Installation Guide

SpectraGuard® Enterprise

An AirTight® Product

Wireless Vulnerability Management and Intrusion Prevention
Version 5.7

AirTight® Networks, Inc., 339 N. Bernardo Avenue, # 200, Mountain View, CA 94043

https://www.airtightnetworks.com

This page has been intentionally left blank.

SpectraGuard® Enterprise

Installation Guide

THE INFORMATION IN THIS GUIDE IS SUBJECT TO CHANGE WITHOUT ANY PRIOR NOTICE.

AIRTIGHT® NETWORKS, INC. IS NOT LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.

THIS PRODUCT HAS THE CAPABILITY TO BLOCK WIRELESS TRANSMISSIONS FOR THE PURPOSE OF PROTECTING YOUR NETWORK FROM MALICIOUS WIRELESS ACTIVITY. BASED ON THE POLICY SETTINGS, YOU HAVE THE ABILITY TO SELECT WHICH WIRELESS TRANSMISSIONS ARE BLOCKED AND, THEREFORE, THE CAPABILITY TO BLOCK AN EXTERNAL WIRELESS TRANSMISSION. IF IMPROPERLY USED, YOUR USAGE OF THIS PRODUCT MAY VIOLATE US FCC PART 15 AND OTHER LAWS. BUYER ACKNOWLEDGES THE LEGAL RESTRICTIONS ON USAGE AND UNDERSTANDS AND WILL COMPLY WITH US FCC RESTRICTIONS AS WELL AS OTHER GOVERNMENT REGULATIONS. AIRTIGHT IS NOT RESPONSIBLE FOR ANY WIRELESS INTERFERENCE CAUSED BY YOUR USE OF THE PRODUCT. AIRTIGHT AND ITS AUTHORIZED RESELLERS OR DISTRIBUTORS WILL ASSUME NO LIABILITY FOR ANY DAMAGE OR VIOLATION OF GOVERNMENT REGULATIONS ARISING FROM YOUR USAGE OF THE PRODUCT, EXPECT AS EXPRESSLY DEFINED IN THE INDEMNITY SECTION OF THIS DOCUMENT.

LIMITATION OF LIABILITY

AirTight will not be liable to customer or any other party for any indirect, incidental, special, consequential, exemplary, or reliance damages arising out of or related to the use of SpectraGuard® Enterprise under any legal theory, including but not limited to lost profits, lost data, or business interruption, even if AirTight knows of or should have known of the possibility of such damages. Regardless of the cause of action or the form of action, AirTight's total cumulative liability for actual damages arising out of or related to the use of SpectraGuard® Enterprise will not exceed the price paid for SpectraGuard® Enterprise.

This product contains components from Open Source software. These components are governed by the terms and conditions of the GNU Public License. To read these terms and conditions visit http://www.gnu.org/copyleft/gpl.html.

This product is protected by one or more of U.S. patent Nos. 7,002,943, 7,154,874, 7,216,365, 7,333,800, 7,333,481, 7,339,914, 7,406,320, Australian patent No. 200429804 and any others listed at www.airtightnetworks.com/patents. More patents pending.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

If this device is going to be operated in 5.15 ~ 5.25 GHz frequency range, then it is restricted in indoor environment only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This product must be installed by a professional technician/installer.

End User License Agreement

BEFORE YOU CLICK “I HAVE READ AND AGREE TO THE LICENSING AGREEMENT ABOVE” OR OTHERWISE USE OR ACTIVATE THE AIRTIGHT PRODUCTS, READ THIS AGREEMENT CAREFULLY. IT IS A LEGALLY BINDING AGREEMENT AND CONTROLS YOUR AND YOUR COMPANY’S USE OF THE AIRTIGHT PRODUCTS.

WHEN YOU CLICK "I HAVE READ AND AGREE TO THE LICENSING AGREEMENT ABOVE" OR OTHERWISE DOWNLOAD, USE OR ACTIVATE THE AIRTIGHT PRODUCTS, THIS AGREEMENT GOVERNS YOUR USE. THIS AGREEMENT IS ENFORCEABLE AGAINST YOU AND ANY ENTITY THAT OBTAINS OR USES THE AIRTIGHT PRODUCTS THROUGH YOU ON THEIR BEHALF. IF YOU OR ANY ENTITY THAT YOU REPRESENT DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BOX THAT SAYS “I DO NOT AGREE TO THE LICENSING AGREEMENT ABOVE” AND DO NOT OTHERWISE DOWNLOAD, INSTALL OR ACTIVATE THE AIRTIGHT PRODUCTS.

IF YOU PAID FOR THE AIRTIGHT PRODUCT(S) AND DID NOT HAVE AN OPPORTUNITY TO REVIEW THIS AGREEMENT PRIOR TO PURCHASING IT AND DO NOT AGREE TO THIS AGREEMENT, CONTACT YOUR PLACE OF PURCHASE TO RETURN THE PRODUCT FOR A REFUND IN ACCORDANCE WITH ITS REFUND POLICIES.

SEE SECTION 11 REGARDING YOUR CONSENT TO AIRTIGHT’S USE OF CERTAIN COLLECTED DATA.

1. DEFINITIONS

1.1 “You” or “Your” shall mean any person, entity or organization that uses AirTight products.

1.2 “AirTight,” shall mean AirTight Networks, Inc.

1.3 “AirTight Competitor” a person or entity in the business of wireless security products or services substantially similar to AirTight’s products or services.

1.4 “Your Customers” means your current or potential customers excluding any AirTight Competitor.

1.5 “Documentation” shall mean the end-user technical documentation that AirTight supplies with the Hardware (if any) and Software. Advertising and marketing materials are not Documentation.

1.6 “Error” shall mean a reproducible failure of the Software or Hardware to perform in substantial conformity with its Documentation.

1.7 “Hardware” shall mean the hardware containing AirTight software. Not all AirTight Products come with hardware.

1.8 “Intellectual Property Rights” shall mean copyrights, trademarks, service marks, trade secrets, patents, patent applications, moral rights, contractual rights of non-disclosure or any other intellectual property or proprietary rights, however arising, throughout the world.

1.9 “Release” shall mean any Update or Upgrade if and when these are made available by AirTight. In the event of a dispute as to whether a particular Release is an Update or an Upgrade, AirTight's published designation will be final.

1.10 “Software” shall mean the software (in object code format) created or licensed by AirTight and licensed to you either as a stand alone product or loaded on AirTight Hardware, and any Release thereto.

1.11 “Update” shall mean, if and when available, any error corrections, fixes, workarounds or other maintenance releases with respect to the Software provided by AirTight that do not add functionality to the Software.

1.12 “Upgrade” shall mean, if and when available, new releases or versions of the Software that materially improve the functionality of, or add material functional capabilities to, the Software. AirTight may charge additional license fees for Upgrades.

2. CONTROLLING AGREEMENT: This electronic Agreement is the entire agreement between you and AirTight and supersedes all prior or contemporaneous agreements, understandings, and communications, whether written or oral unless such agreement is executed by an officer of AirTight. In such event, that agreement shall only supersede this Agreement to the extent such agreement conflicts with this Agreement. Any terms and conditions in your paper or electronic purchase order, request for proposal or quotation, or a response to those documents are superseded by this electronic Agreement. If a third party reseller accepts your purchase order and an officer of AirTight does not sign it and return it to you, AirTight is not accepting its terms and conditions. AirTight is not obligated under any reseller's agreement with you unless an officer of AirTight signs the agreement. Certain third party software may be necessary to operate or run the Software, you are responsible for obtaining and licensing such third party software. Third party software is governed by the license agreement provided by that third party.

3. LICENSE GRANT

3.1 Limited License. All Software is licensed, not sold and subject to this Agreement. All Hardware is sold subject to the license granted in this Agreement. For each unit of Hardware and/or Software that you purchase, AirTight grants you a non-exclusive, non-transferable (except as provided in the Section entitled *Assignment*), non-sublicensable license during the term of this Agreement, to install and execute such Software and Hardware. The Software and Hardware are licensed for your own internal business purposes unless you have purchased or been given a demonstration version or audit version of the Software. If you have a demonstration version of the Software, you may use the Software solely to provide demonstrations to Your Customers. If you have an audit version of the Software, you may use it to provide services to Your Customers. You may make and retain one copy of the Software for back-up and disaster recovery purposes so long as you clearly mark it as a "back-up" or similar language.

3.2 Restrictions on Use. Except as expressly provided for in this Agreement, you shall not: (a) adapt, alter, publicly display, publicly perform, translate, create derivative works of or otherwise modify the Software; (b) sublicense, lease, rent, loan, distribute or otherwise transfer the Software to any third party (except as provided in the Section entitled *Assignment*); (c) allow third parties to access or use the Software or Hardware, including but not limited to ASP, OEM, or time-sharing arrangements. You shall not reverse engineer, decompile, disassemble or otherwise attempt to derive the source code for the Software except to the extent expressly permitted by applicable law to obtain information necessary to render the Software interoperable with other software; provided, however, that you must first request such information from AirTight and AirTight may, in its discretion, either provide such information to you or impose reasonable conditions, including a reasonable fee, on such use of the source code for the Software to ensure that AirTight's and its suppliers' proprietary rights in the source code for the Software are protected; You shall not remove, alter or obscure any proprietary notices on the Software or Documentation. Under no circumstances may you install or execute the Software on more than one computer at the same time. Except to the extent necessary to provide a demonstration or services to Your Customer when you have purchased or been given the demonstration version or audit version of the Software, respectively, you shall not capture screenshots of the Software and share it with other people without AirTight's written consent.

3.3 Installation. You are responsible for installing the Software and Hardware (if any) unless you purchase installation services from AirTight or a third party pursuant to a separate agreement.

4. PROPRIETARY RIGHTS. You acknowledge and agree that the Software and Hardware, including but not limited to their sequence, structure, organization and source code, contains Intellectual Property Rights of AirTight and its suppliers. The Software is licensed and not sold to you, and no title or ownership to such Software or the Intellectual Property Rights embodied therein passes as a result of this Agreement or any act pursuant to this Agreement. The Software (and all Intellectual Property Rights therein) is the exclusive property of AirTight and its suppliers, and all rights in and to the Software not expressly granted to you in this Agreement, are reserved. AirTight owns all copies of the Software, however made. The Software, Hardware and related materials contain trade secrets of AirTight and you shall not provide the Software, Hardware, Documentation, or details regarding the operation of the Software and/or Hardware, or any other AirTight confidential and/or proprietary information to any third party.

5. LIMITED WARRANTY

5.1 Warranty. For a period of one year from your receipt of the Hardware and/or Software (the "Warranty Period"), AirTight warrants to you and for your sole benefit that, subject to the Section entitled *Exclusions*, the Software and Hardware when used as permitted under this Agreement and in accordance with the instructions in the Documentation, will operate substantially without Error.

5.2 Exclusions. AirTight will have no obligation to correct, and AirTight makes no warranty with respect to, Errors caused by: (a) improper installation of the Software or Hardware; (b) changes that you have made to the Software or Hardware; (c) use of the Software or Hardware in a manner inconsistent with the Documentation; (d) the combination of the Software or Hardware with hardware or software not provided by AirTight; (e) malfunction, modification or relocation of your servers; or (f) your failure to make reasonable backups.

5.3 Remedy for Errors. For Errors reported to AirTight during the Warranty Period, your exclusive remedy and AirTight's sole liability for breach of this warranty is that AirTight shall, at its own expense, (a) use commercially reasonable efforts to make available to you, by Internet download, Updates that are intended to correct such Errors and that AirTight makes generally available; (b) at its election, repair or replace any defective Hardware returned to AirTight within the Warranty Period. Any remedy provided under this Section 5.3 will not extend the original Warranty Period. AirTight shall have no obligation regarding Errors reported, or returns made, after the Warranty Period.

