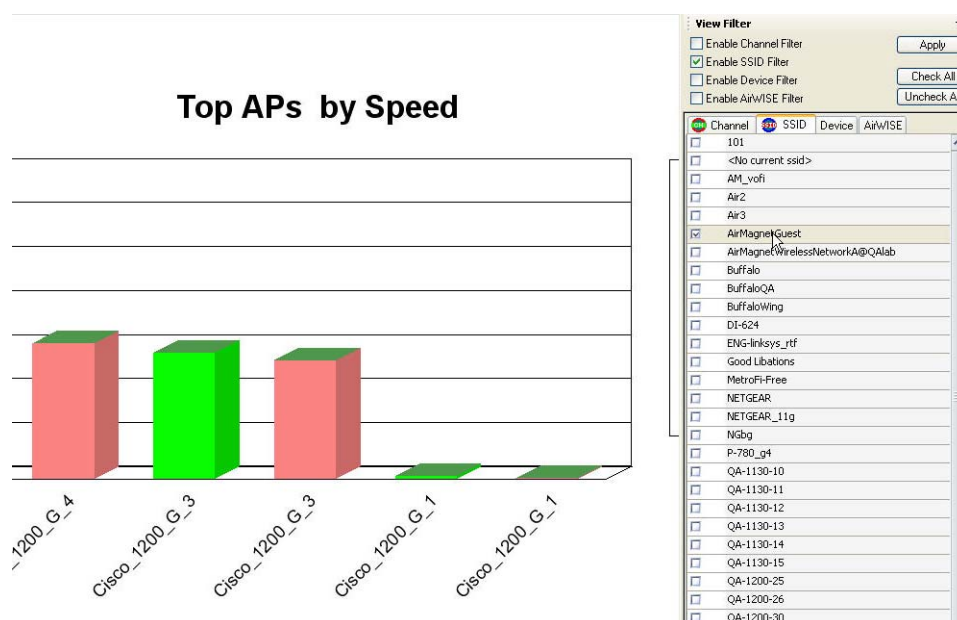



Figure 15-47: Filtering device chart by SSID

Exporting Chart Data

You can export the data contained in the current chart by clicking  (**Export Data**) at the top of the Charts screen and selecting "Export Top Traffic Analysis". A confirmation message will pop up on the screen, indicating that the export is successful. See [Figure 15-48](#).

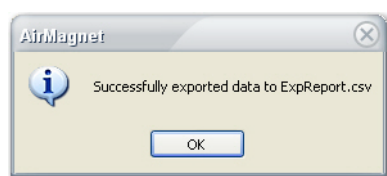



Figure 15-48: Export confirmation

Choosing a Graph Option

AirMagnet allows the user to configure their chart settings using the **Graph Options** button on the Charts screen.

To configure chart settings:

- 1) Click  at the top of the screen. The Graph Options dialog box appears. See Figure 15-49.

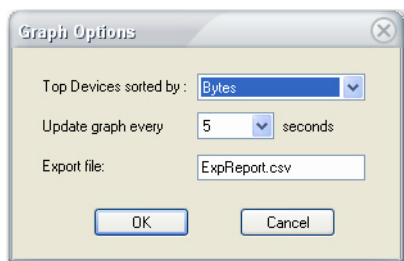


Figure 15-49: Configuring graph settings

- 2) Make the desired selections, and click OK.

Chart Data Tabulation

Below the graph is a table that offers a breakdown of the selected data type for the top 10 devices. See Figure 15-50.

CH	Address/Name	SSID	1	6	9	12	18	24	36	48	54
11	warlord (Cisco:A7:EA:30)	QA-1250-roam	0%	6%	0%	8%	0%	0%	15%	9%	5%
4	3Com:03:04:05	Alarm 54:DoS EAPStart, A...	0%	100%	0%	0%	0%	0%	0%	0%	0%
2	Cisco:44:5E:B1		0%	39%	41%	2%	1%	2%	3%	2%	4%
7	Cisco:4D:E8:F1		0%	6%	10%	10%	18%	35%	17%	0%	0%
13	QA-Euro-Cisco (Cisco:A7:FC:F0)	QA-EURO-CISCO	27%	71%	0%	0%	0%	1%	0%	0%	0%
11	Buffalo:4F:5E:00	AirMagnetNetworkG@QAL...	18%	56%	12%	9%	3%	0%	0%	0%	0%
9	AMS-1200-5 (Cisco:44:13:20)	AMS-1200-5	100%	0%	0%	0%	0%	0%	0%	0%	0%
2	Cisco:4D:E9:11		0%	8%	39%	14%	8%	20%	0%	8%	0%
1	Cisco-linksys:40:B3:C4	XXX-ENG-NGbg	100%	0%	0%	0%	0%	0%	0%	0%	0%

Figure 15-50: Data tabulation

This table complements the information displayed in the chart and helps the user to better understand the chart.

The grid in Figure 15-53 expands dynamically. More columns are dynamically added to each speed grid as data at that particular speed are observed. Also, once a column is added, it is retained in the grid for as long as the capture continues even though data at that speed might not be seen anymore.

Tip: If the top 10 channels are graphed, clicking in the table will open the Channel screen.

Viewing Compliance Charts

The Top Traffic Analysis screen also allows you to view charts that reflect your network's compliance status with government and industry regulations on information security. The compliance charts give you a general idea of your network's health; for more detailed information regarding a specific compliance regulation, you may generate a comprehensive report for your network and view it using the Reports page. [Figure 15-51](#) shows all options for regulatory compliance.

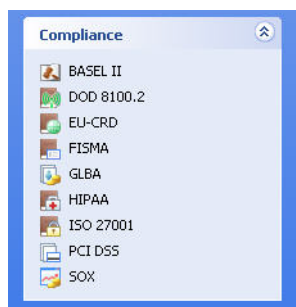


Figure 15-51: Compliance data options

The compliance charts provide you with an easy-to-view summary of your network's compliance with various industry standards. The following sections briefly describe some of the compliance reports provided by AirMagnet.

Basel II

The Basel II Accord promotes greater consistency in the way banks and banking regulators approach risk management. It is designed to establish minimum levels of capital for internationally active banks. In specific regard to AirMagnet, Basel II incorporates an explicit capital charge for operational risk. Operational risk includes the security risks in operating a wireless network. Basel II succeeds the Basel I Accord. Both were developed by the Basel Committee on Banking Supervision (hereinafter, the Committee). The Committee is made up of bank supervisors and central bankers from the Group of Ten (G10) countries. The G10 countries include: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States. International banks can use AirMagnet products and Compliance Reports™ to identify and mitigate the operational risks of maintaining a wireless network.

DOD 8100.2

The Department of Defense (DoD) Directive Number 8100.2 (the Directive hereafter) stipulates the key policy sections regarding the use of commercial wireless devices, services, and technologies in the DoD. Its purpose is to safeguard the DoD networks from the security vulnerabilities inherent with wireless networks, making security a prerequisite for the deployment and use of commercial wireless technologies in the DoD.

EU-CRD

The European Union (EU) Capital Requirements Directive, popularly known as CAD3 (Capital Adequacy Directive), implements the Basel II Accord and introduces new capital requirements for internationally active banks, credit institutions, and investment firms in the EU. It succeeds earlier directives that implemented the capital requirements found in the Basel I Accord. AirMagnet System- and Device-level Compliance Reports™ will identify the operational risks in wireless networks that may lead to system disruptions or failures and external fraud.

FISMA

The Federal Information Security Management Act (FISMA) mandates that Federal agencies like the Department of Health and Human Services, the FCC (Federal Communication Commission), and the FTC (Federal Trade Commission) develop, document, and implement an information security program to provide security for the information and information systems that support the operations and assets of the agencies. This includes the information and information systems provided to the agency from another agency or from a contractor.

FISMA applies to the following:

- All information in the Federal government except information marked as classified.
- All information systems except those operating as national security systems.
- Any organization that is a government agency, sells hardware and/or software to a government agency, or supports the information or information systems of a government agency.

GLBA

The Gramm-Leach Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, mandates that financial institutions protect the security and confidentiality of their customers' personally identifiable financial information.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed to improve the efficiency and effectiveness of the nation's health care system and promote the use of EDI (Electronic Data Interchange) in health care. To accomplish its purpose, regulations were issued by HHS (Department of Health and Human Services) to safeguard the privacy and security of the PHI (Protected Health Information). PHI is any health information that identifies an individual and relates to his or her physical or mental health.

ISO 27001

ISO/IEC 27001:2005 (hereinafter ISO 27001) is an International Standard designed for all sizes and types of organizations (government and non-government). At base, the International Standard should be used as a model to build an Information Security Management System (ISMS). An ISMS is part of an organization's system that manages networks and systems. It is premised on business risks and aims to "establish, implement, operate, monitor, review, maintain, and improve information security." Going beyond the model, organizations can attain an ISO 27001 certification from independent auditors. A certification can show an organizations commitment to security and instill trust with partners and customers. It can also

be used as evidence in compliance with legal requirements, but it will not, in itself, satisfy legal requirements. Independent auditors like ISOQAR and Lloyd's Registered Quality Assurance (LRQA) certify an organization's compliance with ISO 27001. Note that the American National Accreditation Body (ANAB) in the United States and the United Kingdom Accreditation Service in the United Kingdom regulate ISO 27001 auditors. AirMagnet Enterprise can satisfy ISO 27001 and 17799 requirements for wireless networks and devices with System Level, Policy Level, and Device-Specific Compliance Reports. Using the ISO 27001 Plan-Do-Check-Act model, AirMagnet solutions can help an organization PLAN, CHECK, and ACT to improve an ISMS.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed by Visa and MasterCard to prevent identity theft and credit card fraud. It is a standard required of Visa and MasterCard Members, service providers, and merchants and one voluntarily adopted by other card associations like American Express and Discover Card as a condition for participation. Participating businesses must comply with 12 “best practice” requirements for wireline and wireless networks and validate their compliance periodically.

SOX

The Sarbanes-Oxley (SOX) Act, also known as the Public Company Accounting Reform and Investor Protection Act, was passed by the US Congress in 2002 as a comprehensive legislation to reform the accounting practices, financial disclosures, and corporate governance of public companies.

Viewing Compliance Charts

To display a Compliance chart:

- 1) Select the compliance chart you wish to display from the Compliance section in the left-hand pane. See Figure 15-52.

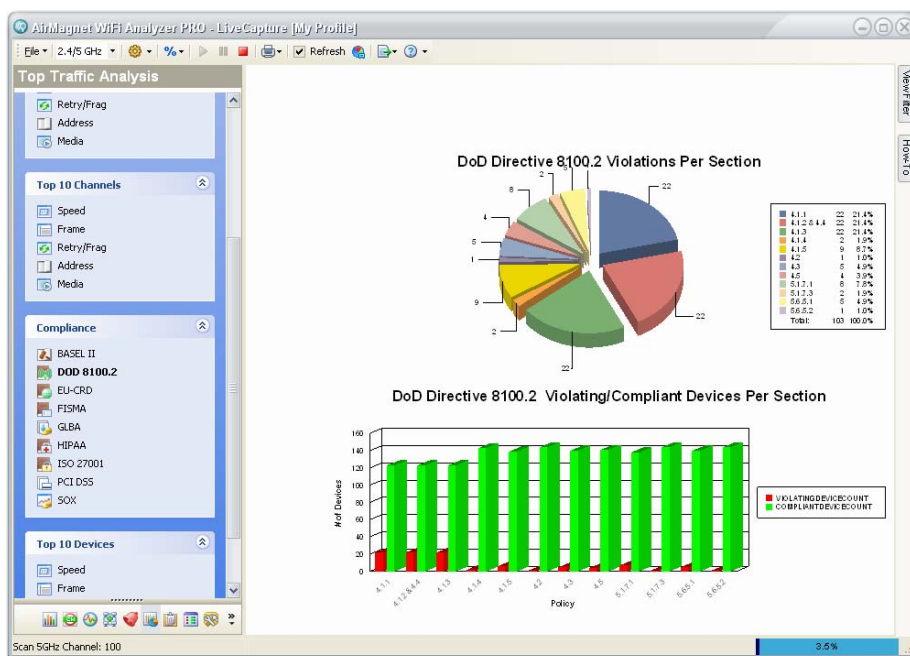


Figure 15-52: A compliance chart

Viewing Compliance Reports

Compliance data are also available in compliance reports. You can access the reports screen by clicking  from the navigation bar and selecting the type of report you wish to generate. See Chapter 10 for more information.


Compliance Reports Disclaimer

AirMagnet DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley, and Payment Card Industry Data Security Standard (PCI DSS) Compliance Reports provide a security framework to comply with regulations in the financial services, health, public accounting, and government sectors. The Policy Compliance Reports focus on wireless network security and aim to guide network administrators in documenting their security policies and responding to security threats and incidents in compliance with industry best practice and government regulations.

AirMagnet Policy Compliance Reports provide information about the law and are designed to help users satisfy government regulations. This information, however, is not legal advice. AirMagnet has gone to great lengths to ensure the information contained in the Policy Compliance Reports is accurate and useful. AirMagnet, Inc. recommends you consult legal counsel if you want legal advice on whether our information and software is interpreted and implemented to fully comply with industry regulations.

The information contained in the Policy Compliance Reports is furnished under and subject to the terms of the Software License Agreement (“License”). The Policy Compliance Reports do not create a binding business, legal, or professional services relationship between you and AirMagnet, Inc. Because business practice, technology, and governing laws and regulations vary by location, full compliance with regulations will depend on your particular circumstances.

Working on Decodes Screen

You can access the Decodes screen by clicking  **Decodes** on the Navigation Bar. See [Figure 15-53](#).

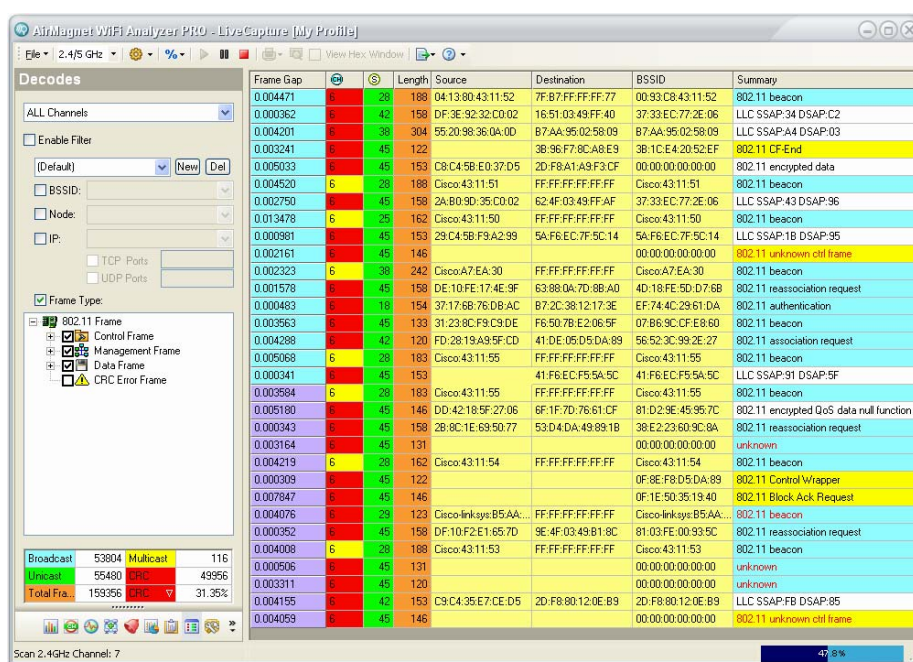


Figure 15-53: Decodes screen

The Decodes screen lets you view a scrolling list of packet frames as they are captured. Table 15-11 briefly describes the information on the Decodes screen.

Table 15-11: Decode Screen Parameters

Field	Description
No	The sequence of the captured packets. Shown only when packet capture is stopped.
M	Check the box in this field to start the frame count from the selected packet. The Delta column will then start with that packet at 0, and number accordingly for future packets. Shown only when packet capture is stopped.
Time	Time the packet was received. Shown only when capture is stopped.
Frame Gap	The time gap between two frames.
Delta	The time elapsed between each packet. Shown only when capture is stopped.
CH	Channel.
S	Signal strength.
Length	Frame length.
Speed	The speed at which the packet was transmitted.
Source	Source node.
Destination	Destination node.
BSSID	The source BSSID.
Summary	Data packet summary.

The bottom portion of the Decodes page provides a meter that gives the user information regarding the current status of the capture buffer. As the buffer fills, the meter will gradually approach 100%. After the first fill, the meter will restart using a different color, thus allowing the user to monitor how many cycles the buffer has been through since the last status check.

Filtering Packet Captures

The left side of the Decodes screen is a Filter pane. When the “enable filter” box is checked, it will activate the filtering feature so that you can define a filter using the fields below. You can configure the capture filter to restrict the capture to a specific channel, SSID, AP, station, or frame type. See the following section for more information.

All filters are optional. They are intended to help the user focus their analysis on a specific channel, SSID, node, IP address, or types of frames if they want to. Also, the filters can be used individually or in any combination that the application allows.

Basic Procedures for Using Filters

The following instructions show how to use the filters on the Decodes screen.

- 1) Decide which channel you want to focus on. If you want to focus on a specific channel, then click the down arrow across the top and select the channel of interest. Otherwise, do nothing so that the screen can show frames captured on all available channels.
- 2) Make sure that the **Enable Filter** check box is checked. (This is required if you want to use any of the filters below).
- 3) If you want to focus on a specific SSID, then check SSID check box and select it from the list menu.
- 4) If you want to focus on a specific node on the network, then check the Node check box and select the MAC address of that node from the list menu.
- 5) If you want to focus on a specific IP address, then check the IP check box and select the IP address from the list menu. You may also want to specify the TCP and/or UDP port if you have that information available.
- 6) Select the frame or frames of interest.

The data shown in the right-hand side of the screen become more and more specific as more and more filters are applied.

Creating Custom Filters

Remote Analyzer Express allows users to create custom filters using the filter settings of their choice. These custom filters, once created, will be automatically saved in the application for future use until they are deleted.

To create a custom filter:

- 1) Click the **New** button. A [New Filter] entry appears in the list menu.
- 2) Override the [New Filter] with a unique name.
- 3) Set the filters using the instructions above.
- 4) Repeat Steps 1 through 3 to create as many custom filters as needed.

Using a Custom Filter

Custom filters, once created, can remain available each time you launch the application. They make it easy for monitoring traffic by channel, SSID, node, or frame type.

To reuse a custom filter:

- 1) Make sure the Enable Filter check box is checked.
- 2) Click the down arrow and select the filter of interest. See [Figure 15-54](#).

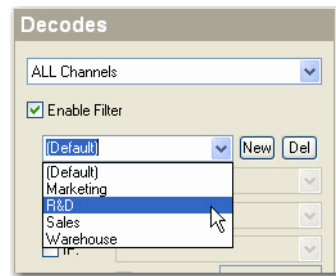


Figure 15-54: Choosing a custom filter

Deleting a Custom Filter

Filters, including the Default filter, can be deleted from the filter list menu at any time.


To delete a filter:

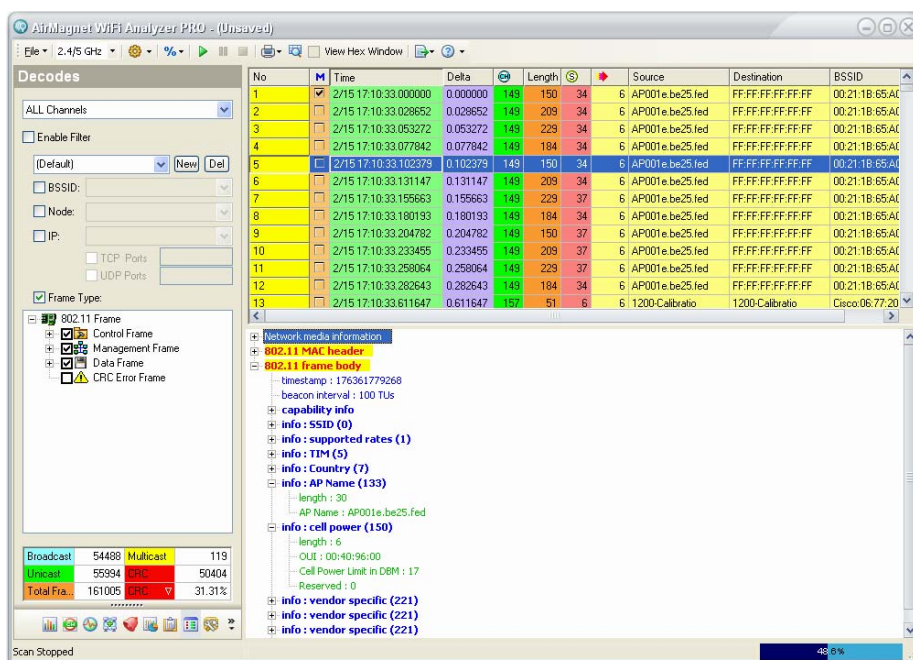
- 1) From the filter list menu, select the filter of interest. See [Figure 15-54](#).
- 2) Click the Del button.


Conducting Packet Decoding

By default, the Decodes screen shows the data packets as they are captured live in a first-in first-out scrolling order. To conduct detailed packet analysis, you have to stop the screen from scrolling so that you can take a close look at any packet you are looking for.


To conduct packet decoding:

- 1) From the Toolbar, click  (Stop Live Capture). The Decodes screen gradually comes to a standstill. See Figure 15-55.

**Figure 15-55: FDecoding a captured packet**

- 2) From the screen, select a packet and review all the information about it.
- 3) Start decoding the packet by expanding all entries in the lower part of the screen.
- 4) Repeat Steps 2 and 3 to analyze all packets of interest.
- 5) To resume live packet capture, click  (Start Live Capture).

Finding Packets on Decodes Screen

When decoding packets, you can quickly locate a particular packet on the screen using  (Find in This View) if you know some basic information about the packet you are trying to find.

To find a particular packet:

- 1) From the Decodes screen, click  (Stop Live Capture).
- 2) From the menubar, click . The Find dialog box appears. See Figure 15-56.

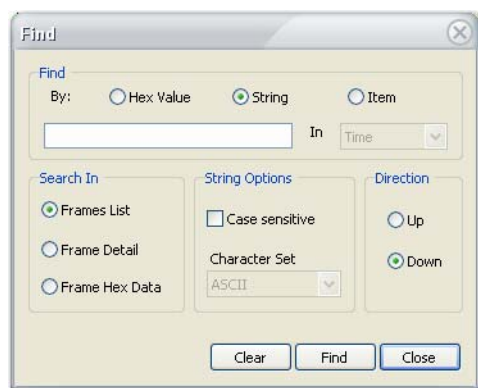


Figure 15-56: Finding a packet

- 3) Make the desired entries and selections and click Find.

The Embedded AirMagnet Remote Spectrum Analyzer

AirMagnet Enterprise comes with the AirMagnet Remote Spectrum Analyzer, which integrates AirMagnet's advanced spectrum-sensing hardware and analytical and visual display software into one application. This new sensor platform brings AirMagnet Enterprise system up to a new level and allows network professionals to use the AirMagnet Enterprise system to monitor and collect spectrum data as the basis for network design and planning, troubleshooting, and optimization.

The Secure Spectrum Protocol (SSP) feature secures communication between the AirMagnet Spectrum XT remote UI on the AirMagnet Enterprise Console application and the AirMagnet SmartEdge Sensor using the SSL (port 443) protocol. It utilizes an HTTPS connection so that mission-critical user data is secure.

Unlike the regular AirMagnet SmartEdge Sensor which comes with only one wireless network card for monitoring network traffic, the AirMagnet Spectrum Sensor comes with an additional wireless card dedicated for spectrum. The AirMagnet Enterprise system is able to differentiate the Spectrum Sensors from the regular SmartEdge Sensors and display them on the Enterprise Console using different icons.

In order to use this feature, you must have the AirMagnet Spectrum Sensors deployed on your network and managed by your AirMagnet Enterprise Server.

Enabling AirMagnet Remote Spectrum Analyzer

By default, the AirMagnet Remote Spectrum Analyzer is automatically enabled upon completion of the system installation. It is an option that can be turned on or off by the user at any time. However, if you want to view and analyze spectrum data on your network, you must have the AirMagnet Remote Spectrum Analyzer feature enabled on your system.

To enable AirMagnet Remote Spectrum Analyzer:

- 1) From the AirMagnet Enterprise Console, click Manage>Server Settings....

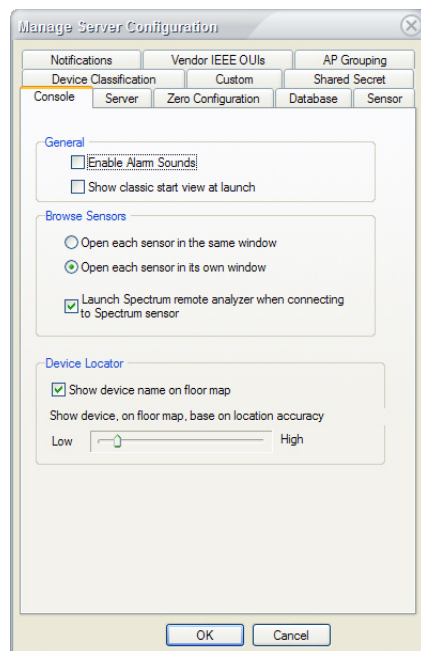


Figure 15-57: Enabling Remote Spectrum Analyzer

- 2) Check the **Launch Spectrum remote analyzer when connecting to Spectrum sensor** check box.
- 3) Click **OK** when completed.

Launching AirMagnet Remote Spectrum Analyzer

Once the Remote Spectrum Analyzer feature is enabled, the AirMagnet Remote Spectrum Analyzer user interface will appear on the screen when you double-click an AirMagnet Spectrum Sensor icon in the network tree structure.

To launch the AirMagnet Remote Spectrum Analyzer:

- 1) From the AirMagnet Console screen, double-click a spectrum sensor icon from the network tree. Spectrum Sensors can be identified by a dark blue sensor icon in the Network tree. See Figure 15-58.



Figure 15-58: Launching AirMagnet Remote Spectrum Analyzer

Both the AirMagnet Remote Analyzer and the AirMagnet Remote Spectrum Analyzer will appear on the screen.

- 2) Click the AirMagnet Remote Spectrum Analyzer window and then select one of the screen options by clicking the corresponding tab across the top of the right-hand side of the screen. Spectrum data appear on the screen. See Figure 15-59.

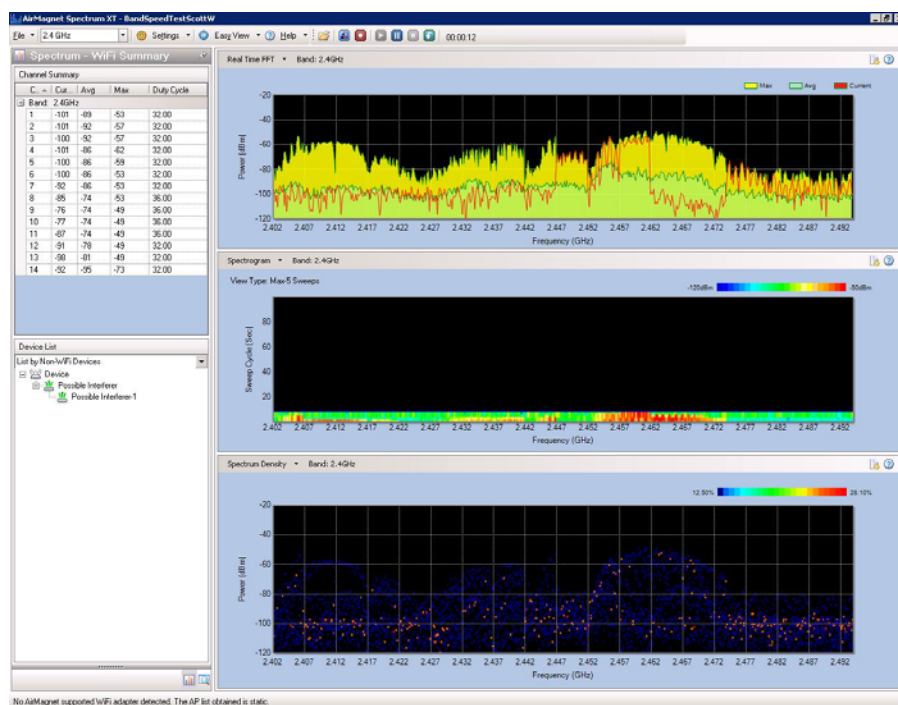


Figure 15-59: AirMagnet Remote Spectrum Analyzer screen

Accessing Remote Spectrum Analyzer User Documentation

The AirMagnet Remote Spectrum Analyzer is a powerful tool for viewing and analyzing spectrum data in the airwave over a wireless network. It's a feature-rich, stand-alone program built into the AirMagnet Enterprise application. This section only shows how to launch the embedded AirMagnet Remote Spectrum Analyzer from the AirMagnet Enterprise Console. Detailed instructions on how to use this application are available either in the AirMagnet Remote Spectrum Analyzer online help or the AirMagnet Remote Spectrum Analyzer User Guide which can be downloaded from our Website at airmagnet.flukenetworks.com free of charge by registered users.

The following paragraph shows how to access the AirMagnet Remote Spectrum Analyzer online help from within the application.

To access the Remote Spectrum Analyzer online help:

- 1) From the AirMagnet Remote Spectrum Analyzer screen, click Help and select Help Topics from the drop-down menu. See Figure 15-60.

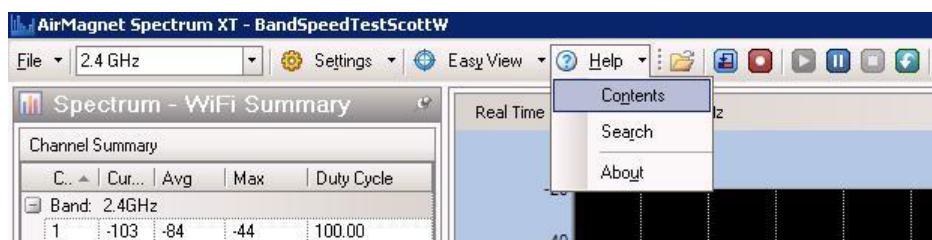


Figure 15-60: Accessing Remote Spectrum Analyzer online help

The Remote Spectrum Analyzer online Help appears.

Device Detection

Spectrum XT can detect and identify various 802.11 or non-802.11 devices that are operating in your WiFi network by looking at the unique patterns of energy emitted from those devices. This chapter discusses the major categories of devices that Spectrum XT is able to detect. It talks about the modulation method, typical RF spectrum pattern, impact on WiFi networks of these devices. It also offers recommendations on how to minimize or eliminate the RF interference to the WiFi network caused by these devices.

Spectrum XT has the capability to detect and identify the following non-WiFi devices based on their unique RF spectrum patterns:

- Bluetooth Devices
- Digital Cordless Phones
- Analog Cordless Phones
- Microwave Ovens
- Baby Monitors
- Wireless Cameras
- Digital Video Monitors
- Zigbee
- Wireless Mouse
- Radar
- Motion Detector
- RF and Narrowband Jammers
- RF Signal Generator
- Non-Bluetooth Wireless Mouse

Spectrum XT is also able to detect all WiFi devices and identify their RF spectrum patterns of 802.11 APs:

- 802.11a/g/n APs
- 802.11b APs

Note that the device pattern examples provided with Spectrum XT are intended to be baselines, not exact matches for the devices detected. The device pattern can vary even between two similar devices (i.e., two microwaves from different vendors). Consequently, the device's pattern may not always be an exact match for the example provided in the application.

Non-WiFi (Spectrum) Devices

The section discusses the various non-WiFi (spectrum) devices that Spectrum XT is able to detect in a wireless network environment. It talks about their typical RF spectrum patterns, impact on WiFi networks, and the best ways to minimize their interference to the 802.11 network.

Bluetooth Devices

Like most cordless phones on the market today, Bluetooth device also operate in the same 2.4-GHz radio band used by 802.11b and 802.11g wireless LANs (WLANs). The problem is that Bluetooth devices and 802.11b/g WLANs are based on two different modulation technologies, which make their radio signals behave so differently that it is difficult for them to operate in the same band without interfering with each other. Bluetooth devices, on the one hand, are based on Frequency Hopping Spread Spectrum (FHSS) modulation. Their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. 802.11b/g WLANs, on the other hand, use Direct Sequence Spread Spectrum (DSSS) modulation technology that allocates only three 22-MHz wide bands within the 2.4-GHz spectrum and transmits over only one of those bands at any given time. Because radio signals from Bluetooth devices hop across all channels randomly across the entire 2.4-GHz radio band, they have a detrimental effect on 802.11b/g WLANs that operate in the same 2.4-GHz band. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, i.e., channels 1, 6, and 11), it is hard for 802.11b/g APs to escape the RF interference caused by Bluetooth devices operating on or in the vicinity of your network. Bluetooth devices can cause performance degradation when used in close proximity to 802.11 stations, especially when the latter are relatively far away from the APs or stations they are associating with, because of weak signal strength.

RF Spectrum Pattern

Figure 15-61 shows the RF spectrum pattern of a Bluetooth-enabled iPhone.

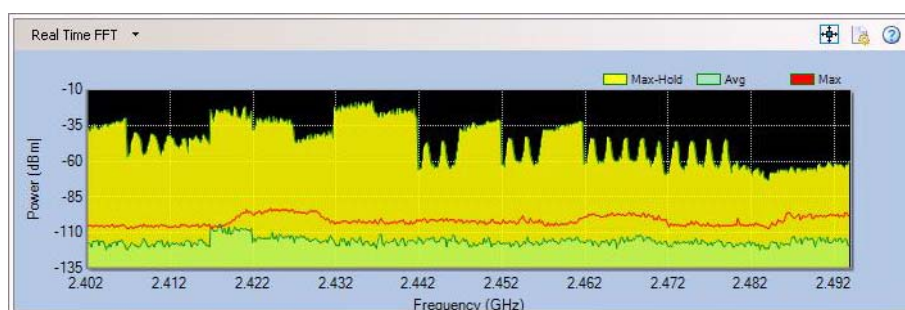


Figure 15-61: RF spectrum pattern of a Bluetooth-enabled iPhone

Impact on 802.11b/g WLAN

Because the 2.4-GHz radio band is unlicensed (free to all), there are numerous Bluetooth-enabled devices by different manufacturers available on the market. The following is a short list of such devices:

- Laptops
- PDAs
- Headsets
- Headphones
- Mice
- Keyboards
- Dongles
- Adapters
- Speakers, etc.

These Bluetooth devices are becoming increasingly popular in homes and businesses where 802.11b/g WLANs are deployed and have been recognized as a source of RF interference to 802.11b/g WLANs. You may tackle these interfering Bluetooth devices by identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering Bluetooth devices are successfully located, the following actions are recommended to minimize or eliminate the RF interference they cause to your 802.11b/g WLAN:

- Change your WLAN from 802.11b/g to 802.11a or upgrade it to 802.11n standard and set it up to run in the 5-GHz channels or frequencies, which will not only avoid RF interference from Bluetooth devices operating in the crowded 2.4-GHz band but also offer greater throughput.
- Try to use Bluetooth devices that are based upon Bluetooth specification version 1.2 or later which uses Adaptive Frequency Hopping (AFH) which limit the use of

pseudorandom frequencies by Bluetooth devices when interference is detected. It helps prevent Bluetooth devices from interfering with other transmissions in the 2.4-GHz band.

Digital Cordless Phones

Most digital cordless phones on the market today operate in either the 2.4-GHz or 5.8-GHz radio band, which happen to be the channel or frequencies used by 802.11b/g or 802.11a wireless LANs (WLANs). The problem is that the two are completely different systems that do not understand each other. As a result, radio signals from the two different systems will collide and cause mutual RF interference. This is especially the case when 2.4-GHz FHSS digital cordless phones are involved. Because they use FHSS modulation, their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. This hopping behavior will cause persistent RF interference to the 802.11b/g WLAN in close proximity. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, i.e., channels 1, 6, and 11), it is hard for 802.11b/g APs to escape the RF interference caused by 2.4-GHz FHSS digital cordless phones. Such sources of interference can cause significant disruption in WLAN service and performance degradation.