5.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTY IN SECTION 5.1, AIRTIGHT AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, RESULT, EFFORT, TITLE AND NON-INFRINGEMENT. THERE IS NO WARRANTY THAT THE SOFTWARE WILL BE ERROR FREE, OR THAT THE SOFTWARE OR HARDWARE WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF YOUR PARTICULAR PURPOSES OR NEEDS. AIRTIGHT PROVIDES NO WARRANTY FOR ANY THIRD PARTY SOFTWARE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: AIRTIGHT, ITS AFFILIATES, SUPPLIERS AND MANUFACTURERS SHALL NOT BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR RELIANCE DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE HARDWARE OR THE SOFTWARE, UNDER ANY LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOST PROFITS, LOST DATA, BUSINESS INTERRUPTION, PERSONAL INJURY, FOR LOSS OF PRIVACY, NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER, EVEN IF AIRTIGHT KNOWS OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

EXCEPT FOR AIRTIGHT'S OBLIGATIONS UNDER THE SECTION ENTITLED INDEMNIFICATION, AIRTIGHT'S, ITS AFFILIATES', SUPPLIERS' AND MANUFACTURERS' TOTAL CUMULATIVE LIABILITY FOR ACTUAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE HARDWARE, OR THE SOFTWARE, SHALL NOT EXCEED THE PRICE AIRTIGHT RECEIVED FOR SUCH HARDWARE OR SOFTWARE, REGARDLESS OF THE CAUSE OR FORM OF ACTION. THIS SECTION SHALL APPLY EVEN IF YOUR EXCLUSIVE REMEDY HAS FAILED OF ITS ESSENTIAL PURPOSE. YOU ACKNOWLEDGE AND AGREE THAT THE PRICES AND FEES REFLECT THE ALLOCATION OF RISK SET FORTH IN THIS AGREEMENT AND THAT AIRTIGHT WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY.

7. INFRINGEMENT INDEMNIFICATION

7.1 AirTight's Obligation. Subject to the Sections entitled *Conditions* and *Exclusions*, if a third party makes a claim against you alleging that the Hardware or Software infringes any U.S. patent or copyright registered or issued as of the Start Date, AirTight shall: (a) pay all reasonable costs to defend you; and (b) pay any damages assessed against you in a final judgment by a court of competent jurisdiction or any settlement that AirTight has agreed upon with such third party.

7.2 Conditions. AirTight shall be obligated to pay these costs only if you: (a) notify AirTight promptly in writing of any such claim; (b) give AirTight full information and assistance in settling and/or defending the claim; and (c) give AirTight full authority and control of the defense and settlement of any such claim. You may also participate in the defense at your own expense.

7.3 Exclusions. AirTight shall not be liable for: (a) any costs or expenses incurred by you without AirTight's prior written authorization; (b) any use of the Hardware or Software not in accordance with this Agreement or the Documentation; (c) for any claim based on the use or a combination of the Hardware or Software with any other software, firmware, hardware or data not provided or approved by AirTight; (d) use of any Release of the Software other than the most current Release made available to you; or (e) any alterations or modification of the Hardware or Software by any person other than AirTight or its authorized agents.

7.4. Cure. In the event AirTight is required, or in AirTight's sole opinion is likely to be required, to indemnify you under

the Section entitled *AirTight's Obligation*, AirTight shall do one of the following: (a) obtain the right for you to continue using the Hardware or Software; (b) replace or modify the Hardware or Software with a functional equivalent that is non-infringing; or (c) terminate this Agreement and refund any fee AirTight received, prorated over 3 years, or the period of your license if shorter than 3 years.

8. RISKS AND YOUR OBLIGATIONS. AirTight products may be capable of operating at frequencies beyond those allowed in your region and locating and disabling targeted wireless devices and computers. YOU USE AIRTIGHT PRODUCTS AT YOUR OWN RISK. If a third party makes a claim against AirTight arising out of your use of the AirTight products or your breach of this Agreement, you shall: (a) pay all costs to defend AirTight; and (b) pay any damages assessed against AirTight in a final judgment by a court of competent jurisdiction or any settlement that you agreed upon with such third party. If you fail to meet your obligations under this Section, AirTight shall have full authority and control of the defense and/or settlement of any such claim at your expense.

9. EXPORT RESTRICTIONS. You acknowledge that the Software is subject to U.S. export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use, and destination restrictions issued by U.S. and other governments. You assume sole responsibility for any required export approval and/or licenses and all related costs. You shall not acquire, ship, transfer or re-export, directly or indirectly, the Hardware and/or Software to proscribed, embargoed, or prohibited countries or their nationals, denied destinations, nor use it for nuclear activities, chemical biological weapons or missile projects. Proscribed countries, destinations, and people are set forth in the United States Export Administration Regulations, and the Office of Foreign Asset Control's Specially Designated Nationals list, and are subject to change without further notice from AirTight.

10. U.S. GOVERNMENT END USERS. The Software covered under this Agreement, is a "commercial item" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software and any other software and documentation covered under this Agreement with only those rights set forth therein.

11. CONSENT TO USE OF DATA. You agree that AirTight and its affiliates may collect and use information that is personally identifiable to you. We collect two types of information.

    - **Technical Information** regarding the AirTight products and your hardware or software, including, but not limited to, server installation and activation information, license key expiration, server logs, Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, wireless network (WLAN) information and sensor details. The product features allowing us to collect Technical Information are enabled by default to connect via the Internet to AirTight's and/or its affiliates' computer systems automatically, and may occur without separate notice to you. You consent to the operation of these features. You may choose not to give us this information by not activating or installing the product.

    - **Personal Information** (name, address, telephone number, company name and email address), collected, for example, as part of shipping, servicing or registering a product. If we collect Personal Information we will expressly ask you for it. You may choose not to give us this information at the time we request it, but it may prevent us from shipping or servicing the product.

AirTight and its affiliates may use Technical and Personal Information solely to improve our products or to provide customized services or technologies to you. AirTight will not disclose this information in a form that personally identifies you except to third party providers that we utilize to service or ship the products. We may disclose the collected information if required to by law or court order. Information that is collected by or sent to AirTight may be stored and processed in the United States, India or any other country in which AirTight, its affiliates, subsidiaries or agents maintain facilities. You may contact us regarding the collection and use of Technical and Personal Information or this provision at support@airtightnetworks.com or by writing us at 339 No. Bernardo Avenue, Suite 200, Mountain View, CA 94043 USA.

12. GENERAL

12.1 Term. This Agreement shall start on the date you click "I have read and agree to the licensing terms above," "I Agree" or otherwise install or activate the Software or Hardware (the "Start Date") and shall continue in full force and effect until it expires pursuant to the period of use that you purchased or unless earlier terminated as described in the Section

entitled *Termination*.

12.2 Termination. Without prejudice to any other rights, AirTight may terminate this Agreement if you do not comply with it. You may terminate this Agreement at anytime. Upon termination of this Agreement for any reason: (a) all license rights granted in this Agreement will immediately terminate and you must promptly stop all use of the Software; (b) AirTight's obligation to provide services under any service agreement terminates; (c) you must erase all copies of the Software from your computers, and destroy all copies of the Software and Documentation on tangible media in your possession or control. Termination of this Agreement will not affect your right to otherwise use or transfer the Hardware purchased from AirTight once the Software is removed.

12.3 Survival. The Sections entitled *Controlling Agreement*, *Proprietary Rights*, *Limited Warranty*, *Limitation of Liability*, *Risks and Your Obligations*, *Export Restrictions*, *Termination*, *Governing Law and Venue* and *Severability* shall survive the expiration or termination of this Agreement. AirTight's obligations under the Section entitled *Infringement Indemnification* shall survive only for claims based on use of the Hardware or Software during the licensed term.

12.4 Assignment. You may not assign or transfer, by operation of law, merger or otherwise, any of your rights or delegate any of your duties under this Agreement (including without limitation, the licenses with respect to the Software) to any third party without AirTight's prior written consent. Any attempted assignment or transfer in violation of the foregoing will be void. AirTight may assign its rights or delegate its obligations under this Agreement.

12.5 Governing Law and Venue. This Agreement will be governed by the laws of the State of California. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement. Any action or proceeding arising from or relating to this Agreement must be brought exclusively in a federal or state court seated in Santa Clara, California, and in no other venue. Each party irrevocably consents to the personal jurisdiction and venue in, and agrees to service of process issued by, any such court. Notwithstanding the foregoing, AirTight reserves the right to file a suit or action in any court of competent jurisdiction as AirTight deems necessary to protect its intellectual property and proprietary rights.

12.6 Equitable Relief. You agree that the Software and Hardware contains AirTight's valuable trade secrets and proprietary information and that any actual or threatened disclosure or misappropriation of such information would constitute immediate, irreparable harm to AirTight for which monetary damages would be an inadequate remedy. Therefore, in addition to any other rights and remedies which may be available to AirTight at law or in equity, any such actual or threatened disclosure may be stopped through injunctive proceedings without the posting of a bond.

12.7 Waivers and Amendments. All waivers must be in writing. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. This Agreement may be amended only by a written document signed by you and AirTight.

12.8 Severability. If any provision of this Agreement is held to be void, invalid, unenforceable or illegal, the other provisions shall continue in full force and effect.

Table of Contents

Table of Figures

Chapter 1 Getting Started

1.1 Before You Begin

Thank you for purchasing SpectraGuard Enterprise (referred to as 'system' hereafter in this document) from AirTight® Networks, Inc. The system assists you to effectively monitor, troubleshoot, administer, and protect your wireless network.

Please read the EULA before installing the Server. Installing the Server constitutes your acceptance of the terms and conditions of the EULA mentioned above in this document. This product cannot be rented or leased–you are the sole owner of the product.

This installation guide gives an overview of the power connector and ports on the Server and explains how to configure it. This guide contains the following chapters:

- **Package Contents:** Lists the components included in the system package.
- **Server and Sensor (Sensor) Overview:** Provides an overview of the Server and Sensor.
- **Configuring the Server:** Describes how to power the Server, connect the Server to the network and your computer, and configure the Server.
- **Installing the Sensor:** Describes how to connect and install the Sensor.
- **Manual Configuration of Sensor:** Describes how to configure the Sensor through the Config Shell.
- **Setting up the System:** Describes how the system Console is launched and setup.
- **Config Shell Commands:** Lists a pre-defined set of commands that allow you to configure and view the status of the Server and Sensors.
- **Troubleshooting:** Provides troubleshooting tips while installing the Server and Sensor.

1.2 How to get more information

To receive important news on product updates, please visit our website at support@airtightnetworks.com.

1.3 Contact Information

AirTight® Networks, Inc.
339 N, Bernardo Avenue, Suite #200,
Mountain View, CA 94043
Tel: (650) 961-1111
Fax: (650) 963-3388

For technical support send an email to support@airtightnetworks.com.

Chapter 2 Package Contents

This chapter lists the components included in the Server and Sensor (both 802.11 a/b/g or 802.11 a/b/g/n) packages.

Note: *The conventions to be followed in the Guide are: 1> 802.11 a/b/g: SS-200-ATand 2> 802.11 a/b/g/n: SS-300-AT.*

Please ensure that the following items are included in the Server package. If the package is not complete, please contact AirTight® Networks, Inc. Technical Support at support@airtightnetworks.com, or return the package to the vendor or dealer where you purchased the product.

- Server with Software
- System Documentation CD-ROM containing:
  - SpectraGuard Enterprise User Guide
  - SpectraGuard Enterprise Installation Guide
  - SpectraGuard Enterprise Quick Setup Guide
  - SpectraGuard Enterprise Reports
  - SpectraGuard Enterprise Release Notes
  - Upgrade Instructions for SpectraGuard Enterprise
  - High Availability Configuration for SpectraGuard Enterprise
  - Network Detector Configuration for SpectraGuard Enterprise
- Power Cord
- Network Interface (Ethernet) Cable
- Serial Cable
- Rack Mounting Accessories

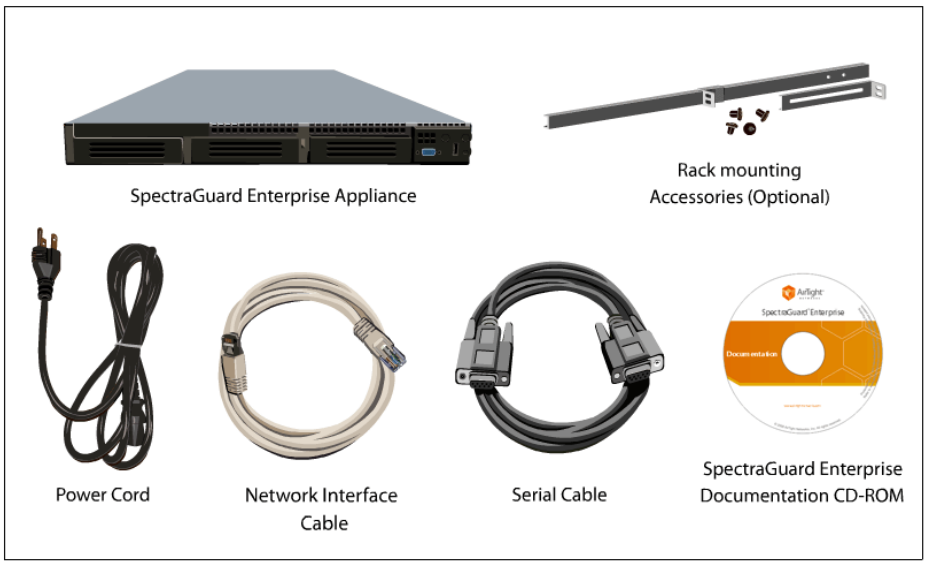


Figure 1. Server Package Contents

The contents of the a/b/g Sensor package are as follows:

- Sensor
- Ethernet Cable
- Wall Mounting Accessories

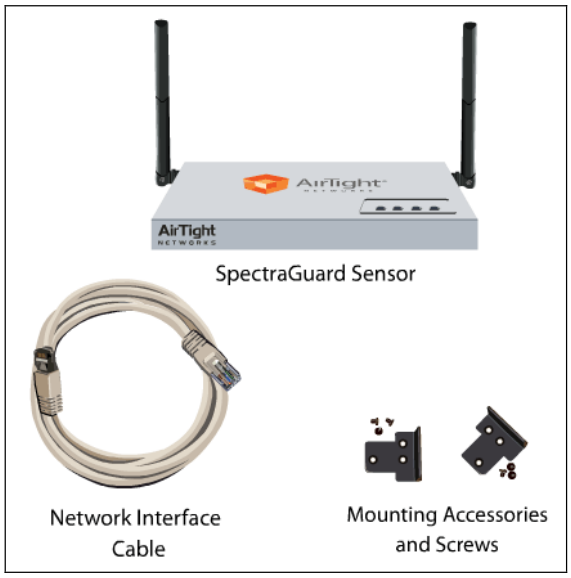


Figure 2. Sensor SS-200-AT Package Contents

***Note**: The MAC address of the Sensor is shown on a label at the bottom of the product and the packaging box*

Chapter 3 Server and Sensor Overview

This chapter provides an overview of the Server and Sensor and describes in detail about the following.