RF Spectrum Pattern

There are numerous digital cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

Below is a short list of digital cordless phones:

- Panasonic KX-TGA271 (2.4-GHz, FHSS)
- Panasonic KX-TG2700S (2.4-GHz, FHSS/DSS)
- Panasonic KX-TG5050 (5.8-GHz, DSS)
- AT&T 2355 (2.4-GHz)
- AT&T E5965C (5.8-GHz, FHSS/DSS. *The base transmits in 5.8 GHz whereas the phone transmits in 2.4 GHz.*)
- Uniden EX15660 (5.8-GHz)

Figure 15-62 and Figure 15-63 show the RF spectrum patterns of a 2.4-GHz cordless phone and Figure 15-64 shows a 5-GHz digital cordless phone, respectively.

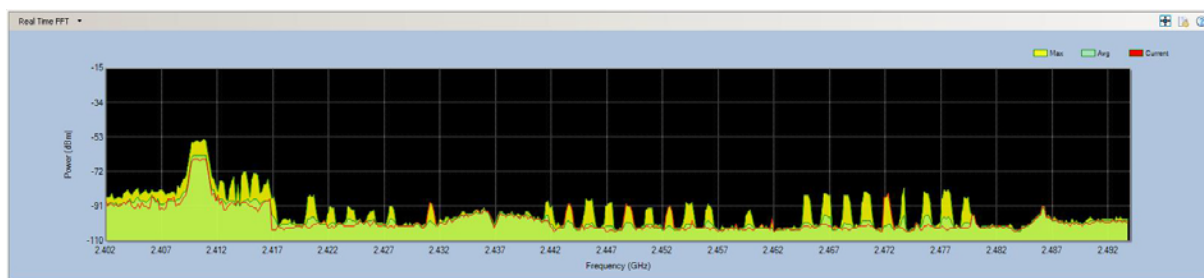


Figure 15-62: RF spectrum pattern of a 2.4-GHz DSSS digital cordless phone



Figure 15-63: RF spectrum pattern of a 2.4-GHz FHSS digital cordless phone

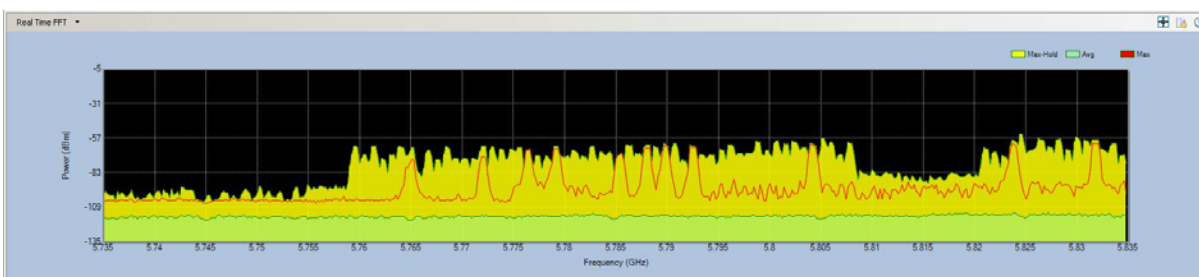


Figure 15-64: RF spectrum pattern of a 5.8-GHz FHSS digital cordless phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz digital cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11b/g or 802.11a WLANs are deployed. They have been recognized as a major source of RF interference for 802.11b/g or 802.11a WLANs. You may tackle these interfering 2.4-/5-GHz cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11b/g or 802.11a WLAN:

- Do not waste your time switching AP channels, because RF signals from digital cordless phones spread over all channels or frequencies in the band they operate. Simply adjusting AP channel is not the solution.
- If you have an 802.11b/g WLAN, avoid or stop using 2.4-GHz FHSS cordless phones. Instead replace them with 5.8-GHz or even old 900-MHz cordless phones which use different radio bands and channels.
- If you have an 802.11a WLAN, avoid or stop using 5-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.

- If you have an 802.11b/g WLAN and 2.4-GHz cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5-GHz cordless phones along with 802.11b/g or 802.11a WLANs but try to maximize the distance between APs and cordless phone bases to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Analog Cordless Phones

Analog cordless phones are another source of interference to 802.11b/g or 802.11a wireless LANs (WLANs). Unlike digital cordless phones, analog cordless phones use narrowband transmission which occupies only a narrow bandwidth of the RF spectrum. Because of this, they can cause severe interference to an 802.11a/b/g AP operating in the same channel or frequency even though no significant interference to APs on other non-overlapping channels has been noticed.

One lab study found that an analog cordless phone transmitting on 2.412-GHz frequency which happens to be the center frequency of Channel 1 of the 802.11b/g WLAN can effectively take out the wireless connection on that channel the moment the phone which is placed next to an AP is turned on, whereas connections on the other two non-overlapping channels (6 and 11) were barely affected. The study also found that network throughput could drop by 99% with the analog cordless phone placed at 50 feet away from the AP, 20% at 100 feet away, and 5% at 150 feet away. The study concluded that analog cordless phones, if placed close to APs, can virtually disrupt wireless connection on the channel they operate.

RF Spectrum Pattern

There are numerous analog cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

Below is a short list of analog cordless phones:

- GE 27923GE (2.4-GHz)
- Uniden EXP4540 (2.4-GHz)

Figure 15-65 shows the RF spectrum pattern of a 2.4-GHz analog cordless phone.

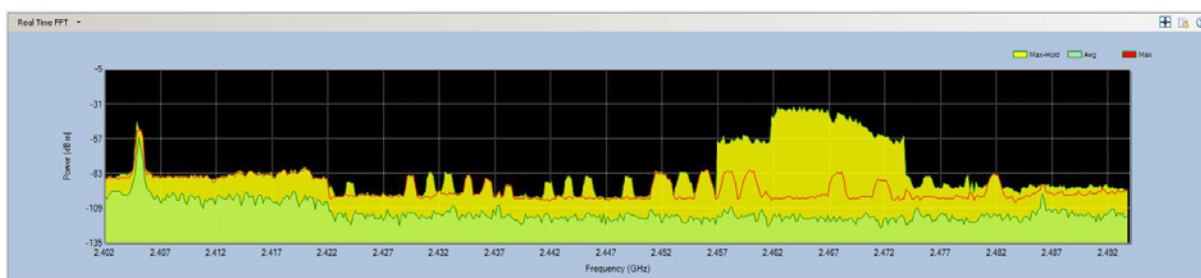


Figure 15-65: RF spectrum pattern of a 2.4-GHz analog cordless phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz analog cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11b/g or 802.11a WLANs are deployed. They have been recognized as a major source of RF interference for 802.11b/g or 802.11a WLANs. You may tackle these interfering 2.4-/5-GHz analog cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering analog cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11 WLAN:

- If you have an 802.11b/g WLAN, avoid or stop using analog cordless phones on the same channel as your 802.11a/b/g APs. Instead try to set them on other non-overlapping channels.
- If you are using an 802.11b/g WLAN, try to use 5.8-GHz or even old 900-MHz analog cordless phones which use different radio bands and channels.
- If you have an 802.11a WLAN, avoid or stop using 5.8-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g WLAN and 2.4-GHz analog cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5.8-GHz cordless phones along with 802.11b/g or 802.11a WLANs but try to maximize the distance between WLAN APs and cordless phone bases to minimize RF interference between or among them.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Microwave Ovens

Most microwave ovens used in homes and businesses today operate in the 2.45-GHz frequency, which is roughly the frequency of Channel 9 in an 802.11b/g WLAN. When a microwave oven is operating, the radio waves emitted from the radio antenna inside the oven are mostly confined within the oven's case, with only a small amount leaking out sometimes, especially with old ovens. To an 802.11b/g WLAN operating within close proximity, the radio waves that leak out of the microwave oven are a source of RF interference that may cause serious performance issues. This is because the interfering radio signals leaking out of the microwave oven will cause WiFi station to hold off transmission until the airwave is clear, causing network delay in the process. Furthermore, interfering RF signals do not follow the rules of the 802.11 protocols and are rather unpredictable: they can come and go at any time, disrupting normal communications between 802.11 devices in the WLAN. Study found that a microwave oven operating within ten feet of an 802.11b/g access point (AP) could cause a 75% drop in network throughput on Channel 9 (2.45 GHz frequency). Significant drop in throughput was also observed on adjacent channels such as Channels 8, 10, and 11. The impact was more severe near the edges of the AP's coverage area.

RF Spectrum Pattern

Figure 15-66 shows the RF spectrum pattern of radio signal from a microwave oven.

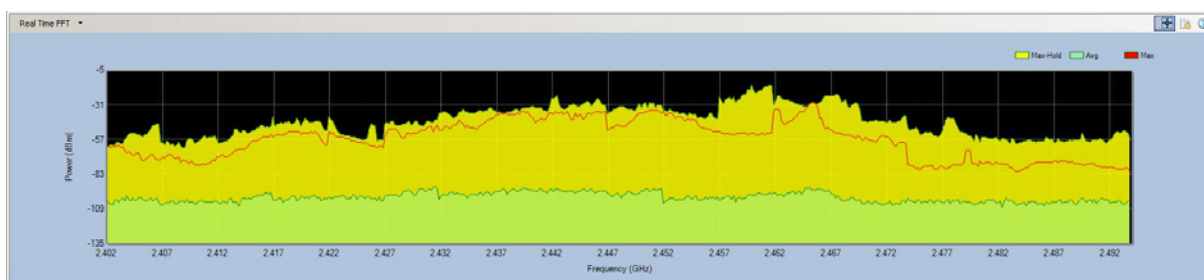


Figure 15-66: RF spectrum pattern of a microwave oven

Impact on 802.11b/g WLAN

Because microwave ovens are widely used in homes and businesses where WLANs are deployed, radio signals leaking out of an operating microwave oven have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down basic Internet applications such as Web file download and surfing. In the worst cases, they can knock out the network connection completely.

Recommended Courses of Action

Once the interfering microwave oven is successfully located, the following actions are recommended to minimize or eliminate the RF interference it causes to the 802.11 WLAN:

- Avoid using 802.11b/g WLAN near a microwave oven.
- When actively using WLAN applications (e.g., downloading files, video-conferencing, searching the Internet), make sure to keep a "safe" distance (at least 10

feet away) from an operating microwave oven. The farther away you are from the microwave oven, the less the interference.

- Find out the center frequency (which may vary depending on make, brand, or model) of a microwave oven from its label, and try to steer your WLAN away from it.
- Change your 802.11b/g WLAN to 802.11a or upgrade it to 802.11n, which will not only avoid RF interference from microwave ovens operating in the crowded 2.4-GHz band but also offer greater throughput.

Wireless Cameras

A wireless security camera is typically made up of three components: a camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a monitor or a recording device.

Most wireless cameras operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, wireless security cameras installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a wireless security camera can travel a relatively long range which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, wireless security cameras installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Wireless cameras come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, etc. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.

Figure 15-67 shows the RF spectrum pattern of a wireless security camera.

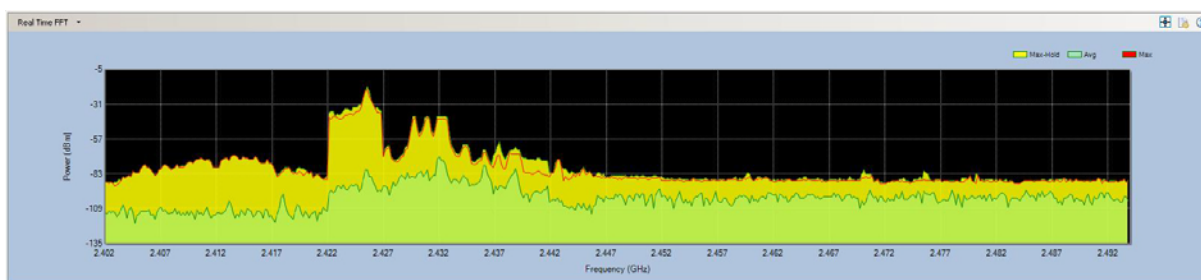


Figure 15-67: RF spectrum pattern of a wireless security camera

Impact on 802.11b/g WLAN

Because wireless cameras are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g WLAN, avoid using 2.4-GHz wireless cameras. Instead, use 5.8-GHz wireless cameras that operate in the licensed, less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11n standard which offers better interference avoidance.
- If you are using an 802.11a WLAN, avoid using 5.8-GHz wireless cameras.
- Check the operating channels on the wireless cameras, making sure that they do not overlap with the operating channels of the WiFi network.

Baby Monitors

Wireless baby monitors (digital or analog) use radio frequencies to transmit their signals. These same radio frequencies are also used by wireless networks installed in the home environment. As a result, RF interference will occur when the two competing systems are operating in the same radio frequencies.

RF Spectrum Pattern

Most wireless baby monitors on the market today use the 2.4-GHz frequency, a bandwidth also used by the 802.11b/g wireless network and many other wireless devices. The figure below shows the RF spectrum pattern of an analog baby monitor in the 2.4-GHz frequency band.

Figure 15-68 shows the RF spectrum pattern of a baby monitor

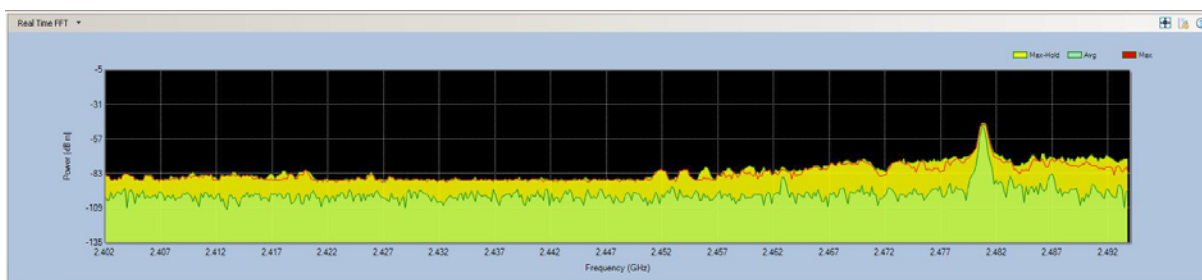


Figure 15-68: RF spectrum pattern of a baby monitor

AirMagnet Spectrum XT will detect FHSS, DSSS and Single Carrier models of baby monitors.

Impact on WiFi Networks

Generally speaking, RF interference is not an issue when a baby monitor is not in use. However, when it is in operation, it could have a negative impact on an 802.11 network, especially when they are in close proximity. When the baby monitor is turned on, the device will compete for bandwidth with the wireless network that is using the same radio frequency, causing the wireless network to experience performance degradation as a result of RF interference, and vice versa. The impact is more obvious for web applications involving downloading files over the Internet or Voice over IP. The figure below shows the RF spectrum pattern of a wireless analog baby monitor using the 2.4-GHz frequency band.

Recommended Courses of Action

Once an interfering wireless baby monitor is successfully identified, you can take all or some of the following actions to minimize or eliminate the RF interference it causes to your 802.11 WLAN.

- Check the channels or frequencies used by your wireless network and wireless baby monitor to make sure that they are not competing on the same channel or frequency.
- Since most of the wireless baby monitors today operate in the 2.4-GHz frequency band, try to upgrade your wireless network to the 802.11n standard.
- If you do not want to upgrade your wireless network, then try to get a wireless baby monitor that uses any radio frequency other than 2.4 GHz, such as 900 MHz.
- Since a baby monitor does not severely disrupt a wireless network unless the two are installed close together, try to place the wireless baby monitor and the wireless router as far apart as possible.

RF and Narrowband Jammer

RF Jammer is designed to block WiFi/WLAN/Bluetooth networks which work on the 2.4-GHz frequency band. It could help you cut off WiFi connections in targeted areas of a WLAN and prevent leaking out sensitive data.

Narrowband Jammer is designed to block Wi-Fi/WLAN/Bluetooth networks for a specific area of the screen on a 2.4GHz frequency. It could help to cut off WiFi connections in targeted areas of a WLAN and prevent leaking out sensitive data.

RF Spectrum Pattern

RF Jammers operate in the 2.410~2.480 GHz frequency range. Their radio signals can transmit in a 15 feet radius with output power of 7 dB.

Figure 15-69 shows the RF spectrum pattern of an RF Jammer.

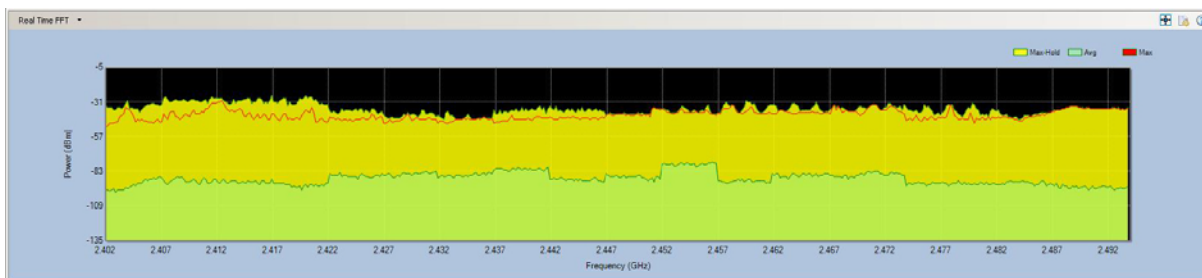


Figure 15-69: RF spectrum pattern of an RF Jammer

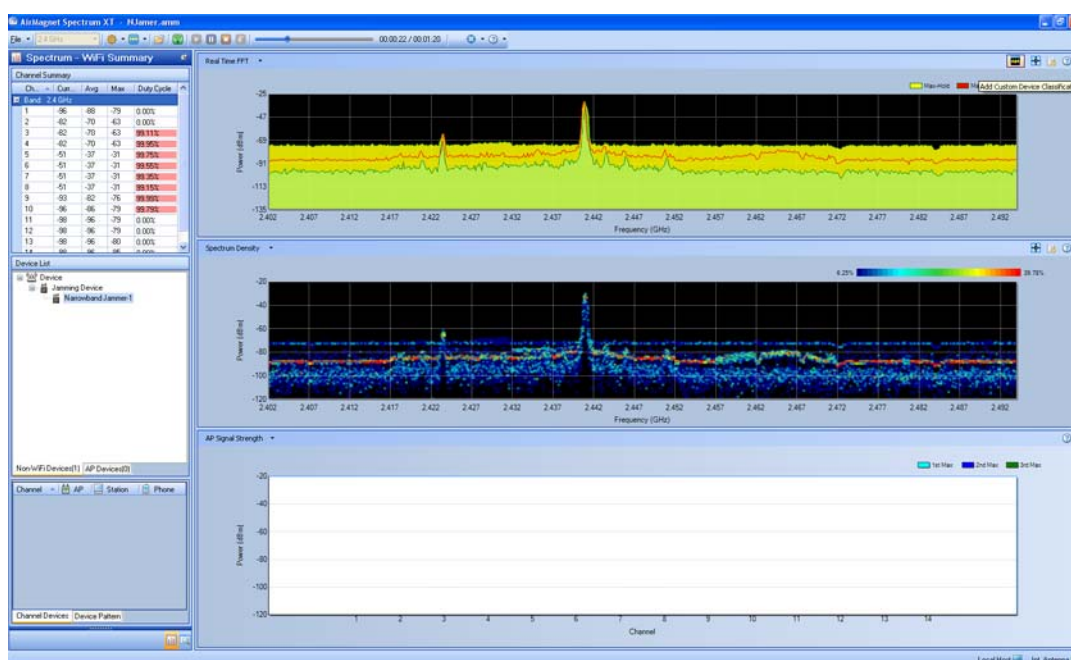


Figure 15-70: Interference Source - Narrowband Jammer

Impact on WiFi on WiFi Networks

WiFi Jammers are designed to protect important working area and avoid leakage of sensitive data by blocking WiFi networks. Since it works in the 2.4 GHz frequency band and channels, this type of device can be a good “defensive” tools against data leakage over wireless network, but can also be a “double-edged sword”. Anyone could use it to disrupt the operation of a wireless network. Because of its compact design, it can be hidden in a pocket or briefcase or elsewhere and can be carried around and deployed at any location of a network without being discovered.

Recommended Course of Actions

Since RF Jammers operate in the same 2.4-GHz frequency band as 802.11b/g networks do, the following actions are recommended in order to minimize or eliminate their interference to 802.11b/g WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF Jamter is causing interference to your WLAN.
- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Jammers, if they are necessary.

Digital Video Monitors

A digital video monitor is typically made up of three components: a video camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a display device (monitor) or a recording device.

Most digital video monitors operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, digital video monitor installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation of the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a digital video monitor can travel a relatively long range which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, digital video monitors installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Digital video monitors come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, etc. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.

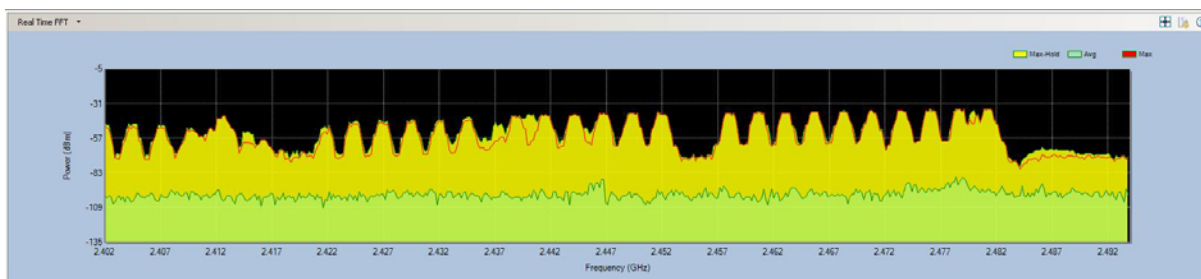


Figure 15-71: RF spectrum pattern of a digital video monitor

Impact on 802.11b/g WLAN

Because digital video monitors are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g WLAN, avoid using 2.4-GHz digital video monitors. Instead, use 5.8-GHz video monitors that operate in the less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11n standard which offers better interference avoidance.
- If you are using an 802.11a WLAN, avoid using 5.8-GHz digital video monitors.
- Check the operating channels on the digital video monitors, making sure that they do not overlap with the operating channels of the WiFi network.

Zigbee

A low-cost, low-power, and short-range wireless mesh networking standard based on the IEEE 802.15.4 specifications. Zigbee devices can operate in the 860-MHz, 915-MHz, or 2.4-GHz band using DSSS modulation. First ratified in 2005, billions of dollars has been invested in Zigbee technology and Zigbee-based devices have now found their way into homes and businesses. Typical applications include:

- Home Entertainment and Control - Audio/video systems, smart lighting, temperature control
- Safety and Security Monitoring - Sensors (access, water, and power), smoke detectors, smart appliances
- Commercial Property Management - Access control, lighting, energy monitoring, HVAC
- Industrial Automation - Process and device control, asset/energy/environmental management.

RF Spectrum Pattern

For network administrators, it is the 2.4-GHz Zigbee devices that cause concern because they use the same radio frequencies as the 802.11b/g wireless networks do. 2.4-GHz Zigbee devices can operate on one of 16 non-overlapping channels (11 in North America) that are 3 MHz wide and 5 MHz apart. Generally, a Zigbee mesh network uses only one channel. Once set up, it stays on the channel until it is changed manually. Zigbee radios use very low transmit power (typically -3dBm or 0.5mW) and receive sensitivity (between -80dBm and -

100dBm depending on radio.) Their maximum bit transfer rate is 250 Kbps. Even though the size and length of Zigbee data packets vary, their target applications are of low duty cycle and low power consumption. Because of this, the Zigbee network does not have as much traffic in comparison to an 802.11b/g network.

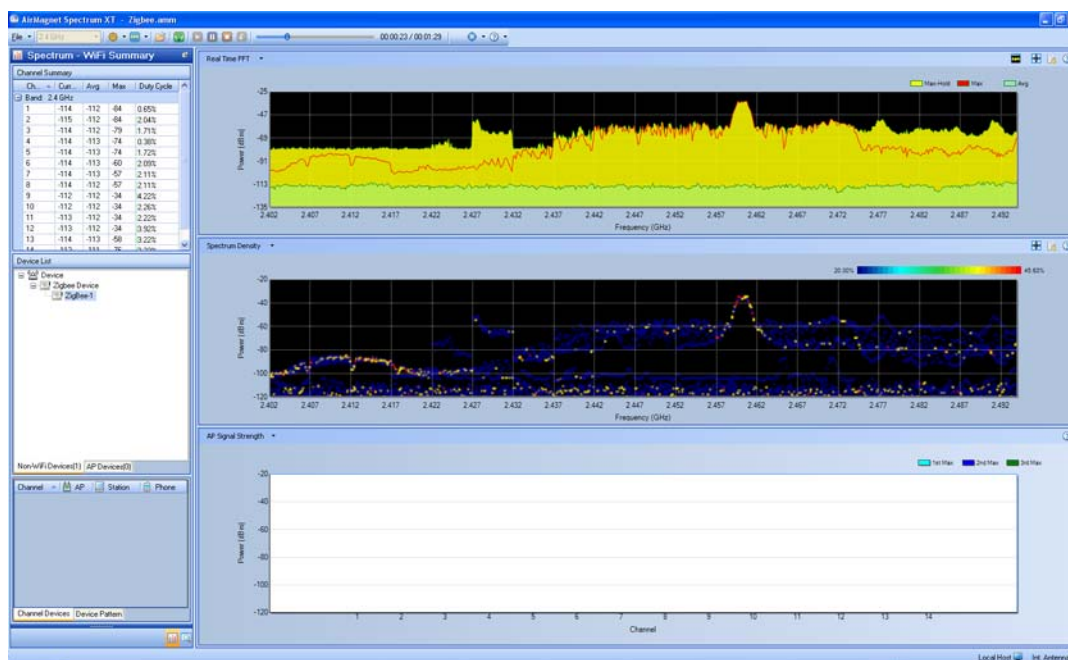


Figure 15-72: Interference Source - Zigbee

Impact on 802.11b/g WLAN

Given the fact that a 2.4-GHz Zigbee network operates on a fixed 3 MHz of bandwidth in the 2.4-GHz band, the chance of collision between a Zigbee device and an 802.11b or g device depends on the channels on which they operate. If the channels overlap, the chance are high. Otherwise, the chances are very low.

Recommended Courses of Action

Once a ZigBee network or devices are identified, the following actions are recommended to minimize or eliminate the potential RF interference that they may cause to the WiFi network:

- Try to set your ZigBee network to a non-overlapping channel not used by an 802.11b or g network.
- Try to keep ZigBee devices physically away from WiFi devices to minimize the chances of interaction.

Radar

Introduction

The 5-GHz band is an Unlicensed National Information Infrastructure (UNII) band, which is divided into several segments, each being designated for a specific use. The UNII-2 (5.25 GHz~5.35 GHz) and UNII-2 extended (5.47 GHz~5.725 GHz) bands used to be set aside exclusively for military and weather radar systems. When the FCC decided to open these bands up for Wi-Fi network, its ruling came with an important caveat: Dynamic Frequency Selection version 2, or DFS2, compliance.

DFS is a mechanism that tells the transmitter to dynamically listen for radar signals in the airwave and automatically switch to another channel if a radar signal is detected. The mechanism is designed to protect the incumbent military and weather radar systems from the RF interference from 802.11a/n devices in their vicinity. With DFSA, the transmitter on a Wi-Fi device will continuously listen for radar signals, both before and during transmission. If a radar signal is detected on a channel, it will either vacate that channel or flag it as unavailable.

DFS2 is a must-have on 802.11a/n APs in order for 802.11a/n network systems to co-exist with military and weather radar systems. According to the latest FCC ruling, all Wi-Fi devices operating in the UNII-2 and UNII-2 extended bands are required to support DFS, to detect and automatically switch channels to prevent WLAN operations from interfering with military or weather radar systems. The mandate became effective on July 20, 2007 in the US and Canada. A similar mandate became effective on April 1, 2008 in the EU.

Since then, in April 2009 new EN 301 893 v1.5.1 requirements also called DFS-3 Compliance have also been enforced for 802.11 APs operating in Europe.

AirMagnet Spectrum XT can detect all 5 types of radar waveforms as described in "FCC Memorandum Opinion and Order 06-96", bins 1-5 and radars as specified in the ETSI specification EN 301 893 v1.5.1.

Impact on 802.11 WLAN

Since the 802.11a/n wireless network shares the same radio frequency bands/channels with military and weather radar systems, the FCC regulation and requirements on DFS/DFS2/DFS3 undoubtedly puts some serious challenge to the operation of the 802.11a/n wireless network. Care must be taken to ensure that WLAN operation will not interfere with or disrupt the normal operation of radar systems.

Recommended Courses of Action

Based on FCC regulations, the following actions are recommended on the part of the 802.11a/n wireless network in order to minimize or eliminate its potential interference with military and/or weather radar systems:

- Make sure all 802.11a/n devices that are operating on your WLAN are DFS2 or 3-certified.
- If you have uncertified 802.11a/n devices on your network, make sure that the UNII-2 and UNII-3 bands/channels are blocked.
- If you have 802.11a/n devices that are manufactured prior to July 20, 2007 (US), then check with the vendors for possible firmware upgrade. The same goes for DFS3 requirements in Europe.

Motion Detector

Motion detectors are devices that use a variety of methods to determine if a body of a significant size is moving through an area, usually as part of a security or energy management system. While most models use infrared detection system, some newer models incorporate a microwave detection system. In some models, this microwave detection system transmits on a narrow band of frequency in the 2.4GHz band. While only active at times of motion detection, in areas of high pedestrian traffic, or areas of high WLAN traffic, these devices present the possibility of disrupting WLAN traffic if the transmitting frequency of the device corresponds with the channel the WLAN is operating on. AirMagnet Spectrum XT will detect S-Band radar based motion detectors that are operating in the environment.

RF Spectrum Pattern

Below is a sample of what the spectrum pattern for a motion detector would look like in a relatively noiseless 2.4GHz spectrum.

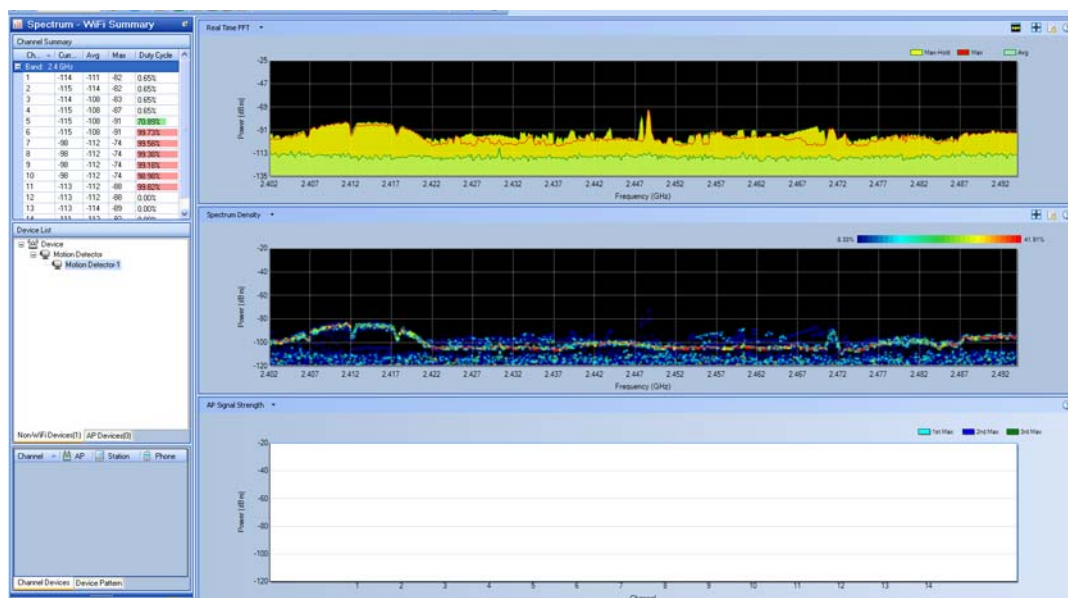


Figure 15-73: Interference Source - Motion Detector

Impact on 802.11 WLAN

The impact on 802.11 networks depends on the amount of pedestrian traffic near the motion detector.

- Because this technology only transmits a signal when the correct parameters for motion detection are met, in areas of low pedestrian traffic, the impact on a WLAN network will be low. The device may cause intermittent interference only if it is transmitting on a frequency within the channel width of a WLAN AP, and only if it is significantly close enough to the WLAN network to have an impact.
- If the motion detector is in an area of high pedestrian traffic, is on a frequency within the channel width of the WLAN AP, and if it is significantly close enough to interfere with the WLAN, this device type can have a significant impact on a WLAN, behaving almost as a Narrow-band Jammer would.

Recommended Courses of Action

- If possible, change the channel that your WLAN is operating on to one that is unaffected by the Motion Detector.
- You may consider changing from the 2.4GHz band to one of the 5GHz bands, as these bands will not be affected by the Motion Detector.
- If you have to use your Motion Detectors along with 2.4GHz WLANs, try to maximize the distance between APs and Motion Detectors to minimize their RF interference.

RF Signal Generator

A device that generates repeating or non-repeating RF signals. An example of this type of device is the AirHORN Channel-Signal Generator. This USB PC-based product aids users in testing Wi-Fi antennas, RF shields and wireless networks. This RF Signal Generator covers the 2.4 and 5 GHz bands and generated RF signals for each Wi-Fi channels in those spectrums.

Recommended Courses of Action

AirHORN Channel-Signal Generator is a proprietary hardware/software solution sold by Nuts About Nets. Only the devices in this product category will show up as this device type.

Below is an example of what the spectrum pattern for what an AirHORN Channel-Signal Generator would look like in a relatively noiseless 2.4GHz spectrum.

Impact on 802.11 WLAN

Used incorrectly, the AirHORN Channel-Signal Generator can create a signal that will essentially block all WiFi and WLAN traffic across a 2.4 or 5 GHz ISM band, until it is either turned off or switched to a different channel.

Recommended Course of Action

Please follow the recommended actions to minimize or eliminate their interference to 802.11a/b/g/n WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF signal generator is causing unintended interference to your WLAN.
- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Signal Generators, if they are necessary.
- If it is necessary to use the RF Signal Generator, only use it on channels that do not overlap with the channels used by your WLAN.
- If optimal WLAN performance is not an issue, you may continue to use your RF Signal Generator along with your WLANs, and try to maximize the distance between APs and RF Signal Generator to minimize their RF interference.

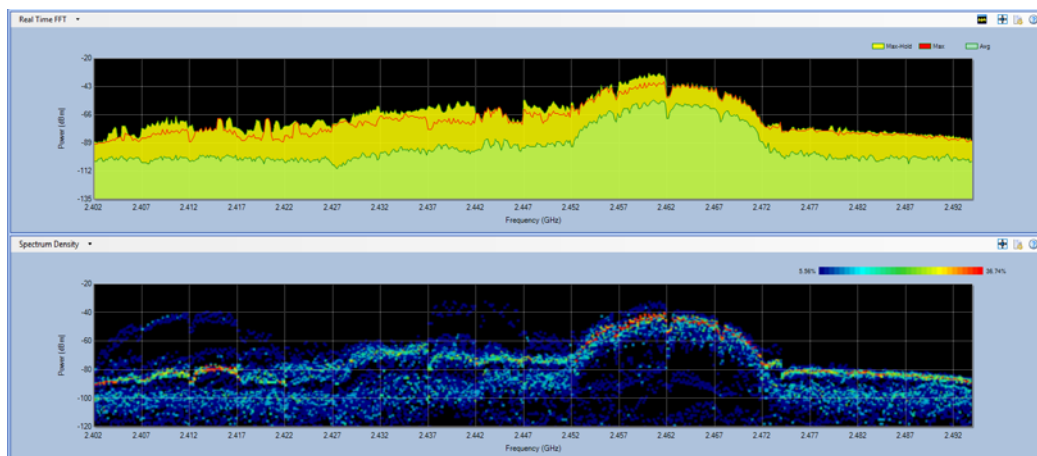


Figure 15-74: Interference Source - AiHorn Signal Generator

Non-Bluetooth Wireless Mouse

Since the 2.4 GHz and 5 GHz wireless spectrums are unregulated, companies are allowed to use those bands for more than just WLAN traffic. In response to some of the concerns about the interference between WLAN and Bluetooth networks, or between WLAN and continuous transmitter technologies like some cordless phones, some companies have developed technologies that allow their devices to operate in a way that minimizes the impact on WLAN networks. With the ability to find a frequency with the least amount of WLAN traffic in the 2.4 GHz spectrum, non-bluetooth wireless mice minimize their impact on the WLAN network. See Figure 15-75 below.

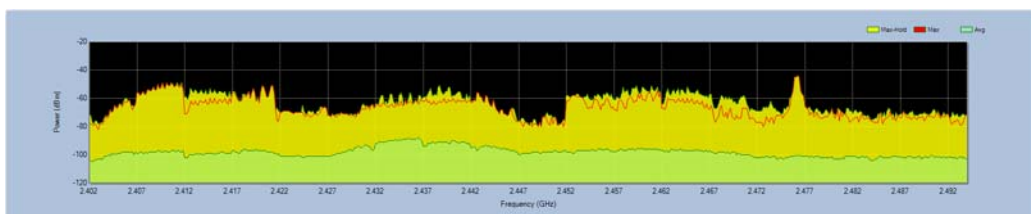


Figure 15-75: Non-Bluetooth Wireless Mouse Fill

RF Spectrum Pattern

To date, the only devices detected for this device type are made by Logitech. This is based on the new Logitech Advanced 2.4GHz wireless technology. The current models ship with this technology:

- Marathon Mouse M705
- Marathon Mouse M310
- Anywhere Mouse MX™
- Wireless Mouse M510
- Wireless Mouse M305
- Performance Mouse MX™
- Wireless Mouse M505
- MX™ 1100 Cordless Laser Mouse
- VX Nano Cordless Laser Mouse
- MX Air™ Rechargeable Cordless Air Mouse

Here are some details from the Logitech website on the technology (**Source:** White paper from <http://www.logitech.com/en-us/mice-pointers/mice/devices/3443>)

In particular, Logitech advanced 2.4 GHz wireless technology hops at 250 times/sec and supports bi-directional data transmission with error correction to maintain a reliable RF link. And Logitech's architecture automatically pairs your peripheral to the provided transceiver that is attached to your computer, while avoiding conflicts with other devices. In other words, when you use a Logitech peripheral with advanced 2.4GHz technology, you can be certain that when you move your mouse or type on your keyboard, your commands will be carried out instantaneously.

Logitech's proprietary wireless protocol is used together with a high-performance RF transceiver. This is a highly integrated, single-chip transceiver that operated in the 2.4 GHz ISM band and is really suited for the most demanding applications. In addition to the technical features described above, this technology also provides the lowest-power RF solution on the market today, translating into significantly longer battery life.

Table 15-12: Logitech non-bluetooth vs Bluetooth

Feature	Logitech advanced 2.4 GHz wireless technology	Bluetooth
Range	10m	10-100 m
Bandwidth	2 Mbps bursts	1-3 Mbps bursts
Latency at reconnection	<90 ms	.5-2 seconds
Interference resistance	Best	Best
Battery life	Best	Good
Report rate	125 rpt/s or faster	80 rpt/s
USB interface	FS	FS

Below is a sample of what the spectrum pattern for a Non-Bluetooth Wireless Mouse would look like in a relatively noiseless 2.4GHz spectrum.

Impact on 802.11 WLAN

Since this technology is designed to minimize its interference with WLANs, the impact of having a few of these devices in the spectrum should be low. If there are no frequencies that have low levels of WLAN traffic, the device will choose the least use frequency, which may cause minor disruptions to the WLAN.

Recommended Course of Action

- Ensure that the WLAN network is operating on non-overlapping channels like 1,6, and 11. This will maximize the number of frequencies with little to no WLAN traffic on them.
- If multiple devices of this type exist in the spectrum, begin removing devices until the interference clears up.
- If you have to use your non-Bluetooth wireless mouse along with 802.11b/g WLANs, try to maximize the distance between APs and wireless mice to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offers greater throughput.

Game Controller

Wireless game controllers are handheld devices for gaming consoles without wires. Using wireless technology, wireless game controllers allow players to sit virtually anywhere (up to 30 feet away from the game console) in the room, making game play less restrictive.

For better coverage, most wireless game controllers operate on the 2.4-GHz frequency—an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, wireless game controllers installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation of the WLAN.

Wireless game controllers are available for all major gaming consoles and computers. The following are some of the major brands:

- Nintendo Wii/Gamecube Classic Wireless
- Sony PS 2 PlayStation 2 Wireless Game Controller
- Microsoft Xbox 360 Wireless Remote Controller, etc.

RF Spectrum Pattern

Wireless game controllers come in all shapes and sizes. They are widely used in homes and even some businesses settings where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless game controller using the 2.4-GHz frequency band. See [Figure 15-76](#).

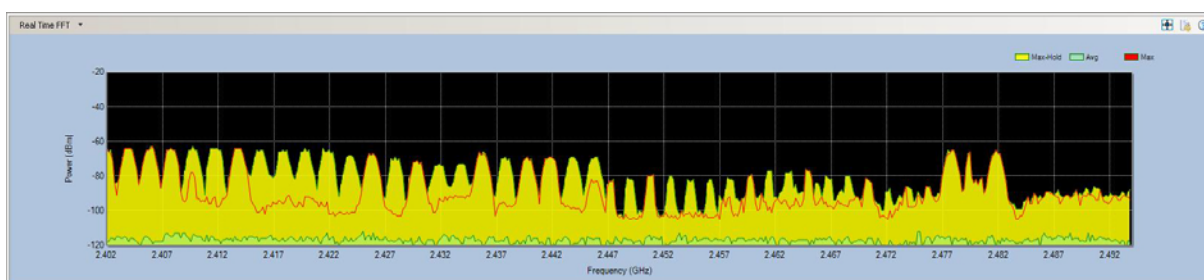


Figure 15-76: RF spectrum pattern of a 2.4-GHz game controller transmitter

Impact on 802.11b/g WLAN

Because wireless game controllers operate in the same radio frequency as the 802.11b/g WLAN, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in homes and businesses where they are used. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless game controllers are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- Try to keep a “safe distance” between your 802.11b/g AP and wireless game controller so as to keep interference to the minimum.
- Check the operating channels on the wireless game controller to make sure that they do not overlap with the operating channels of your 802.11b/g network.
- If possible, consider using an 802.11a AP or even upgrading your WLAN to the 802.11n standard.

WiFi Devices

Spectrum XT not only can detect and present spectrum data of various WiFi devices as it does with non-WiFi devices, but also has the capability to capture various WiFi data about those devices and pinpoint their physical locations in a WiFi network with the help of an AirMagnet-supported wireless network adapter.

This section discusses 802.11 APs. It breaks them up into two groups: 802.11a/g/n APs and 802.11b APs, and talks about their spectrum patterns, impact on the network, and best ways to use them in a wireless network environment.

802.11 a/g/n APs

In general, 802.11a/g/n WLANs offer great advantage over 802.11b WLANs in terms of data rate, signal modulation, etc. The table below provides a brief summary of some key parameters involving all APs built upon different IEEE 802.11 standards.

The 802.11a standard uses Orthogonal Frequency Division Multiplexing (OFDM) modulation which is a more efficient data transmission method than DSSS used by 802.11b, enabling raw data rates up to 54 Mbps. Unfortunately, despite its greater data rates, the 802.11a WLAN never reached the point to replace the 802.11b WLAN due to the fact that it operates in the 5-GHz radio frequency which is incompatible to 802.11b.

The 802.11g standard which uses the same radio frequencies and channels as the 802.11b standard but also supports OFDM offers the best of both worlds: 802.11g WLANs can achieve raw data rates up to 54 Mbps on the same radio frequencies and channels used by 802.11b WLANs. Nowadays, the vast majority of commercial wireless network devices support the 802.11g standard. Much of the WLAN client devices are dual-band supporting both 802.11a and 802.11g.

The emerging 802.11n standard, though not yet ratified, employs several techniques that promise greater throughput, reliability, and stability of WLANs. The key 802.11n technological breakthroughs include (but are not limited to):

- Multiple Input Multiple Output (MIMO) – capable to support up to 4 spatial streams.
- Packet Aggregation – allows transmission bursts of multiple data packets to improve efficiency.
- Channel Bonding (40-MHz channels) – doubles channel width from 20 MHz to 40 MHz to effectively double data rates.
- Improved OFDM – uses a higher maximum code rate and lightly wider bandwidth than the OFDM employed in 802.11a/g standards.

RF Spectrum Pattern

802.11a APs operate in the “regulated” 5-GHz frequency band, meaning that they use radio frequencies that are not used by other commercial wireless products. Unlike 802.11 b/g WLANs which have only three non-overlapping channels, 802.11a WLANs have eight non-overlapping channels to choose from.

Figure 15-77 shows the RF spectrum pattern of an 802.11g/n AP in the 2.402-2.482 GHz frequency range.

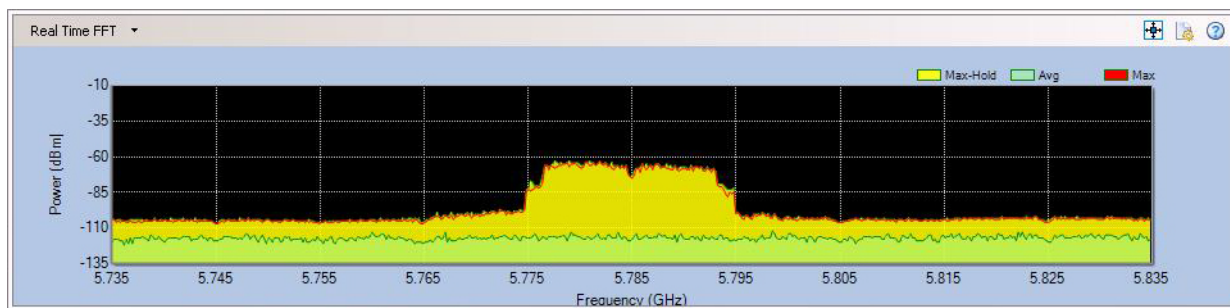


Figure 15-77: RF spectrum pattern of an 802.11g/n AP (OFDM)

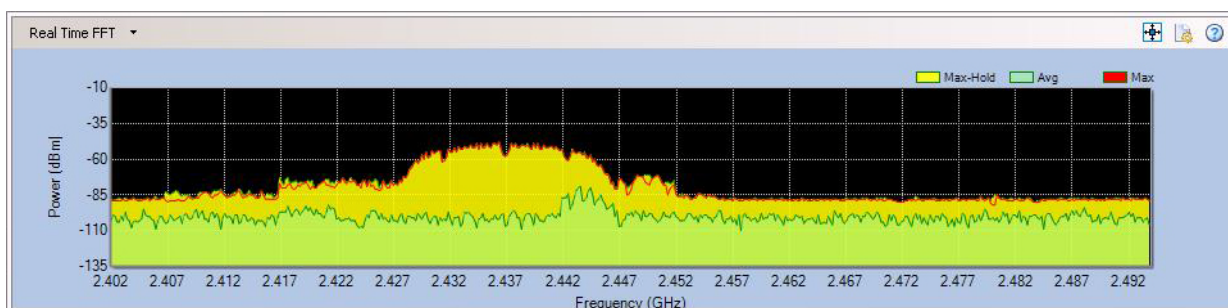


Figure 15-78: RF spectrum pattern of an 802.11g/n AP (CCK)

Impact on WiFi Networks

802.11a uses Orthogonal Frequency-Division Multiplexing (OFDM) signal modulation method, which differs from DSSS signal modulation used by 802.11b WLANs. Since 802.11a WLANs are installed mostly indoors, OFDM is the perfect choice in that it offers better data rates than DSSS and reduces effects of multipath on signal quality and WLAN throughput.

Even though the 802.11a standard helps improve WLAN performance and reduce interference, radio signals from an 802.11a AP can travel a much shorter distance than those of 802.11b/g APs. An 802.11a AP transmitter may cover less than a quarter of the area of a comparable 802.11b AP. Brick walls and other obstructions affect 802.11a WLANs far more than they do to comparable 802.11b/g WLANs.

802.11g APs are backward-compatible with 802.11b APs but offer greater data rates. However, since they operate in the same radio frequencies as their 802.11b counterparts, they are susceptible to RF interference caused by all wireless devices operating in the 2.4-GHz frequency band. See [802.11b APs](#).

802.11n APs, by design, can co-exist with 802.11a APs in the 5-GHz band and 802.11g APs in the 2.4-GHz band since they all use OFDM. The presence of 802.11b devices makes communications a little challenging in the 2.4-GHz band because it cannot understand OFDM which is used by both 802.11b and n standards. In that case, OFDM client devices may have to switch to the older signal modulation (DSSS) to protect their high-rate OFDM transmissions, resulting reduced network efficiency.

Recommended Courses of Action

If you are running an 802.11a/g WLAN, the following action should be taken into consideration when installing and managing your WLAN:

- Since radio signals from 802.11a APs travel a much shorter distance, make sure that you have enough APs to offer adequate WLAN coverage if you are using an 802.11a WLAN.
- If you need more than one AP, make sure to point them to different non-overlapping channels.

- Be aware of other wireless devices that may also be operating in the same radio frequencies and channels as your WLAN APs do. Make sure that your 802.11 WLAN APs use different channels than those used by those competing devices.
- Upgrade your WLAN to the 802.11n standard, if you can.
- When updating to 802.11n, make sure to use “IEEE 802.11n Draft Compliant” hardware devices.

802.11b APs

802.11b APs operate at frequencies in the unlicensed 2.4-GHz Industrial, Medical and Scientific (IMS) band. Because the band is free and used globally, it is crowded with all kinds of 2.4-GHz-compliant commercial products, including:

- WLAN devices (802.11g)
- Cordless phones (digital or analog)
- Bluetooth devices
- Wireless (security) cameras
- Baby Monitors (video and/or audio)
- Microwave ovens

As the number of these devices increases, the 2.4-GHz IMS band is becoming more and more congested. As a result, network performance degradation has become a major issue facing network administrators managing 802.11b/g WLANs. It has long been recognized that the main culprit for WLAN performance degradation is RF interference caused by these competing devices in the 2.4-GHz band. RF interference occurs when two or more RF devices are transmitting at the same frequency at the same time. RF interference causes over-the-air collision which can lead to data corruption and loss.

802.11b APs can operate on one of 13 (11 in the US) channels in the 2.4-GHz IMS band, each being 22 MHz wide and 5 MHz apart. Because each of these channels takes up roughly a quarter of the 2.4-GHz spectrum and adjacent channels tend to interfere with each other, 802.11b WLANs are typically installed using one of three non-overlapping channels, namely Channels 1, 6, and 11.

The table below shows the operating channels for 802.11b WLANs in North America, with Channels 1, 6 and 11 highlighted in grey as non-overlapping channels.

RF Spectrum Pattern

802.11b APs use Direct Sequence Spread Spectrum (DSSS) signal modulation method which is very susceptible to signal multipath. Signal multipath occurs when radio signals are reflected on their way between the transmitter and the receiver. This could happen when radio signals from an AP are blocked by metal furniture, dry walls, and other structural elements common in office buildings. Signal multipath has a huge impact on data quality and WLAN throughput because it causes transmission errors and requires retransmission.

802.11b WLAN APs typically use up to +20 dBm (100mW) transmit power and -80 dBm ~ -90dBm of receive sensitivity. Their bit transfer rate is 11 Mbps (maximum).

Figure 15-79 shows the typical RF pattern of an 802.11b AP.

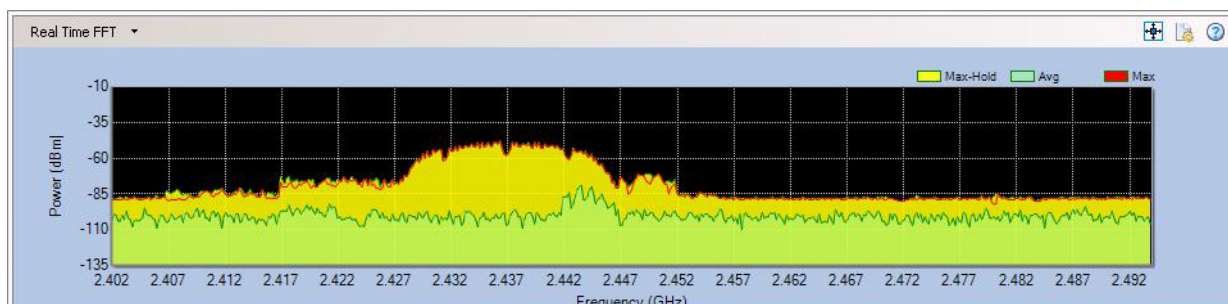


Figure 15-79: RF spectrum pattern of an 802.11b AP

Impact on WiFi Networks

Since 802.11b APs use a fixed bandwidth of 22 MHz in the 2.4-GHz spectrum, the probability of collisions or interference between 802.11b APs or with other 2.4-GHz devices largely depends on the channel they operate. If they are on the same channel or overlapping channels, the probability is high. Otherwise, the chances of collision are low.

Recommended Courses of Action

Since 802.11b/g WLANs are operating in the crowded 2.4-GHz IMS band with so many competing devices (including 802.11b/g devices themselves), the following actions are recommended in order to minimize or eliminate RF interference to 802.11b/g WLANs:

- Prior to installing an 802.11b WLAN, conduct a thorough RF survey of the WLAN site to know all 2.4-GHz devices operating in the WiFi environment and the channels they are using.
- Install 802.11b WLANs by setting the APs to non-overlapping channels 1, 6, and 11, especially when more than one AP is needed.
- Try to avoid the use of HFSS devices in close proximity of an 802.11b WLAN to minimize RF interference.
- If you have more than one 802.11b AP, adjust the transmit power levels on the APs to minimize mutual interference between APs.
- Try to keep WLAN APs at a good physical distance to avoid mutual interference.
- Upgrade your WLAN to 802.11g or n standard

Chapter 16: Configuring Remote Analyzer

Introduction

This section discusses the configuration of “local” settings on the AirMagnet SmartEdge Sensor. By local, it means that these features only affect the individual AirMagnet SmartEdge Sensor on which the configurations are performed. These features allow users to fine-tune the settings of each individual AirMagnet SmartEdge Sensor according to their specific needs.

Sensor configurations are conducted in the AirMagnet Config dialog box which can be opened by clicking File>Configure... from the menu bar. Sensor configuration involves the following tasks, each represented by a tab in the AirMagnet Config dialog box:

- Sensor settings
- General settings
- 802.11 configuration
- Packet Capture filter
- Channel scan settings
- User Interface customization

Sensor Settings

By default, the AirMagnet Remote Analyzer Configuration opens to the Sensor tab, which shows the name of the AirMagnet SmartEdge Sensor currently in use as well as the Packet sliced size. Neither field within the tab can be modified by the user because these settings must be configured by connecting directly to the sensor via a serial or ethernet connection. Consult the User Guide provided with the sensor for more information.

General Settings

The General tab of the configuration window allows the user to customize various aspects of the Remote Analyzer interface.

To modify general settings:

- 1) From the AirMagnet Remote Analyzer screen, click **File>Configure...** and select the General tab. The *AirMagnet SmartEdge General Configuration* screen appears. See [Figure 16-1](#).

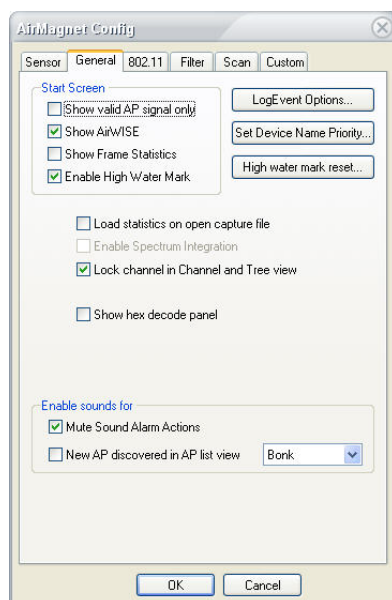


Figure 16-1: AirMagnet SmartEdge Sensor Name

- 2) Make the selections as described in [Table 16-1](#).

Table 16-1: Configuring General Settings

Parameters	Description
Show valid AP signal only	If checked, the system will not display brown bars representing Cross Channel Interference in the signal graph. (Start screen)
Show AirWISE	If selected, AirWISE will appear in the lower-left part of the Start screen.
Show Frame Statistics	If selected, the Start page will display a small box containing frame summary information below the pie chart. (Start Screen)
Enable High Water Mark	If checked, the graphs in the top left corner of the start screen will store a high point during a user-specified interval. This allows you to see the highest point your network traffic has reached within a given time. To specify this time, click the Start screen high water mark reset button.

Table 16-1: Configuring General Settings

Parameters	Description
Load statistics on open capture file	If checked, a loaded capture file will display all the information that was captured during the saved session. A normal playback will only display devices detected until the capture buffer has been filled; this option allows you to view devices that were logged previously but then overwritten as the buffer became full.
Enable Spectrum Analyzer	If checked, AirMagnet Spectrum Analyzer integration will be enabled. See “The Embedded AirMagnet Remote Spectrum Analyzer” on page 366 for more information.
Lock channel in Channel and Tree view	If checked, the system will stop scanning other channels when you are viewing a selected channel in detail on the Channel screen.
Disable Email Notification	If selected, no email notification will be sent.
Show hex decode panel	If selected, the hexadecimal panel will be displayed on the Decodes screen.
Trace rogue devices on wired network	If checked, the system will trace rogue devices on the wired side of the network. Note that your laptop must be connected via an ethernet connection to use this option.
Enable sound for	
• Mute Sound Alarm Actions	If checked, the system will not beep when a new alarm is generated.
• New AP discovered in AP list view	If checked, the system will beep when a new AP is detected. Click the down arrow to select a sound option.

3) Click OK.

Configuring SmartEdge Sensor's 802.11 Settings

The 802.11 screen allows you to set the parameters to allow AirMagnet SmartEdge Sensor to function as an active 802.11 device on the network. It is important that these parameters be set up properly before using any of the active tools (i.e., Diag, DHCP, Ping, Trace).

For each SSID entered, there is a set of 802.11 parameters associated with it, including Authentication and Advanced configurations.

To configure AirMagnet SmartEdge Sensor's 802.11 settings:

- 1) From the AirMagnet SmartEdge Sensor Configuration screen, select the **802.11** tab. The screen refreshes. See [Figure 16-2](#).

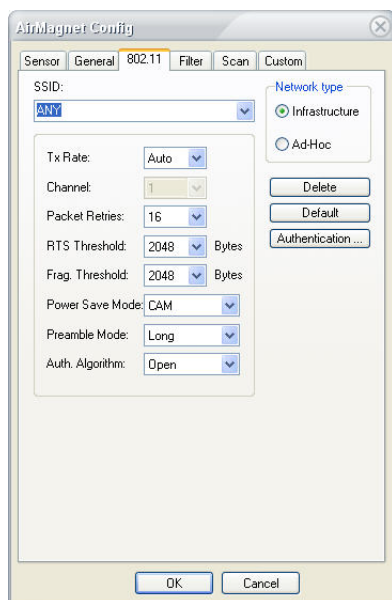


Figure 16-2:Configuring Sensor 802.11 settings

- 2) Make the selections as described in [Table 16-2](#).

Table 16-2: 802.11 Options

Option	Description
SSID	Choose ANY or a specific SSID to associate. When AirMagnet active tools such as Ping or DHCP try to associate within a given SSID or with a given AP, all the configured parameters in this dialog box will be applied to the WLAN card.
Network Type – Infrastructure	The infrastructure mode bridges a WLAN with a wired Ethernet LAN.
Network Type – Ad-Hoc	The Ad-Hoc mode is a method for wireless devices to directly communicate with each other, all wireless devices within range of each other being able to discover and communicate in a peer-to-peer fashion without involving access points.
Tx Rate	Select a transmission speed at which your AirMagnet is to be operated. Keep in mind that the higher the speed, the more bandwidths you will consume. The default setting is Auto, which allows the system to select whatever speed that is appropriate.

Table 16-2: 802.11 Options

Option	Description
Channel	Specify a channel when Ad-Hoc mode is selected. See Network type above.
Packet Retries	Specify the maximum number of transmission retries at the 802.11 protocol level.
RTS Threshold	Specify the threshold of packet length to trigger the use of the 802.11 RTS/CTS mechanism.
Frag. Threshold	Specify an 802.11 frame fragmentation threshold.
Power Save Mode	Choose Active or Power Save mode. The former keeps the system active all the time whereas the latter will switch the system to a energy-saving mode it is left idle for some time.
Preamble Mode	Select Long or Short (for 802.11 preamble).
Auth. Algorithm	Select Open if you do not wish to use a secret key or Shared Key to require the use of a shared secret key for authentication.
Country	Select the country where AirMagnet is used.
Delete	Click this button to delete the selected SSID.
Default	Click this button to restore the 802.11 configuration to the settings configured by the manufacturer.
Authentication	Opens the Wireless Authentication dialog box, where you can configure WEP authentication settings.

- 3) Click OK.

Configuring WEP Settings

AirMagnet Remote Analyzer supports WEP authentication, which can be configured by clicking the Authentication... button on the AirMagnet Config>802.11 window.

Before attempting to use any authentication mechanisms within AirMagnet Remote Analyzer, please ensure that the computer is able to associate to the AP without the application loaded. If it cannot, the mechanisms may be misconfigured within Windows or the wireless client utility, thus leaving Remote Analyzer unable to associate as well.

Wired Equivalent Privacy (WEP) protocol is an IEEE 802.11 security protocol that provides WLAN with a minimum level of security and privacy comparable to that of a typical wired LAN. If this option is selected, users will be required to enter a WEP key to use active tools.

To configure SmartEdge Sensor's WEP settings:

- 1) From the AirMagnet Config>802.11 screen, click **Authentication....** The Wireless Authentication screen appears.
- 2) Select WEP from the drop-down box, and the WEP screen appears. See Figure 16-3.

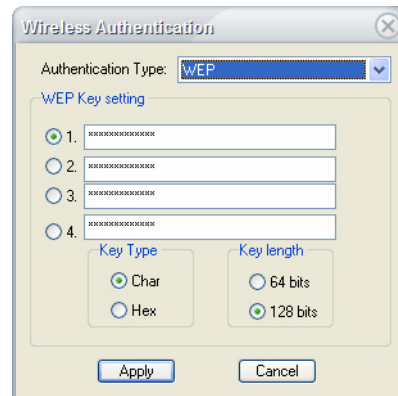


Figure 16-3:Configuring Sensor WEP Settings

- 3) Make the following selections:
 - WEP Key Setting
 - Key Type
 - Key Length
- 4) Click **Apply**.

Configuring SmartEdge Sensor Packet Capture Filters

AirMagnet uses various data sampling techniques to scan all available channels for 802.11 frames for statistical analysis. In order to find and solve complex protocol problems quickly, you must first narrow the scan down to a specific SSID or AP and the associated channel. Then you should use various filter options to discard those unwanted 802.11 packets. These basic troubleshooting techniques will help detect and pinpoint any problem that may exist.

To configure Sensor filter settings:

- 1) From the AirMagnet Config screen, click the **Filter** tab. The screen refreshes. See 14-4.

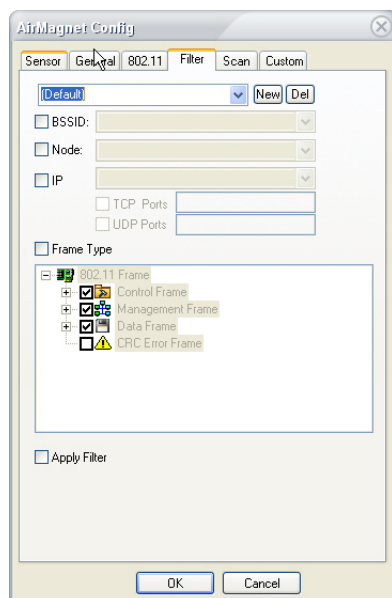


Figure 16-4:Configuring Sensor data capture filters (1)

- 2) Click **New**, and enter a name for the filter.

You can select one filter option from the remaining fields; click the radio button next to the filter type you wish to implement (BSSID, Node, IP, or Frame Type) and make the selections as described below.

- 3) To use BSSID, click the BSSID radio button, and select a BSSID from the drop-down list.
- 4) To use Node, click the Node radio button, and select a Node from the drop-down list.
- 5) To use IP, click the IP radio button and select an IP address; then check the TCP Ports and/or UDP Ports check box and enter the port number(s).
- 6) To use Frame Type, click the Frame Type radio button.
 - a Expand the frame options one by one.
 - b Uncheck all frame types, and then select only those you want to include in the filter.
- 7) Optionally, check the Enable Filter check box. This box must be checked if you wish to use your filter.
- 8) Click **OK**.

When **Enable display filter** is selected, the **Filter** check box on the Decodes screen will be automatically checked, meaning that only the frames that match the parameters of the filter will pass through the filter.

Removing an Existing Filter

You can remove a filter that is no longer in use.

To delete a filter:

- 1) From the AirMagnet *Config>Filter* screen, highlight the filter from the filter drop-down list.
- 2) Click **Delete**.
- 3) Click **OK**.

Configuring Sensor Channel Scan Settings

Configuring AirMagnet SmartEdge Sensor channel scan settings allows you to decide which channels are to be scanned and the frequency at which they are scanned.

Regulatory rules dictate the radio frequencies (channels) and emission powers for the 802.11 standards. To comply with these regulatory domains, WLAN devices are preconfigured to operate on various channels in different countries worldwide. [Table 16-3](#) summarizes the channel allocation in major parts of the world.

Table 16-3: Worldwide Radio Channel Assignments

Region/Country	802.11b/g	802.11a
America	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
Most parts of Europe and Australia	1 ~ 13	36, 40, 44, 48, 52, 60, 64
France	10 ~ 14	36, 40 44, 48, 52, 56, 60, 64
Spain	10 ~ 11	36, 40 44, 48, 52, 56, 60, 64
Japan	1 ~ 14	34, 38, 42, 46
Pacific Rim (China, Taiwan, Hong Kong, Singapore, Korea)	1 ~11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Despite these regulatory requirements, there are occasions where the prohibited channels do contain 802.11 devices due to misconfiguration or the presence of a malicious rogue AP. Since AirMagnet SmartEdge Sensor scanning does not emit any radio waves, it is completely compliant to all the regulatory rules.

The benefits of using the worldwide operation mode are threefold:

- 1) For WLAN administrators and consultants who travel around the globe, AirMagnet's world-mode feature allows easy selection among the regulated channels.
- 2) Since rogue APs may operate in any channel regardless of regulatory requirements, the ability to scan all channels for rogue APs is essential.
- 3) Being able to spot misconfigured WLAN devices operating in violation of regulatory rules is also an added benefit.

To configure SmartEdge Sensor channel scan settings:

- 1) From the AirMagnet Config screen, select the Scan tab. The screen refreshes. See [Figure 16-5](#).

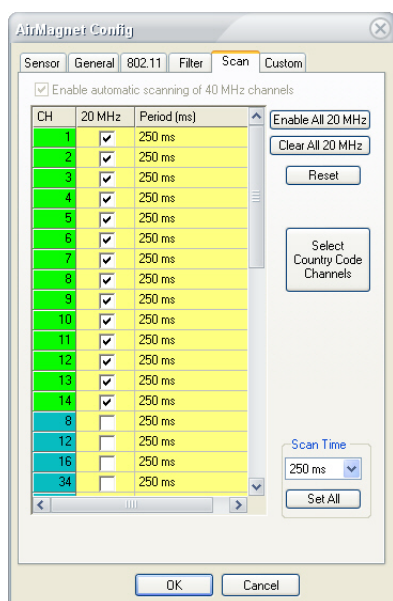


Figure 16-5:Configuring Sensor scan settings

As displayed, the channels are color-coded; those highlighted in green are 802.11b/g channels, and those in blue are 802.11a channels.

- 2) Click **Clear All** to remove the default scan settings, and then check only the channel(s) you want to focus on.
- 3) Click in the Periods (ms) field, and specify a scan time interval from the drop-down list.
- 4) Optionally, click the down arrow below **Scan time** to select a time, and then click **Set All** to change the scan time of all channels to the selected value.
- 5) If necessary, click **Reset** to restore the default scan settings.

- 6) Click **OK** when completed.

Customizing the User Interface

The Custom tab allows the user to modify the current "skin" in use by Remote Analyzer. The skin alters the general appearance of the user interface, allowing a great deal of customization, as described in the [Table 16-4](#) below.

To customize Remote Analyzer's skin:

- 1) From the Configuration window, select the Custom tab. See [Figure 16-6](#).



Figure 16-6: Custom Tab

- 2) Make the selections as described in [Table 16-4](#).

Table 16-4: Custom Tab Options


Option	Description
Skin	The Skin drop-down allows you to select from the three pre-defined skins. Alternatively, you can select Custom and select a skin of your own, as described below.
Custom Skin Name	If you have selected Custom from the Skin drop-down, you can click the Browse button and browse to the location you have saved your custom skin. Skins must be in the .msstyle file format, and can be downloaded from various sources on the Internet.
Show Menu Bar	Checking this box will display the File, Tools, and Help menus across the top of the program. These options perform many of the same tasks as the buttons in the tool bar do.

Chapter 17: WLAN Management Tools

Introduction

This section discusses the use of various advanced WLAN network management tools in Remote Analyzer. The tools allow you to conduct the following WLAN management tasks:

- Diagnosing Connectivity Problems
- Troubleshooting Link Connections
- Tracing Network Devices

You can open the WiFi Tools screen by clicking  on the navigation bar.

Troubleshooting the Link Connection

WLAN connectivity problems can stem from a 802.11 data link layer malfunction, or IP network layer configuration issues. These end-to-end connectivity tests can be performed using AirMagnet's Connection Test tool.

In order to troubleshoot and pinpoint the root cause, the interaction between the two networking layers must be investigated in a different way than you would with a wired LAN. AirMagnet provides a set of uniquely integrated tools to address these anomalies.

In order to achieve end-to-end network connectivity, a wireless device typically goes through the following four phases to reach the other end node for communication:

- Associate with a WLAN access point at the data link layer
- Use DHCP to acquire IP address for itself, default gateway, and DNS server
- Use DNS server to resolve the other end node's domain name to an IP address
- Use the default gateway to reach the end node, via the resolved IP address


Diagnosing Network Connectivity Problems

Various network circumstances can make these steps misbehave, thereby breaking the end-to-end connectivity. AirMagnet assists IT professionals in identifying these issues. The following four diagnostic steps are developed so one can use AirMagnet integrated tools to track down problems.

Verifying Station-AP Association

AirMagnet's Connection Test utility emulates a WLAN client acquiring IP level connectivity beginning from the initial 802.11 client association procedure. It can be used to confirm the association with a WLAN access point.

To activate the Connection Text tool:

- 1) From the Tools screen, click  **Connection Test**. The Connection Test tool screen appears. See [Figure 17-1](#).

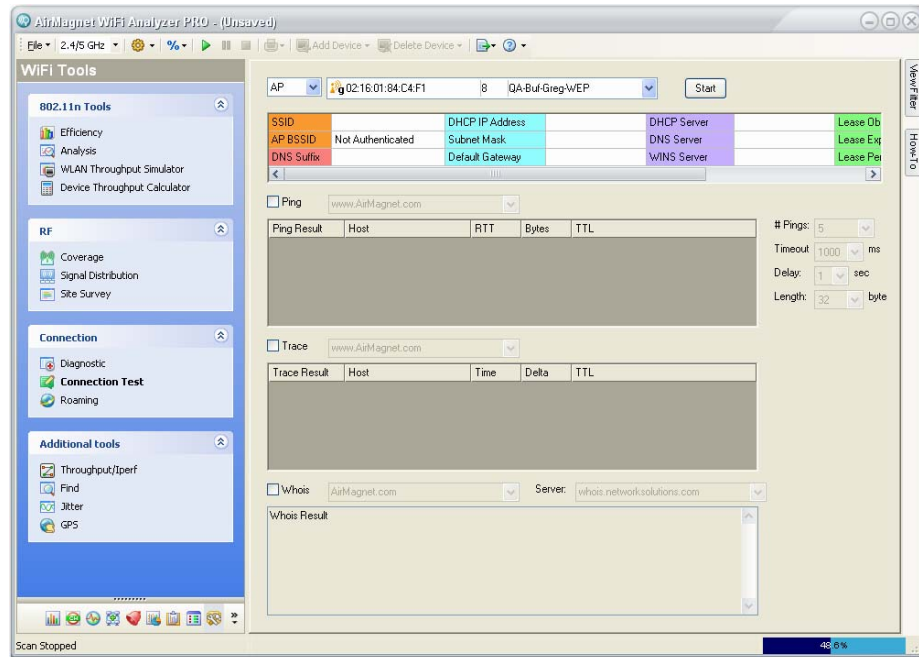



Figure 17-1: Connection Test

- 2) For STA, select the client station MAC address from the STA drop-down list.
- 3) For AP, select the AP that the client is supposed to connect with from the AP drop-down list.

You may select ANY if you are not sure which AP to use, but the accuracy of the diagnosis will be reduced.

- 4) Click  (**Start**). The Diagnostic tool screen shows the progress in the association process with the AP. See [Figure 17-2](#).