- Front Panel of the Server and Sensor
- Rear Panel of the Server and Sensor

3.1 Front Panel of the Server

The front panel of the Server has a Power switch and LEDs that indicate its state. The following figure shows the location of the Power switch and LEDs on the front panel of the Server.

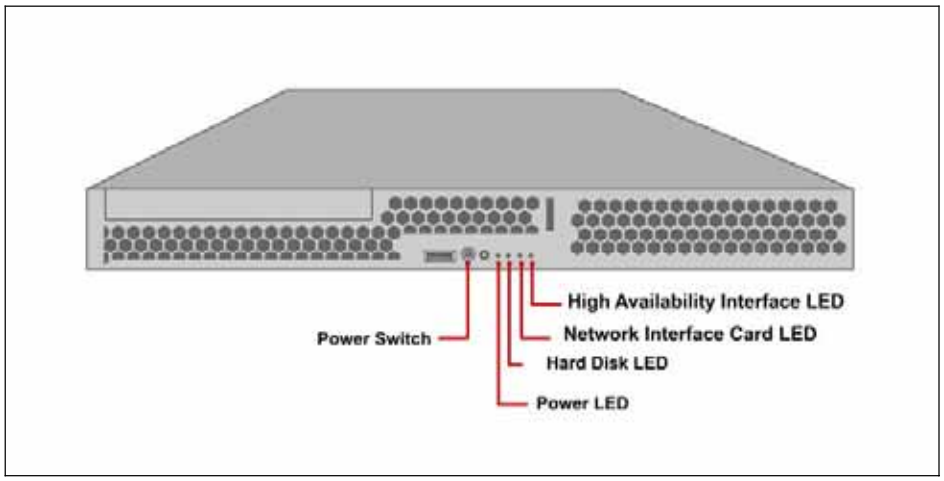


Figure 3. Front Panel of the Server

The following table describes the behavior of the Power switch.

Table 1. Behavior of Power Switch

Action	System Behavior	Recommended User Action
Push Power switch for two seconds	Graceful shutdown of the Server (similar to restarting the Server)	No action is required as the Server restarts automatically.
Push Power switch for more than three seconds	Hard shutdown of the Server (similar to disconnecting the power cable)	Press the Power switch again to power on the Server. Do not press the Power switch for a longer time as this may cause damage to the hard disk and thereby cause severe data loss.

The following table describes the status LEDs on the front panel of the Server.

Table 2. Front Panel LEDs

LED	LED Color	Meaning of LED
Power	Solid Green	Indicates that the Server is powered on and working normally
	Off	Indicates that the Server is not powered on or not receiving power
Hard Disk	Blinking Green	Indicates that the hard disk drive is being accessed
	Off	Indicates that the hard disk drive is not being accessed
Network Interface Card	Blinking Green	Indicates that the Server is connected to the network
	Off	Indicates that the Server is not connected to the network
High Availability Interface	Blinking Green	Indicates that the Server is a part of a high availability cluster
	Off	Indicates that the Server is not a part of a high availability cluster

3.2 Rear Panel of the Server

The rear panel of the Server has a power connector and ports that enable you to power up the Server and connect it to the network and a computer.

***Note**: Other connectors such as parallel port, 25- pin Serial port, keyboard connector, sound card, and so on are shown in the following figure. However, these connectors are **disabled** and cannot be used.*

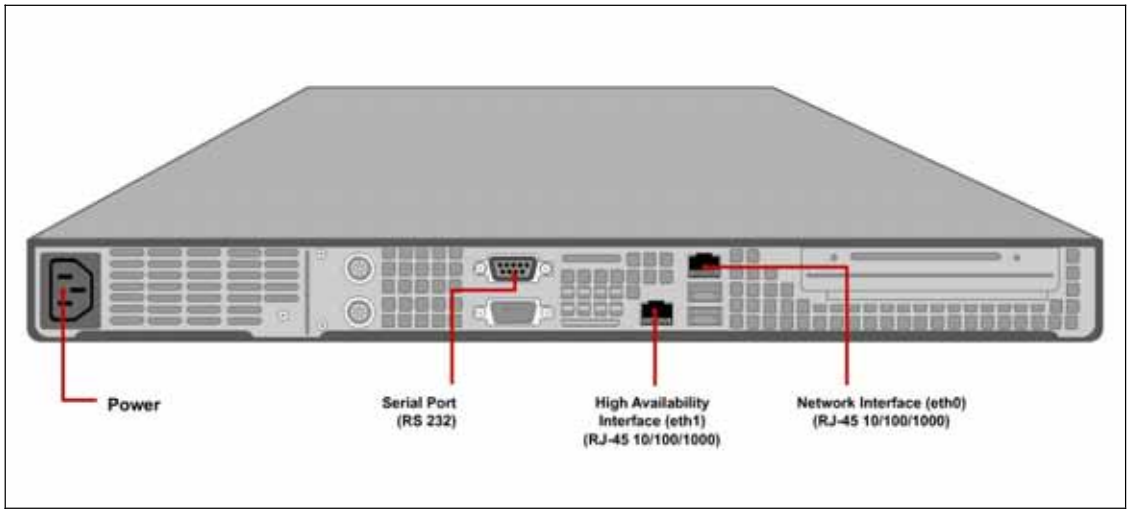


Figure 4. Rear Panel of the Server

The rear panel of the Server has a Serial (RS 232 F-F) port, a Network Interface port (RJ-45 10/100/1000 Ethernet), a High Availability (HA) port (RJ-45 10/100/1000 Ethernet), and a Power connector. The Power connector is used to power the Server using 110-240V 50/60 Hz AC input. The following table describes the Serial, Network Interface, and High Availability ports.

Table 3. Rear Panel Ports

Port	Description	Connector Type	Settings/Protocol
Serial	Enables a serial (RS-232) connection to establish terminal sessions using terminal emulation programs such as HyperTerminal for Windows or minicom for Linux	DB-9	**Settings**: Bits per second: 9600 Data Bits: 8 Parity: None Stop Bits: 1 Flow Control: None **Protocol**: RS-232

High Availability Interface	Used to connect the Server to a high availability cluster	RJ-45	**Settings**: 10/100/1000 Mbps **Protocol**: Ethernet
Network Interface	Used to connect the Server to the wired LAN through a hub or a switch Allows the Server to talk to Sensors	RJ-45	**Settings**: 10/100/1000 Mbps **Protocol**: Ethernet

3.3 Front Panel of Sensor

3.3.1 Sensor SS-200-AT

The front panel of the Sensor has LEDs that indicate the working of the Sensor.

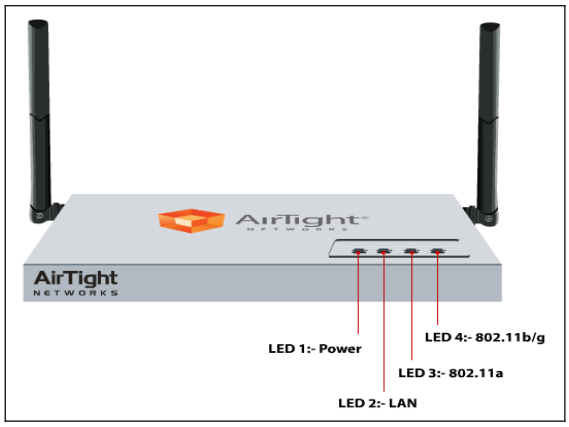


Figure 5. Front Panel of Sensor SS-200-AT

These LEDs are described in the following table.

Table 4. LED details for Sensor SS-200-AT and SS-300-AT

LED1 or Power	LED2 or LAN	LED3 or 802.11a	LED4 or 802.11 b/g	Description
Solid Green	Solid Green	Solid Green	Solid Green	The Sensor is receiving power and is working normally. The Sensor is connected to the Server.
Solid Green	Solid Green	Solid Green	Fast Blink	The Sensor is performing Troubleshooting on 802.11b/g.
Solid Green	Solid Green	Solid Green	Slow Blink	The Sensor is performing Intrusion Prevention on 802.11b/g.
Solid Green	Solid Green	Fast Blink	Solid Green	The Sensor is performing Troubleshooting on 802.11a.
Solid Green	Solid Green	Fast Blink	Fast Blink	The Sensor is performing Troubleshooting on 802.11a and 802.11b/g.
Solid Green	Solid Green	Fast Blink	Slow Blink	The Sensor is performing Troubleshooting on 802.11a and Intrusion Prevention on 802.11b/g.
Solid Green	Solid Green	Slow Blink	Solid Green	The Sensor is performing Intrusion Prevention on 802.11a.
Solid Green	Solid Green	Slow Blink	Fast Blink	The Sensor is performing Intrusion Prevention on 802.11a and Troubleshooting on 802.11b/g.
Solid Green	Solid Green	Slow Blink	Slow Blink	The Sensor is performing Intrusion Prevention on 802.11a and 802.11b/g.
Solid Green	Slow Blink	Slow Blink	Slow Blink	The Sensor upgrade is in progress.

Solid Orange	Solid Green	Any	Any	The Sensor is unable to get Ethernet link.
Solid Orange	Fast Blink	Any	Any	The Sensor did not receive a valid IP address via the DHCP.
Solid Orange	Slow Blink	Any	Any	The Sensor is unable to connect to the Server.
Solid Orange	Any	Solid Green	Any	There is an error on 802.11a/b/g interfaces.
Solid Orange	Any	Any	Solid Green	The Sensor is experiencing a software error.
Off	Off	Off	Off	The Sensor is not powered on or it is in the process of starting up.

3.3.2 Sensor SS-300-AT

The front panel of the Sensor has LEDs that indicate the working of the Sensor

Figure 6. Front View of Sensor SS-300-AT

Table 5. LED Details for Sensor SS-300-AT

LED1 or Power	LED2 or LAN	LED3 or 802.11an	LED4 or 802.11 b/gn	Description
Solid Green	Solid Green	Solid Green	Solid Green	The Sensor is receiving power and is working normally. The Sensor is connected to the Server.
Solid Green	Solid Green	Solid Green	Fast Blink	The Sensor is performing Troubleshooting on 802.11b/g/n.
Solid Green	Solid Green	Solid Green	Slow Blink	The Sensor is performing Intrusion Prevention on 802.11b/g/n.
Solid Green	Solid Green	Fast Blink	Solid Green	The Sensor is performing Troubleshooting on 802.11a/n.
Solid Green	Solid Green	Fast Blink	Fast Blink	The Sensor is performing Troubleshooting on 802.11a/n and 802.11b/g/n.
Solid Green	Solid Green	Fast Blink	Slow Blink	The Sensor is performing Troubleshooting on 802.11a/n and Intrusion Prevention on 802.11b/g/n.
Solid Green	Solid Green	Slow Blink	Solid Green	The Sensor is performing Intrusion Prevention on 802.11a/n.
Solid Green	Solid Green	Slow Blink	Fast Blink	The Sensor is performing Intrusion Prevention on 802.11a/n and Troubleshooting on 802.11b/g/n.
Solid Green	Solid Green	Slow Blink	Slow Blink	The Sensor is performing Intrusion Prevention on 802.11a/n and 802.11b/g/n.