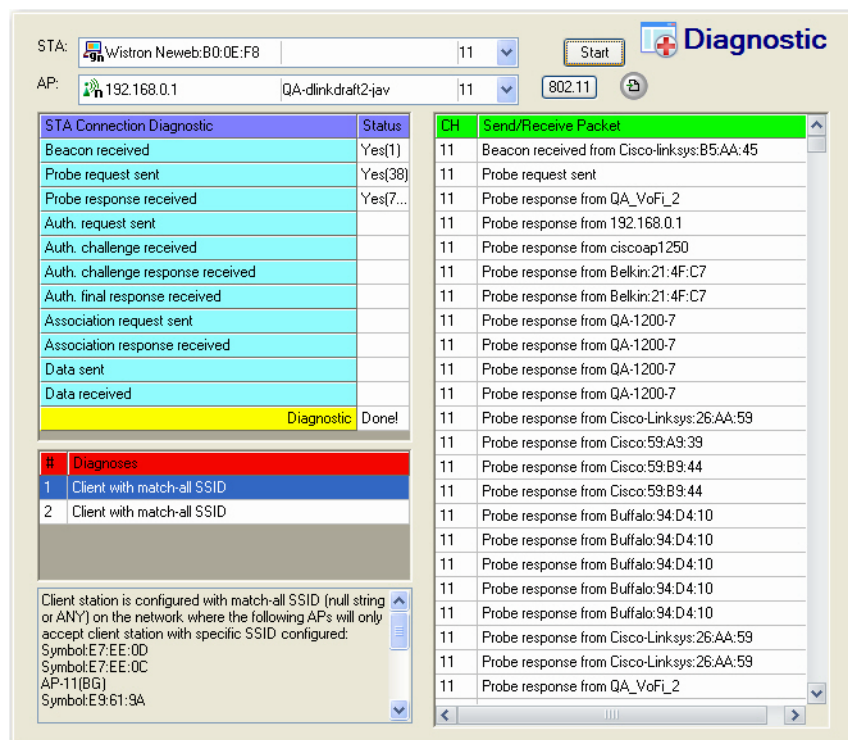


Figure 17-2: A completed diagnostic test

*The diagnostic test automatically ends once it is 100% completed. However, if you want to stop a diagnostic test that is still in progress, simply click **Stop**.*


- 5) Look in the middle- and lower-left parts of the screen for diagnostic results (which suggest the likely causes of the connection and association problems).
- 6) Look in the right part of the screen for step-by-step log.
- 7) Click **802.1X** to display 802.1x information.
- 8) Click **Export** (Export) to export the log data.

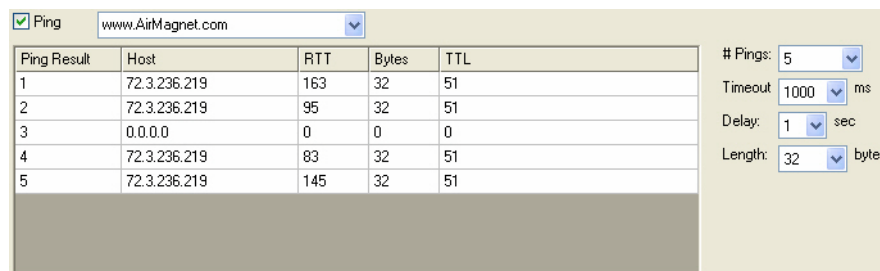
If an unintended AP was associated or the association fails as will be indicated by an AirMagnet error message, you have confirmed that a data link layer problem exists. Such a problem can be best diagnosed with AirMagnet by using the tools described here.

Verifying DHCP IP Address Acquisition

After the proper association to the desired AP has been confirmed in Phase 1, the next step is to verify the DHCP acquisition of IP addresses for client service, default gateway, and DNS server.

To verify DHCP IP address acquisition:

- 1) Check the Ping box. To start testing the IP subnet connectivity, enter the default gateway IP address and tap  (Start). You should see Ping responses on the screen with RTT (Round Trip Time) less than 100 milliseconds. See [Figure 17-3](#).



Ping Result	Host	RTT	Bytes	TTL
1	72.3.236.219	163	32	51
2	72.3.236.219	95	32	51
3	0.0.0.0	0	0	0
4	72.3.236.219	83	32	51
5	72.3.236.219	145	32	51

Pings: 5
 Timeout: 1000 ms
 Delay: 1 sec
 Length: 32 byte


Figure 17-3: Ping Test

If the Ping test shows a timeout, then IP connectivity with the local LAN has failed. At this point, check on the health of the default gateway and the physical connection between the associated AP and the wired LAN.

Verifying DNS Name Resolution

Now that you have verified connectivity with the local subnet and your default gateway, you will confirm DNS name resolution.

To confirm DNS name resolution:


- 1) In the Ping section, enter a host name on your corporate network, such as your internal Web server, for example, `www.internal.MyCompany.com`.
- 2) Click  (Start). The Ping test should report Ping responses and their corresponding RTT (Round Trip Time).

If AirMagnet displays an error message on the domain name resolution, check on the health of your DNS server.

Reaching an End Node with Default Gateway

The final test is to communicate with the end node, which may be on the internet.


To connect to an end node from the default gateway:

- 1) From the same Ping page, enter the end node's domain name, for example, `www.yahoo.com`.
- 2) Click  (Start). This Ping test verifies end-to-end IP network connectivity.

Tracing Network Devices

If Ping requests time out, the AirMagnet Trace utility can be used to isolate the routing path and locate breakage.

To run the AirMagnet Traceroute utility:

- 1) From the Connection Test screen, check the Trace box.
- 2) Enter the end node domain name, and click  (Start). This will start the trace-route process.

Functional IP routers capable of responding to ICMP messages on the path between AirMagnet and the end node will then appear on the screen. By examining the list of routers, you may be able to spot routing anomalies that exist.

802.11n Network Tools

Remote Analyzer comes with 802.11n tools that allow the user to analyze the performance of the 802.11n wireless network – the next generation of wireless networking technology that offers unprecedented network throughput, range, and stability. The tools are focused on helping the user to understand and troubleshoot the most common 802.11n-related issues they may encounter.

Note that 802.11n tools require that an 802.11n-enabled Sensor and license are in use.

Remote Analyzer provides the following 802.11n-related tools:

- Efficiency
- Analysis
- WLAN Throughput Simulator
- Device Throughput Calculator

802.11n Efficiency

The 802.11n wireless network protocol introduces substantial enhancements in WLAN efficiency at both the physical (PHY) and the medium access control (MAC) layers. The Efficiency tool is intended to provide the basic knowledge that the user needs in order to take full advantage of the benefits of the 802.11n network.

The Efficiency tool allows you to see the network efficiency between any (chosen) pair of AP and STA, or AP alone. The Efficiency tool screen displays 802.11n issues in the following categories:

- **PHY** – covers the issues related to improved data throughput at the physical layer.

- **MAC** – covers issues related to protocol efficiency improvements at the Medium Access Control layer such as frame aggregation and block acknowledgements.
- **Coexistence** – covers issues related to 802.11n network's backward compatibility with legacy 802.11 networks (i.e., 802.11a/b/g).

To analyze the network efficiency between an AP and a STA:

- 1) From the navigation bar, click  **WiFi Tools** . The WiFi Tools screen opens.

By default, the 802.11n Tools>Efficiency screen when the WiFi Tools screen opens. If you are on another WiFi Tools screen, you can navigate to the Efficiency screen simply by clicking Efficiency. See Figure 17-4.

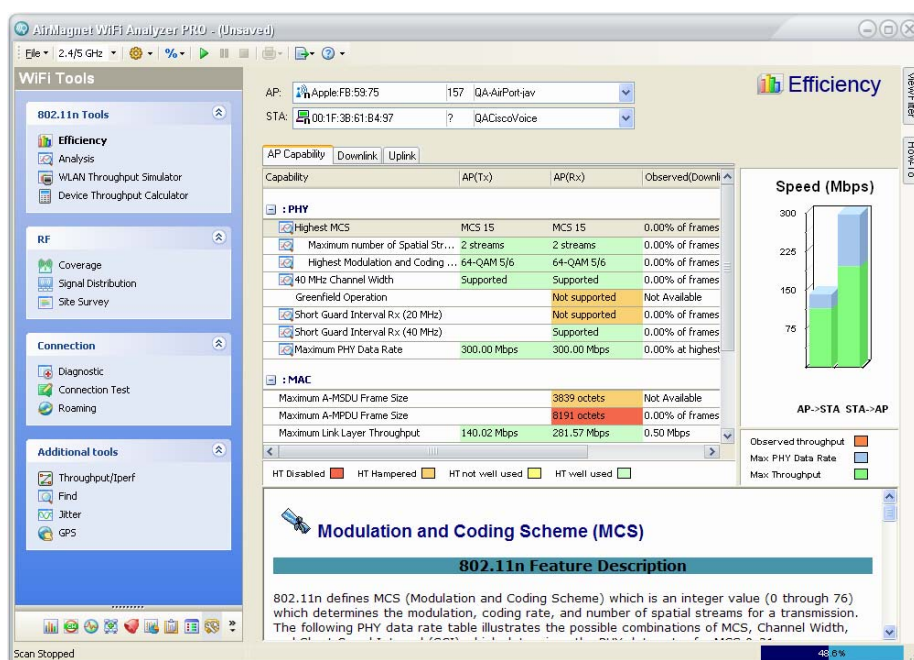


Figure 17-4: Analyzing 802.11n network efficiency

- 2) From the Efficiency screen, select an AP and a STA.

The STA marked in bold green in the STA list is the one that is associated with the AP selected from the AP list above.

- 3) Use the tabs on the upper part of the screen to view the various data regarding the network efficiency between the AP and the STA, as described in Table 17-1.

Table 17-1: 802.11n Efficiency Tool Parameters

Parameter	Description
Tab	<p>Click any of the following tabs to view the pertinent data in the table.</p> <ul style="list-style-type: none"> • AP Capability – Shows the maximum theoretical capability that an AP could reach if associating with a hypothetical “golden” STA that supports all 802.11n features. • Downlink – Displays data about the link from the selected AP to the selected STA. • Uplink – Displays data about the link from the selected STA to the selected AP.
Table Fields	<ul style="list-style-type: none"> • Capability – Lists major features that an 802.11n device is capable of. • AP (TX) – The transmit capabilities of the AP. • AP (Rx) – The receive capabilities of the AP. • AP->STA – The downlink capabilities (from the AP to the STA). • STA->AP – The uplink capabilities (from the STA to the AP). • Observed (Downlink) – The level or state of a certain capability as observed from the downlink (i.e., from the AP to the STA). • Observed (Uplink) – The level or state of a certain capability as observed from the uplink (i.e., from the STA to the AP).
Color Legends	<ul style="list-style-type: none"> • HT Disabled (Red) – High Throughput feature disabled or not used. • HT Hampered – High Throughput feature is impaired. • HT Not Well Used – High Throughput feature is used for only 50~75%. • HT Well Used – High Throughput is used almost to its full potential.

- 4) Observe the various data rates for both the downlink (AP->STA) on the left and the uplink (STA->AP) on the right in the bar chart, as described in [Table 17-2](#).

Table 17-2: 802.11n Efficiency Bar Chart

Screen Data	Description
Bar Chart	Left Chart —Shows downlink (AP->STA) data rate. Right Chart —Shows uplink (STA->AP) data rate.
Color Legend	<ul style="list-style-type: none"> • Light green—Represents Maximum throughput. • Light blue—Represents Maximum PHY Data Rate • Brown—Represents Observed Throughput.

Note: The Observed (Downlink) and Observed (Uplink) columns show any of the following depending on the situation:

- When an AP-STA pair which is known to be associated by Remote Analyzer, the Observed column contains metrics which are specific to the AP-STA association (i.e., only displays traffic measurements made between the combination of the AP and STA).
- When an AP-STA pair is not known to be associated, the Observed column contains metrics which are independent of any association (i.e., all outgoing [data] traffic metrics from the AP and STA are displayed).
- When an AP and “any” STA are selected, the APs outgoing (data) traffic metrics are used and the STA (and subsequently Uplink) metrics are zero (i.e., no traffic is indicated). In this case, the AP’s capability is compared against a “virtual” STA, which has parameters defined at the limit of the 802.11n specification.

802.11n Analysis

The Analysis screen provides detailed analysis (explanation) about a number of 802.11n-related issues. You can navigate to the Analysis tool screen by clicking Analysis under 802.11n Tools.

The Analysis tool allows you to see the following 802.11n network data between any (chosen) pair of AP and STA, or AP alone:

- 20/40 MHz Statistics
- Short Guard Interval (SGI)
- A-MPDU
- MCS
- PHY Data Rate

To analyze 802.11n data on your WLAN:

- 1) From the WiFi Tools screen, click Analysis in the 802.11n Tools section. See Figure 17-5.

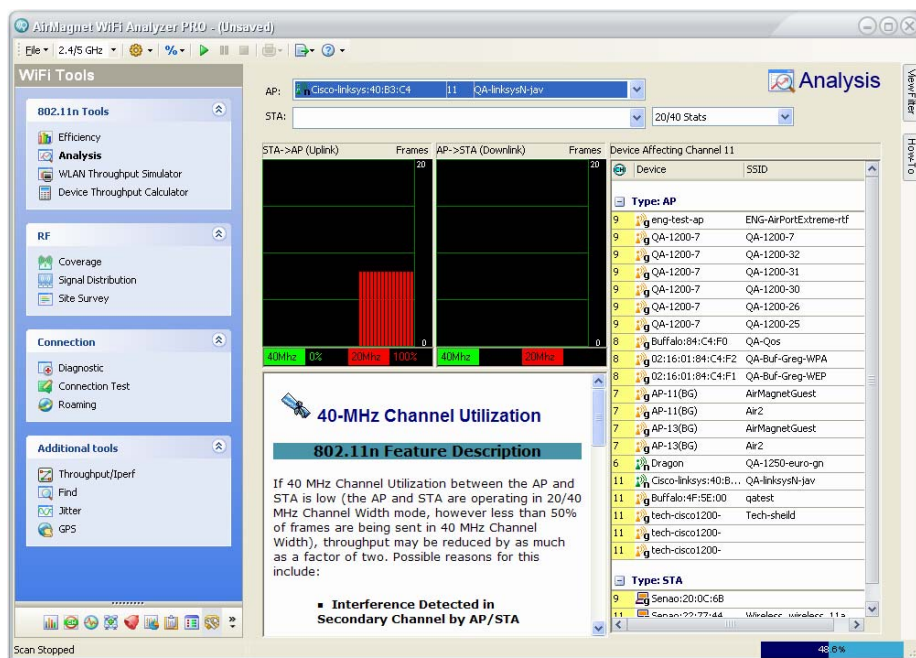


Figure 17-5: Analyzing 802.11n data

- 2) From the top of the screen, select a AP and station, as shown in Figure 17-6.

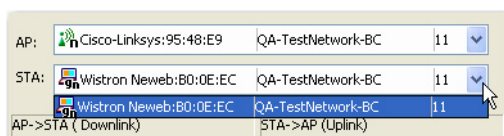


Figure 17-6: Selecting an AP

- 3) Select a data type of interest, as shown in Figure 17-7.

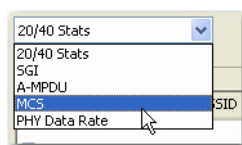


Figure 17-7: Selecting a station

- 4) Use the bar charts to observe the downlink (AP->STA) and uplink (STA->AP).

- 5) Read the description in the lower-middle part of the screen.
- 6) From the right-hand side of the screen, look through the list of devices that are affecting the selected channel.


Simulating WLAN Throughput

The WLAN Throughput Simulator is a utility for calculating network, node and media throughput, utilization and overhead (as measured at the 802.11 Link Layer) under various network and node configurations. It allows the user to add and configure up to fifty 802.11a, 802.11b, 802.11g and/or 802.11n nodes on a “virtual channel”. The Simulator’s engine applies additional network and node parameters based upon the type and settings of the nodes present. The Simulator runs in a “perfect” environment, assuming that all nodes can “hear” each other (negating the possibility of packet collisions and frame retries) and that all nodes transmit as much (and as fast) as they possibly can (based upon their individual and overall network parameters). The result of such simulation provides a baseline measurement of the (somewhat theoretical) maximum link-layer throughput that can be achieved for a particular configuration.

Configuring WLAN Throughput Simulator

Before using the WLAN Throughput Simulator, you may want to configure it in a way so that the tool can best simulate the WLAN throughput you desire.

To configure the WLAN Throughput Simulator:

- 1) From the WLAN Throughput Simulator screen, click  and select Configure Simulator. . . from the drop-down menu. The Simulator Configuration dialog box appears. See [Figure 17-8](#).

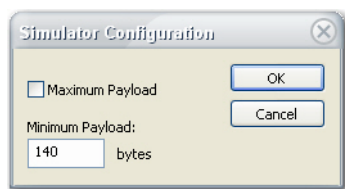


Figure 17-8: Configuring WLAN Simulator

- 2) Check the Maximum Payload check box or specify a minimum packet size.


If the Maximum Payload check box is checked, the Simulator will simulate the condition in which all nodes will transmit the maximum packet size possible. Otherwise, the WLAN Throughput Simulator will simulate WLAN throughput using a payload value between the specified Minimum Payload and the Maximum Payload, which varies depending on the 802.11 protocol used on the devices. According to the IEEE 802.11n Specifications, the maximum payload that can be transmitted is up to 2.3 Kb for 802.11a/b/g devices and 65 Kb for 802.11n devices if MPDU is enabled.

- 3) Click OK.

Conducting WLAN Throughput Simulations

The WLAN Throughput Simulator allows the user to simulate WLAN throughput under user-specified conditions. All you have to do is to select the APs and STAs, set the parameters, and then click Simulate. Remote Analyzer will generate the results and display them on the screen.

To simulate your WLAN throughput:

- 1) From the 802.11n Tools screen, click WLAN Throughput Simulator.
- 2) Select the appropriate frequency band by clicking the 2.4 GHz or 5 GHz radio button.
- 3) From the menubar, click  and select an option from the drop-down menu.

Depending on the frequency band being used, the options in the Add Device drop-down list may vary slightly. [Table 17-3](#) describes all possible options.

Table 17-3: Adding Device Drop-Down Menu Options

Menu Option	Description
Add Existing Device	Opens a dialog box that allows you to select and add APs and/or STAs from a list of devices detected on the WLAN.
802.11a Device	Adds 802.11a APs and/or STAs.
802.11b Device	Adds 802.11b APs and/or STAs.
802.11g Device	Adds 802.11g APs and/or STAs.
802.11n Device	Adds 802.11n APs and/or STAs.

- 4) Associate STAs with APs by clicking an STA and then the down arrow next to it to select an AP to associate with, as shown in [Figure 17-9](#).

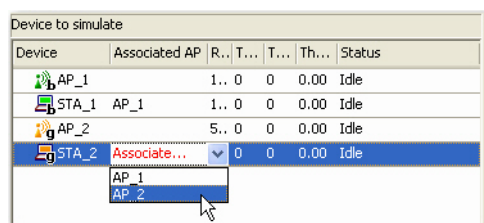


Figure 17-9: Associating station with AP

- 5) Repeat Step 3 to make sure that all APs and STAs are associated.

Note that every STA needs to be associated with an AP in order to run WLAN throughput simulation.

- 6) Click the Run button in the upper-right corner of the screen. The simulation starts and the results are shown on the screen. See Figure 17-10.

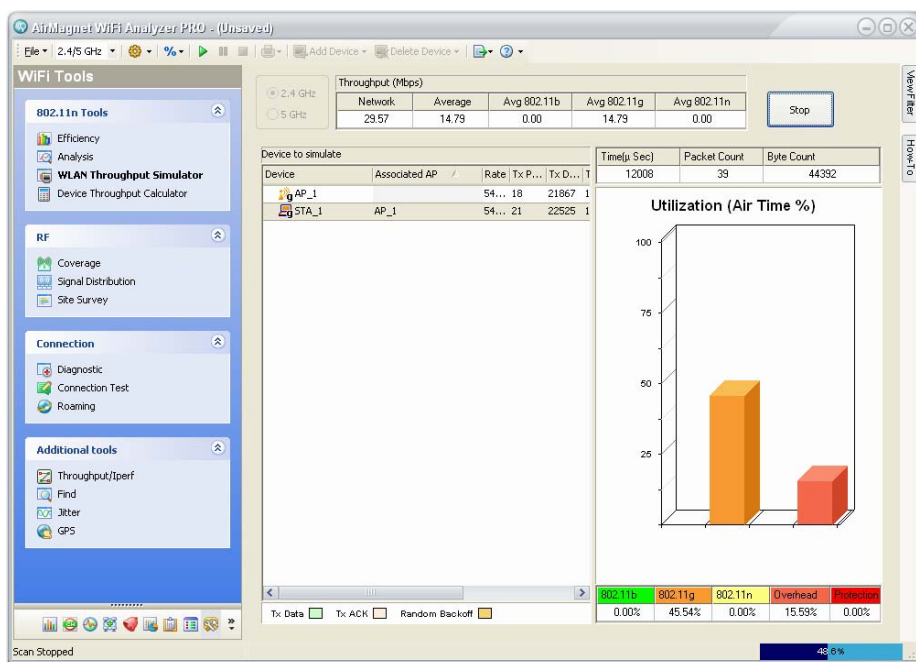


Figure 17-10: Simulated WLAN Throughput

Simulated WLAN Throughput

The Table 17-4 explains the simulated WLAN data as shown on the WLAN Throughput Simulator screen.

Table 17-4: WLAN Throughput Simulator Screen Data

Data Field	Description
Throughput (Mbps)	<p>Shows WLAN throughput in Mbps in the following categories:</p> <ul style="list-style-type: none"> • Network – The network throughput which is the combined, aggregate throughput of the wireless all media (which may include 802.11a/b/g/n, depending on the frequency band selected, i.e., 2.4 GHz vs. 5 GHz). • Average – The average node throughput (which the network throughput divided by the number of nodes). • Avg 802.11a – The average node throughput for all 802.11a devices. (5 GHz only). • Avg 802.11b – The average node throughput for all 802.11b devices. • Avg 802.11g – The average node throughput for all 802.11g devices. • Avg 802.11n – The average node throughput for all 802.11n devices.
Device to Simulate	<p>Shows information about each of the devices involved in the simulation:</p> <ul style="list-style-type: none"> • Device – The name or MAC address of the node. • Associated AP – The name of APs associated with a station or stations. • Rate – The PHY Data Rate used by the node for all DATA transmissions. • Tx Packets – The number of DATA frames (packets) sent from the node. • Tx Data Bytes – The number of DATA bytes sent from the node. • Throughput – The throughput of individual nodes. • Status – The current operating state of the nodes which can be TX Data, Tx ACK, Random Backoff, and Virtual Carrier Sense. • Time (µsec) – The simulation time (in µsec). <p>Note: The simulation engine runs at 1/1000th time scale, which means that every second of “real-time” represents one millisecond of “simulation time”.</p> <ul style="list-style-type: none"> • Packet Count – The number of packets sent over the channel. • Byte Count – The number of bytes sent over the channel.

Calculating Device Throughput

The Device Throughput Calculator is a utility for calculating a device’s theoretical throughputs. The user simply clicks to specify the parameters such as MCS index, SGI, bandwidth, max frame size, block ACK, least capable device, and/or protection mechanism used, and AirMagnet will calculate the maximum PHY rate, maximum data rate, percentage of overhead, the number of spatial frames, and the modulation coding rate in a flick of second. It also displays 802.11 frame exchange data in a graph which showing the percentage of DIFS, preamble/PLCP, Data, SIFS, preamble/PLCP, and ACK frames.

The Device Throughput Calculator allows the user to calculate the maximum throughput level of a device based on user-specified parameters and coexistence conditions. The results of all calculations can be retained on the screen. They can serve as a quick reference as to the level of performance a device can achieve in various conditions.

To calculate device throughput:

- 1) From the WiFi Tools screen, click Device Throughput Calculator. The Device Throughput Calculator screen appears. See Figure 17-11.

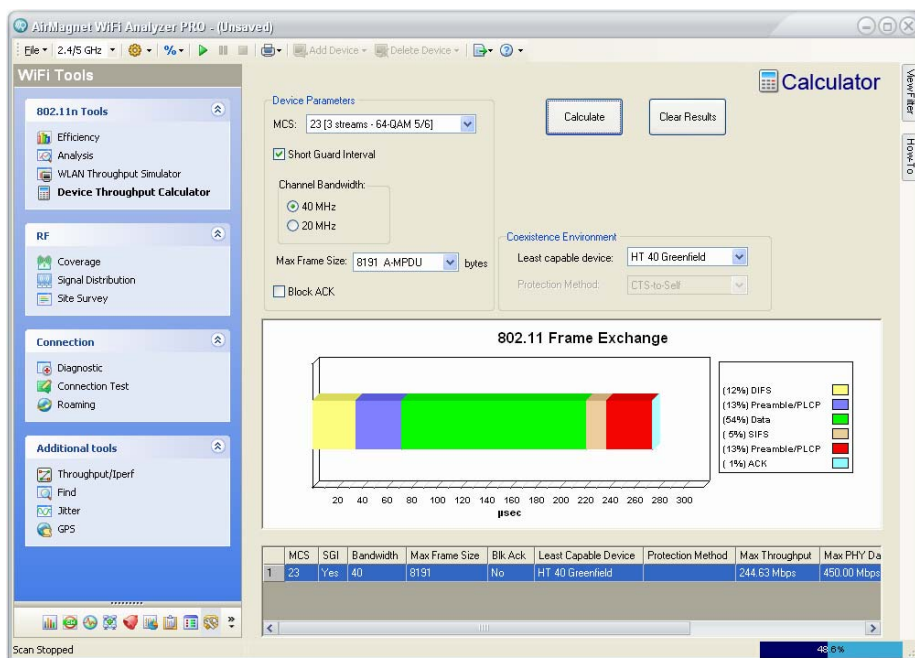


Figure 17-11: Calculating Device Throughput

- 2) On the Device Throughput Calculator screen, make the selections as described in the Table 17-5.

Table 17-5: Device Throughput Calculator Parameters

Parameter	Description
MCS	Click the down arrow and select an option from the drop-down list. <i>Note:</i> Each Modulation and Coding Scheme (MCS) is associated with a specific number of spatial streams and a modulation and coding rate, as indicated by the values within the brackets.
Short Guard Interval	If checked, Short Guard Interval (SGI) is enabled. <i>Note:</i> When SGI is enabled, PHY data rate (in Mbps) is increased by roughly 11% for each Modulation and Coding Scheme (MCS) on both the 20- and 40-MHz channels.

Table 17-5: Device Throughput Calculator Parameters

Parameter	Description
Channel Bandwidth	Select either of: <ul style="list-style-type: none"> • 40 MHz • 20 MHz
Max Frame Size	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none"> • 3839 A-MSDU • 7935 A-MSDU • 8191 A-MPDU • 16383 A-MPDU • 32767 A-MPDU • 65535 A-MPDU
Block ACK	If checked, Block Acknowledgement is enabled.
Least Capable Device	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none"> • HT 40 Green Field • HT 40 Mixed Mode • HT 20 Green Field • HT 20 Mixed Mode • 802.11g • 802.11b • 802.11a
Protection Method	Click the down arrow and select an option from the drop-down list: <ul style="list-style-type: none"> • CTS-to-Self • RTS/CTS • L-SGI TXOP <p><i>Note: None of these protection methods applies to HT 40 Greenfield.</i></p>

- 3) Click the Calculate button. Remote Analyzer starts to calculate the device throughput based on the parameters you have specified, displaying the result on the screen.
- 4) Repeat Steps 2 through 3 to make more calculations using different combinations of the parameters.

Remote Analyzer generates a calculation result at each click of the Calculate button. All results will be shown on the screen, making it easy to compare the device's throughputs under various conditions. Figure 17-12 shows a Device Throughput screen with calculation results.

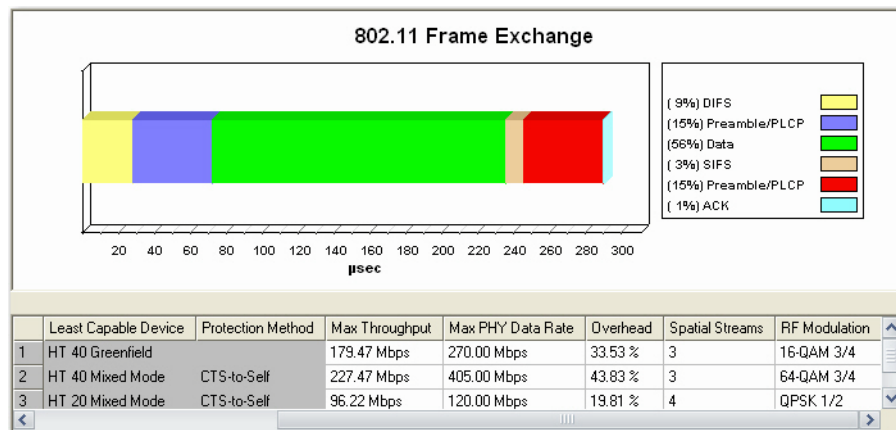


Figure 17-12: Device throughput calculation results

Chapter 18: Managing Data Files

Introduction

This section discusses how to manage the RF signal data log files you have captured using AirMagnet Remote Analyzer. AirMagnet Enterprise not only captures and displays wireless network data in real time, but also allows you to save, print, and export those data files for archiving, sharing, or further analysis.

This chapter covers the following topics:

- Saving Captured Data
- Opening a Saved .amc File
- Previewing Data Prior to Printing
- Viewing Recently Opened Files
- Exporting Database Files

Saving Captured Data

AirMagnet Enterprise is capable to display the data in real time as they are captured. However, due to the limitation of the buffer, the system discards old data as new data come in. To keep certain data for further analysis, you need to save the data. Click the links below for more information on saving data.

AirMagnet-Supported File Formats

AirMagnet Enterprise supports the following file formats:

- .amc – AirMagnet’s proprietary file format, which can play back the saved data as if you were playing a video. It lets you revisit the data in the way they were captured.
- .ecp – Ethernet’s file format.
- .cap – Sniffer’s file format.

Saving a New .amc File

To save a .amc data file:

- 1) From any AirMagnet Remote Analyzer screen, click File>Save. The Save As dialog box appears.
- 2) Select a file path, name the file, and choose a file format.
- 3) Click Save. AirMagnet starts to download frames from the sensor.
- 4) Wait until the download is completed.

Saving an Existing File in a Different Format

After viewing an existing file (see Opening a Saved .amc File), you can save it in a different name or format.

To rename a file:

- 1) Click File>Save As. The Save As dialog box appears.
- 2) Choose a file path, rename the file, or select another file format.
- 3) Click Save. AirMagnet starts to download frames from the sensor.
- 4) Wait until the download is completed.

Opening a Saved File

Files saved in any of the AirMagnet-supported file formats can be opened in AirMagnet Remote Analyzer. This allows you to revisit the historical RF data captured on your wireless network.

To open a .amc file:

- 1) Click File>Open.... The Open dialog box appears.
- 2) Select the .amc file, and click Open. The file data start to appear on the screen.
- 3) Wait until the value on top of the screen becomes 100% (meaning the data is completely loaded).

The live capture function is suspended while and after the file is (being) opened. To resume live capture, click File>Live Capture.

Previewing Data Prior to Printing

You can back up or share your wireless network data in print. AirMagnet Remote Analyzer's Print Preview feature helps make sure that you print what you want to.

To preview data:

- 1) Click File>Print Preview. The Print Preview screen appears.
- 2) Use the buttons on the screen to preview the page(s).
- 3) Click Print.

Part IV: Appendices & Index

Appendix A: Secure Communication

Firewall Configuration

The AirMagnet SmartEdge Sensors communicate with both the AirMagnet Enterprise Server and the AirMagnet Enterprise Server using Secured Socket Layer (SSL) and Transport Layer Security (TLS) at TCP Port 443. Both protocols require that any intervening firewalls be configured for port forwarding on Port 443. In the event that the SSL/TLS port is not open across the network segments spanned by the AirMagnet Enterprise system components, the following information may be helpful when configuring firewalls:

- The AirMagnet SmartEdge Sensors initiate an SSL/TLS connection with the AirMagnet Enterprise Server.
- The AirMagnet Enterprise Server initiates an SSL/TLS connection with the AirMagnet Sensor.
- The AirMagnet Enterprise Server initiates an SSL/TLS connection with the AirMagnet Sensors (during remote drill-down).
- The AirMagnet Enterprise Server does not initiate outbound connections.

If a VPN tunnel is implemented across the sites where AirMagnet Enterprise is deployed, AirMagnet Enterprise will operate without the need for any special configuration. For instance, if the AirMagnet Enterprise Server is launched remotely on a system running a VPN client, the system is designed so that communication will work without the need for special configuration. However, keep in mind that, if NAT (Network Address Translation) is used, the nodes hidden behind the NAT firewall cannot be addressed without special mapping configurations on the external firewall.

Proxy Servers

Outgoing Proxy

AirMagnet **does** work with non-authentication proxies in the scenario:

Console>Proxy>Internet>Management Server. In this situation we utilize the built-in proxy settings of Internet Explorer. If your proxy server requires a login, we do not have a solution at this time.

Incoming Proxy

AirMagnet **does** work with non-authentication proxies in the scenario:

Console>Internet>Firewall>Enterprise Server where a firewall/proxy on the far end is used. The configuration of the firewall/proxy needs to be changed in one of the following two ways. IMPLEMENT ONLY ONE!

Static NAT

In other words, a public static address and all of its ports are forwarded to another static private address behind it. And vice-versa.

Example:

A firewall has an external public address of 203.57.156.30 and an internal private address of 192.168.1.1. The AirMagnet Enterprise Server is 192.168.1.10 and a Sensor is 192.168.2.10. Each of the AirMagnet devices needs to have a corresponding routable public IP address mapped to it.

You can configure the firewall/proxy to map 192.168.1.10 to 203.57.156.40 and 192.168.2.10 to 203.57.156.59.

Port Forwarding

Some firewalls/proxy share a single routable public IP for all inbound and/or outbound traffic, and anyone attempting to connect to a device behind it needs to have the ports forwarded to an IP/Port combo.

Example:

Using the same IP address as in the example above, all requests to Port 443 (https) at the firewall's external address (203.57.156.30) need to be forwarded to 192.158.1.10 Port 443. Another port number is needed for the AirMagnet SmartEdge Sensor so that all requests to Port 444 on 203.47.157.30 can be forwarded to 192.168.2.10 Port 443.

Regardless of which "Incoming Proxy" method is used, you must make the required change within the AirMagnet Enterprise Server. This can be done by right-clicking the sensor icon from the AirMagnet Enterprise Server user interface, and then select Properties and enter the correct public IP address and port number in the address field.

Appendix B: System Troubleshooting

Before contacting AirMagnet Technical Support (contact information is provided in Chapter 1 of this user guide), some information should be gathered. The following is a suggested list of troubleshooting procedures for use before calling AirMagnet Technical Support.

- Determine the DNS name and IP address of the AirMagnet SmartEdge Sensor (or Server) which is experiencing a problem.
- Can a Web browser connect to the AirMagnet SmartEdge Sensor (or Server) using the URL `https://Sensor/`? If so, what is the reported status of the AirMagnet SmartEdge Sensor (or Server)? If not, determine the IP address of the AirMagnet SmartEdge Sensor (or Server) and try to connect using the IP address rather than the DNS name. Be certain to use the secure protocol `https` when connecting with the web browser.
- Can the AirMagnet SmartEdge Sensor (or Server) station be pinged by another node on the 10/100 network? If not, can other nodes that are on the same network segment be pinged? Try using the IP address for each node if the DNS name fails.
- If the AirMagnet SmartEdge Sensor (or Server) can be reached via ping but the web services are not running, it is necessary to check on the status of the service using the services control panel. If the optional installation of VNC was performed after AirMagnet Enterprise installation, then this may be done remotely. If not, then the station will need to be attended physically. Depending on the version of Windows operating system that is installed, the services control panel is reached in different ways. Method one: From the Start button select Settings: Control Panel and then double click the Services control panel Icon. Method two: Right click on the My Computer icon and choose Manage. Open the Services and Applications folder and then double click on the Services icon. Once the services control panel has been opened, check the status of the AirMagnet Enterprise Server and AM Monitor services. Attempt to restart them if they are not running.

Appendix C:Enterprise Deployment

Introduction

AirMagnet Enterprise is the most powerful and complete solution in the industry for protecting and monitoring your wireless networks and assets. This document is designed to provide you with some of the tips and tricks learned from our experience in the field that will help you get the most out of your AirMagnet Enterprise deployment.