Solid Green	Slow Blink	Slow Blink	Slow Blink	The Sensor upgrade is in progress.
Solid Orange	Solid Green	Any	Any	The Sensor is unable to get Ethernet link.
Solid Orange	Fast Blink	Any	Any	The Sensor did not receive a valid IP address via the DHCP.
Solid Orange	Slow Blink	Any	Any	The Sensor is unable to connect to the Server.
Solid Orange	Any	Solid Green	Any	There is an error on 802.11a/b/g/n interfaces.
Solid Orange	Any	Any	Solid Green	The Sensor is experiencing a software error.
Off	Off	Off	Off	The Sensor is not powered on or it is in the process of starting up.

3.4 Rear Panel of Sensor SS-200-AT

The rear panel of the Sensor SS-200-AT has a power connector and ports that enable you to power up the device and connect it to the network or a computer.

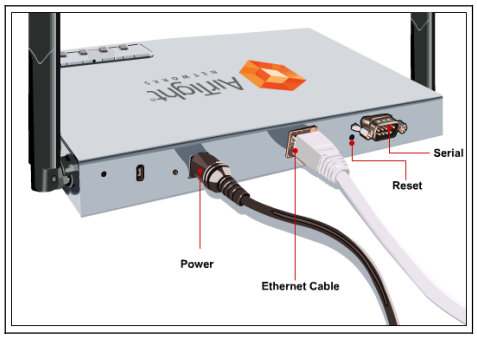


Figure 7. Rear Panel of Sensor

The Sensor has the following ports:

- **Serial port:** Connects the Sensor to serial terminal emulation programs such as Hyper Terminal for Windows or minicom for Linux.
- **Ethernet port:** Connects the Sensor to the network.
- **Reset switch:** Resets the Sensor to factory defaults. To reset the Sensor, press the **Reset** switch and power cycle (remove the power cable once and connect it back again) the Sensor till all LEDs blink green. Pressing <**Reset**> while the Sensor is running will not have any effect. The following settings are reset:
  - Config Shell Password is reset to **config**.
  - Server Discovery value is erased and changed to the default, **wifi-security-server**.
  - All the **VLAN configurations** are lost.
  - Sensor mode is changed to **Sensor Only**.
  - If **static IP** was configured on the Sensor, the **IP** is **erased** and **DHCP mode** is **set**.

After reset, all the LEDs will blink once, implying that the reset is successful.

Table 6. Rear Panel Port Settings for SS-200-AT

Port	Description	Connector Type	Speed/Protocol
Serial	Enables a serial connection to establish terminal sessions; used for launching Config Shell sessions	DB-9	**Settings**: Bits per second: 9600 Data Bits: 8 Parity: None Stop Bits: 1 Flow Control: None **Protocol**: RS-232
Ethernet	Enables the device to be connected to the wired LAN through a switch or a hub. This connection allows the Sensor to communicate with the Server	RJ-45	**Settings**: 10/100 Mbps **Protocol**: Ethernet

***Note**: The **Speed/Protocol** settings mentioned in the above table are the same for Hype Terminal and minicom.*

3.5 Rear and Side Panels of Sensor SS-300-AT

The rear panel of the Sensor SS-300-AT has an Ethernet port that enables the device to be connected to the wired LAN through a switch or a hub and also provides the power for the device using 802.3af standard.

Figure 8. Rear Panel of Sensor SS-300-AT

The Sensor has the following ports:

- **Ethernet port:** Connects the Sensor to the network and also provides the power.

Table 7. Rear Panel Port Settings for SS-300-AT

Port	Description	Connector Type	Speed/Protocol
Ethernet	This enables the device to be connected to the wired LAN through a switch or a hub. This connection allows the SpectraGuard Sensor to communicate with the SpectraGuard Enterprise® Server. This port also provides the power for the device using 802.3af standard	RJ-45	10/100/1000 Mbps Ethernet Power over Ethernet

***Note**: The **Speed/Protocol** settings mentioned in the above table are the same for Hype Terminal and minicom.*

The side panel of the Sensor SS-300-AT has a Reset Switch and a Serial Port.

Figure 9. Side Panel of Sensor SS-300-AT

The side panel has the following ports:

- **Serial port:** Connects the Sensor to serial terminal emulation programs such as Hyper Terminal for Windows or minicom for Linux
- **Reset switch:** Resets the Sensor to factory defaults. To reset the Sensor, press the **Reset** switch and power cycle (remove the power cable once and connect it back again) the Sensor till all LEDs blink green. Pressing <**Reset**> while the Sensor is running will not have any effect. The following settings are reset:
  - Config Shell Password is reset to **config**.
  - Server Discovery value is erased and changed to the default, **wifi-security-server**.
  - All the **VLAN configurations** are lost.
  - Sensor mode is changed to **Sensor Only**.
  - If **static IP** was configured on the Sensor, the **IP** is **erased** and **DHCP mode** is **set**.

After reset, all the LEDs will blink once, implying that the reset is successful.

Table 8. Side Panel Port Settings for SS-300-AT

Port	Description	Connector Type	Speed/Protocol
Reset	Allows resetting of SpectraGuard Sensor™ to factory settings.	Pin-hole push-button	Hold down and power cycle the Sensor to reset
Console	Enables a serial connection to establish terminal sessions. Used for launching Config Shell sessions.	RJ-45	RS 232 Serial Bits per second: 115200 Data Bits: 8 Parity: None Stop Bits: 1 Flow Control: None

Chapter 4 Installing the Server

You need to set up the Server before using it to monitor and protect your network. This chapter explains how to connect and configure the Server.

4.1 Connecting the Server

This involves mounting the Server appliance, powering it up, and connecting it to the network.

4.1.1 Mount the Server Appliance

Place the Server on the rack and mount it using the rack mounting accessories.

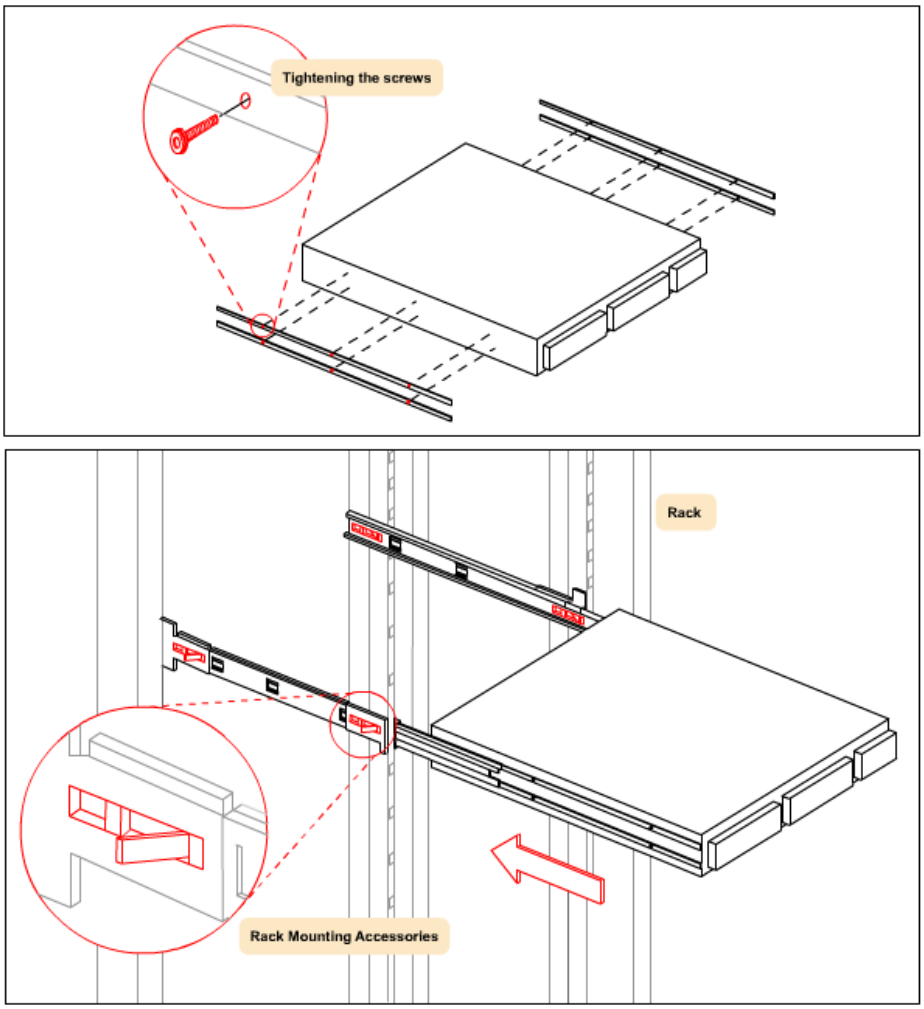


Figure 10. Mount the Server

4.1.2 Power up the Server

The Server appliance runs at 110-240V, 3-5A, 50-60 Hz AC power. AirTight® Networks recommends that you provide surge-free stable power to the Server.

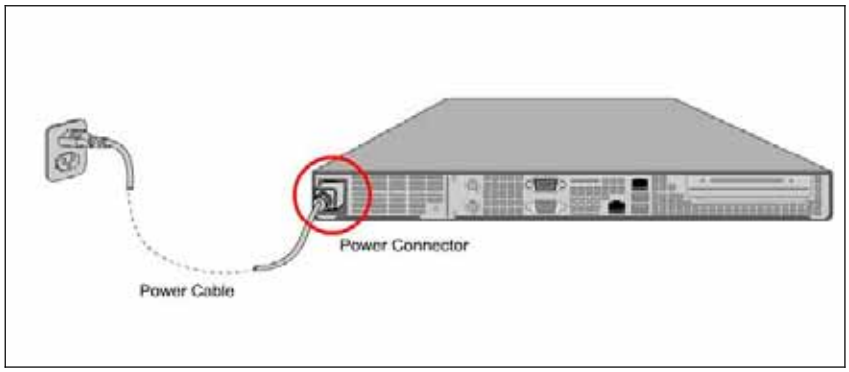


Figure 11. Power up the Server

To power up the Server, perform the following steps:
1. Connect one end of the Power cable to the Power socket on the rear panel of the Server.
2. Connect the other end of the Power cable to a 110-240V, 50/60 Hz AC power source.
3. Press the **Power** switch on the front panel of the Server.

***Note**: On connecting the **Power** cable, the **Power** LED should turn solid green.*

4.1.3 Connect the Server to the Network

Connect the Server to the desired network segment (subnet). The Server should be able to communicate with all the network segments that it tries to protect.

***Warning**! The default IP address of the Server is **192.168.1.246**. Please ensure that no other device on your network uses the same IP address as the Server. Connect the Network Interface Port on the Server to the desired subnet using the Ethernet cable provided to you as shown in the following. **Do not** connect the High Availability (HA) Interface Port to the subnet.*

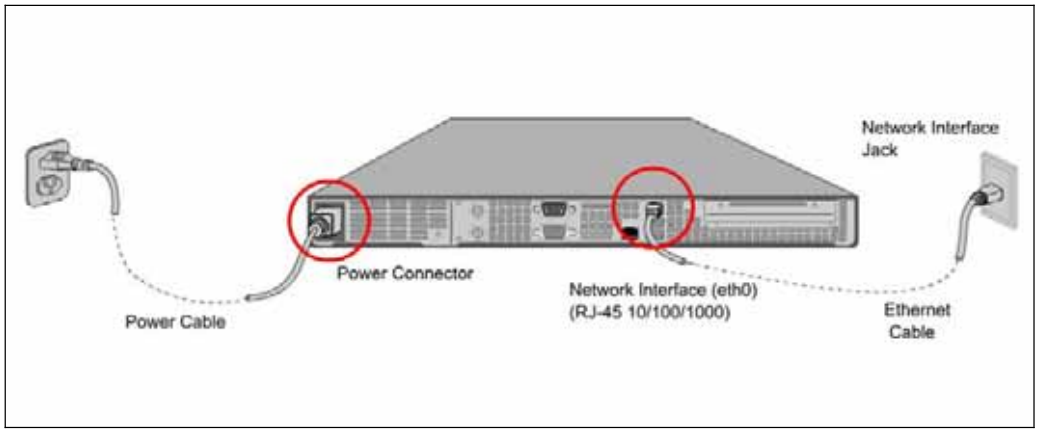


Figure 12. Connect the Server to the Network

To connect the Server to the network, perform the following steps:
1. Connect one end of the Network Interface cable to the **Network Interface** port on the rear panel of the Server.
2. Connect the other end of the Network Interface cable to the **Network Interface** jack located on the wall.

***Note**: On connecting the Network Interface cable, the **Network Interface Card LED** should turn solid green.*

4.2 Accessing the Server

You can access the Server in two ways:
- Using SSH Secure Shell (SSH) Client to access the Server (**Recommended**)
- Using a Serial RS-232 cable

4.2.1 *Accessing the Server using SSH (Recommended)*

To access the Server using SSH, perform the following steps:

1. Connect your computer to the same subnet where the Server is connected.

***Note**: The default IP address of the Server is **192.168.1.246**.*

2. Change your computer's IP address to 192.168.1.XXX, for example, 192.168.1.244.
3. Open SSH on your computer and press <**Enter**> or <**Space**> on the **SSH Secure Shell** dialog.
4. Access the default Server IP address, 192.168.1.246 as shown in the following figure.

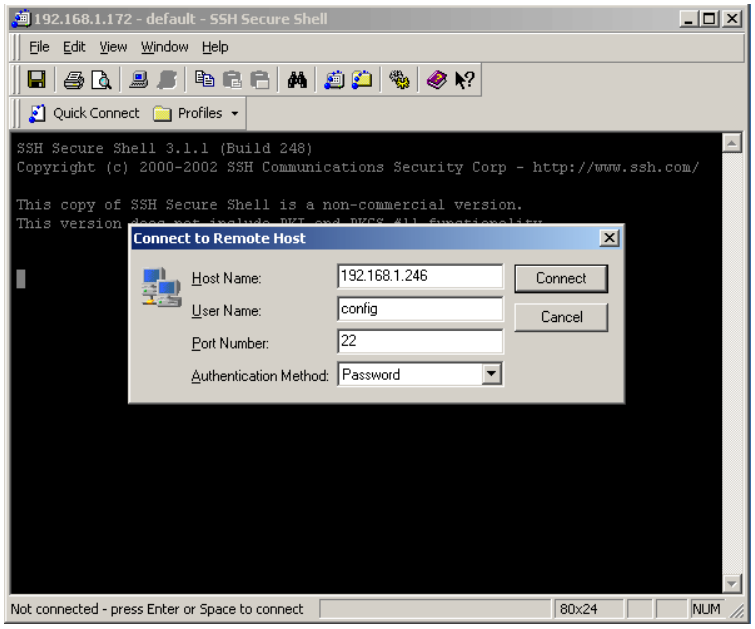


Figure 13. Open SSH

5. Login using the Username: **config** and Password: **config**.

4.2.2 *Accessing the Server using a Serial Cable*

Alternatively, you can access the Server using a Serial RS-232 cable as shown in the following figure and then following the steps listed below the figure.

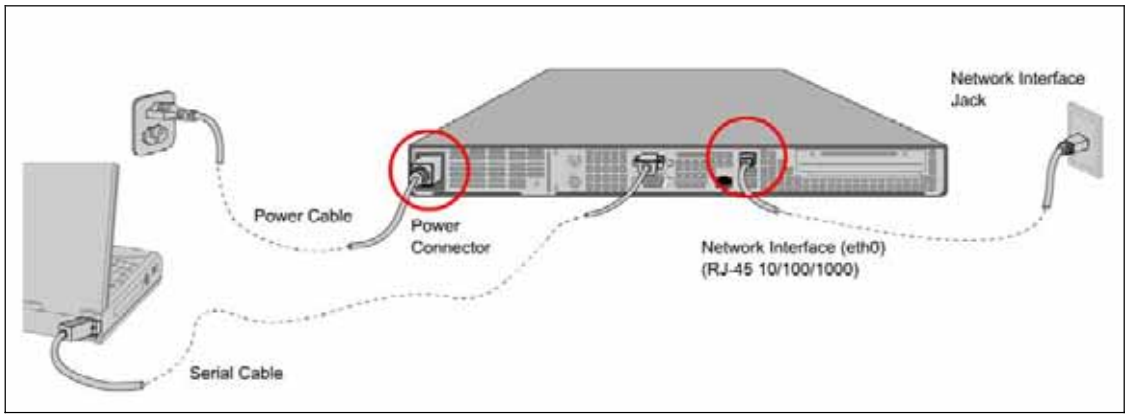


Figure 14. Connect the Server to your Computer using a Serial Cable

1. For Windows XP, launch the HyperTerminal application by clicking **Start→ Programs→ Accessories→ Communications→ HyperTerminal** on your desktop.

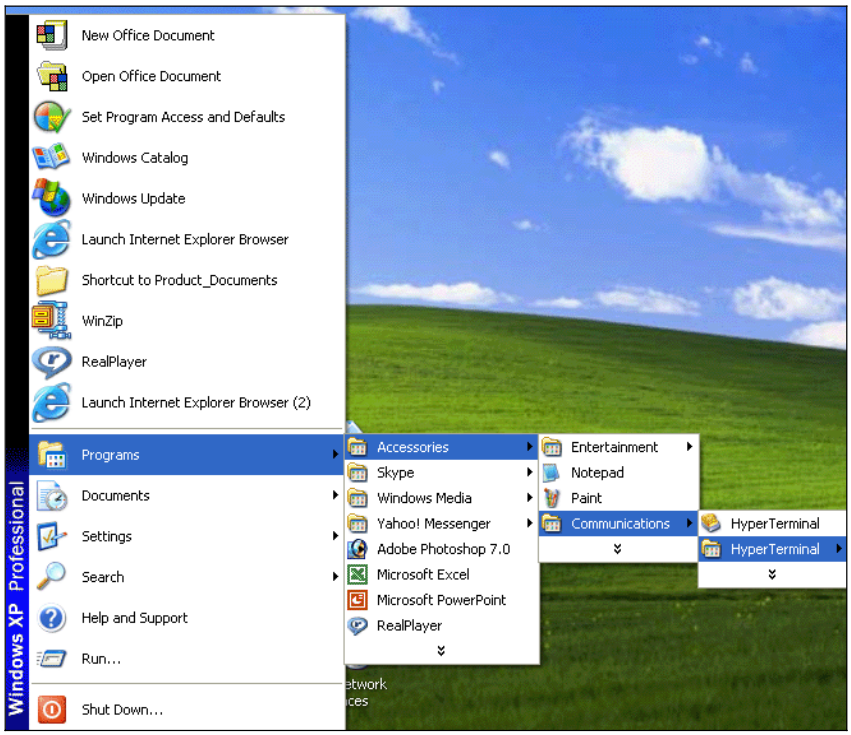


Figure 15. Launch HyperTerminal Application

2. Define a new HyperTerminal connection.
   - Select an icon to identify the new connection.
   - Type the user defined name for the HyperTerminal connection in the **Name** field
   - Click <**OK**> on the **Connection Description** dialog.

Figure 16. Define a New HyperTerminal Connection for the system

3. Specify the HyperTerminal connection details by selecting or entering the appropriate connection details and clicking <**OK**> on the **Connect To** dialog.

Figure 17. Specify HyperTerminal Connection Details

4. Edit the serial port settings as follows or click <**Restore Defaults**> to ensure proper communication between the Server and your computer.
   - **Bits per second**: 9600
   - **Data bits**: 8
   - **Parity**: None
   - **Stop bits**: 1
   - **Flow control**: None

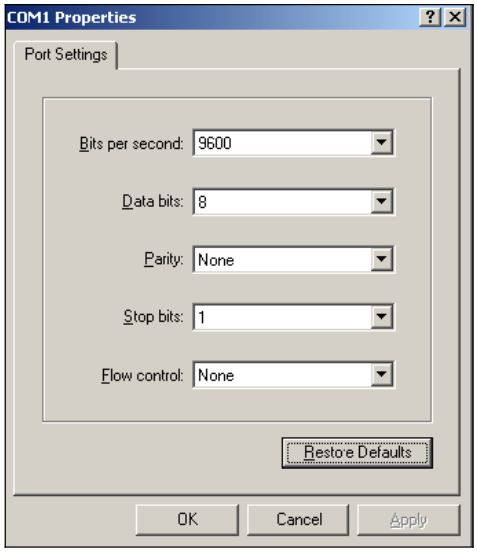


Figure 18. Edit Serial Port Settings

5. Click <**OK**> on the **COM Properties** dialog.
6. Press <**Enter**> or <**Space**> on the **HyperTerminal** screen. The login prompt appears.
7. Login using the Username: **config** and Password: **config**.

Important: *If you are configuring the Server for HA mode, you can skip the Server Initialization and Setup wizard and go to the config prompt. Change the config shell password, set the time zone, date and time, set the Server ID, and then use the* ***set ha*** *command to configure the Server in HA mode.*

4.3 Accessing the Server Initialization and Setup Wizard

The simple and intuitive Server Initialization and Setup Wizard allows you to map the Backspace key, change the configuration password, set the date and time and the time zone, change the network settings, and set the Server ID of the Server. You can retain the default values at each step by pressing <**Enter**>. Just follow the instructions in the Initialization and Setup Wizard to configure the Server. The wizard guides you through the rest of the setup of the Server.

4.3.1 Configure the Backspace Key

Map the **Backspace** key to work properly using the **set erase** command as shown in the following figure.

```
To configure backspace, use the 'set erase' command.
[config]$ set erase
Configures the backspace key.

Press the backspace key: ^?
[config]$ _
```

Figure 19. Map the Backspace key

The Server Initialization and Setup Wizard appears as shown in the following figure.

```
Server Version: [5.7]
Server Build: [5.7.148]

This Initialization and Setup Wizard will guide you through the Server setup.

Server Setup Steps:
1. Change config shell password
2. Change network settings
3. Set time zone, date and time
4. Set Server ID

Skip Server Setup Wizard? (y/[n]): n
```

Figure 20. Server Initialization and Setup Wizard Screen

4.3.2 Step 1: Change Config Shell Password

For security reasons, AirTight recommends that you change the config shell password. The Server deliberately avoids strong password checking because it does not want to force passwords that are difficult to remember.

The following figure shows how to change the config shell password.

```
Server Setup Step 1
Change Config Shell Password:
----------------------------
Choose a password that is difficult for others to guess but easy
for you to remember. Ideally, a password should be at least 8
characters and should contain a combination
of numbers, special characters, upper and lower case alphabets. Note the
password  and  keep it in a safe place.

Keeping the default password is a security risk.
Change default password? (y/[n]): y
Changing password for user config.
Changing password for config
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password: _
```

Figure 21. Change Config Shell Password

4.3.3 Step 2: Change Network Settings

The network settings of the Server specify its unique IP address on the network. Sensors use this IP address to identify the Server. The default IP address assigned to the Server is **192.168.1.246**.

Important: *Note the network settings on paper. If you forget the network settings, you can no longer access the Server over the network after it is rebooted. Use the Serial cable to access the Server and change its network settings.*

To change the network settings, provide the following input.

- **IP Address:** Choose an IP address that is compatible with the network segment on which the Server is to be connected. The Server should belong to the same subnet.
- **Subnet Mask:** Enter the mask of the network segment to which the Server is to be connected.
- **Gateway IP Address:** Enter the IP address of the gateway, for the subnet on which this Server is to be connected. Ethernet traffic from the subnet is forwarded to another network through the gateway.
- **Primary DNS IP Address:** Specify the IP address of the primary DNS Server used by the enterprise server to resolve DNS entries.
- **Secondary DNS IP Address:** Specify the IP address of the secondary (alternate) DNS Server used by the enterprise server to resolve DNS entries.
- **Tertiary DNS IP Address:** Specify the IP address of the tertiary (alternate) DNS Server used by the enterprise server to resolve DNS entries.
- **DNS Suffix:** Append this suffix to the unqualified domain name to generate a fully qualified domain name.