AirMagnet Enterprise Server Deployment

The AirMagnet Enterprise Server can be installed from the AirMagnet Enterprise CD. To ensure that the installation goes smoothly, it is advised that the user read the following important notes prior to starting the installation.

Notes on AirMagnet Enterprise Server Installation

- The AirMagnet Enterprise Server should be installed on a machine dedicated to running the AirMagnet services only.
- The AirMagnet Enterprise Server should have a static IP address and should NOT have any other Web servers running on it, including the Microsoft® Internet Information Service (IIS) which may have been added to the system while installing the Microsoft Windows operating system.
- No other AirMagnet application, such as the AirMagnet Laptop Wireless LAN Analyzer, should be installed on the same machine on which the AirMagnet Enterprise Server is installed. If you have such programs installed on the machine, uninstall them using Add/Remove Programs from Microsoft Windows' Control Panel before installing the AirMagnet Enterprise Server.
- If you are installing the AirMagnet Enterprise Server from AirMagnet's Website, make sure that you have WinZip installed on the machine before downloading the AirMagnet Enterprise Server.
- Make sure that the "proxy server" option within the LAN settings for Microsoft Internet Explorer on the AirMagnet Enterprise Server is turned OFF for your network setup.
- Make sure that the "automatic detect settings" option within the LAN settings for Microsoft Internet Explorer on the AirMagnet Enterprise Server is NOT checked.
- Make sure not to apply a database name with spaces or an error message will appear.
- AirMagnet Enterprise installs Microsoft Visual 2005 Redistribution and Microsoft .NET.

Special Notes on Backup Server Installation

You need to install a backup AirMagnet Enterprise Server in order to take advantage of AirMagnet Enterprise's server redundancy feature.

Microsoft SQL Server or Oracle Database Server must be used if you want to use AirMagnet Enterprise's server redundancy feature. If you select Microsoft SQL™, continue with all the following steps; if you select Microsoft Access™, skip Steps 5-7 and go to Step 8. AirMagnet Enterprise supports Oracle Database 10g ONLY. For instructions on use of the Oracle Database Server with AirMagnet Enterprise, see [Appendix G, "Installing Oracle Database"](#).

All the notes on AirMagnet Enterprise Server installation outlined in the previous paragraph also apply when installing the back-up server. In addition, you must also keep the following important points in mind if you choose to use the server redundancy feature:

- You must set up a Microsoft SQL/Oracle Database server on your network on a dedicated PC, prior to installing the AirMagnet Enterprise Servers (primary and backup), if you have not already have one.
- You must install a primary AirMagnet Enterprise Server and a backup AirMagnet Enterprise Server, making sure that they are installed on two separate PCs.
- You must select Microsoft SQL/Oracle (Server) as your database server when configuring the primary AirMagnet Enterprise Server and the back Server.
- Make sure that the primary AirMagnet Enterprise Server and the backup Server point to the same database on the Microsoft SQL/Oracle server using the same username and password.
- The same administrator password and the shared secret key must be used for both the primary AirMagnet Enterprise Server and the backup server.

Configuring AirMagnet Sensors

Note: AirMagnet Sensor user guides are located under the Documents/Drives section of your My_AirMagnet account.

AirMagnet Sensors require basic configuration in order to properly find and interface with their AirMagnet Server. There are multiple options available for configuring Sensors outlined below.

Sensors can be configured manually or via AirMagnet's Zero Config feature.

Zero Configuration Options

AirMagnet's Zero Config option vastly improves the speed and efficiency of configuring your sensors. There are two different ways of using the Zero Config option. Regardless of which Zero Config option you choose, you will need to enable the feature on the AirMagnet Console. To enable Zero Config, open the AirMagnet Console and go to Manage > Server Options > Zero Config and check the Enterprise Zero Config dialog box.

- Local Sensor Configuration – To use this option, you will need to plug the sensor to be configured into the network on the same subnet where the server resides. In this

situation, the sensor will automatically locate the AirMagnet Server and learn the static IP address of the server.

- **Sensor Configuration Using DNS** – The second Zero Config option allows the sensor to use DNS to find the AirMagnet Server. To use this option, you will need to add an entry into your enterprise DNS specifying `airmagnetenterprise.domain.com`. This will allow the sensor to find the Enterprise Server even when connected remotely from the server. If you have multiple domains in your network you may need to create a C name record to point devices to the appropriate domain where the Enterprise Server resides. See examples below.

- **“Flat” Network Example**

The entire enterprise operates under the domain `Acme.com`

In this case simply add the DNS record for `airmagnetenterprise.Acme.com` and Sensors will be able to automatically find the server from anywhere in the corporate network.

- **Complex Example**

In this case the network may be broken out along lower level domains such as `campusA.Acme.com` and `campusB.Acme.com`. A sensor deployed on `campusA.Acme.com` would not be able to find the server if the server lives on `campusB.Acme.com`. In this situation a C name record is required in order to ensure that the sensor can find the server.

Manual Configuration Options

The manual configuration options are more time consuming as they require you to configure each sensor individually, but provide complete access to all config parameters on the sensor. Instructions for these manual methods are detailed in the Enterprise User Guide under “AirMagnet SmartEdge Sensor Configuration”.

- Via Web Browser – Connect to the sensor directly on the same subnet.
- Via Sensor Serial Console Port – Direct connection to the Sensor.

Working with Firewalls, VPNs, and NATs

Firewall Configuration

The AirMagnet SmartEdge Sensors communicate with both the AirMagnet Enterprise Server and the AirMagnet Enterprise Console using Secured Socket Layer (SSL) and Transport Layer Security (TLS) at TCP Port 443. Both protocols require that any intervening firewalls be configured for port forwarding on Port 443. In the event that the SSL/TLS port is not open across the network segments spanned by the AirMagnet Enterprise system components, the following information may be helpful when configuring firewalls:

- The AirMagnet SmartEdge Sensors initiate an SSL/TLS connection with the AirMagnet Enterprise Server.
- The AirMagnet Enterprise Console initiates an SSL/TLS connection with the AirMagnet Enterprise Server.

- The AirMagnet Enterprise Console initiates an SSL/TLS connection with the AirMagnet Sensors (during remote drill-down).
- The AirMagnet Enterprise Server does not initiate outbound connections.

If a VPN tunnel is implemented across the sites where AirMagnet Enterprise is deployed, AirMagnet Enterprise will operate without the need for any special configuration. For instance, if the AirMagnet Enterprise Server is launched remotely on a system running a VPN client, the system is designed so that communication will work without the need for special configuration. However, keep in mind that, if NAT (Network Address Translation) is used, the nodes hidden behind the NAT firewall cannot be addressed without special mapping configurations on the external firewall.

Proxy Servers

- Outgoing Proxy AirMagnet does work with non-authentication proxies in the scenario: Console>Proxy>Internet>Management Server. In this situation we utilize the built-in proxy settings of Internet Explorer. If your proxy server requires a login, we do not have a solution at this time.
- Incoming Proxy AirMagnet does work with non-authentication proxies in the scenario: Console>Internet>Firewall>Enterprise Server where a firewall/proxy on the far end is used. The configuration of the firewall/proxy needs to be changed in one of the following two ways. IMPLEMENT ONLY ONE!
- Static NAT - When a public static address and all of its ports are forwarded to another static private address behind it, and vice-versa.

Example: A firewall has an external public address of 203.57.156.30 and an internal private address of 192.168.1.1. The AirMagnet Enterprise Server is 192.168.1.10 and a Sensor is 192.168.2.10. Each of the AirMagnet devices needs to have a corresponding routable public IP address mapped to it. You can configure the firewall/proxy to map 192.168.1.10 to 203.57.156.40 and 192.168.2.10 to 203.57.156.59.

- Port Forwarding - Some firewalls/proxy share a single routable public IP for all inbound and/or outbound traffic, and anyone attempting to connect to a device behind it needs to have the ports forwarded to an IP/Port combo.

Example: Using the same IP address as in the example above, all requests to Port 443 (https) at the firewall's external address (203.57.156.30) need to be forwarded to 192.158.1.10 Port 443. Another port number is needed for the AirMagnet SmartEdge Sensor so that all requests to Port 444 on 203.47.157.30 can be forwarded to 192.168.2.10 Port 443. Regardless of which "Incoming Proxy" method is used, you must make the required change within the AirMagnet Enterprise Server. This can be done by right-clicking the sensor icon from the AirMagnet Enterprise Server user interface, and then select Properties and enter the correct public IP address and port number in the address field.

Wireless Policies and Enforcement

Your wireless policy is the foundational logic that AirMagnet Enterprise uses in order to identify problems, respond to threats and coordinate with your overall network and security management process. AirMagnet Enterprise constantly scans for all types of wireless threats – network vulnerabilities, rogue devices, network intrusions, hacking behavior, improperly configured devices, performance issues and much more. In all the solution supports over 130 policy classes covering hundreds of specific attack tools devices and threats to your network.

Initially, this can lead to a steep learning curve, so we have designed this section to help guide you through the process of setting up your initial policies that you can grow along with your understanding of the wireless environment. First, we will step through the logic of the policy and then show with examples how to set your policy using the AirMagnet Console.

- 1) **Identify Your Most Critical Issues** – Prior to even opening the AirMagnet Policy Manager, write out your top 5 most important WLAN issues that you want to address. This could be something such as “detect and prevent Rogue Devices, detect and prevent ad-hoc devices, monitor the uptime of the APs on the manufacturing floor” etc.
- 2) **Disable All Alarms Not Directly Related to Your Top 5 Issues** – Don’t worry, we will go back and turn these alarms back on later. The goal here is to initially focus on the most critical issues, and to establish a strong baseline of what is normal in your network in regard to your top issues. IN short, we want to learn to manage wireless issues well, instead of trying to learn policy management and hundreds of alarms all at once.
- 3) **Define Your Policies** – The next steps will walk you through the logic of how you will handle your wireless issues. These steps will apply to most any policies you want to enforce, so it’s good to get in the habit of documenting the following steps for each alarm or policy rule.
 - a **Decide Who the Policies Should Apply To** – Policies can be targeted to certain locations (e.g. New York Campus), WLAN groups (SSIDs), or devices (specific device Access Control Lists). For each of the top issues, identify “who” the policy should apply to. Keep in mind, AirMagnet lets you define any number of groups (SSIDs, locations, ACLs) to tie policies to.
 - b **Define the Thresholds** – This step will be unique to the specific alarms that you are interested in and relates to how sensitive you want the system to be. For example, you may want to prevent ad-hoc devices from being in your WLAN. Your process could be to identify and alarm when any ad-hoc device shows up in the environment. On the other hand, you may only care about ad-hoc devices that are sending traffic and wish to ignore ad-hocs that are not. In this case, you could set a policy to alert on ad-hocs that have sent a certain number of frames. The key here is to have full control over the thresholds of your policies so that you know that when an alarm is triggered, it is alerting you to an issue that you actually care about.
 - c **Decide How You Want to Be Notified** – AirMagnet will always display generated alarms in the Console user interface, but there are also many additional notification methods available that can alert you or your staff beyond the Console. So enumerate the methods (Email, IM, SNMP, etc.) and the targets (staff members, management system) that you want to link to when the policy is violated.

- d Decide the Actions to Take – Now that we have identified and alerted on threats to the network, we need to decide what we are going to do about it. This is a critical portion of the wireless policy as it will require coordination and agreement throughout the organization. For example, should the response to a certain event be manual or automated (blocking of rogues for example)? Should we perform a forensic capture of the event? How will the event be documented, etc....
- 4) Enable the Policy – Once we have identified the logic of our policies, it is relatively straightforward to configure the policy in the AirMagnet Console, which can then be automatically enforced.
- 5) Monitor, Investigate and Streamline– When you initially begin using the system, it is common to see a relatively high number of alarms. This should be expected as you are beginning to enforce policies with more technical and procedural rigor than you have in the past. As you investigate these issues you will alleviate problems and potentially learn information about your wireless environment that you can use to make your policies more precise. For example, you may find rogue devices that you will need to remove from the building. Likewise, you may investigate a rogue and discover it is actually a neighbor. You can use this information to improve the auto-classification rules in order to avoid triggering the device as a rogue (Note; refer to the AirMagnet Enterprise User Guide for complete instructions on using the auto-classification features). Additionally, you may notice that you want to tweak the thresholds for a particular alarm. Again, this is why it's best to initially work with a small set of your most important alarms, as this process will ensure that when an alarm is generated in the future, you know that it is a significant issue.
- 6) Repeat the Process with Additional Alarms – Once we have confidence and solid baseline for our most important issues, we can repeat the process with more and more alarms. This allows us to build a policy gradually that is rooted in the realities of the network.

System Troubleshooting

The following is a suggested list of troubleshooting procedures for use before calling AirMagnet Technical Support.

- Determine the DNS name and IP address of the AirMagnet SmartEdge Sensor (or Server) which is experiencing a problem.
- Can a Web browser connect to the AirMagnet SmartEdge Sensor (or Server) using the URL `https://Sensor/?` If so, what is the reported status of the AirMagnet SmartEdge Sensor (or Server)? If not, determine the IP address of the AirMagnet SmartEdge Sensor (or Server) and try to connect using the IP address rather than the DNS name. Be certain to use the secure protocol `https` when connecting with the web browser.
- Can the AirMagnet SmartEdge Sensor (or Server) station be pinged by another node on the 10/100 network? If not, can other nodes that are on the same network segment be pinged? Try using the IP address for each node if the DNS name fails.
- If the AirMagnet SmartEdge Sensor (or Server) can be reached via ping but the web services are not running, it is necessary to check on the status of the service using the services control panel. If the optional installation of VNC was performed after AirMagnet Enterprise installation, then this may be done remotely. If not, then the

station will need to be attended physically. Depending on the version of Windows operating system that is installed, the services control panel is reached in different ways. Method one: From the Start button select Settings: Control Panel and then double click the Services control panel Icon. Method two: Right click on the My Computer icon and choose Manage. Open the Services and Applications folder and then double click on the Services icon. Once the services control panel has been opened, check the status of the AirMagnet Enterprise Server and AM Monitor services. Attempt to restart them if they are not running.

Database Issues

- Which version of SQL server does Enterprise Server support?

AirMagnet Enterprise 7.5 supports SQL 2000 (included in the Enterprise installation).

AirMagnet Enterprise 8.0 supports SQL 2000 or 2005 (SQL 2005 is not provided by AirMagnet). AirMagnet Enterprise 7.5 and 8.0 support Oracle 10 g.

- Problem: Poor system performance.

Solution: Reducing the size of the transaction log.

When the transaction log of the database grows too large, the performance of the AirMagnet Enterprise server as a whole will be affected. Connecting to AirMagnet Enterprise server might take long time, or the AirMagnet Enterprise server might take a longer time to load. At this point, the user will need to check the transaction log file of the database to make sure the file has not grown too large. If the file has grown too large, the user might want to shrink the transaction log file to improve the performance of the system as a whole. To shrink the transaction log file, the user will need to bring up the SQL query analyzer and run the SQL command from the SQL query Analyzer window to shrink the size of the transaction log file.

We recommend backing up the transaction log prior to the database truncate procedure. Use the following step to backup.

```
BACKUP LOG airmagnet_log TO airmagnet_log_backup
```

To truncate the transaction log in SQL Query Analyzer, follow the procedure below:

- a Back up the log file for truncation with the following command:

```
BACKUP LOG [AirMagnet Database Name] WITH TRUNCATE_ONLY
```

- b Run the next command to shrink the log file to about 10 MB:

```
DBCC SHRINKFILE (airmagnet_log, 10)
```

Sensor Issues

- Problem: Following a server migration, the Enterprise server IP address has changed. The original sensors are no longer reporting back to the new Enterprise server.

Solution: If the IP address of the Enterprise Server changes, you will need to update the sensors with the server's new IP address. You can do this by logging in to the sensor's remote webpage and go to Configuration > Sensor Setup link> to set the new server IP.

If you need to migrate to a new server, the ideal approach is to manually provide the new server with the same IP address and system used by the previous server. In this case, you will remove the need to update the sensors with any new information.

Please refer to the AirMagnet Enterprise Server Migration Checklist for more details on migrating your Enterprise Server.

- **Problem:** The A5120 sensors (spectrum sensors) are not reporting back to the server.

Solution: Verify that the spectrum sensor license is installed. Without the spectrum license, the spectrum sensor cannot communicate with the Enterprise server.

- **Problem:** Cannot log in to the sensor.

Solution: Users may forget the shared secret key created during installation which is needed to log in to the sensor. If they do not remember it, we recommend resetting the sensor to factory defaults.

If the Sensor is accessible you can reset it to the factory defaults by pressing and holding down the reboot/reset button for more than 5 seconds. After the sensor reboots, it will be reset its factory default settings. To configure the sensor again, follow the instructions in the user guide.

If you are having trouble connecting to a sensor that is not related to the unknown shared key issue, then it will be necessary to telnet into the sensor provided it is a 5020 model. It is advised to work with AirMagnet Technical Support for additional information and guidance on how to troubleshoot your particular problem via Telnet.

- **Problem:** My sensors are behind NAT and I am not able to access the remote Sensor UI or unable to connect to sensor details while in the AirMagnet Console.

Solution: Sensors that are behind NAT will need to be marked as such before information can flow between the Console and the Sensor. To mark a sensor behind NAT, right click your sensor in the sensor tree, found on the Start page, then select the "Sensor Behind NAT" option.

General and Administrative Issues

- **Problem:** I forgot the user name and password for the default admin profile

Solution: If you lose or forget the admin login to the enterprise system, it is possible to recreate the default admin profile. To recreate the default admin profile uninstall and reinstall the same version of AirMagnet Enterprise on the Enterprise Server. The admin profile will be re-created during the new installation.

- **Problem:** Valid devices showing up as "Rogue" after being configured in the ACL

Solution: Verify that the sensor reporting the device as rogue is using the correct profile that the ACL was configured in. A sensor using a different profile will report the device as "Rogue"

- Problem: In AirMagnet Enterprise 7.5 all devices that were not in my ACL were marked as "Rogue" but now they are all "Unknown."

Solution: In AirMagnet Enterprise 8.0 a new "Unknown" classification has been created. To mark all "Unknown" devices as "Rogue" on the console go to Manage>Server Options> Device Classification and select the option to "Classify Unknown Devices as Rogues"

- Problem: I prefer to the old look and feel of AirMagnet Enterprise 7.5 over AirMagnet Enterprise 8.0.

Solution: To revert to our classic look and feel select the "Classic View" option at the top of the console. If you want to set the Classic View as your default startup screen go to Manage > Server Option > Console tab, then check the show classic view at launch check box.

- Problem: I just upgraded my AirMagnet Enterprise server and now I am unable to login.

Solution: On updating AirMagnet Enterprise server, it takes some times for the Enterprise Server to load all of its components from the database to the memory. Additionally the server will need to update all the sensors in the system. While the server is performing these update tasks you may not be able to login to the server – Suggestion: you will need to give the server some times to finish updating the sensors then try to log on again.

Appendix D: SNMP Integration

SNMP Support

The AirMagnet Enterprise Server provides a MIB file (i.e., AirMagnetWLANAlarm.mib), which allows the AirMagnet Enterprise Server to send SNMP traps to multiple SNMP management stations (CA Unicenter/HP OpenView) when an alarm is generated by an AirMagnet SmartEdge Sensor. Upon receiving a trap, the user can launch the AirMagnet Remote Analyzer interface (Windows 2000/2003/XP only) for the AirMagnet SmartEdge Sensor to view detailed description of the trap and thereby the functioning of your wireless network.

Enabling SNMP

To enable the AirMagnet Enterprise Server to send traps to your SNMP management stations, do the following:

- 1) Activate SNMP notification. From the AirMagnet Enterprise Server, click Manage>Configure... to bring up the Manage Server Configuration dialog box. Select Notifications, click Add New Notification, choose SNMP, and click OK to bring up the SNMP Notification dialog box. Make the desired entries and/or selections, and click OK.
- 2) Download the AirMagnetWLANAlarm.mib from the download page of the AirMagnet Enterprise Server into your SNMP management station.
- 3) Compile the MIB file and enable your SNMP management station to receive traps. Currently, the AirMagnet Enterprise Server is able to generate more than 115 traps, with different levels of severity: Critical, Urgent, Warning, and Informational. The levels of severity will be automatically assigned for your SNMP management console once the MIB file is compiled.
- 4) Download and install AirMagnet Enterprise Console from the download page of the AirMagnet Enterprise Server. This will allow you to launch AirMagnet Remote Analyzer from your SNMP management stations.
- 5) Create AirMagnet SmartEdge Sensor Objects on your SNMP management console. You will receive traps from these SmartEdge Sensors. The AirMagnet Enterprise Server does not control the state of the SmartEdge Sensor Objects on your SNMP console. You should configure the state of the SmartEdge Sensor Objects manually.
- 6) To launch the AirMagnet Remote Analyzer to the AirMagnet SmartEdge Sensors from your Windows 2000/XP SNMP management stations, run WinAirMagnet.exe with /S /U and /P arguments. Specify the name of your AirMagnet SmartEdge Sensor after /S. The name of the SmartEdge Sensor will always be the ninth argument (one based) in the trap. Specify the username and password of your AirMagnet SmartEdge Sensor after /U and /P, respectively. Double-clicking a SmartEdge Sensor Object will launch the AirMagnet Remote Analyzer for that AirMagnet SmartEdge Sensor.

Below is a sample format of the trap on your SNMP management console:

```
"Time: %s, Sensor Name: %s, Sensor IP: %s, Sensor Location: %s, Title: %s, Category: %s, Description: %s"
```

where time is the time the trap is generated; SmartEdge Sensor Name is the host name of the AirMagnet SmartEdge Sensor; Sensor IP is the IP address of the Sensor; Sensor Location is the location where the Sensor is deployed; Title is the title of the trap; Category is either Security or Performance; and Description is the detailed description of the trap.

The InterNet Assigned Numbers Authority (IANA) assigned Private Enterprise Number for AirMagnet, Inc. is 16603.

Appendix E: Manual Rogue Trace

If a rogue AP is connected to an infrastructure network, one of the measures to be taken is to quarantine the rogue AP from the network. This can be done by shutting down the switch port to which the rogue AP is connected.

Assuming that "192.168.1.26" is the IP address of a rogue AP. You can manually trace to the switch port of the rogue AP wirelessly by taking the following procedures:

- 1) Run a rogue trace operation to detect the IP address of the rogue AP.
- 2) Determine if there is any switch residing on the same subnet as the rogue AP. If you know for sure that there is such a switch, then go to Step 3; if you are not sure, then run the command "traceroute 192.168.1.26" on Linux or "tracert 192.168.1.26" in a cmd window under Windows. This will allow you to determine the last hop router.
- 3) Log into the last hop router, and run the command "show cdp neighbor". From the output, identify the switch that is connected to the router port with an IP address in the same subnet as the rogue AP. See Step 8 for sample output from this command.
- 4) Log into the switch on the same subnet as the rogue AP.
- 5) Ping the rogue AP using the command "ping 192.168.1.26".
- 6) Run the command "show arp". The resulting printout is something like:

```
Internet 192.168.1.27 - 0003.6bf1.be40 ARPA VLAN1
Internet 192.168.1.26 0 00c0.9f2d.398d ARPA VLAN1
Internet 192.168.1.28 71 000d.c844.0244 ARPA VLAN1
Internet 192.168.1.200 0 00d0.b76c.3bfb ARPA VLAN1
```

- 7) Note down the MAC address of the rogue AP. It is "00c0.9f2d.398d" in this case.
- 8) Then run the command "show mac-address-table". You'll get a printout like this:

```
00c0.9f2d.398d 1 FastEthernet0/3
00d0.b76c.3bfb 1 FastEthernet0/24
```

- 9) Determine if the port FastEthernet0/3 is an uplink port to another switch, using one of the following:
 - If there are multiple MAC addresses associated with the port, we can immediately assume that the port is connected to another switch.
 - Run the command "show cdp neighbor". The printout would be something like:

<i>Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge</i>					
<i>S - Switch, H - Host, I - IGMP, r - Repeater</i>					
<i>Device ID</i>	<i>Local Intrfce</i>	<i>Holdtme</i>	<i>Capability</i>	<i>Platform</i>	<i>Port ID</i>
<i>switch</i>	<i>Fas 0/24</i>	<i>172</i>	<i>T S</i>	<i>AirMagnetF</i>	<i>eth0</i>

The above output indicates that FastEthernet 0/24 port on the switch is connected to another switch device called "AirMagnetF" port "eth0". Hence FastEthernet 0/24 is an uplink port. However, since FastEthernet0/3 is not an uplink port, we can shut it down.

- 10)** If FastEthernet0/3 turns out to be an uplink port, then go over to the switch connected to the port and start the same search procedure there. Run the same procedure with all the switches in that IP subnet until you find the switch to which the rogue AP is connected.
- 11)** Run the command "configure terminal interface FastEthernet 0/3 shutdown" to shut down the switch port.
- 12)** Then run the command "configure terminal interface FastEthernet 0/3 no shutdown" to reactivate the port.

Appendix F: FIPS 140-2 Secure Operation

This Appendix provides information that is required to install, configure, and maintain the sensor in FIPS *approved mode*. Failure to maintain the correct settings will remove the sensor from the approved mode of operation.

This Appendix provides operation information for the following audiences:

- **Administrators** – (Referred to as “crypto officers” in FIPS terminology) are responsible for installing and configuring the AirMagnet SmartEdge Sensor for use. These may be the same person or different people. Administrators authenticate as “local crypto officers” using the shared key and logging in to the Sensor Serial Console Port. Administrators authenticate as “remote crypto officers” using the administrator name and password, logging in to the sensor via the Web UI.
- **Power users and basic users** – (Referred to as “users” in FIPS terminology) are responsible for using the sensor instrumentation (wireless analyzer) features. Users authenticate (log in to the sensor) via the Web UI using a username and password.

Information for Local Crypto Officers

The local crypto officer installs and configures the module for secure operation in the FIPS approved mode. The local crypto officer also maintains the module in the approved mode.

Installation and configuration for secure operation in the FIPS approved mode and maintenance in the FIPS approved mode of A5023 sensor is performed by a Remote Crypto Officer.

Installing and Configuring the Sensor

This section explains the specific steps a local crypto officer must take to configure the sensor in FIPS approved mode.

With the exceptions or additional steps specified below, follow the instructions in “[Configuring SmartEdge Sensor via Sensor Serial Console Port](#)” on page 40 which provides sensor CLI commands needed to configure the sensor in FIPS approved mode.

- 1 Examine the sensor shipping container for any signs of tampering. The sensor is shipped in a sealed container that should not be opened except by a crypto officer. If the container shows signs of tampering, contact AirMagnet for a replacement.
- 2 Apply the tamper evident seals as shown in the FIPS Required Features section of Chapter 3.
- 3 Perform Steps 1 through 8 in “[Configuring SmartEdge Sensor via Sensor Serial Console Port](#)” on page 40 of this guide as documented.
- 4 Enter the `show fipsmode` command. If the command output indicates FIPS mode is ON, continue with step 5 below.

If FIPS mode is OFF, Enter `set fipsmode`. This command sets the shared key to the default value (in this case it is already set to the default value) and disables the Telnet and SSH Servers. This also sets the sensor to use TLS instead of SSL for secure communications.

Remote crypto officers and users must also set their Internet browsers to only use the TLS 1.0 protocol to communicate with the sensor.

- 5 Perform Step 9 with the following restrictions:
 - Do not enable the telnet or SSH server.
 - Set the sensor shared key to a value between 6 and 36 characters in length. The shared key must include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note, the AirMagnet Enterprise Server uses the same shared key.
- 6 Perform Step 10 as documented.
- 7 Enter “show ssh” and “show telnet” commands to verify that both SSH server and telnet server have been disabled. “set ssh” and “set telnet” commands shall be used to disable the servers.
- 8 Perform Step 11 as documented. The browser must be set to use TLS as described below.
- 9 Make sure that “Provide all the approved sensors with the updated Sensor Shared Secret” check box is unchecked. This box shall always be unchecked in the FIPS approved mode. See Chapter 12, “Configuring System Settings” for details.
- 10 Make sure that “Enterprise Zero Configuration” check box is unchecked. This box shall always be unchecked in the FIPS approved mode. See Chapter 12, “Configuring System Settings” for details.

The AirMagnet SmartEdge Sensor is now in the FIPS approved mode.

Maintaining the Sensor in FIPS Approved Mode

This section explains the specific steps a local crypto officer must take to maintain the sensor in the approved mode.

- Local crypto officers must periodically inspect the module for evidence of tamper by examining the tamper evident seals for signs of tampering and the module itself for any scratches, holes, or dents that may indicate someone has tried to open the module. For frequency of inspection, refer to your organization’s security policy. If a tamper is suspected, the module must be zeroized (see [“Zeroizing an AirMagnet Sensor” on page 47](#)) before it is discarded or returned to the manufacturer.
- Local crypto officers may run the self-test on demand by rebooting the module. This may be performed as a troubleshooting step. If the self test fails repeatedly, the

module must be zeroized, as described above, before it is discarded or returned to the manufacturer for replacement.

- If you need to set the sensor shared key, it must be a value between 6 and 36 characters in length and include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note the AirMagnet Enterprise Server uses the same shared key.
- Exercise care to prevent unauthorized access to the sensor by setting a shared key that is not easy to guess. The shared key must be at least 6 characters in length and include at least one upper case character, one lower case character, a number, and a punctuation character. Do not write down the shared key and leave it where others may find it.
- Update of sensor application image is only allowed in the FIPS approved mode. The sensor must be returned to the manufacturer for replacement if sensor application image was updated in the non-approved mode.
- Do not disable FIPS approved mode. Do not enable telnet or SSH server.

Setting the Shared Key

When setting the shared key via the Sensor Serial Console Port, set it to a value between 6 and 36 characters in length. The shared key must include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note, the AirMagnet Enterprise Server and the sensor use the same shared key.

Protect the shared key from discovery by unauthorized persons. Do not write down the shared key and leave it where others may find them.

Removing the Sensor from Service

When removing the sensor from service for the purpose of discarding it or returning it to the manufacturer for replacement, you must zeroize the module using the **zeroize** command (see [“Zeroizing an AirMagnet Sensor” on page 47](#)). This operation zeroizes all cryptographic keys and CSPs.

Information for Remote Crypto Officers

The remote crypto officer installs and configures the module for secure operation in the FIPS approved mode. The remote crypto officer also maintains the module in the approved mode. Remote crypto officer procedures consist of enabling FIPS approved mode, setting the shared key (if necessary) and setting the browser to communicate with the sensor using TLS.

Installation and configuration for secure operation in the FIPS approved mode and maintenance in the FIPS approved mode of A5023 sensor model must be performed by a Remote Crypto Officer.

Installing and Configuring the Sensor

This section explains the specific steps a remote crypto officer must take to configure the sensor in FIPS approved mode.

With the exceptions or additional steps specified below, follow the instructions in Chapter 3, “Configuring SmartEdge Sensor via Web Browser” as this method provides sensor Web UI commands needed to configure the sensor in FIPS approved mode.

- 1 Examine the sensor shipping container for any signs of tampering. The sensor is shipped in a sealed container that should not be opened except by a crypto officer. If the container shows signs of tampering, contact AirMagnet for a replacement.
- 2 Apply the tamper evident seals as shown in the FIPS Required Features section of Chapter 3.
- 3 Remote crypto officers and users must set their internet browsers to only use the TLS 1.0 protocol to communicate with the sensor. Perform Steps 1 through 16 in Chapter 3, “Configuring SmartEdge Sensor via Web Browser” of this guide as documented. In Step 15 make sure to set the sensor shared key to a value between 6 and 36 characters in length. The shared key must include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note, the AirMagnet Enterprise Server uses the same shared key.
- 4 Proceed to Step 17. Make sure that FIPS Mode drop-down menu item is set to “Enable”. This setting disables Telnet and SSH servers. It also sets the sensor to use TLS instead of SSL for secure communication.
- 5 Perform Steps 18 through 22 as documented.
- 6 Make sure that “Provide all the approved sensors with the updated Sensor Shared Secret” check box is unchecked. This box shall always be unchecked in the FIPS approved mode. See Chapter 12, “Configuring System Settings” for details.
- 7 Make sure that “Enterprise Zero Configuration” check box is unchecked. This box shall always be unchecked in the FIPS approved mode. See Chapter 12, “Configuring System Settings” for details.

The AirMagnet SmartEdge Sensor is now in the FIPS approved mode.

Setting the Shared Key

When setting the shared key via the web interface, set it to a value between 6 and 36 characters in length. The shared key must include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note, the AirMagnet Enterprise Server and the sensor use the same shared key.

Protect the shared key and password from discovery by unauthorized persons. Do not write down the shared key or password and leave them where others may find them.

Removing the Sensor from Service

When removing the A5023 sensor model from service for the purpose of discarding it or returning it to the manufacturer for replacement, you must zeroize the module using the Web UI. This operation zeroizes all cryptographic keys and CSPs. Zeroization of other sensor models must be performed by a local crypto officer using the **zeroize** command as described in “Zeroizing an AirMagnet Sensor” on page 47.

Maintaining the Sensor in FIPS Approved Mode

This section explains the specific steps a remote crypto officer must take to maintain the sensor in the approved mode.

- Remote crypto officers must periodically inspect the module for evidence of tamper by examining the tamper evident seals for signs of tampering and the module itself for any scratches, holes, or dents that may indicate someone has tried to open the module. For frequency of inspection, refer to your organization’s security policy. If a tamper is suspected, the A5023 sensor model must be zeroized (using the Web UI) before it is discarded or returned to the manufacturer. Zeroization of other sensor models must be performed by a local crypto officer using the **zeroize** command as described above.
- Remote crypto officers may run the self-test on demand by rebooting the module. This may be performed as a troubleshooting step. If the self test fails repeatedly, the module must be zeroized, as described above, before it is discarded or returned to the manufacturer for replacement.
- If you need to set the sensor shared key, it must be a value between 6 and 36 characters in length and include at least one upper case character, one lower case character, one numeric character, and one punctuation character. Note the AirMagnet Enterprise Server uses the same shared key.
- Exercise care to prevent unauthorized access to the sensor by setting a shared key that is not easy to guess. The shared key must be at least 6 characters in length and include at least one upper case character, one lower case character, a number, and a punctuation character. Do not write down the shared key and leave it where others may find it.
- Update of sensor application image is only allowed in the FIPS approved mode. The sensor must be returned to the manufacturer for replacement if sensor application image was updated in the non-approved mode.
- Do not disable FIPS approved mode. Do not enable telnet or SSH server.

Setting the Browser to Use TLS

To communicate with the sensor in FIPS approved mode using a browser, remote crypto officers must set the browser to use TLS instead of SSL for secure communication with the sensor.

To configure Internet Explorer to use TLS:

- 1 Start the Internet Explorer program.
- 2 Click Tool s>I nternet Opti ons>Advanced.
- 3 Scroll down and select the setting Use TLS 1. 0.
- 4 Clear the checkboxes for Use SSL 2. 0 and Use SSL 3. 0.
- 5 Click OK.

It is strongly recommended that users completely close all internet browser windows after logging out of the Enterprise Server or Sensor web interfaces. Additionally, users are discouraged from opening multiple tabs in the browser window while logged into the web interface.

Information for Users

Users are responsible setting their browsers to communicate with the sensor using TLS instead of SSL for secure communication. Users must also protect their password from use by unauthorized people.

To configure Internet Explorer to use TLS:

- 1 Start the Internet Explorer program.
- 2 Click Tool s>I nternet Opti ons>Advanced.
- 3 Scroll down and select the setting Use TLS 1. 0.
- 4 Clear the checkboxes for Use SSL 2. 0 and Use SSL 3. 0.
- 5 Click OK.

Protect Your Password

Protect your password from use or discovery by unauthorized persons. Do not *loan* your password to anyone or write it down where others may find it.

Reference Information

- 1 *AirMagnet SmartEdge Sensor AM-5010-11AG, AM-5012-11AG, A5020, and A5023 Security Policy*
- 2 *AirMagnet 5010-11AG User Guide*
- 3 *AirMagnet 5012-11AG User Guide*
- 4 *AirMagnet A5020 Sensor User Guide*
- 5 *AirMagnet A5023 Sensor User Guide*

Appendix G: Installing Oracle Database

AirMagnet Enterprise can use a database to store data collected by AirMagnet SmartEdge Sensors. However, it is important to note that the installation procedures are slightly different when installing AirMagnet Enterprise using Oracle as the database from using the other three database options, i.e., Microsoft SQL or Microsoft Access.