The following figures show how to change the network settings.

```
Server Setup Step 2
Change Network Settings:
------------------------

Settings for Server Network Interface (eth0):
IP Address: [192.168.1.246 ]
Subnet Mask: [255.255.255.0]
Gateway IP Address: []
Primary DNS IP Address: []
Secondary DNS IP Address: []
Tertiary DNS IP Address: []
DNS Suffix: []
Change Server Network Interface (eth0) settings? (y/[n]): y

IP Address [192.168.1.246]: 192.168.1.255
Set: IP Address = [192.168.1.255]
Subnet Mask [255.255.255.0]:
Set: Subnet Mask = [255.255.255.0]
Gateway IP Address []: 192.168.1.253
Set: Gateway IP Address = [192.168.1.253]
Primary DNS IP Address []: 192.168.1.13
Set: Primary DNS IP Address = [192.168.1.13]
Secondary DNS IP Address []: 192.168.1.49
Set: Secondary DNS IP Address = [192.168.1.49]
Tertiary DNS IP Address []:
Set: Tertiary DNS IP Address = []
DNS Suffix []: pune.wibhu.com
Set: DNS search path = [pune.wibhu.com]

Settings for Server Network Interface (eth0):

IP Address: [192.168.1.255]
Subnet Mask: [255.255.255.0]
Gateway IP Address: [192.168.1.253]
Primary DNS IP Address: [192.168.1.13]
Secondary DNS IP Address: [192.168.1.49]
Tertiary DNS IP Address: []
DNS Suffix: [pune.wibhu.com]
```

Figure 22. Change Network Settings

```
If you are using SSH over the network to access the
Server config shell,after confirmation, you may lose
connectivity to this Server because of an IP address change.
Start a new SSH session with the IP Address [192.168.1.255] to continue.
Confirm? ([y]/n): y_
```

Figure 23. Confirm Network Settings Changes

4.3.4 Step 3: Set Server Time Zone, Date and Time Settings

To set the Time Zone (TZ) correctly, select a continent, a country, and then a time zone region. You can use the Network Time Protocol NTP (NTP) to synchronize the Server clock with another Server or reference time source by specifying the IP address or the URL of the NTP Server.

The following five figures show how to change the time zone settings and the date and time settings.

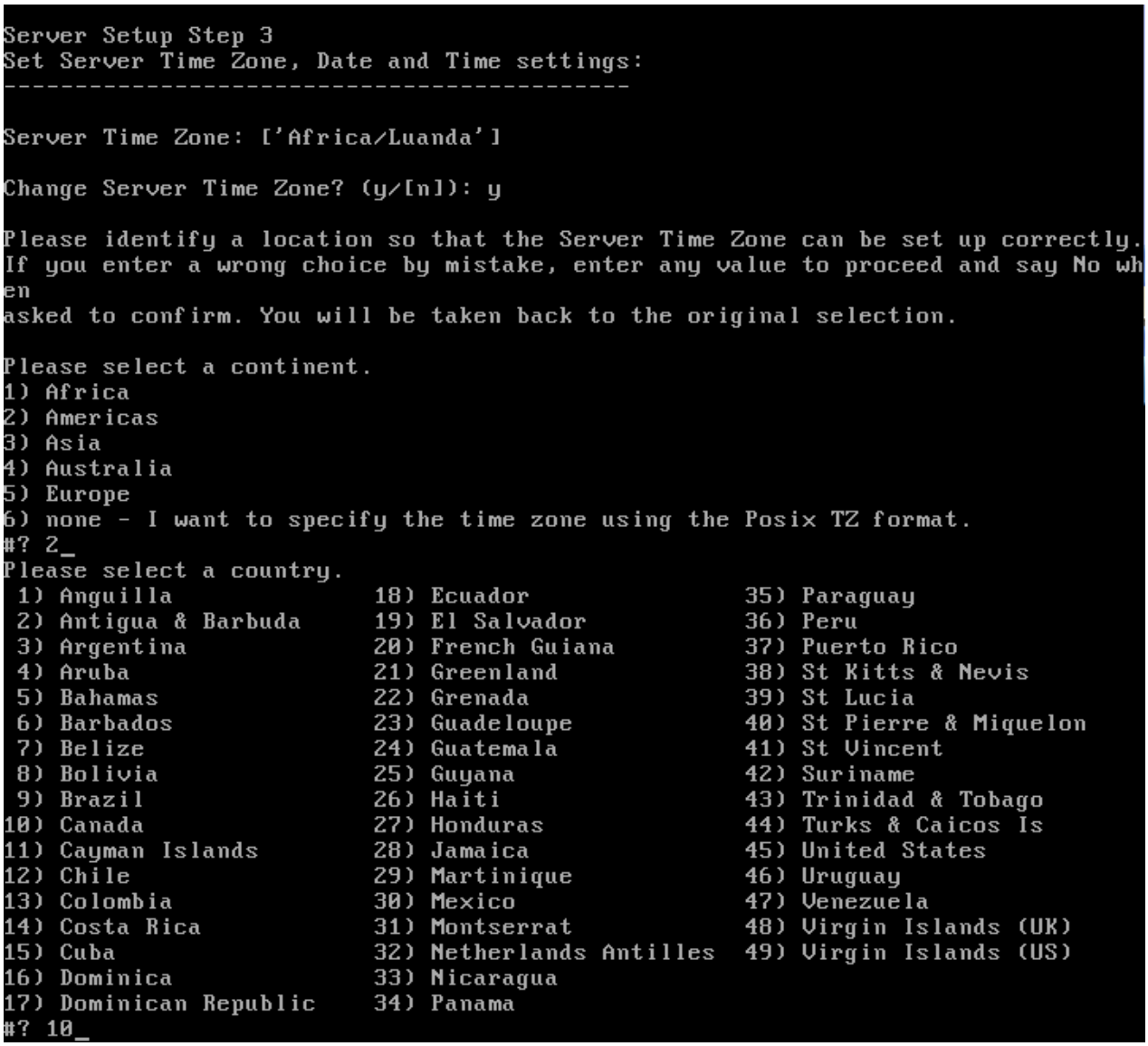


Figure 24. Specify Continent and Country for Time Zone Settings

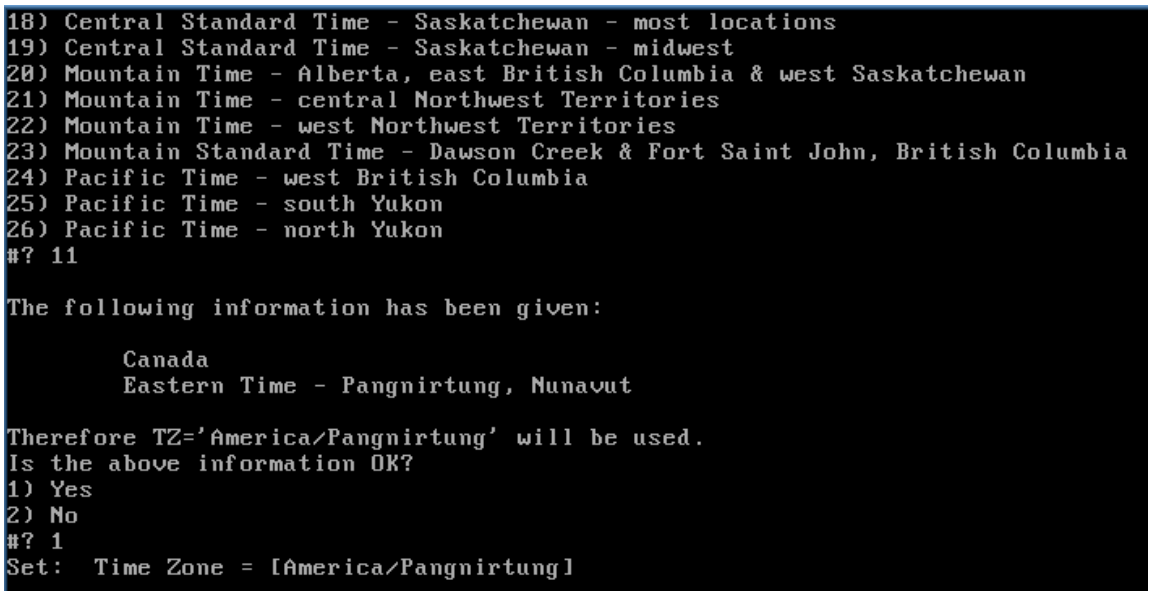


Figure 25. Select Time Zone Region

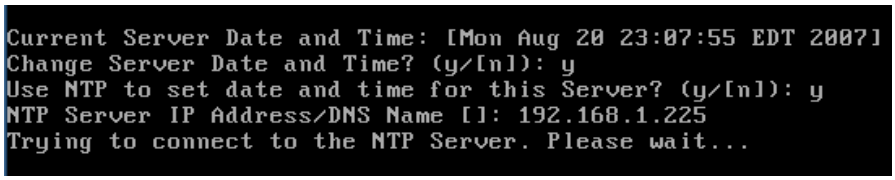


Figure 26. Specify IP Address of NTP Server for Synchronization

You can also specify the time zone using the Posix TZ [1]format as shown in the following figure.

[1] In Posix TZ systems, a user can specify the time zone by means of the TZ environment variable. The format used when there is no Daylight Saving Time (or summer time) in the local time zone is **std offset**, where 'std' specifies the name of the time zone and 'offset' specifies the time value one must add to the local time to get a Coordinated Universal Time value. It has a syntax [+ |-] hh [: mm [: ss]]. This is positive if the local time zone is west of the Prime Meridian and negative if it is east. The hour must be between 0 and 24, and the minute and seconds between 0 and 59.

```
Server Setup Step 3
Set Server Time Zone, Date and Time settings:
-----------------------------------------

Server Time Zone: ['America/Pangnirtung']

Change Server Time Zone? (y/[n]): y

Please identify a location so that the Server Time Zone can be set up correctly.
If you enter a wrong choice by mistake, enter any value to proceed and say No wh
en
asked to confirm. You will be taken back to the original selection.

Please select a continent.
1) Africa
2) Americas
3) Asia
4) Australia
5) Europe
6) none - I want to specify the time zone using the Posix TZ format.
#? 6
Please enter the desired value of the TZ environment variable.
For example, GST-10 is a zone named GST that is 10 hours ahead (east) of UTC.
gst-12_
```

Figure 27. Specify Time Zone using Posix TZ format

```
Set Server Date and Time manually? (y/[n]): y
Date in MM/DD/YYYY format [08/20/2007]: 08/28/2007
Time in HH:MM (24 hour) format [23:09]: 15:30

Confirm? ([y]/n): y_
```

Figure 28. Specify Date and Time

Important: *On the Date and Time settings screen, if the day exceeds 31 and the month exceeds 12, the system automatically sets the day to 31 and month to 12.*

4.3.5 Step 4: Set Server ID Settings

The Server ID is identifies a unique Server instance when there are multiple Server instances on the network. Sensors can be configured to communicate with a specific Server instance. The default Server ID is **1**.

Recommended*: Server ID setting is important only if you have a multi Server installation. If you have only one Server, the Server ID should be left at the default value* ***1****.*

The following figure shows how to set the Server ID.

```
Server Setup Step 4:
Server ID settings:
------------------

The Server ID is used to identify a unique Server instance
when there are multiple Server devices on the network.
Sensors can be configured to communicate with a specific Server instance.

The default Server ID is 1. If there is only one Server
instance on the network, you should leave the Server ID unchanged.

Change Server ID? (y/[n]): y

Server ID (1-65535) [1]:
Set: Server ID = [1]
Confirm? ([y]/n): y
Committing Server ID...
```

Figure 29. Set Server ID

The Server initialization completion message screen appears as shown in the following figure.

```
Server Setup is now complete. Server settings are as follows:

IP Address: [192.168.1.246]
Subnet Mask: [255.255.255.0]
Gateway IP Address: [192.168.1.253]
Primary DNS IP Address: [192.168.1.13]
Secondary DNS IP Address: [192.168.1.49]
Tertiary DNS IP Address: []
DNS Suffix: [pune.wibhu.com]
Server Time Zone: ['gst-12']

Server Date and Time: [Tue Aug 28 16:53:05 gst 2007]
Server ID: [1]

Confirm? ([y]/n): y_

To help you better with installation and problem resolution, support
information is periodically sent to a support website using https protocol.
A copy of this information is also sent to the administrator of this Server,
if email via SMTP is set up correctly. To set up the administrator email,
use Server Console (GUI).

Support information contains Server information and logs, WLAN Environment
and Sensor details. It is used solely for the purpose of providing you
better support. Support information will be sent on Wed Aug 29 00:12:00 gst 2007
.

If you want to control sending of support information, log in to the Server
Config Shell and use 'get support' and 'set support' commands to select
notification options. For more information on our collection and use of
personally identifiable information, see our "End User License Agreement"
by clicking the About button in the Server Console (GUI).

Press Enter to continue...
```

Figure 30. Server Setup Completion Screen

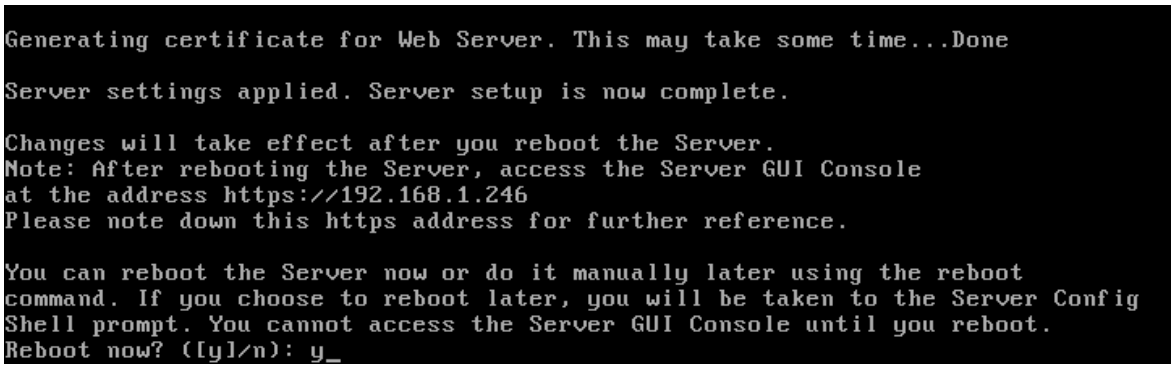


Figure 31. Generating Certificate for Web Server

Press **y** to reboot the Server for the changes to take effect. If you choose to reboot later press **n**. The Server Config Shell.prompt appears. You need to reboot the Server on completion of the Initialization and Setup Wizard before you access the Server Console ("GUI").

***Note**: On the Server Config Shell prompt, type the command **help** to view the list of available commands.*

4.3.6 Set up the Server DNS Entry

Add a DNS entry 'wifi-security-server' in your organization's/enterprise DNS Server. This entry should point to the Network Interface IP Address of the Server configured in Step 2: Change Network Settings.

Adding this entry serves two purposes:

- Sensors can connect to the Server with **zero configuration** if they are connected to a DHCP enabled subnet.
- You can access the Server using the address 'https://wifi-security-server'.

4.4 Launching the System Console (GUI)

4.4.1 System Requirements

Ensure that the following hardware and software is available on your computer before launching the system.

Table 9. Hardware Requirements

Hardware	Requirements
Processor	Intel P4 X86 architecture platform (or equivalent)
Processor Speed	1.4 GHz (minimum)
Memory	512 MB (minimum)
Screen Resolution	1024X768 (recommended)

Table 10. Software Requirements

Software	Requirements
Operating System (OS)	Windows 2000 or XP
Browser	Internet Explorer (IE) 5.5 or higher
Java Runtime Environment (JRE) version	JRE 1.6.0 or above

***Recommended**: In IE, under **Tools →Internet Options → Advanced**, deselect the option, **Reuse windows for launching shortcuts**. Additionally, under **Tools →Pop-up Blocker**, select **Turn Off Pop-up Blocker**.*

To launch the Console, perform the following steps:

1. Launch a Web browser such as IE 5.5 or higher on a client computer on the network that has Windows 2000 or XP Operating System (OS).
2. Enter the default IP Address for the Server, that is, **192.168.1.246**.
3. Click <**Yes**> on each of the security message pop-up dialogs to proceed.

Figure 32. Web Site Certificate Verification

The dialog shown below appears under the following conditions:

- If the correct version, that is, Sun JRE 1.6.0 is not detected on your computer
- If the version installed has not been activated for usage

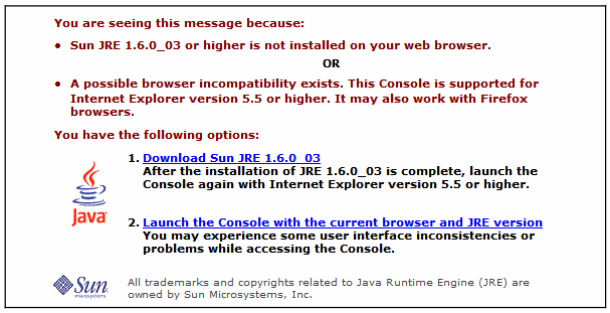


Figure 33. Installing JRE

4. Disable all pop-up blockers active on your Web browser to eliminate the warning message shown in the following figure.

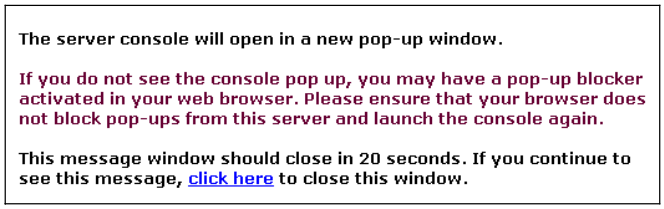


Figure 34. Pop-up Blocker Message

Figure 35. Detecting Java Runtime Environment (JRE)

Figure 36. Web Site Certificate Warning

5. Add a DNS entry for the hostname wifi-security-server and the IP address of the Server in the **hosts** file of the client computer to eliminate the warning shown in the following figure.

The hosts file is located at the following path:

- C:\WINNT\system32\drivers\etc\hosts, for Windows 2000
- C:\windows\system32\drivers\etc\hosts, for Windows XP

6. Save the **hosts** file and restart the browser to invoke the Console.

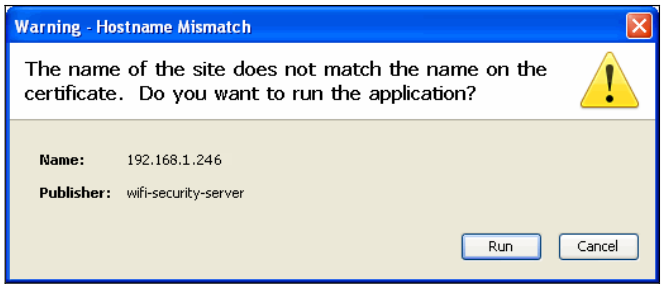


Figure 37. Hostname Mismatch Warning

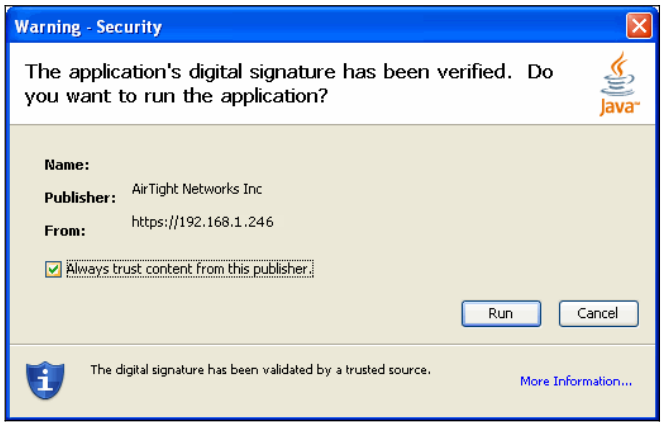


Figure 38. Digital Signature Verified

4.5 Activating the License

1. Save the license key file shipped with the Server on your desktop.
2. Browse to the license key file and select it. Click <**Apply**>.

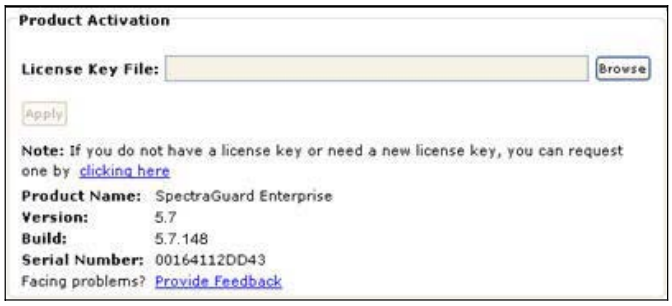


Figure 39. Activate License

If the license key is valid, you will see the **Login** screen. Otherwise, you will see an error message.

Chapter 5 Installing the Sensor

Sensor is the probe that monitors your network and communicates with the Server to guard your corporate network against over-the-air attacks. The Sensor must be plugged to your corporate network to perform the above operations.

Sensor can be configured in one of the following three modes:

- **Sensor Only (SO) Mode:** This is the default mode. In this mode, the Sensor should be connected into an access port on a switch. It then monitors a single VLAN that is configured on that access port. The wireless interface of the Sensor is enabled.
- **Network Detector (ND) Mode:** This mode needs to be explicitly configured. In this mode, the ND should be connected into a trunk port (802.1Q capable) on a switch. It then monitors multiple VLANs that are configured on that trunk port and are chosen by the user using the ND CLI. The wireless interface of the ND is disabled. An SS-200-AT Sensor in ND mode can monitor up to 32 VLANs. Similarly, an SS-300-AT can monitor upto 100 VLANs.
- **Sensor/ND Combo (SNDC) Mode:** This mode needs to be explicitly configured. In this mode, the Sensor should be connected into a trunk port (802.1Q capable) on a switch. It then monitors multiple VLANs that are configured on that trunk port and are chosen by the user using the ND CLI. The wireless interface of the Sensor is enabled. A SS-200-AT Sensor in SNDC mode can monitor up to 4 VLAN. Similarly, an SS-300-AT can monitor upto 16 VLANs.

Important: *To prevent abuse and intrusion by unauthorized personnel, it is extremely important to install the Sensor such that it is difficult to unplug the device from the network or from the power outlet.*

5.1 Zero Configuration of Sensors

Zero configuration is required if the following conditions are satisfied:

- The Sensor is in SO mode.
- A DNS entry 'wifi-security-server' is set up on all DNS Servers. This entry should point to the IP address of the Server. By default the Sensor looks for the Server DNS entry 'wifi-security-server'.
- Sensor is placed on a subnet that is DHCP enabled.

Important: *If a Sensor is placed on a network segment that is separated from the Server by a firewall, you must first open port 3851 for User Datagram Protocol (UDP) and Transport Control Protocol (TCP) bidirectional traffic on that firewall. This port number is assigned to AirTight® Networks. If multiple Sensors are set up to connect to multiple Servers, zero configuration is not possible. In this case manual configuration of Sensors is needed. Refer to* *Manually Configuring the Sensor* *for details.*

The steps to install the Sensor with no configuration (zero configuration) are as follows.

- Mount the Sensor
- Power up the Sensor
- Connect the Sensor to the network

5.2 Connecting the Sensor

This involves mounting the Sensor, powering it up, and connecting it to the network.

5.2.1 Mount the SS-200-AT Sensor

Take a configured Sensor, that is, make sure that the Sensor is given a static IP or the settings have been changed for DHCP. Note the MAC address and the IP address of the Sensor in a safe place before it is installed in a hard-to-reach location. The MAC address of the Sensor is printed on a label at the bottom of the product and the packaging box.

Recommended*: You should label the Sensors using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the Sensors.*

5.2.1.1 Ceiling Mounting

To mount the Sensor to a ceiling, perform the following steps:

1. Place the mounting bracket/mount on the Sensor and align the bracket slots with those on the Sensor as shown in the following figure.

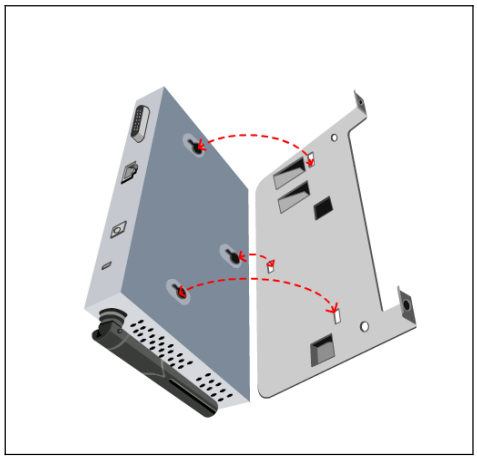


Figure 40. Aligning the Sensor and Mount Slots

2. Slide the mount and bend the two retaining plates forward to prevent the Sensor from sliding as shown in the following figure.

Figure 41. Fixing the Mounting Bracket to the Sensor

***Note**: You need to use only one of the two tabs on the mount at a time. For **U.S Installations**, use the tab **nearest** the edge for drop ceiling/t-bars that are approximately **1 inch** wide. You need to **bend** the **inner tab** for the smaller **European** drop ceilings so it is **flush/flat** with the bottom of the mount. Therefore, the inner tab does not protrude at all. You need to bend down the tab for US drop ceilings so that it protrudes approximately ¼ **inch** from the bottom. For **European Installations**, use the **inner** tab for drop ceilings/t-bars that are approximately ½ **inch** wide.*

Figure 42. Tab orientations for US Installations

3. Press the Sensor/bracket mount against the t-bar at an angle with the t-bar running between the two tabs that will eventually grab the drop ceiling t-bar as shown in the following figure.

Figure 43. Pressing the Mount against the T-Bar

4. Turn/twist the mount so that the two tabs begin to engage the t-bar and the t-bar passes over the **European** tab, which was pushed down flush. The t-bar should also push against the **US** tab, which was bent up approximately ¼ inch as shown in the following figure.

Figure 44. Initial Twisting of the Mount

5. Turn/twist the mount all the way, so that the two tabs completely engage the t-bar. The US tab bends up approximately ¼ inch and pushes against the side of the t-bar preventing the mount from twisting backward and disengaging form the t-bar as shown in the following figures.