With Microsoft SQL or Microsoft Access, the database will be created automatically and connected to the AirMagnet Enterprise Server while you are installing AirMagnet Enterprise. You do not need to create the database beforehand. With Oracle, however, the database must be set up in advance. This section discusses the procedures on how to set up an Oracle database.

The installation of an Oracle database server for use with the AirMagnet Enterprise involves two major steps:

- 1 First of all, create the database on the Oracle Database server.
- 2 On the machine where the AirMagnet Enterprise Server is to be installed, install the Oracle database Client, make sure that the connection to the Oracle database server from this machine is established successfully, and then install the AirMagnet Enterprise Server.

Creating an Oracle Database

To use an Oracle database to keep information recorded by AirMagnet Management Server, users must first create the database on the Oracle server. Then they must create and configure user profiles to access to the database for writing/reading data. This must be done before installing the AirMagnet Management Server.

To create an Oracle database:

- 1 Click *Start>All Programs>Oracle>Configuration and Migration Tools>Database Configuration Assistant*. A welcome page will appear. See Figure J-1.

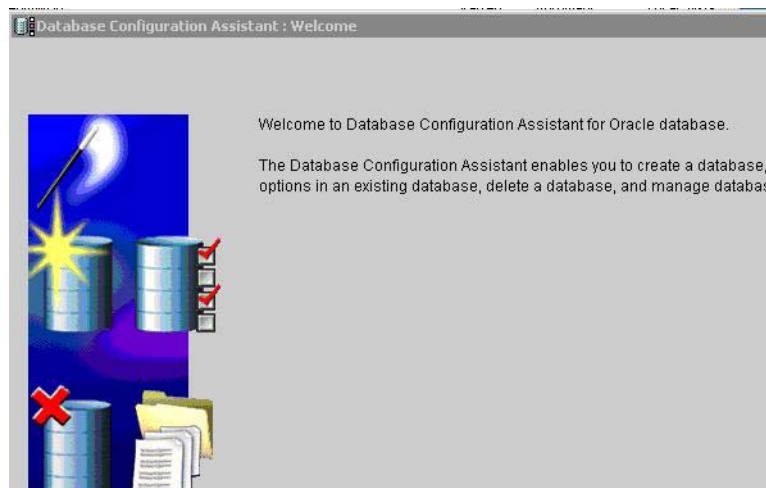


Figure G-1:Welcome Screen

- 2 Click *Next*. The Operations selection screen will appear. See Figure J-2.

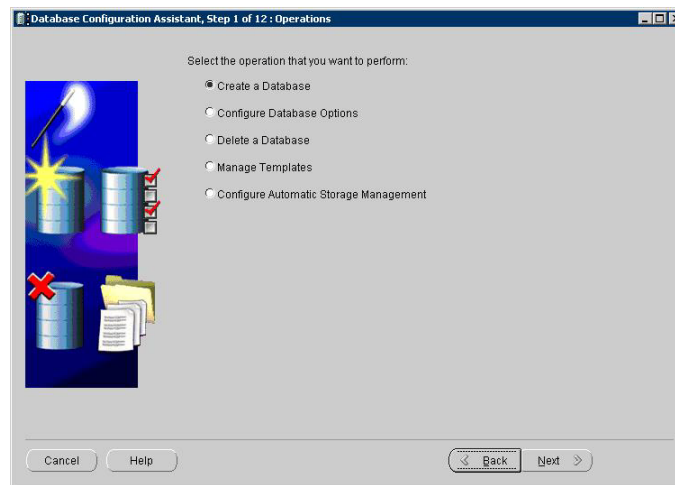


Figure G-2:Operations Selection Screen

- 3 Select *Create a Database* and click *Next*. The *Database Templates* screen appears. See Figure J-3.

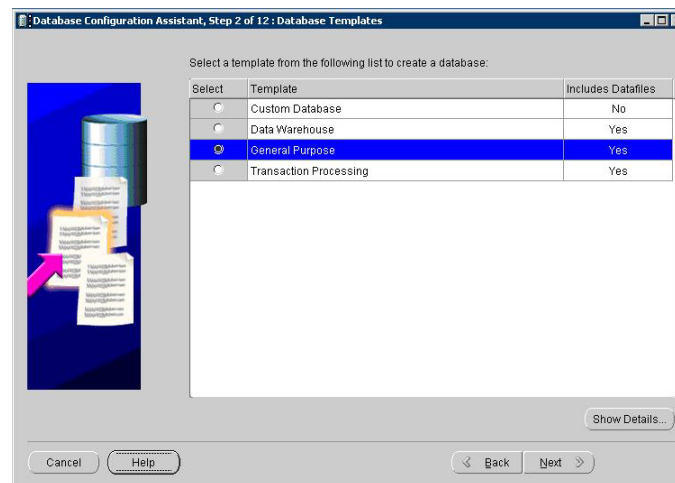
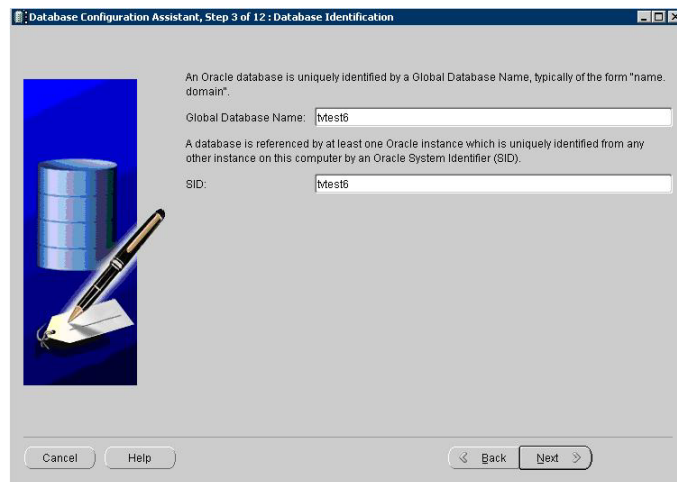


Figure G-3:Templates Selection

- 4 Select *General Purpose* and click *Next*. The *Database Identification* screen appears. See Figure J-4.



Database Configuration Assistant, Step 3 of 12: Database Identification

An Oracle database is uniquely identified by a Global Database Name, typically of the form "name.domain".

Global Database Name:

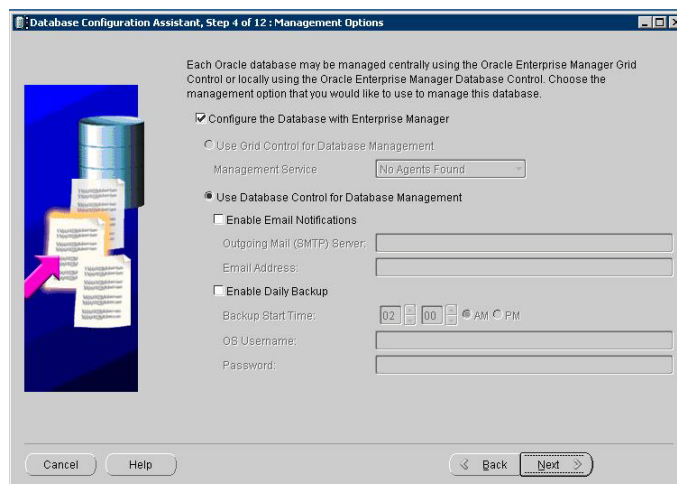
A database is referenced by at least one Oracle instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

Cancel Help Back Next

Figure G-4:Database Identification Options

- 5 Enter your database name in the fields provided and click *Next*. The *Management Options* screen appears. See Figure J-5.



Database Configuration Assistant, Step 4 of 12: Management Options

Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.

☒ Configure the Database with Enterprise Manager

☐ Use Grid Control for Database Management

Management Service:

☒ Use Database Control for Database Management

☐ Enable Email Notifications

Outgoing Mail (SMTP) Server:

Email Address:

☐ Enable Daily Backup

Backup Start Time: : : AM PM

OS Username:

Password:

Cancel Help Back Next

Figure G-5:Management Options

- 6 Leave the options as shown above and click *Next*. The *Database Credentials* screen appears. See Figure J-6.

Database Configuration Assistant, Step 5 of 12: Database Credentials

For security reasons, you must specify passwords for the following user accounts in the new database.

☒ Use the Same Password for All Accounts

Password:

Confirm Password:

☐ Use Different Passwords

User Name	Password	Confirm Password
SYS		
SYSTEM		
DBSNMP		
SYSMAN		

Cancel Help Back Next

Figure G-6:Database Credentials

- 7 Enter a password. The database's default user name, "System", will use this entry as its password. Click *Next*. The *Storage Options* screen appears. See Figure J-7.

Database Configuration Assistant, Step 6 of 12: Storage Options

Select the storage mechanism you would like to use for the database.

☒ File System
Use the File System for Database storage.

☐ Automatic Storage Management (ASM)
Automatic Storage Management simplifies database storage administration and optimizes database layout for I/O performance. To use this option you must either specify a set of disks to create an ASM disk group or specify an existing ASM disk group.

☐ Raw Devices
Raw partitions or volumes can provide the required shared storage for Real Application Clusters (RAC) databases if you do not use Automatic Storage Management and a Cluster File System is not available. You need to have created one raw device for each datafile, control file, and log file you are planning to create in the database.

☐ Specify Raw Devices Mapping File Browse...

Cancel Help Back Next Finish

Figure G-7:Storage Options

- 8 Use the default settings (shown above) and click *Next*. The *Database File Locations* screen appears. See Figure J-8.

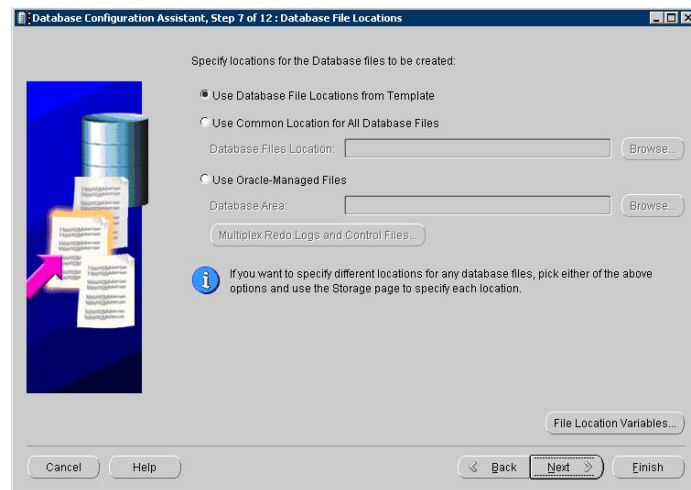


Figure G-8:Database File Locations

- 9 Use the default settings (shown above) and click *Next*. The *Recovery Configuration* screen appears. See Figure J-9.

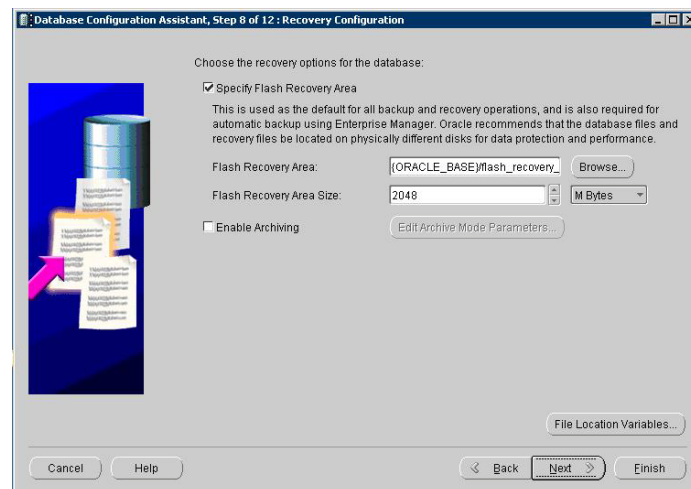


Figure G-9:Recovery Configuration

- 10 Use the default settings (shown above) and click *Next*. The *Database Content* screen appears. See Figure J-10.

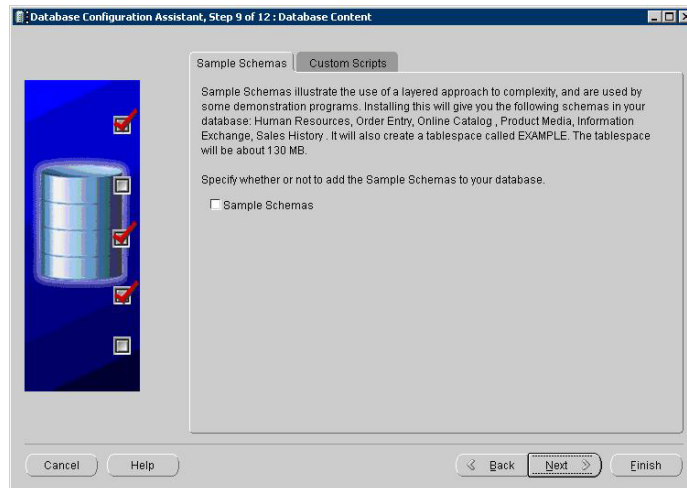


Figure G-10:Database Content

- 11 Use the default settings (shown above) and click *Next*. The *Initialization Parameters* screen appears. See Figure J-11.

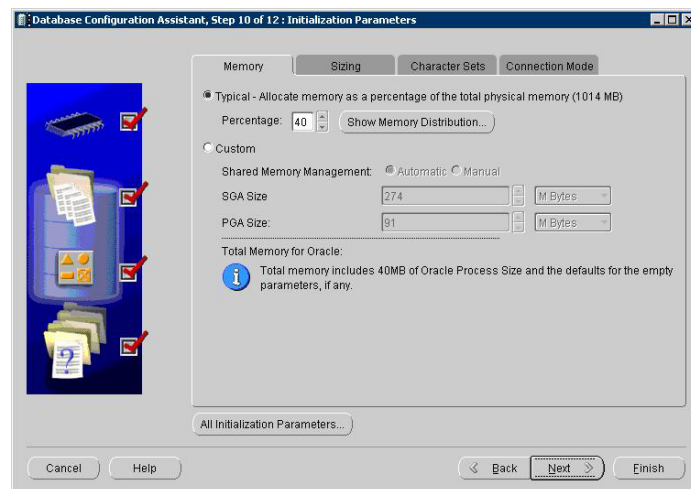


Figure G-11:Initialization Parameters

- 12 Use the default settings (shown above) and click *Next*. The *Database Storage* screen appears. See Figure J-12.

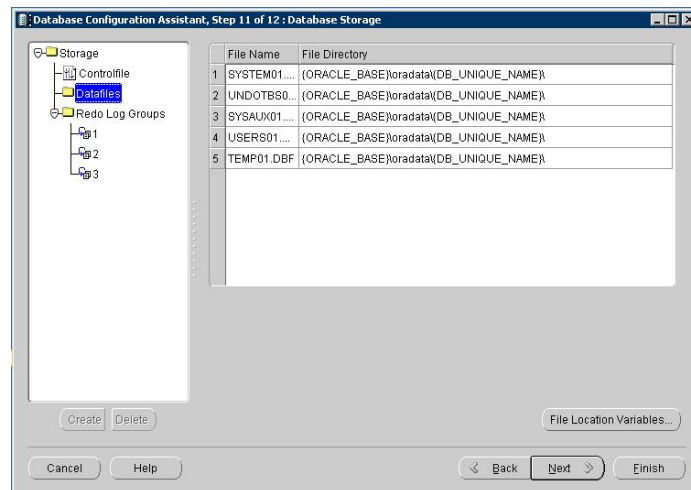


Figure G-12: Database Storage

- 13 Use the default settings (shown above) and click *Next*. The *Creation Options* screen appears. See Figure J-13.

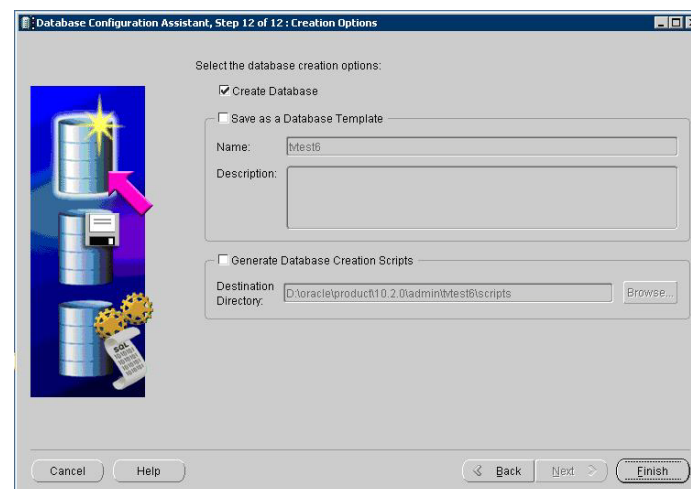


Figure G-13: Creation Options

- 14 Use the default settings (shown above) and click *Next*. The *Confirmation* screen appears. Click *OK* to continue.
- 15 When the creation process completes, the Database Configuration Assistant dialog appears to show that the process has finished.

Now that the database has been created, perform the steps in the following section to create user accounts for the new database.

Creating User Profiles

The database's default user name (system) acts as a master user account. Consequently, it has access privileges beyond those required for most users. To limit access to the database, create a new account with access privileges specific to the tasks required. In this case, the user needs to logon to the Oracle database, create tables, and read and write to the database to store information that is passed over from the AirMagnet Enterprise server.

To create a user account:

- 1 Click *Start>All Programs>Oracle>Database Control - [your database name]*. This will launch an internet browser window to the database login page. See Figure J-14.

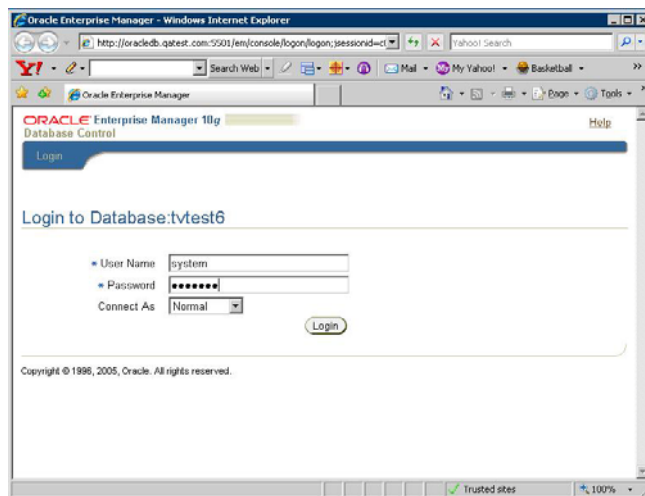


Figure G-14: Database Login Page

- 2 Enter "system" for the user name and your password from step 7 of the previous section and click *Login*. The *Oracle Database 10g Licensing Information* page will appear. See Figure J-15.

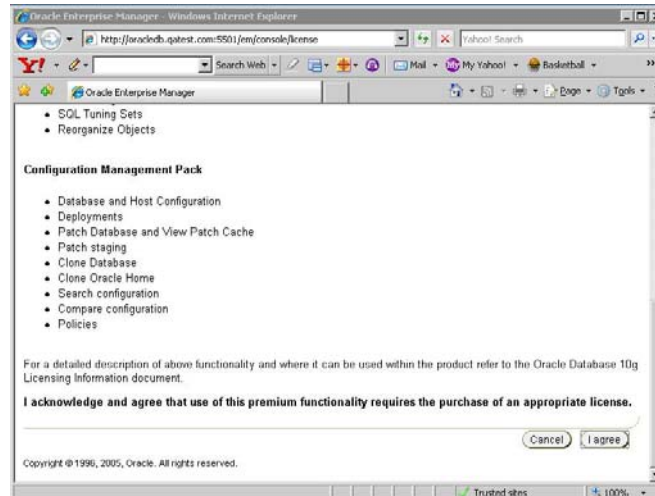


Figure G-15:Licensing Information

- 3 Review the agreement and click *I agree* at the end to continue. The screen for your database will appear. See Figure J-16.

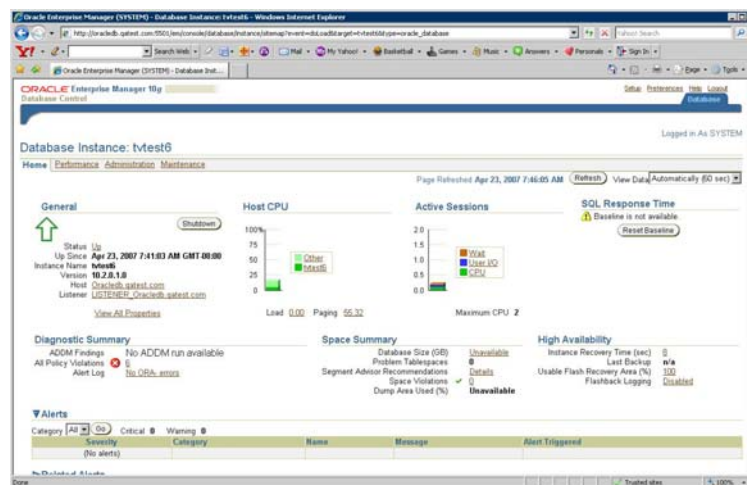


Figure G-16:Database Instance Page

- Click on the *Administration* tab and locate the *Users & Privileges* section on the resulting screen. See Figure J-17.

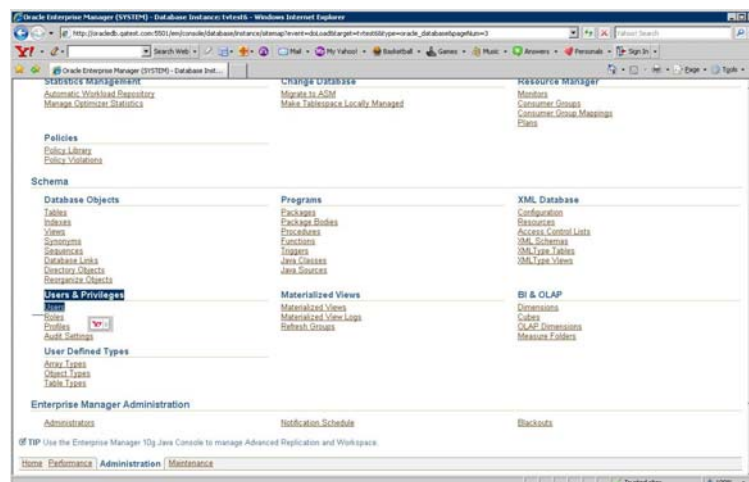


Figure G-17:Users & Privileges Section

- Click the *Users* link to display current database users. See Figure J-18.

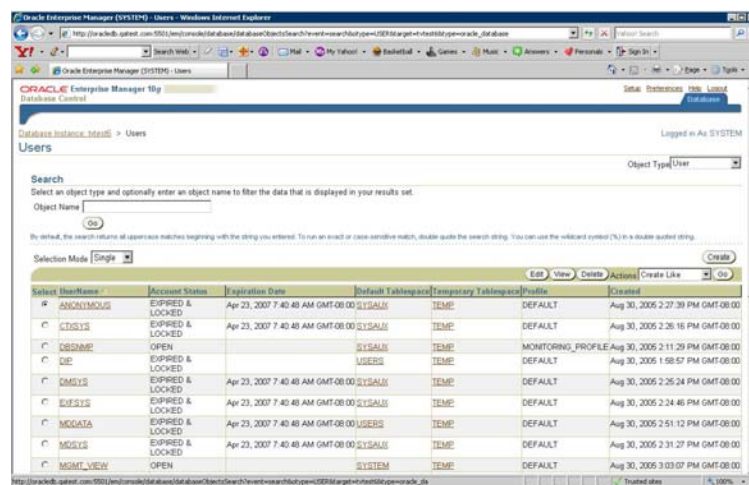


Figure G-18:Current Users

- 6 Click *Create* to create a new user account to work with the database. The *Create User* page will appear. See Figure J-19.

Figure G-19: Create User Page

- 7 Enter a user name and password for the new user account.
- 8 Click the Flashlight icon next to the *Default Tablespace* field. In the resulting dialog, select *USERS* and click *Select*.
- 9 Click the Flashlight icon next to the *Temporary Tablespace* field. In the resulting dialog, select *TEMP* and click *Select*.
- 10 Click *OK* to save the new user.
- 11 Navigate back to the *Users* page. The newly-created user account should appear in the list as a link. Click it to view the account details. See Figure J-20.

Figure G-20: User Settings

- 12 Click **Roles**. On the resulting screen, click **Edit List** to bring up the *Modify Roles* screen. See Figure J-21.

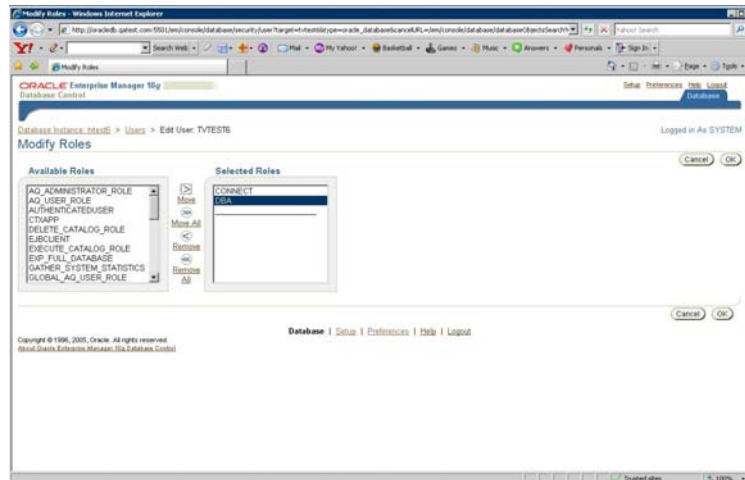


Figure G-21: Modify Roles

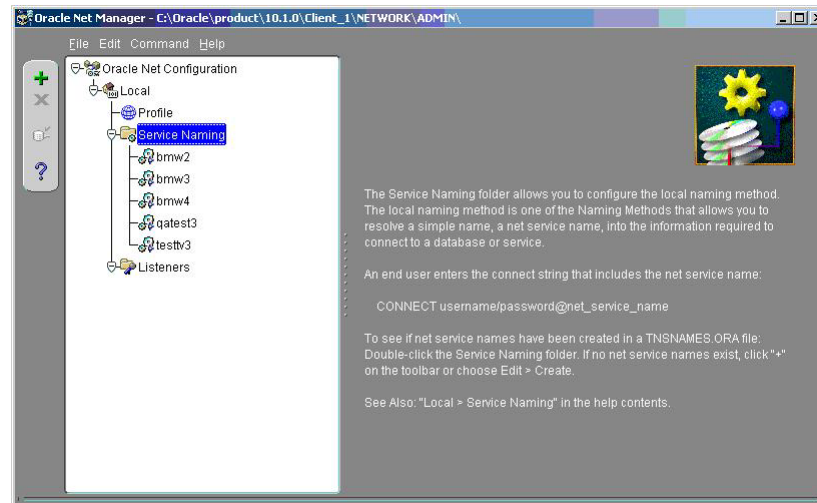
- 13 From the *Available Roles* list to the left, click **DBA** and click **Move** to move it into the *Selected Roles* list. Click **OK** to save the modification.
- 14 On the *User* page, check the *Admin Options* for both roles listed (**CONNECT** and **DBA**).
- 15 Click the *System Privileges* link. On the resulting screen, click **Edit List** to bring up the *Modify System Privileges* page.
- 16 This page works similarly to the *Modify Roles* screen described previously. Select the following privileges from the *Available System Privileges* list (hold the **Ctrl** key to make multiple selections):
- **CREATE SEQUENCE**
 - **CREATE SESSION**
 - **CREATE TABLE**
 - **CREATE VIEW**
 - **ALTER TABLE**
- 17 Click **Move** to move them into the *Selected System Privileges* area and click **OK**.
- 18 On the *System Privileges* screen, check the *Admin Option* field for all the new options.
- 19 Click **Apply** to save all changes.

Configuring Oracle Client

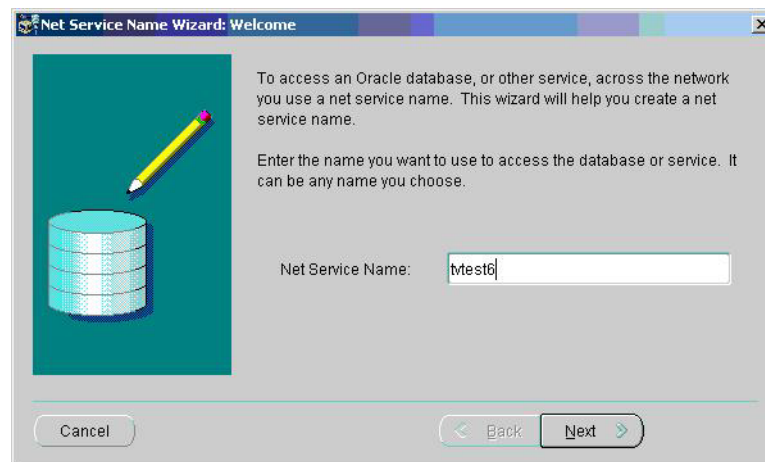
Now that the database and user account have been created, the computer acting as the Enterprise server must have the Oracle Client installed on it. The client must then be configured properly so that it can communicate with the Oracle Server.

To configure the Oracle client:

- 1 Click *Start>All Programs>Oracle>Configuration and migration Tools>Net Manager*. The Net Manager will appear. See Figure J-22.

**Figure G-22:Net Manager Screen**

- 2 Click *Service Naming* and then click the '+' at the top right of the screen. The *Net Service Name Wizard* will appear. See Figure J-23.

**Figure G-23:Name Wizard**

- 3 In the *Net Service Name* field, enter the name of the Oracle database created in the preceding sections. Click *Next* to continue. The *Protocol* screen appears. See Figure J-24.

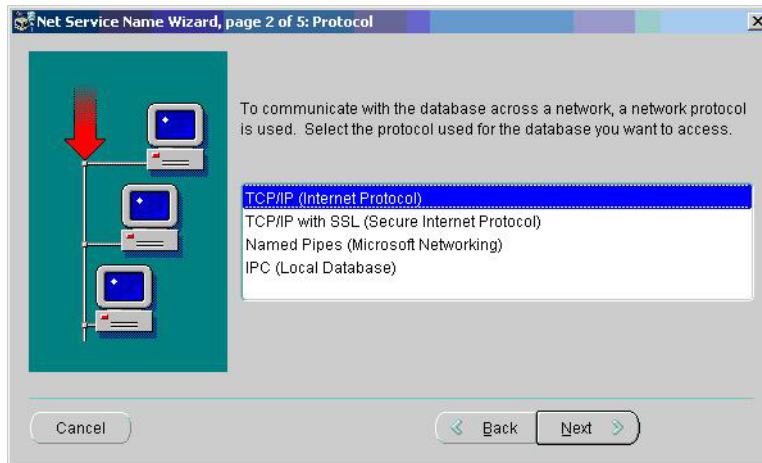


Figure G-24: Protocol Selection

- 4 Select *TCP/IP (Internet Protocol)* and click *Next* to continue. The *Protocol Settings* screen appears. See Figure J-25.

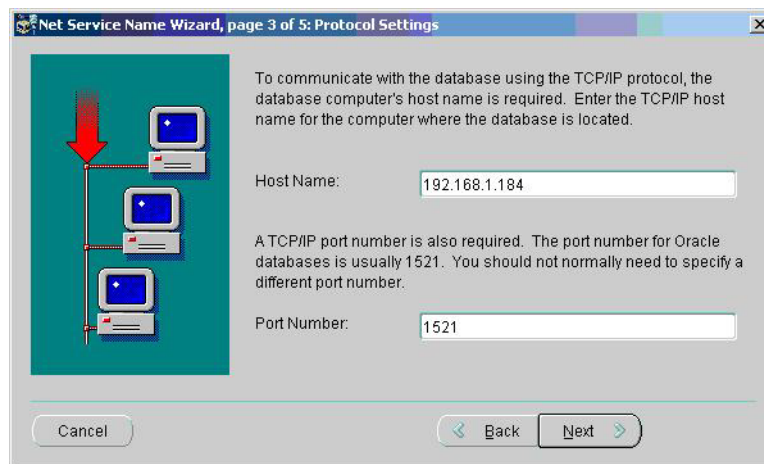


Figure G-25: Protocol Settings

- 5 In the *Host Name* field, enter the IP address of the Oracle server. Leave the *Port Number* field at the default and click *Next*. The *Service* screen appears. See Figure J-26.

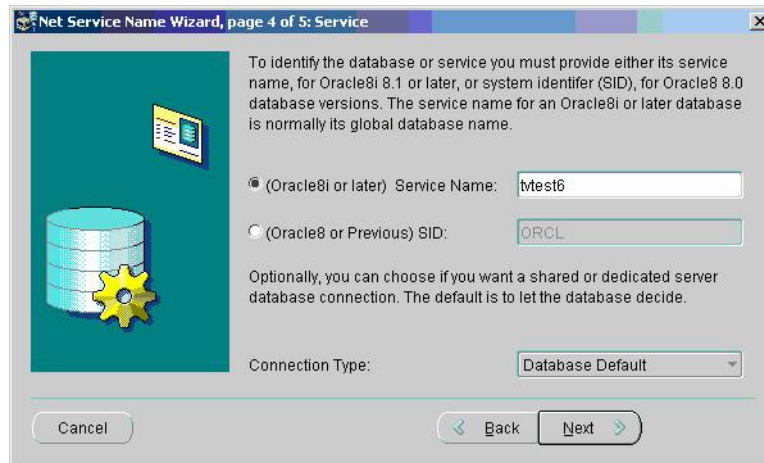


Figure G-26:Service Configuration

- 6 Verify that *(Oracle 8i or later) Service Name:* is selected and enter the name specified for the service in step 3 above. Click *Next* to continue. The *Test* screen appears. See Figure J-27.

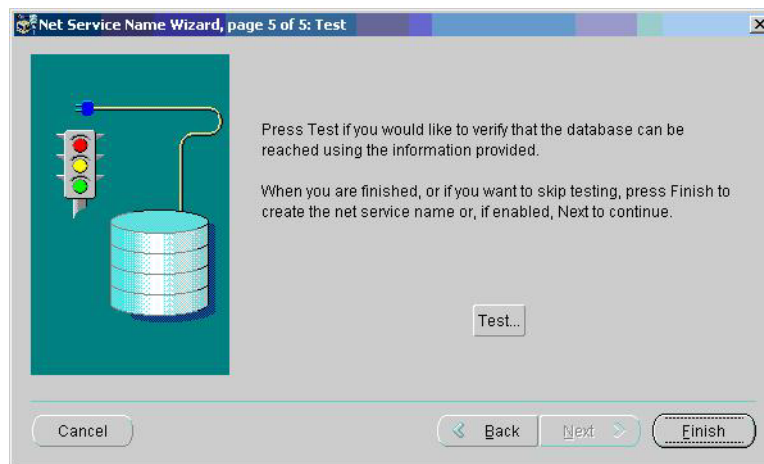


Figure G-27:Test Screen

- 7 Click *Test...* to test the connection between the client and server. The *Connection Test* screen will appear, displaying the test's progress. See Figure J-28.

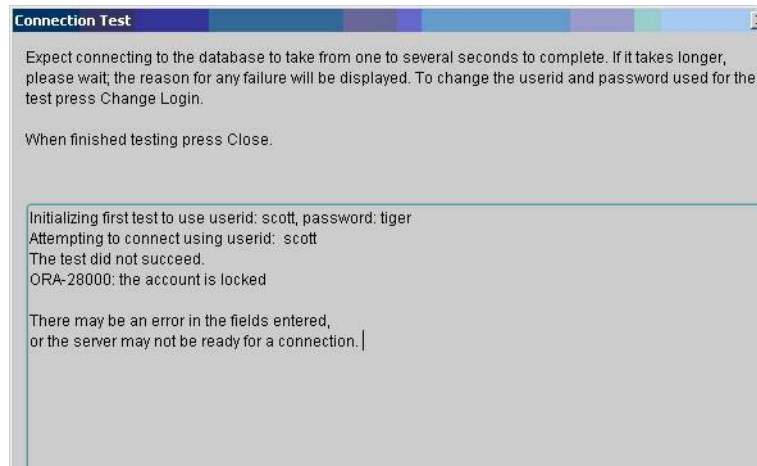


Figure G-28:Connection Test Progress

- 8 It is important to note that the first test will **always** fail. By default, the connection test attempts to specify "scott" as the user name and "tiger" as the password. These fields must be changed for the test to succeed. Click the *Change Login* button.
- 9 In the *Login Information* screen, enter the user name and password specified for the database during creation (in the steps earlier in this chapter). Click *OK* to return to the test screen.
- 10 Click *Test* again to retry the test. If the user information was entered correctly, the test should be successful, which means that the client can now communicate with the server using the new database. See Figure J-29.

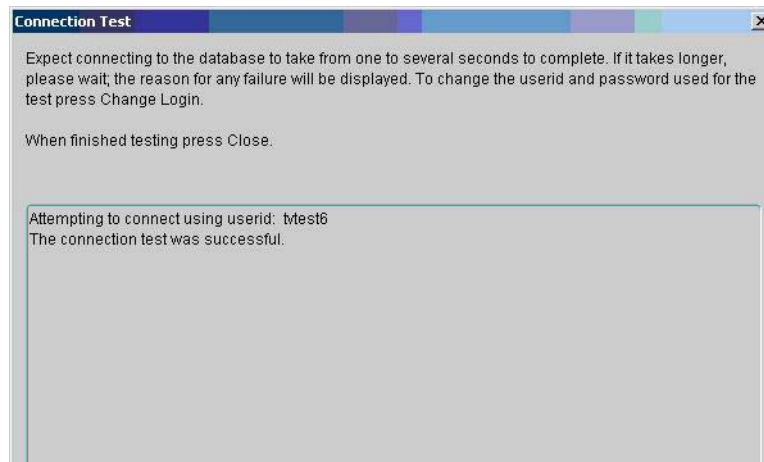


Figure G-29:Connection Successful

- 11 Click *Close* to exit the *Connection Test* screen.
- 12 Click *Finish* to complete the setup process. The *Net Manager* screen will appear again.

- 13 Click *File>Save Network Configuration* to save the changes. The Oracle client is now properly configured.

Using an Oracle Database Server

To use an Oracle database server with the AirMagnet Enterprise:

- 1 When prompted to select a database (during AirMagnet Enterprise installation), select the Oracle Database. See Figure J-30.

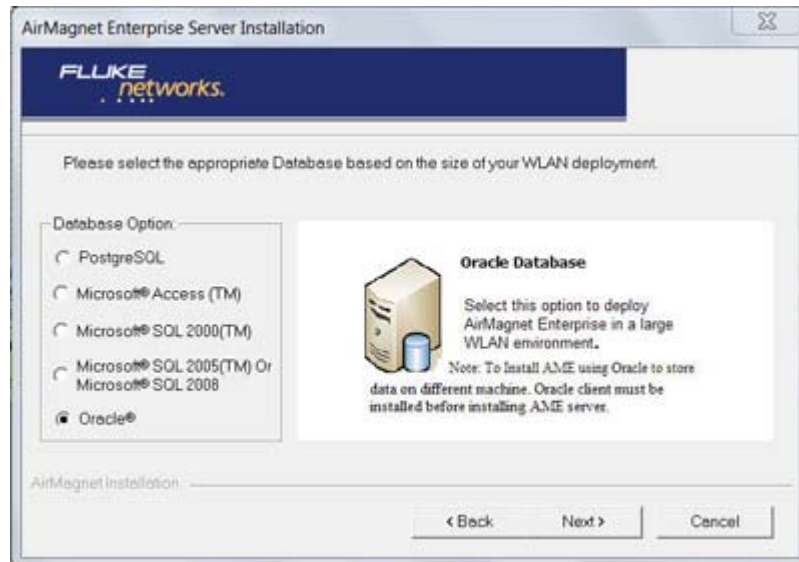


Figure G-30:Using Oracle database

- 2 Click **Next**. The Setting up Database Server dialog box appears. See Figure J-31.

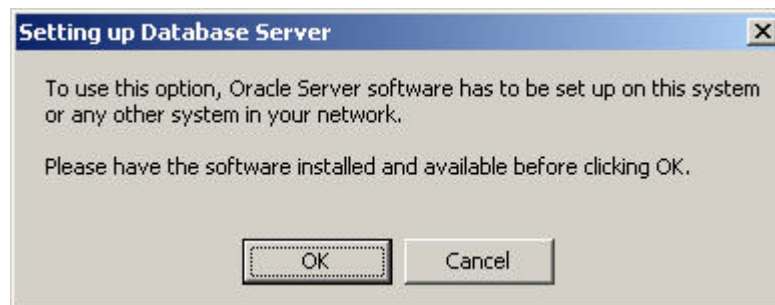


Figure G-31:Setting up Database Server

- 3 Assuming that you have already set up an Oracle database for use with the AirMagnet Enterprise, click **OK**. The AirMagnet Database Connection Utility dialog box appears. See Figure J-32.

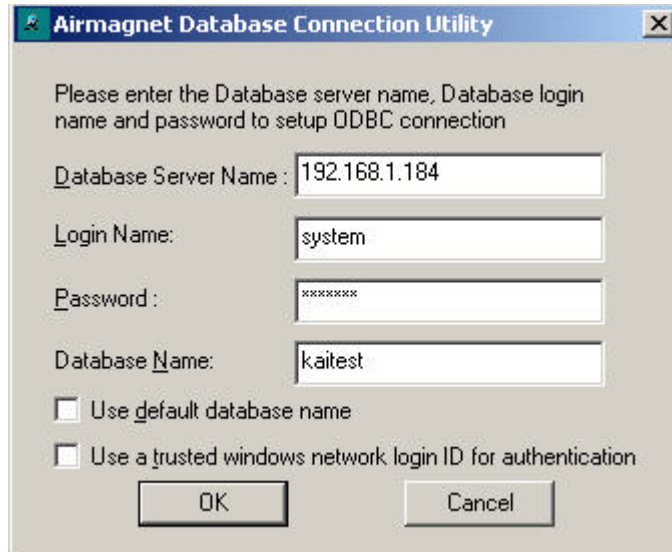


Figure G-32: AirMagnet Database Connection Utility

- 4 In the dialog box, make the required entries or selections as described below.
 - **Database Server Name** – The name or IP address of the Oracle database server.
 - **Login Name** – This can “system” or a user account that is associated with the database. See the previous sections for how to configure the database properly.
 - **Password** – The password for the system user at the time the database is created or the password for a user at the time with which a user account is set up.
 - **Database name** – The name given to the database when it was created.

- 5 Click **OK**. The Oracle ODBC Driver Connect dialog box appears. See Figure J-33.



Figure G-33:Oracle ODBC Driver Connect

- 6 From the Oracle ODBC Driver Connect dialog box, make the entries as described below:
 - Service Name — The name of the database on the server.
 - User Name — The Login Name used previously.
 - Password — The password used to access the database.
- 7 Click **OK**.

If all the information you have entered is correct, the connection to the Oracle database will be established. The AirMagnet Enterprise Server Installation will continue on the screen. Refer to “AirMagnet Enterprise Server Installation” on page 15 for installation instructions.

Appendix H: Installing PostgreSQL Database

AirMagnet Enterprise can use PostgreSQL database to store data collected by AirMagnet SmartEdge Sensors. However, it is important to note that the installation procedures are slightly different when installing AirMagnet Enterprise using PostgreSQL as the database from using two other database options, i.e., Microsoft SQL or Microsoft Access.

With Microsoft SQL or Microsoft Access, the database will be created automatically and connected to the AirMagnet Enterprise Server while you are installing AirMagnet Enterprise. You do not need to create the database beforehand. With PostgreSQL, however, the database must be set up in advance. This section discusses the procedures on how to set up a PostgreSQL database.

The installation of a PostgreSQL database server for use with the AirMagnet Enterprise involves three major steps:

- 1 Setting up the PostgreSQL database.
- 2 Creating a new AirMagnet database.
- 3 Installing AirMagnet Enterprise.

Setting up the PostgreSQL Database

To use a PostgreSQL database to keep information recorded by AirMagnet Management Server, users must first create the database on the PostgreSQL server. Then they must create and configure user profiles to access to the database for writing/reading data. This must be done before installing the AirMagnet Management Server.

To setup a PostgreSQL database:

- 1 In the setup welcome screen, click *Next*. See Figure K-1.

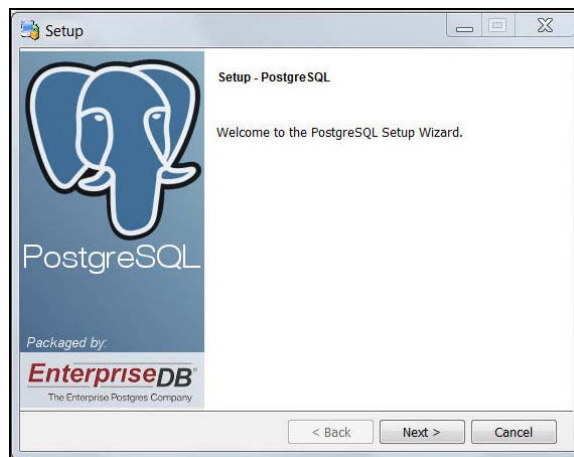


Figure H-1:Welcome Screen

- 2 Specify the directory where PostgreSQL should be installed. Click *Next*. The Data Directory screen will appear. See Figure K-2.

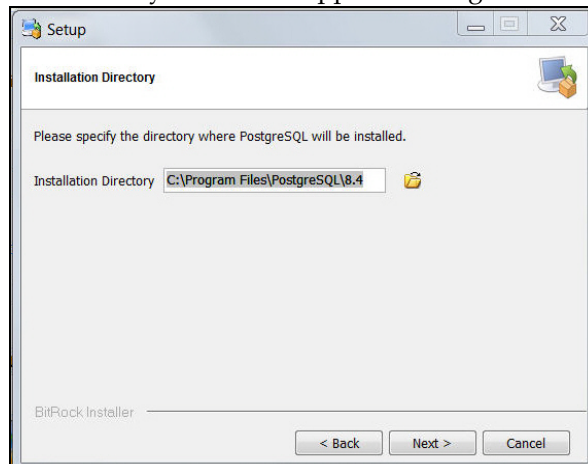


Figure H-2:Installation Directory Screen

- 3 Select a directory to where you will be storing your data and click *Next*. See Figure K-3.

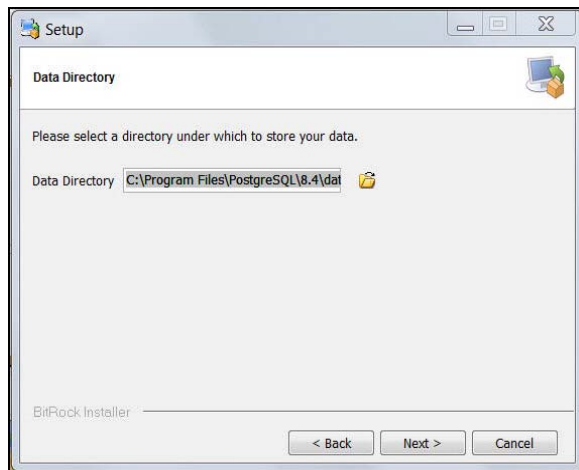


Figure H-3:Data Directory Screen

- 4 The setup is now complete. Click Next to begin installation. The *Database Identification* screen appears. See Figure K-4.

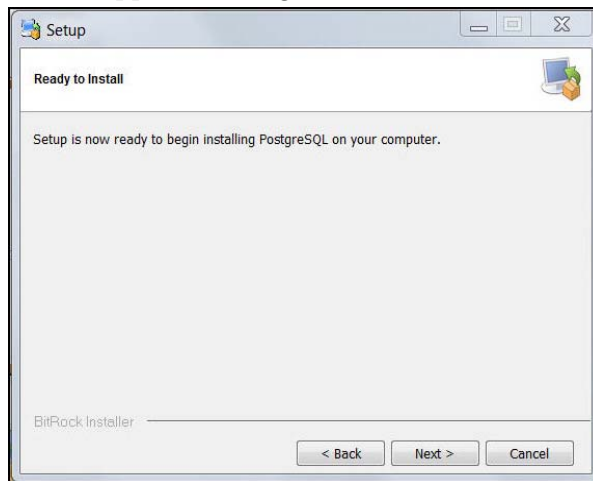


Figure H-4:PostgreSQL Installation Screen

- 5 The installation is now complete. Click *Next*. See Figure K-5.

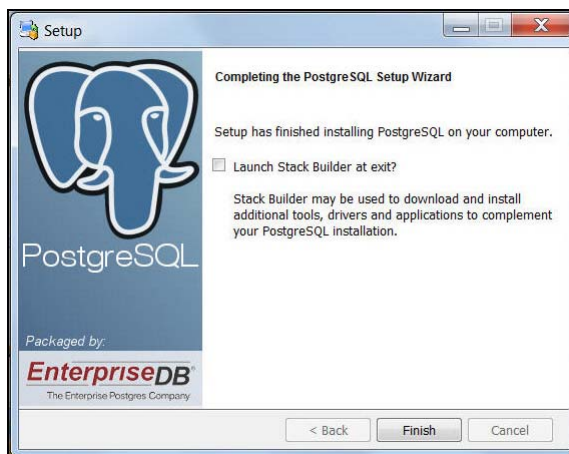


Figure H-5:PostgreSQL Setup Complete

Creating a new AirMagnet Database

You must now log into the PostgreSQL database server and create a blank AirMagnet database for the installation to use.

- 6 Browse to the pgAdmin III PostgreSQL Tools application. The following screen will appear. Double-click on the server name. See Figure K-6.

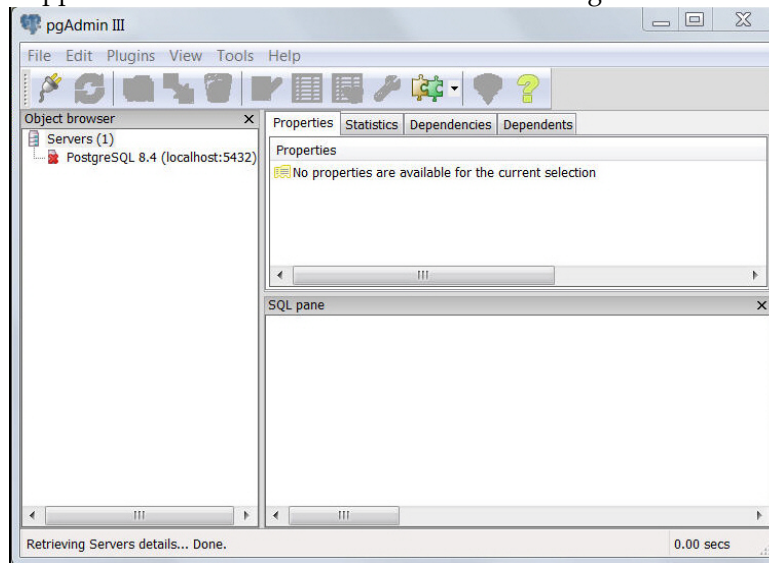


Figure H-6:Database Credentials

- 7 Enter a password for user postgres (use same password that was used during installation) Two databases will appear. See Figure K-7.

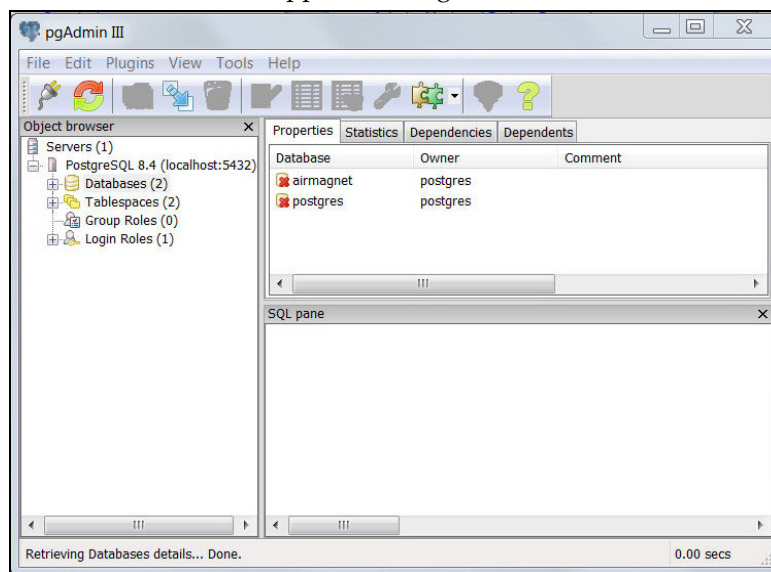


Figure H-7:Storage Options

- 8 Select Databases and right click. Click on **New Database...** Enter all required information and click OK. You have now completed Configuration.

Installing AirMagnet Enterprise

Note: Prior to installing AirMagnet Enterprise with PostgreSQL database, you must first install the ODBC driver.

- 9 On your CD, you will find `psqlodbc` installation file. Run that file. The ODBC welcome screen will appear. Click *Next*. See Figure K-8.

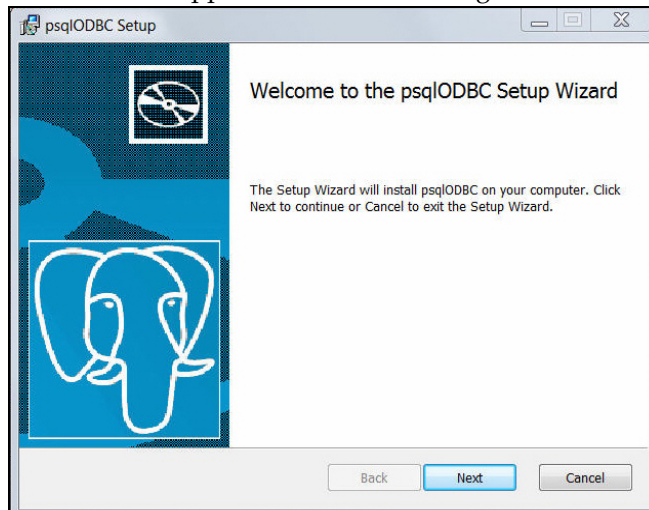


Figure H-8: ODBC Driver Setup

- 10 Click *Next* to install the ODBC driver. Follow the screen by clicking *Install*. See Figure K-9.

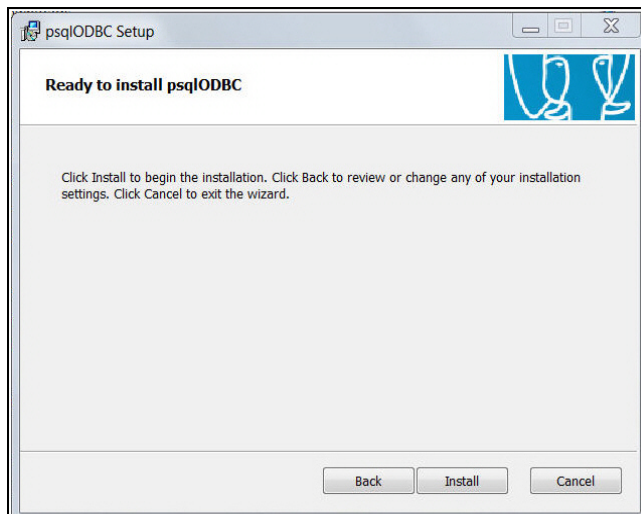


Figure H-9: ODBC Driver Ready to Install

- 11 The ODBC driver has now been installed. Click *Finish*. See Figure K-10.

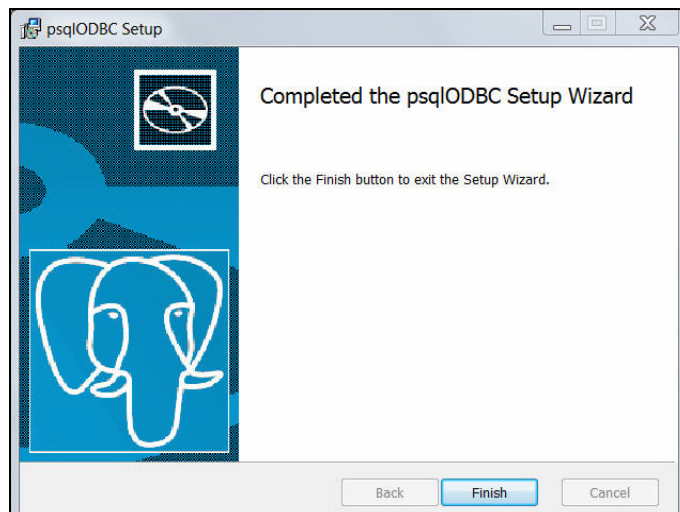


Figure H-10:ODBC Driver Setup Complete

The ODBC driver has now been installed. You can now install AirMagnet Enterprise with PostgreSQL database.

- 12 Launch installation from the provided CD and click on Enterprise installation. See Figure K-11.

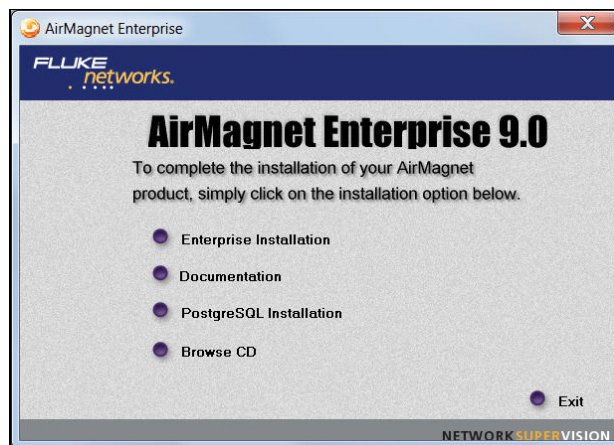


Figure H-11:Enterprise Installation

- 13 Select the PostgreSQL database and click Next. See Figure K-12.

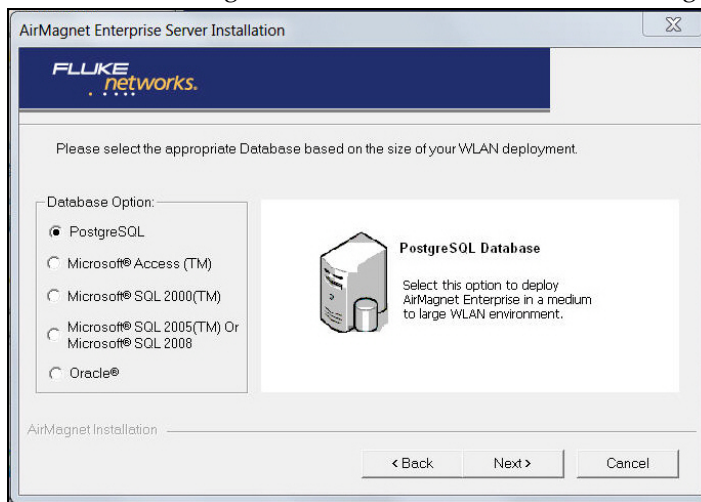


Figure H-12:Database Options

- 14 Enter all necessary information in to fields and click OK to continue. See figure K-13.

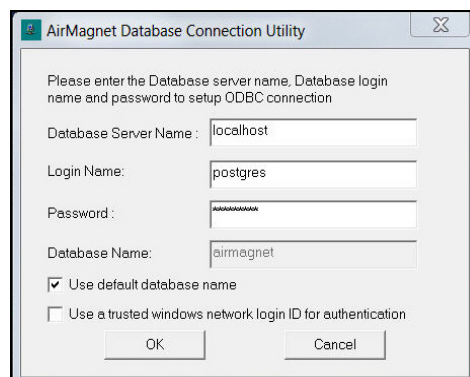


Figure H-13:Database Login Screen

- 15 Continue with AirMagnet Enterprise Installation. For further details, refer to Chapter 2 of user guide.

Appendix I: Third-Party Copyrights

D. Young Copyright

Copyright (c) 2003, 2004 David Young. All rights reserved.

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

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

THIS SOFTWARE IS PROVIDED BY DAVID 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 DAVID YOUNG 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.

A. Onoe & S. Leffler Copyright

Copyright (c) 2001 Atsushi Onoe

Copyright (c) 2002-2005 Sam Leffler, Errno Consulting

All rights reserved.

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

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

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

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.

S. Leffler Copyright

Copyright (c) 2002-2005 Sam Leffler, Errno Consulting

All rights reserved.

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

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

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

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.

B. Paul Copyright

Copyright (c) 1997, 1998, 1999

Bill Paul <wpaul@ctr.columbia.edu>. All rights reserved.

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

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by Bill Paul.
- 4 Neither the name of the author nor the names of any co-contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY Bill Paul 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 Bill Paul OR THE VOICES IN HIS HEAD 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.

Apache License

Version 2.0, January 2004

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

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

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

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

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

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

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

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

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

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

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

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

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

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

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

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

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

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

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

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

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

END OF TERMS AND CONDITIONS

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

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

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

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

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

GNU Library General Public License

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example,

Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND

FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <<http://www.gnu.org/licenses/>>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type ``show w'`.

This is free software, and you are welcome to redistribute it under certain conditions; type ``show c'` for details.

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary.

For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License.

Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Go Ahead License Agreement

THIS LICENSE ALLOWS ONLY THE LIMITED USE OF GO AHEAD SOFTWARE, INC. PROPRIETARY CODE. PLEASE CAREFULLY READ THIS AGREEMENT AS IT PERTAINS TO THIS LICENSE, YOU CERTIFY THAT YOU WILL USE THE SOFTWARE ONLY IN THE MANNER PERMITTED HEREIN.

1. Definitions.

1.1 "Documentation" means any documentation GoAhead includes with the Original Code.

1.2 "GoAhead" means Go Ahead Software, Inc.

1.3 "Intellectual Property Rights" means all rights, whether now existing or hereinafter acquired, in and to trade secrets, patents, copyrights, trademarks, know-how, as well as moral rights and similar rights of any type under the laws of any governmental authority, domestic or foreign, including rights in and to all applications and registrations relating to any of the foregoing.

1.4 "License" or "Agreement" means this document.

1.5 "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications.

1.6 "Original Code" means the Source Code to GoAhead's proprietary computer software entitled GoAhead WebServer.

1.7 "Response Header" means the first portion of the response message output by the GoAhead WebServer, containing but not limited to, header fields for date, content-type, server identification and cache control.

1.8 "Server Identification Field" means the field in the Response Header which contains the text "Server: GoAhead-Webs".

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

2. Source Code License.

2.1 Limited Source Code Grant.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims, to use, reproduce, modify, copy and distribute the Original Code.

2.2 Binary Code.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license to copy and distribute the binary code versions of the Original Code together with Your Modifications.

2.3 License Back to GoAhead.

You hereby grant in both source code and binary code to GoAhead a world-wide, royalty-free, non-exclusive license to copy, modify, display, use and sublicense any Modifications You make that are distributed or planned for distribution. Within 30 days of either such event, You agree to ship to GoAhead a file containing the Modifications (in a media to be determined by the parties), including any programmers' notes and other programmers' materials. Additionally, You will provide to GoAhead a complete description of the product, the product code or model number, the date on which the product is initially shipped, and a contact name, phone number and e-mail address for future correspondence. GoAhead will keep confidential all data specifically marked as such.

2.4 Restrictions on Use.

You may sublicense Modifications to third parties such as subcontractors or OEM's provided that You enter into license agreements with such third parties that bind such third parties to all the obligations under this Agreement applicable to you and that are otherwise substantially similar in scope and application to this Agreement.

3. Term.

This Agreement and license are effective from the time You accept the terms of this Agreement until this Agreement is terminated. You may terminate this Agreement at any time by uninstalling or destroying all copies of the Original Code including any and all binary versions and removing any Modifications to the Original Code existing in any products. This Agreement will terminate immediately and without further notice if You fail to comply with any provision of this Agreement. All restrictions on use, and all other provisions that may reasonably be interpreted to survive termination of this Agreement, will survive termination of this Agreement for any reason. Upon termination, You agree to uninstall or destroy all copies of the Original Code, Modifications, and Documentation.

4. Trademarks and Brand.

4.1 License and Use.

GoAhead hereby grants to You a limited world-wide, royalty-free, non-exclusive license to use the GoAhead trade names, trademarks, logos, service marks and product designations posted in Exhibit A (collectively, the "GoAhead Marks") in connection with the activities by You under this Agreement. Additionally, GoAhead grants You a license under the terms above to such GoAhead trademarks as shall be identified at a URL (the "URL") provided by GoAhead. The use by You of GoAhead Marks shall be in accordance with GoAhead's trademark policies regarding trademark usage as established at the web site designated by the URL, or as otherwise communicated to You by GoAhead at its sole discretion. You understand and agree that any use of GoAhead Marks in connection with this Agreement shall not create any right, title or interest in or to such GoAhead Marks and that all such use and goodwill associated with GoAhead Marks will inure to the benefit of GoAhead.

4.2 Promotion by You of GoAhead WebServer Mark.

In consideration for the licenses granted by GoAhead to You herein, You agree to notify GoAhead when You incorporate the GoAhead WebServer in Your product and to inform GoAhead when such product begins to ship. You agree to promote the Original Code by prominently and visibly displaying a graphic of the GoAhead WebServer mark on the initial web page of Your product that is displayed each time a user connects to it. You also agree that GoAhead may identify your company as a user of the GoAhead WebServer in conjunction with its own marketing efforts. You may further promote the Original Code by displaying the GoAhead WebServer mark in marketing and promotional materials such as the home page of your web site or web pages promoting the product.

4.3 Placement of Copyright Notice by You.

You agree to include copies of the following notice (the "Notice") regarding proprietary rights in all copies of the products that You distribute, as follows: (i) embedded in the object code; and (ii) on the title pages of all documentation. Furthermore, You agree to use commercially reasonable efforts to cause any licensees of your products to embed the Notice in object code and on the title pages or relevant documentation. The Notice is as follows: Copyright (c) 20xx GoAhead Software, Inc. All Rights Reserved. Unless GoAhead otherwise instructs, the year 20xx is to be replaced with the year during which the release of the Original Code containing the notice is issued by GoAhead. If this year is not supplied with Documentation, GoAhead will supply it upon request.

4.4 No Modifications to Server Identification Field.

You agree not to remove or modify the Server identification Field contained in the Response Header as defined in Section 1.6 and 1.7.

5. Warranty Disclaimers.

THE ORIGINAL CODE, THE DOCUMENTATION AND THE MEDIA UPON WHICH THE ORIGINAL CODE IS RECORDED (IF ANY) ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EXPRESS, STATUTORY OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The entire risk as to the quality and performance of the Original Code (including any Modifications You make) and the Documentation is with You. Should the Original Code or the Documentation prove defective, You (and not GoAhead or its distributors, licensors or dealers) assume the entire cost of all necessary servicing or repair. GoAhead does not warrant that the functions contained in the Original Code will meet your requirements or operate in the combination that You may select for use, that the operation of the Original Code will be uninterrupted or error free, or that defects in the Original Code will be corrected. No oral or written statement by GoAhead or by a representative of GoAhead shall create a warranty or increase the scope of this warranty.

GOAHEAD DOES NOT WARRANT THE ORIGINAL CODE AGAINST INFRINGEMENT OR THE LIKE WITH RESPECT TO ANY COPYRIGHT, PATENT, TRADE SECRET, TRADEMARK OR OTHER PROPRIETARY RIGHT OF ANY THIRD PARTY AND DOES NOT WARRANT THAT THE ORIGINAL CODE DOES NOT INCLUDE ANY VIRUS, SOFTWARE ROUTINE OR OTHER SOFTWARE DESIGNED TO PERMIT UNAUTHORIZED ACCESS, TO DISABLE, ERASE OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY OTHER SUCH ACTIONS.

Any warranties that by law survive the foregoing disclaimers shall terminate ninety (90) days from the date You received the Original Code.

6. Limitation of Liability.

YOUR SOLE REMEDIES AND GOAHEAD'S ENTIRE LIABILITY ARE SET FORTH ABOVE. IN NO EVENT WILL GOAHEAD OR ITS DISTRIBUTORS OR DEALERS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE ORIGINAL CODE, THE INABILITY TO USE THE ORIGINAL CODE, OR ANY DEFECT IN THE ORIGINAL CODE, INCLUDING ANY LOST PROFITS, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You agree that GoAhead and its distributors and dealers will not be LIABLE for defense or indemnity with respect to any claim against You by any third party arising from your possession or use of the Original Code or the Documentation.

In no event will GoAhead's total liability to You for all damages, losses, and causes of action (whether in contract, tort, including negligence, or otherwise) exceed the amount You paid for this product.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, AND SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

7. Indemnification by You.

You agree to indemnify and hold GoAhead harmless against any and all claims, losses, damages and costs (including legal expenses and reasonable counsel fees) arising out of any claim of a third party with respect to the contents of the Your products, and any intellectual property rights or other rights or interests related thereto.

8. High Risk Activities.

The Original Code is not fault-tolerant and is not designed , manufactured or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the Original Code could lead directly to death, personal injury, or severe physical or environmental damage. GoAhead and its suppliers specifically disclaim any express or implied warranty of fitness for any high risk uses listed above.

9. Government Restricted Rights.

For units of the Department of Defense, use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Contractor/manufacturer is GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004.

If the Commercial Computer Software Restricted rights clause at FAR 52.227-19 or its successors apply, the Software and Documentation constitute restricted computer software as defined in that clause and the Government shall not have the license for published software set forth in subparagraph (c)(3) of that clause.

The Original Code (i) was developed at private expense, and no part of it was developed with governmental funds; (ii) is a trade secret of GoAhead (or its licensor(s)) for all purposes of the Freedom of Information Act; (iii) is "restricted computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity; and (iv) in all respects is proprietary data belonging solely to GoAhead (or its licensor(s)).

10. Governing Law and Interpretation.

This Agreement shall be interpreted under and governed by the laws of the State of Washington, without regard to its rules governing the conflict of laws. If any provision of this Agreement is held illegal or unenforceable by a court or tribunal of competent jurisdiction, the remaining provisions of this Agreement shall remain in effect and the invalid provision deemed modified to the least degree necessary to remedy such invalidity.

11. Entire Agreement.

This Agreement is the complete agreement between GoAhead and You and supersedes all prior agreements, oral or written, with respect to the subject matter hereof.

If You have any questions concerning this Agreement, You may write to GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004 or send e-mail to info@goahead.com.

BY CLICKING ON THE "Register" BUTTON ON THE REGISTRATION FORM, YOU ACCEPT AND AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. IF YOU DO NOT WISH TO ACCEPT THIS LICENSE OR YOU DO NOT QUALIFY FOR A LICENSE BASED ON THE TERMS SET FORTH ABOVE, YOU MUST NOT CLICK THE "Register" BUTTON.

Exhibit A

GoAhead Trademarks, Logos, and Product Designation Information

01/28/00

Libpcap License

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

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

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

NetSNMP License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

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

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

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

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

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

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

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

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

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

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

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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

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

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

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

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

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

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

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

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

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

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

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

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

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

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

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

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS 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 APPLE 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.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

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

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

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

OpenSSL License

LICENSE ISSUES

=====

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

OpenSSL License

```
-----
/*
=====
* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
```

```
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
=====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----

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

- * This package is an SSL implementation written
- * by Eric Young (eay@cryptsoft.com).
- * The implementation was written so as to conform with Netscapes SSL.
- *
- * This library is free for commercial and non-commercial use as long as
- * the following conditions are aheared to. The following conditions
- * apply to all code found in this distribution, be it the RC4, RSA,
- * lhash, DES, etc., code; not just the SSL code. The SSL documentation
- * included with this distribution is covered by the same copyright terms
- * except that the holder is Tim Hudson (tjh@cryptsoft.com).
- *
- * Copyright remains Eric Young's, and as such any Copyright notices in
- * the code are not to be removed.
- * If this package is used in a product, Eric Young should be given attribution
- * as the author of the parts of the library used.
- * This can be in the form of a textual message at program startup or
- * in documentation (online or textual) provided with the package.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- * 1. Redistributions of source code must retain the copyright
- * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.
- * 3. All advertising materials mentioning features or use of this software
- * must display the following acknowledgement:
- * "This product includes cryptographic software written by
- * Eric Young (eay@cryptsoft.com)"
- * The word 'cryptographic' can be left out if the rouines from the library
- * being used are not cryptographic related :-).
- * 4. If you include any Windows specific code (or a derivative thereof) from
- * the apps directory (application code) you must include an acknowledgement:

```

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* 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.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

PuTTY License

PuTTY is copyright 1997-2006 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.

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

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

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

SSH Server License

The MIT License

Copyright (c) <year> <copyright holders>

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

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

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

ZipArchive License

```
////////////////////////////////////  
//  
//  ZipArchive 1.5.1, March 2001  
//  
//  
//  This library allows to crate ZIP files in the compatible way with  
//PKZIP version 2.6. Some important issues:  
// - multiple disk spanning is supported  
// - encyption is not supported  
// - allows to create disk spanning archive also on non removable devices  
//and with user-defined volume size  
// - this library uses the zlib library by Jean-loup Gailly and Mark Adler
```

```
//to perform inflate, deflate operations
//
//
//
// Copyright (C) 2000 - 2001 Tadeusz Dracz
//
//
// Permission is granted to anyone to use this software for any purpose
// and to alter it and redistribute it freely, subject to the
// following restrictions:
//
// 1. Using this software in commercial applications requires an author permission.
// The permission will be granted to everyone excluding the cases when
// someone simply tries to resell the code.
//
// 2. The origin of this software must not be misrepresented; you must not
// claim that you wrote the original software. If you use this software
// in a product, an acknowledgment in the product documentation would be
// appreciated but is not required.
//
// 3. Altered source versions must be plainly marked as such, and must not be
// misrepresented as being the original software.
//
// 4. This notice may not be removed or altered from any source distribution.
//
//
//You can contact me at:
//tdracz@artpol-software.com
//
//For new versions check the site:
//http://www.artpol-software.com
//
////////////////////////////////////
```

ZLib License

/* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.2, October 3rd, 2004

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

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

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <http://www.ietf.org/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](http://www.ietf.org/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](http://www.ietf.org/rfc/rfc1952.txt) (gzip format).

*/

Appendix J: A. Onoe & S. Leffler Copyright

Copyright (c) 2001 Atsushi Onoe

Copyright (c) 2002-2005 Sam Leffler, Errno Consulting

All rights reserved.

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

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

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

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.

Appendix K: S. Leffler Copyright

Copyright (c) 2002-2005 Sam Leffler, Erno Consulting

All rights reserved.

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

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

Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

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.

Appendix L: B. Paul Copyright

Copyright (c) 1997, 1998, 1999

Bill Paul <wpaul@ctr.columbia.edu>. All rights reserved.

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

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by Bill Paul.
- 4 Neither the name of the author nor the names of any co-contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY Bill Paul 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 Bill Paul OR THE VOICES IN HIS HEAD 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.

Index

Symbols

Pre-Installation Model 277
#STA 319, 322

Numerics

10/100 Ethernet 9, 55
2.4 GHz vs. 5 GHz 327
2.4-GHz 58, 333
2.4-GHz (802.11b/g/n) channels 314
2.4-GHz channels 333
20- and 40-MHz channels 316
20 MHz 329, 337
20/40 MHz Statistics 416
2nd Channel 323
40 GHz Intolerant 323
40-MHz wide band 316
5-GHz 58
5-GHz 802.11a/g/n channels 314
5-GHz channels 333
802.11 58, 321
802.11 a/b/g 325
802.11 band 2
802.11 media band 337
802.11 media type 166
802.11 protocols 347
802.11 RF Media Types 58
802.11 settings 243, 400
802.11 standards 327
802.11 traffic 58
802.11 wireless networking standards 326
802.11a 169
802.11a/b 169
802.11a/g 169
802.11b 169
802.11d 345
802.11g 169
802.11h 345
802.11n 73
802.11n License 73
802.11n tools 413
802.1x process 411
802.3af Power-over-Ethernet 4

A

About 77
AC power 55
AC power connections 55
access 132
access control 61
access control list 2, 167
Access Point 169
access point 57
access points 128
accountability 1, 3
accuracy 410
ACL 167
ACL Expiration 170
ACL expiration time 165
ACL Status 322
ACL Type 169
ACL – Active 129, 130
ACL-Down 129
acoustic-tile drop ceilings 61
activate 802.11n 73
active 802.11 device 399
active analytical trace 2
active defense 1
Active Directory 96
Active Directory® 96
active protection 2
Active Time for Device 320
active tools 399
Ad Hoc 130, 169
adapt 230
Adapter 25
add a notification 242
Add New Device 170
Add New Notification 242
add or remove users 92
Adding AirMagnet Enterprise Servers to the Console 81
Adding Devices 90
Adding Notification Options 241
addition of wireless devices 139
Ad-Hoc 244, 316
admin 42, 95, 101
Administrator 99, 101
Administrator Password 26

- Administrator role 95
- Advanced 313
- Advanced configurations 399
- aggregated data 125
- air handling ducting 61
- AirMagnet 95
- AirMagnet Alert Window 132
- AirMagnet application 16
- AirMagnet Enterprise 11
- AirMagnet Enterprise Console 8, 9, 29, 31
- AirMagnet Enterprise Console screen 67
- AirMagnet Enterprise Console Start screen 121
- AirMagnet Enterprise Console's AirWISE screen 139
- AirMagnet Enterprise Console's Infrastructure screen 159
- AirMagnet Enterprise Policy Reference Guide 128
- AirMagnet Enterprise Release Notes 11
- AirMagnet Enterprise Server Administration 55
- AirMagnet Enterprise Server Installation 15
- AirMagnet Enterprise Server page 49
- AirMagnet Enterprise Server Setup 57
- AirMagnet Enterprise Software CD 11
- AirMagnet Enterprise System Components 8
- AirMagnet Remote Analyzer 9
- AirMagnet services 16
- AirMagnet SmartEdge Sensor 8, 9, 34
- AirMagnet SmartEdge Sensor Objects 445
- AirMagnet SmartEdge Sensor Web page 40
- AirMagnet Software License Agreement 11
- AirMagnet's AirWISE expert engine 227
- AirMagnet's Website 16
- airports 61
- AirWISE 69, 325
- AirWISE Advice 317
- AirWISE analysis engine 9
- AirWISE filter 309
- AirWISE Screen 347
- AirWISE screen 139, 307, 317, 320, 345
- Alarm Information 351
- Alarm Overview 127
- Sensors 71
- Alarm Severity and Color Codes 349
- Alarm Status 345
- alarms 3, 8, 241, 259, 261
- Alert 345, 351
- Alias 165
- Alias Name 168
- Allow Access 101
- Alternate DNS 39
- Altitude 322
- AM Monitor services 433
- America 404
- Americas 327
- A-MPDU 416
- Analog Cordless Phones 369
- Analysis 413, 416
- analysis 1
- Analyze 62
- analyze 57, 121
- analyzing 139
- anomalies 10
- antenna 58
- AP 57, 316
- AP (Rx) 415
- AP (TX) 415
- AP Capability 415
- AP density 63
- AP Details 351
- AP Information by Hour 127, 128
- AP->STA 415
- approach 237
- APs 159
- argument 445
- around-the clock 2
- assessment 4
- assign 227, 241
- assign a notification 240
- assign notifications to policies 240
- assign or modify 92
- Assigning Devices to ACL Groups 90
- Associated AP 322, 421
- association process 410
- attacks 139
- Audit Log 84
- Audit Log Components 85
- Audit Log Customizing 86
- Audit Log Exporting 86
- Audit Log Printing 86
- Australia 327, 404
- Auth. Algorithm 245
- Authentication 263, 399
- authentication 23, 238
- authentication mechanism 245
- Authentication Mechanisms 245
- Authentication required 261
- Authentication Type 96
- Automated Blocking 2
- Automated Response 2
- automated threat response 1
- automatic rogue tracing and blocking 186
- automatically block rogue APs 271
- autosensing 39

available throughput 61

B

Baby Monitors 369

Backing Up Database 114

backup server 28, 255

backward compatibility 414

bad license 44

bands 58

bandwidth 4

bandwidth overhead 9

Basel II 222, 357, 360

Basel II Accord 357

Basic User 99

beacon 59

beacon frame 59

beacon frames 62

beep 241

BI 59, 319, 322

bits per second 40

block 184

Block ACK 423

Blocked Devices 135

blocking 2, 184

blocking status 2

Bluetooth Devices 369

boundary 60

Bridge Mode 319, 322

broadcast 59, 318

broadcast message 278

BSS 59

Bubble Help 324

budget 57

buffer 326

building structure 61

buildings 55

built-in proxy settings 431

business needs 3

business park 58

Byte Count 421

bytes 330

C

CA Unicenter 445

Channel Throughput 328

calculating 418

campuses 55

Capability 415

capture 57

Category 446

Cell Power 323

central core area 61

central engineering core 61

central point 55

central server 9

Centralized alarm view 8

Changing Server Login Settings 82

Channel 185, 245, 320

Channel Bandwidth 423

Channel Data Graphical Display 331

Channel Data Summary 330

Channel filter 308

channel interference summary 337

Channel Occupancy 332

channel occupancy 333

Channel or Device Overload 127

channel scan list 315

channel scan settings 404, 405

Channel screen 307, 328

Channel Screen Control Buttons 330

channel throughput 328

Channel Utilization 328

channel utilization 328

Channel 2

characteristics 139

Chart Data Tabulation 356

Charts 70

Charts Screen Samples 196

China 327, 404

Choosing User Display Options 103

classes of threats 1

Classic Tree View 349

cmd window 447

Coexistence 414

collapsed 317

collecting network performance data 139

color-coded 314, 347

command 447

communication devices 61

comparable products 285

compiled 445

Compliance Charts 357

compliance charts 354

Compliance Reports 360

compliance reports 4

Compliance Reports Disclaimer 224, 360

components 135

configuration 55

Configuration Button 136

Configuration Vulnerabilities 127

configure 802.11 settings 400

- configure a print notification 271
 - configure a shared secret key 275, 280
 - configure a sound notification 268
 - Configure an ACL 56
 - configure channel scan settings 405
 - configure Console settings 251
 - configure email notification 260
 - configure filter settings 403
 - configure Instant Messenger Notification 269
 - configure Notification List 257
 - configure Page-over-Internet notifications 267
 - configure Page-over-Phone notifications 265
 - configure rogue AP blocking 272
 - configure Sensor settings 256
 - configure Server settings 253
 - configure SMS-via-Email Notifications 264
 - configure SNMP notification 262
 - configure SysLog notification 259
 - configure WEP settings 246, 402
 - configured nodes 56
 - configuring 227
 - Configuring Email Notification 259
 - Configuring Event-Log Notification 270
 - Configuring General Settings 398
 - Configuring Instant Messenger Notification 268
 - Configuring Page-over-Internet Notification 266
 - Configuring Scan Channels 246
 - Configuring SNMP Notification 261
 - Configuring Sound Notification 268
 - Configuring SysLog Notification 258
 - Configuring the Shared Secret Key 275
 - Configuring Vendor ID 279
 - connect 49, 55
 - Connect Server 67
 - Connecting to AirMagnet SmartEdge Sensors 83
 - connection states 62
 - Connections between Devices 345
 - connectivity design 62
 - connectivity status 62
 - consolidated view 2
 - Contents 77
 - Context String 263
 - context-driven advice 139
 - context-sensitive 9
 - Control Buttons 104
 - Control Frames 345
 - Control frames 351
 - Control Panel 433
 - controlled environment 56
 - conversations 1
 - Copy From 231
 - cordless phones 314
 - corporate network 39, 139
 - corporate WLAN 227
 - corrective actions 4
 - cover 57
 - coverage 60
 - coverage area 56
 - Create 62
 - create 227
 - create a network tree 79
 - Creating Report Book 213
 - Crib Sheet 11
 - Critical 128, 317, 349, 445
 - critical information 59
 - cross-channel interference 314
 - crossover cable 35, 39
 - customers 10
 - customize 315
 - Customizing AirMagnet Alert Window Display 136
- ## D
- Data Analysis 351
 - data bits 41
 - data capture filters 403
 - Data Frames 345, 351
 - Data Selector 331
 - database 8
 - Database Management 113
 - Database Name 22
 - database problem 70
 - Database Server Name 22
 - database server selection 20
 - Decode screen 307
 - Decode Screen Parameters 362
 - Decodes Screen 361
 - Decodes screen 361
 - Defaul 245
 - default 95, 101
 - default database name 22
 - Default Gateway 39
 - Default gateway 35
 - default gateway 41
 - default notifications 240
 - default policy profile 102, 228
 - default scan settings 405
 - defend 2
 - Delete 245
 - Delete User 103
 - Deleting an Notification 242
 - Deleting Reports 214
 - Deleting Sensors 109

- dense area 61
- Deny Access 101
- Department of Defense (DoD) Directive Number 8100.2 357
- Department of Defense Directive 8100.2 221, 357
- deployment 277
- Deployment & Operation Error 127
- Description 446
- deselect 235
- Design 62
- design 61
- design methods 57
- design point 57
- design requirements 63
- desired area 63
- desired FOV 61
- desired monitoring capabilities 63
- desired total FOV 62
- Destination Folder 32
- destination folder 23
- detect 1, 2, 184
- detected 271
- detection 58
- Device 321, 421
- Device Charts 354
- device count exceeded 44
- Device filter 309
- Device List 167
- Device Locator 199
- Device name 165
- Device Throughput Calculator 413, 421
- Device to Simulate 421
- device vendors 285
- device-centric 351
- devices 1
- device-specific 57
- Device-Specific Alarm 5
- DHCP 40, 56
- DHCP server 278
- diagnostics screen 410
- Digital Cordless Phones 369
- digits 317
- disable 2
- disclosure 1
- Display latest # events 136
- Distance 322
- distance 63
- diversity antenna 60
- DNS nam 433
- DNS server 39, 278
- DNS Server Address 39

- document 2
- documents 9
- DoD 4
- DOD 8100.2 357
- Domain Name 39
- down 70
- Downlink 415
- download page 445
- download speed 44
- Downloading 29
- drill down 3
- Dual Beacon 324
- Dual CTS Protection 324

E

- Easy View 313
- edge device 57
- Edit Device 170
- Edit Notification 242
- Efficiency 413
- Efficiency tool 413
- electrical and mechanical equipment 61
- elevators 61
- Email 3
- email 227
- email account 259
- Email server password 261
- Email server username 261
- emission powers 327, 404
- enable 802.11n 73
- enclosed areas 61
- Enterprise Console 4
- Enterprise Console-Server communication 32
- Enterprise Server 4
- Enterprise Server Name 38
- equipment 57
- Erase 349
- estimating tool 63
- Ethernet 35, 55
- EU CRD/CAD3 223, 360
- EU-CRD 358
- Europe 327, 404
- European Union (EU) Capital Requirements Directive 358
- event correlation 3
- event escalation 3
- Event Log server 270
- event signatures 62
- EventLog 3
- events 1
- Excel 3

- existing policy profiles 231
- Exit 84
- expanded signal meter screen 315
- Expert Advice 350
- Exporting and Importing Policy Profiles 231
- Exporting Data 355
- Exporting Policy Profiles and Notifications 231
- Exporting Reports 217
- Exporting Sensor Data 112
- expose 139
- Exposed 130
- exposed mounting location 61
- external firewall 431
- external intrusions 139
- external public address 432

F

- factory-default IP address 34
- fail-over 4
- FAQ 10
- far end 431
- Federal Information Security Management Act 358
- File Download screen 31
- Filter Check Box 136
- Filtering Packet Captures 362
- Final Test 56
- Find in This View 365
- FIPS 140-2 compliant 4
- firewall 55
- firewalls 431
- First 322
- FISMA 223, 358
- floor 61
- floor plan 57
- floor plans 63
- flow control 41
- Forensics 154
- Forensics Notification 273
- formats 3
- FOV 58, 59
- FOV boundary 59
- FOV pattern 60
- Frag. Threshold 245
- frame communication 312
- frame types 403
- Frames 345, 351
- France 404
- frequency 169, 404
- frequency spectrum 314
- From (email address) 260

- Full Disclosure Policy View 3

G

- general categories 127
- general settings 398
- generate alarms 139
- generated 259
- Generation 260, 272
- geographical location 327
- GLBA 3, 4
- global interface 1
- government sites 61
- Sensors 71
- Gramm-Leach Bliley Act 222, 358
- Graph Option 355
- Graph Options 331
- graphs of trends 3
- Greenfield Supported 323
- Guest WLAN 227
- Guests SSID group 238
- guidelines 63

H

- hardware 56
- hardware analysis 3
- Hardware vendor 2
- Health Insurance Portability and Accountability Act 222, 358
- health of a WLAN 139
- heart beats 278
- Help Menu 77
- hidden devices 338, 339
- high ceilings 63
- HIPAA 3, 4, 358
- Hong Kong 327, 404
- host mismatch 44
- host name 446
- Hot Swap (backup) Server 255
- hot swap server 255
- hotspot 58
- How-To guide 309
- HP OpenView 445
- HT Disabled 415
- HT Not Well Used 415
- HT Well Used 415
- HTML 3
- HTML-based 9
- https 432
- hub 35
- Hyper Terminal 41

I

- identify 1, 121, 139
- Identifying 139
- identifying 184
- IDS – Denial-of-Service Attack 127
- IDS – Security Penetration 127
- IEEE (OUI) 185
- IEEE 802.11g Issues 127
- IIS 16
- implement 227
- implementation 227
- Import Profile and Notification 233
- important questions 227
- importing 231
- Importing a policy profile 228
- Importing ACL from Other Vendors 285
- Importing and Exporting ACL Data 164
- Importing Policy Profiles and Notifications 233
- Importing Sensor Data 112
- inbound 432
- indoor areas 60
- influence 60
- Informational 128, 317, 445
- Infrastructure 69, 244
- Infrastructure Data Graphs 343
- Infrastructure Data Pie Chart 345
- Infrastructure Data Summary Report 344
- infrastructure elements 57
- infrastructure network 447
- Infrastructure screen 307, 316, 320, 341
- inspect 2
- instal 56
- Installation 29
- installation 20, 55
- installation destination 23
- Installation Overview 13
- Installation Restrictions 61
- Installing 31
- Instant Message 3
- Instant Messenger application 268
- intelligence 4
- intelligent network management technology 227
- inter-beacon interval 59
- Interference 333
- Interference Score 321
- interference score 333, 334
- interference score graph 340
- interference scores 338
- internal private address 432
- Internet Explorer 431
- interpolate 171

- interruption of communication 255
- intrusion 1
- intrusion detection & prevention 227
- intrusion detection system 184
- IP Address 39
- IP address 34, 35, 41, 80, 255, 433
- IP Configuration Method 39
- IP subnet 448
- IP/Port combo 432
- ireless assets 159
- ISO 27001 223, 358
- ISO/IEC 27001
 - 2005 358
- IT security group 61
- IT staff 4

J

- Japan 327, 404

K

- Key Length 402
- Key Type 402
- known active channels 315
- known issues 10
- Korea 327, 404

L

- lab environment 56
- lab setting 278
- large-scale 277
- large-scale enterprise Wireless networks 227
- Last 319, 323
- last hop router 447
- last-minute enhancements 10
- Latest # events from selected sensors 135
- Latitude 322
- Launch 35
- launch 67, 445
- Launching AirMagnet Laptop 305
- layered policy structure 227
- layers of defense 1
- LDPC 324
- Least Capable Device 423
- legacy 802.11 networks 414
- levels of severity 317, 445
- library of pre-built reports 3
- library of wireless events 1
- license 40
- license expired 44

- license file installation 24
- license file not found 44
- license granted 44
- license status 44
- Link Budget 58
- link rate 59
- Link Speed 330
- Linux 447
- Live Capture 312
- live capture mode 312
- location 1, 9, 62, 206
- Location/Policy Tree 68
- locations 63
- log events 270
- Log Level 38
- log out 84
- login 431
- Login Name 22
- login screen 32
- Longitude 322
- loss of data 28
- Lower 40 MHz 329, 337
- lowest basic rate 59
- L-SIG TxOP Full Support 324

M

- MAC 168, 414
- MAC Address 25, 321
- MAC address 2, 319, 410, 447
- MAC address - Media 165
- MAC address (ACL) 185
- magnitude 63
- Maintenance Commands 42
- Major Components of the Infrastructure Screen 159
- malicious 404
- Manage Users and Roles 103
- Management Frames 345, 351
- management system 2
- managing 163
- Managing ACL Groups 87
- Managing Alarm List 349
- Managing Sensors 103
- map 2, 432
- mapping configurations 431
- match 263
- Max Frame Size 423
- maximum rate 59
- MCS 416, 422
- MDI/MDIX hub/switch 39
- measurement 61
- measurement data 62

- measurement process 62
- measurements 62
- Media 330
- Media Type 325, 330
- media type 319
- Medium Access Control layer 414
- Menu Bar 68
- method of authentication 237
- methods of notification 186
- MIB file 445
- microcell 61
- microcell coverage environment 61
- Microcell Network 61
- Microsoft Internet Explorer 16
- Microsoft® Internet Information Service 16
- Microwave Ovens 369
- microwave ovens 314
- minimum signal level 60
- misconfiguration 404
- misconfigured WLAN devices 405
- modify 227
- modify existing notifications 242
- Modifying Existing Notification Settings 242
- Modifying Sensor Properties 106
- modulated 336, 339
- modulated spectrum 336
- modulated spectrum usage 332
- modulation types 335
- monitor 1, 9, 227
- Monitored Device 169
- Monitoring 139
- Monitoring Sensors 105
- monitoring WLAN environments 58
- Most Active APs 131
- Most Events per AP 130
- multicast 318
- multi-mode radio 58
- multiple 80
- multiple ACL groups 90
- multiple MAC addresses 447
- multiple SNMP management stations 445
- multi-use office building 58
- My Computer 433
- MyWLAN SSID group 238

N

- Name 446
- name 255
- NAT 55, 431
- NAT firewall 431
- Navigation Bar 68, 306

- Navigation Bar and Buttons 307
 - navigation buttons 68, 306
 - Neighbor 129
 - Neighbor Device 169
 - Neighbor SSID group 238
 - neighboring tenants 58
 - neighboring WLAN 227
 - Network Address Translation 431
 - network administrators 139
 - Network Audit Log 84
 - network building tools 79
 - network data 8
 - network design 57, 62
 - Network Design Objectives 61
 - network devices 55
 - network engineers 61
 - network environment 9
 - network hub/switch 39
 - network infrastructure 312
 - Network Infrastructure Color Codes 343
 - Network Operating Center 125
 - network operating specification 59
 - network operating specifications 62
 - network operational characteristics 60
 - network operations center 55
 - network policy 2
 - Network Policy Hierarchy 348
 - network policy profile 184
 - network security 347
 - network security and performance status 125
 - network segment 433
 - network segments 431
 - network settings 277
 - Network Setup 38
 - network staff 3
 - network topology 8
 - Network Tree 126
 - Network Tree Structure 342
 - Network Type 244
 - networks 1
 - neutralizing 184
 - New AP/STA/AdHoc 132
 - New City/Campus 72
 - New Floor 72
 - New Profile 229, 231
 - New User 95
 - no license 44
 - NOC 9, 55, 61, 125
 - Node Type 165
 - Noise 321
 - noise 314, 319
 - noise level 315, 326, 338
 - non-802.11 interference 334
 - non-authentication proxies 431
 - Non-Greenfield STA Present 323
 - Non-HT OBSS 323
 - normal locations 56
 - normal operation 1
 - normal working condition 70
 - notes 10
 - Notification 228, 236
 - Notification List 445
 - notification messages 270
 - Notification Name 260, 272
 - notification system 3
 - Notification Type 242
 - Notification Wizard 240
 - notifications 227, 241
 - number 63
- O**
- Objects 445
 - Observed (Downlink) 415, 416
 - Observed (Uplink) 415, 416
 - Occupancy 332
 - occupancy 332
 - office towers 61
 - online 56
 - online help 9
 - online knowledge base 28
 - Open areas 63
 - open areas 60
 - Open LDAP 96
 - operating frequencies 326
 - Operating Mode 323
 - operating models 277
 - operating system 433
 - operational redundancy 2
 - optimal 57
 - Option 243
 - organizational summary 316
 - outbound 432
 - outbound connections 431
 - Outgoing email server 261
 - Outgoing server port 261
 - output 447
 - outside areas 60
 - over the Internet 266
 - overall procedure 62

P

- P Group 320
- Pacific Rim 327, 404
- packet 9
- Packet Capture Filters 402
- Packet Count 421
- packet frames 362
- Packet Frames Summary 318
- Packet Retries 245
- packet sniffing probes 9
- packet transmission rate 59
- packets 4
- page 265, 266
- Page-Over-Phone Notification 265
- Pager 3
- parameters 263, 399
- parity 41
- Password 22, 33, 36, 82, 84
- password 42, 80, 277, 445
- patent-pending 227
- Payment Card Industry Data Security Standard 222, 359
- PCF/DCF 319, 322
- PCO 323
- PDF 3
- peak WLAN use 4
- Peer-AP-Peer Connections 346
- Peer-to-Peer Connections 345
- pending-approval 278
- percentage 326
- Perform 62
- perform 61
- performance 9, 10
- performance compliance 62
- Performance Intrusion 227
- Performance Intrusion policies 127
- performance management 61
- performance metrics 57
- performance monitoring 227
- performance status 347
- perimeter 62
- perimeter of a building 61
- perimeter of the network 56
- PHY 413
- PHY Data Rate 416
- physical characteristics 63
- Physical layer 169
- physical layer 413
- physical layou 55
- physical sectors 61
- physical space 62
- physical structure 63
- pie chart 316, 317, 345
- planned measurements 63
- planning a deployment 55
- plenum-rated 4
- plug-and-play 56
- PoE 55
- policy category 227
- policy configuration 228
- policy conformance 57
- Sensors 71
- policy profile 102
- Policy Profile Creation Procedures 227
- policy profiles 227
- Policy Reference Guide 10
- policy rules 235
- policy settings 227
- policy violations 227
- Policy Wizard 237
- policy-based management 3
- port 2
- Port 443 431, 432
- Port 444 432
- port FastEthernet0/3 447
- port forwarding 431
- port number 432
- ports 431
- ports forward 432
- position 62
- Post-deployment verification 62
- Post-Installation Model 278
- potential threats 1
- Power Save Mode 245
- power source 55
- power specification 48
- Power User 99, 101
- Preamble 319, 322
- Preamble Mode 245
- Pre-configure 56
- pre-configured 24, 56, 245
- preconfigured 404
- pre-configured policies 3
- pre-configured policy profile 24, 228, 230
- precursor 62
- primary channel 329
- primary Server 255
- primary server 28, 255
- Print 3
- print out 270
- Printing Reports 216
- Privacy 263
- privileges 99, 101

- proactive 62
- proactively 9
- problem resolution 139
- Problematic Traffic Pattern 127
- product package 10, 11
- Product Registration 11
- product support 28
- professional tools 1
- Profile 102
- prohibited channels 404
- project 63
- Properties 72
- Protection Method 423
- provide coverage 57
- proxy server 16, 431
- public access venues 61
- public static address 431

Q

- quarantine 447
- question-and-answer 10

R

- Radio Channel Allocation 327
- radio frequencies 327, 404
- radio operating frequencies 325
- Radio Receiver Sensitivity 58
- Radius 96
- random unauthorized device 59
- Rate 421
- reactivate the port 448
- real-time network connectivity 62
- real-time remote diagnostics 61
- receive traps 445
- receiver 58
- receiver sensitivity profile 58
- receiver sensitivity value 58
- recipient 264
- records 4
- reduce 61
- redundant management servers 4
- reference AP 62
- reference unauthorized device 59
- register 28
- registration-only 28
- regulated channels 405
- regulatory requirements 3, 404
- regulatory rules 404
- regulatory standards 3, 4
- Release Notes 10

- Reliable Detection 59
- reliable detection condition 62
- reliable monitoring 61
- remote connection 62
- remote connectivity 4
- remote locations 56
- remove 184
- remove a filter 404
- Removing Servers from the Console 82
- Report Book Adding 214
- Report Book Parameters 213
- reported status 433
- reports 3
- requests 432
- reseller 11
- resources 55
- Restoring Database 115
- restrict 61
- RF channel 166
- RF Interference 333
- RF Management 127
- RF propagation 63
- RF signal quality 312
- RIFS Mode 323
- RJ-45 35
- Rogue 129, 130
- rogue AP 1, 58, 404
- Rogue AP and Station 127
- rogue APs 60, 405
- rogue APs and stations 315
- rogue detection 2
- Rogue Device 169
- Rogue devices 2
- rogue devices 184
- Rogue in Network 322
- rogue management 2
- rogue management mechanisms 243
- rogue trace 447
- role 101
- troubleshooting procedures 433
- routable public IP address 432
- RTS Threshold 245
- rule of thumb 63
- Rx Ch Width 323
- Rx STBC 324

S

- sample format 445
- Sarbanes-Oxley 4, 359
- Sarbanes-Oxley Act 222, 359
- scalability 4

- scan frequency 315
- Scan time 405
- scan time interval 405
- Scenarios 57
- scratch 228
- screen size 317
- screens 306
- scrolling list 362
- scrolling screen 134
- Searching Reports 214
- secondary channel 329
- Secured Socket Layer 431
- security 1, 9, 319
- security and performance status 312
- Security IDS/IPS 227
- security IDS/IPS 10
- Security IDS/IPS policies 127
- security intrusion detection 57
- security measures 2
- Security Mechanisms 321
- Security Policy by Hour 127
- Security/Performance 137
- security-only 3
- segment 125, 128
- send email messages 259
- send notifications 258
- send out 268
- send traps 445
- sending data 56
- Sensor 4, 83
- sensor 9
- Sensor Field of View 58
- sensor filter 71
- Sensor FOV measurement 61
- Sensor FOV Types 59
- Sensor Information Page 36
- Sensor installation methods 60
- Sensor IP 446
- Sensor Location 446
- Sensor management 8
- Sensor Name 38
- Sensor network trending information aggregation 9
- sensor options 227
- Sensor RF specifications 60
- Sensor Shared Secret Key 27, 38
- Sensor Statistics 135, 137
- Sensor Table Data Fields 105
- Sensors 71
- Sensor-Server communication 277
- serial cable 40
- Serial Key 25
- serial keys 28, 255
- Serial Number 25
- serial numbers 28, 255
- Serial Port 40
- serial port 40
- serial port configuration 34
- Server 4, 33, 81
- server name 80
- server redundancy 28
- service level 59
- set up 255
- set up a network tree 80
- Severity 228, 236
- SGL 323
- share policy profiles 231
- shared secret key 277
- Short Guard Interval 422
- Short Guard Interval (SGI) 416
- Show Commands 42
- shut down 448
- shutting down 447
- Signal 321
- signal 319
- signal level 60
- Signal Meter 313
- signal meter 315, 317
- signal propagation 61
- signal quality 314
- Signal Quality Codes 314
- signal strength 315, 326
- Signal-to-Noise Ratio 321
- signal-to-noise ratio 315, 319, 326
- simplicity 1
- simulate 62
- simulated WLAN data 420
- Simulator 418
- Singapore 327, 404
- site survey 56
- SM Power Save 324
- small-scale 278
- SmartEdge Sensor 4
- SmartEdge Sensor Administration 55
- SmartEdge Sensor density 63
- SmartEdge Sensor Design measurements 63
- SmartEdge Sensors 4
- SMS 3
- SMS messages 264
- SNMP 3, 227
- SNMP management console 445
- SNMP management stations 445
- SNMP notification 263, 445

- SNMP server 261
- SNMP trap collector 263
- SNMP traps 261, 445
- Software Installation 56
- software installation 56
- Software License Agreement i
- software version mismatch 44
- solve 121
- sound 227
- Spain 327, 404
- specific policies 227
- spectral distance 336
- spectral properties 336
- Spectrum Analyzer Integration 341
- Speed 330, 345, 351
- SSID 2, 62, 165, 185, 228, 244, 316, 319, 322
- SSID filter 309
- SSID groups 237
- SSIDs 159
- SSL 431
- SSL/TLS connection 431
- STA 316
- STA association 62
- STA Information by Hour 129
- STA type 62
- STA->AP 415
- Staging 56
- staging area 56
- staging process 56
- staging setup 56
- Start 69
- Start screen 67, 126, 307, 312
- STAs 159
- static IP 56
- static IP address 40
- static private address 431
- Station 169
- Station Detail 351
- station probing 314
- statistical confidence level 59
- statistics 132
- Status 421
- stop bit 41
- straight-through cable 35, 39
- straight-through RJ-45 Ethernet cable 41
- streamline 228
- structural composition and type 60
- subnet 447
- Subnet Mask 39
- Subnet mask 35
- subnet mask 41

- summarized information 312
- switch 2, 35
- switch port 447, 448
- switches 2
- Switching media type 326
- SysLog 3
- Syslog server 258
- System Components 8
- system configuration 251
- System Deploymen 55
- system design data 62
- System Requirements 29

T

- tabulation 318
- Taiwan 327, 404
- TCP Port 443 431
- technical background 57
- technical support 11
- technical teams 1
- telco and data cable conduits 61
- Telnet Server 39
- Telnet server 41
- test location 62
- test locations 62
- test power-on duration 62
- test-drive 278
- Text 3
- threat detection 1
- threats 1, 10
- Threshold 228
- threshold 62
- Thresholds 236
- Throughput 421
- time 446
- Time (μsec) 421
- Time Frame Selector 127
- time period 127
- Time Zone 38
- time zone 41
- Title 446
- TK & MIC 319
- TKIP/MIC 322
- TLS 431
- To (email address) 260
- tool tip screen 128
- toolbar 310, 312
- tools 306
- Tools screen 307
- Top Traffic Analysis screen 353
- total number 62

- trace 2, 184
- tracing 2, 184
- Tracing network device 409
- tracking wireless devices 139
- traffic 432
- traffic characteristics 62
- transmission 169
- transmit 59
- transmit spectrum masks 335
- Transport Layer Security 431
- trap 445
- trending 8
- triggered 258
- troubleshooting 9
- Troubleshooting link connection 409
- Trusted AP Monitoring 60
- trusted APs 60
- trusted device 58
- trusted stations and APs 59
- trusted system 2
- trusted traffic 59
- Trusted Traffic Monitoring 59
- trusted zone 58
- Tx channel width 323
- Tx Data Bytes 421
- Tx Packets 421
- Tx Rate 244
- Tx STBC 323
- Type A boundary 60
- Type B boundary 60
- Type C boundary 60
- type of notification 258

U

- unauthorized device 59
- Unauthorized Device Detection 60, 62
- unauthorized devices 58
- Unauthorized WLAN Devices 58
- unconfigured network tree 79
- Uncontrolled 139
- unicast 318
- unidentified RF signals 314
- Unit of Measurement 326
- unlimited access 28
- un-modulated 336, 339
- unplanned 139
- unused channels 315
- update 275
- updates 28
- Uplink 415
- uplink port 447

- Upper 40 MHz 329, 337
- up-to-date 10
- urban area 58
- Urgent 128, 317, 445
- URL 433
- User administration 8
- User Authentication & Encryption 127
- user filter 103
- User Guide 9
- user interface 4, 9
- User Management 92
 - Adding Users 94
 - Choosing User Display Options 103
 - Removing Users 103
 - Roles and Privileges 93
- User management 55
- User Name 33, 82, 83
- User name 36
- user name 80, 277
- User Roles & Privileges 93
- Username 26
- username 42, 445
- Users 55
- users 237
- users and roles 55
- Using AirMagnet Alert Window 103

V

- Valid Known Device 169
- Vendor List 239
- vendor list 237
- verification 32, 61
- Verifying 32
- via email 264
- View by 802.11n 313
- View by AirWISE Category 349
- View by Channel 313
- View by Device 313
- View by Device/Channel 349
- View by Media Type 313
- View by Node Type 313
- View by SSID 313
- View by Time 349
- View Filter 308
- View Report 76
- View Reports 327
- viewing and managing data 159
- violation 405
- violations 139
- visible 56
- VLAN 3

VNC 433
voice message 241
volume of data 4
VoWLAN 227
VPN 55
VPN client 431
VPN tunnel 431
vulnerabilities 1

W

walk-about 63
Warning 128, 317, 445
Web Browser 34
Web browser 433
Web cameras 314
Web server page 29
Web-based client-server application 29
Web-based configuration 34
WEP 245
WEP Key Setting 402
WIDS 61, 62
Wi-Fi 3
window 252
Windows 2000/XP SNMP management stations 445
Windows network login ID 23
Windows-based 8
WinZip 16
Wire/Wireless 272
wired 55
wired infrastructure 2
wired network 1, 62
wired port 1
Wired-Side Blocking 1
Wireless 1
wireless assets 163
Wireless Blocking 2
Wireless blocking 1

wireless card 326
wireless connections 1
wireless deployment 1
wireless devices 4
wireless intrusion detection system 61
wireless LAN 3
wireless LAN infrastructure 316
Wireless media type 185
wireless packets 57
wireless performance and security monitoring platform 139
wireless real estate 159
wireless traffic 1
WLAN assets 125
WLAN coverage 61
WLAN health 61
WLAN management responsibilities 3
WLAN network structure 72
WLAN policies 227
WLAN security 1
WLAN security and performance issues 121
WLAN structural components 344
WLAN Throughput Simulator 413, 418
Word 3
world-mode 405
Worldwide 327
worldwide 404

X

XML 3

Z

zero configuration 4, 277
zero percentage increase 62
Zeroize 47
zero-tolerance approach 1
zone of operation 58