Figure 45. Final Twisting of the Mount with the US tab supporting the Mount

5.2.1.2 Flat Surface Installation

You can place the Sensor on a flat surface such as a table, desktop, or filing cabinet. Do not install the Sensor on any type of metal surface. If you choose a flat surface mount, select a location that is clear of obstructions and provides good reception.

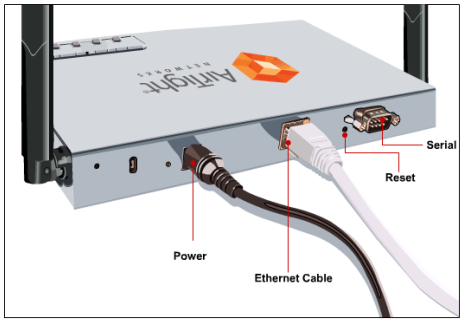


Figure 46. Flat Surface Installation

***Recommended**: AirTight does not recommend wall mounting of the Sensor as it uses omni directional antennas.*

5.2.2 Mount the SS-300-AT Sensor

Take a configured Sensor, that is, make sure that the Sensor is given a static IP or the settings have been changed for DHCP. Note the MAC address and the IP address of the Sensor in a safe place before it is installed in a hard-to-reach location. The MAC address of the Sensor is printed on a label at the bottom of the product.

***Recommended**: You should label the Sensors using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the Sensors.*

5.2.2.1 Ceiling/Wall Mounting

To install the Sensor on a wall or ceiling, use the mounting bracket that comes with the device. Follow these steps:

1. Following these guidelines, screw the mounting bracket to a wall or ceiling:
   - The mounting bracket tabs should be pointing upward.
   - If mounting to drywall, use the 4 screws and 4 wall anchors.
   - If mounting to an EU electrical box (60.3mm), use 2 threaded screws and insert into the holes marked “A” in the diagram shown below.
   - If mounting to a US electrical box (83.3mm), use 2 threaded screws and insert into the holes marked “B” in the diagram shown below.

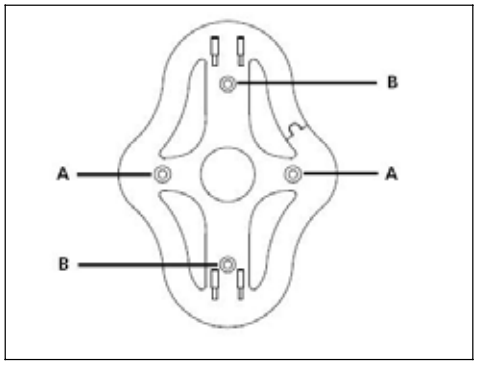


Figure 47. Holes for inserting screws

2. Connect the Ethernet cable (for power and network connection) to the LAN port on the back of the Sensor.
3. To mount the Sensor onto the mounting bracket, insert the mounting-bracket tabs into the slots on the back of the AP.

***IMPORTANT:** If you are mounting the Sensor on a wall, you cannot use the slots on the bottom narrow edge of the device. Instead, the slots on the back of the Sensor must be used.*

5.2.2.2 Flat Surface Installation

To install the Sensor on a flat surface such as a table or desktop, follow these steps:

1. Insert the tabs on the table stand into the slots on the side of the Sensor, as shown in the illustration. Align the cable routing cut out toward the upper part of the stand.

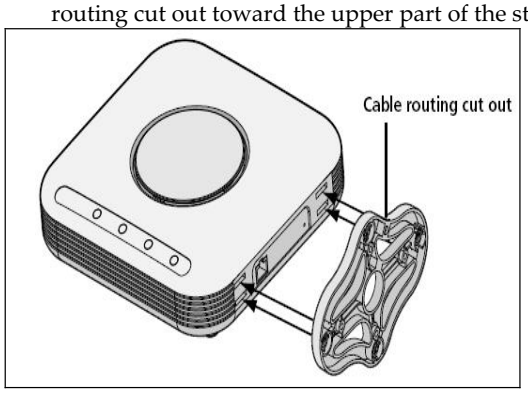


Figure 48. Inserting tabs on the table stand

2. To lock the stand to the Sensor, slide the stand back and the Sensor forward, as shown here:

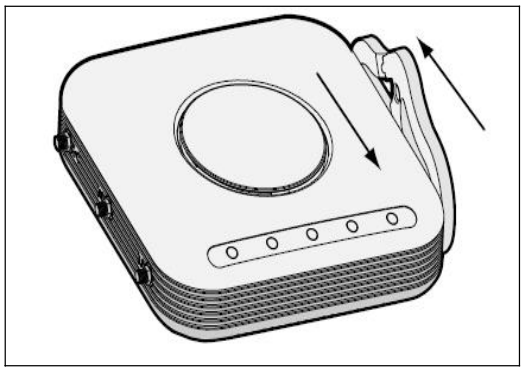


Figure 49. Locking the Stand to the Sensor

3. Place the Sensor and table stand on the table.

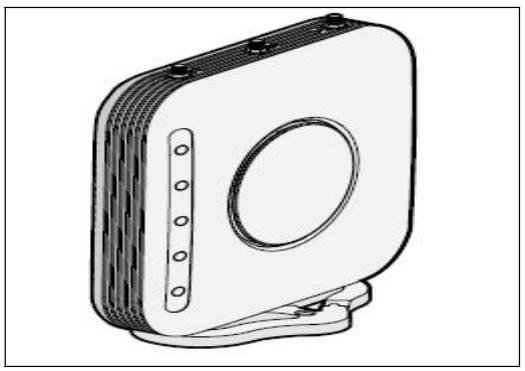


Figure 50. Sensor Mount on a Table

4. Connect the Ethernet cable for power and network connection to the LAN port on the back of the AP.

5.2.3 Power up the Sensor

An SS-200-AT Sensor runs on a 5V DC connection. Use the power adapter provided to power the Sensor from an 110V~240V 50/60 Hz AC power connection.

To power up the Sensor, perform the following steps:

1. Plug the power cable into the DC power receptacle at the rear of the Sensor.
2. Plug the other end of the power cable into an 110V~240V 50/60 Hz AC power source.

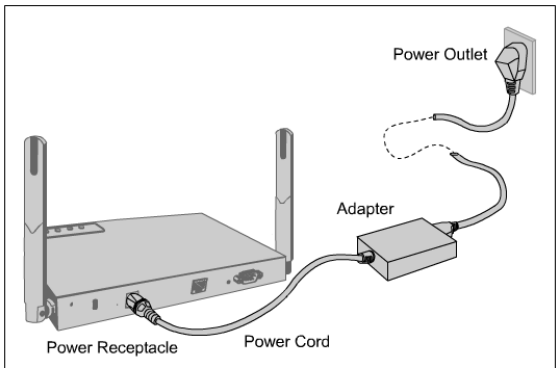


Figure 51. Power up the Sensor

Wait for two minutes!

3. Check the Status LEDs. You will see LED1 turn Orange and LED2 turn green, indicating that the Sensor is powered on correctly and waiting to be connected to the network.

An SS-300-AT Sensor can be Powered on by 802.3af Class 0 Power Over Ethernet of Nominal input voltage 48V DC.

5.2.4 Connect the Sensor to the Network

Ensure that the Server is already running on your network. Add the DNS entry 'wifi-security-server' on all DNS Servers. This entry should point to the IP address of the Server.

To connect the Sensor to the network, perform the following steps:

1. Ensure that DHCP is running on the subnet to which the Sensor will be connected.
2. Connect one end of the Network Interface cable to the Ethernet port at the rear of the Sensor.
3. Connect the other end of the Network Interface cable to an Ethernet jack that is connected to the desired subnet.

Important: *If DHCP is not enabled on a subnet, Sensors cannot connect to that subnet with zero configuration. Refer to Manually Configuring the Sensor for details on manual configuration of Sensor.*

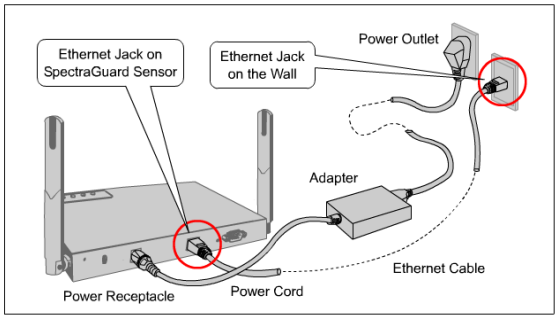


Figure 52. Connect the Sensor to the Network

Wait for two minutes!

Check the Status LEDs on the Sensor. If all LEDs glow green, then the Sensor is operational and connected to the Server.

Log on to the Server through SSH. Run the 'get sensor list' command. You will see a list of all Sensors that are recognized by the Server.

The Sensor is configured and ready to go. Check the Console to ensure that this Sensor has been detected.

If all the Sensors have connected with zero configuration, you need not read this installation guide further.

***Note**: If LED1 turns Orange, it means that the zero configuration was not successful and the Sensor must be configured manually. Refer to Manually Configuring the Sensor for details*

Chapter 6 Manually Configuring the Sensor

Important: *If the installation in Installing the Sensor was successful, stop! You do not need to configure the Sensor manually.*

6.1 Introduction

Manual configuration of a Sensor is typically required in the following cases:

- Sensor needs to be configured in ND or SNDC mode.
- Sensor Only (SO) devices cannot connect to the Server through zero configuration. The DNS entry for the Server has been changed to an entry other than "wifi-security-server" or there is no DNS Server present in the network. This is applicable for multi-server installations.
- Sensor is placed on a subnet that is not DHCP enabled.

6.2 Configuring Sensor through Config Shell

To use the Config Shell, connect a Serial (RS-232) cable between your computer and the Sensor. The Config Shell supports a pre-defined set of commands used to configure the Sensor.

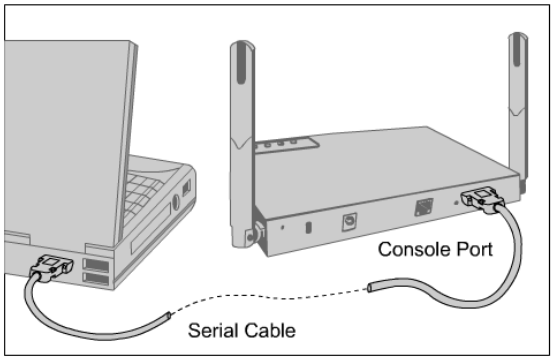


Figure 53. Connecting the Sensor to your computer using a Serial Cable

The steps to configure the Sensor manually are as follows:

1. Invoke Hyper Terminal (or minicom)
2. Log in and change the default password
3. Set Server Discovery
4. Set Sensor Mode
5. Set Network Settings for that Sensor Mode

The above steps are explained in detail below.

6.2.1 Invoke HyperTerminal (or minicom)

To configure the Sensor, follow the steps described below to invoke the Config Shell.

6.2.1.1 Launching HyperTerminal

To start HyperTerminal, click **Start→Programs→Accessories→Communications→HyperTerminal** as shown in the following figure.

Figure 54. Opening HyperTerminal

Note: If you are using a Linux laptop, you can use minicom to connect to the Config Shell.

6.2.1.2 Defining a New HyperTerminal Connection

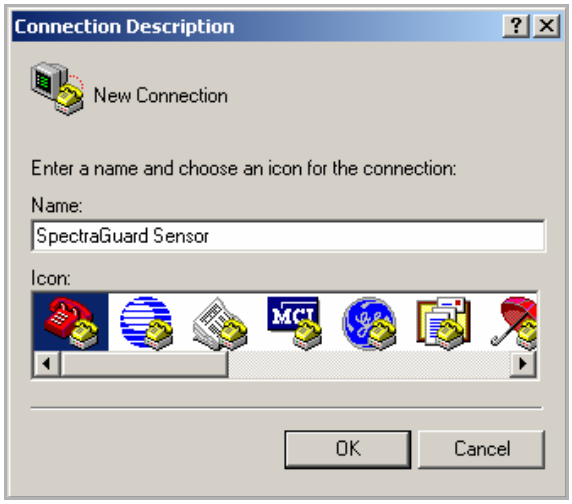


Figure 55. Define a New HyperTerminal Connection for Sensor

- Select an icon to identify the new connection.
- Type the required name for the HyperTerminal connection in the Name field
- Click <**OK**> on the **Connection Description** dialog.

6.2.1.3 Specifying HyperTerminal Connection Details

Figure 56. Specify HyperTerminal Connection Details

- Select or enter the appropriate connection details.
- Click <**OK**> on the **Connect To** dialog.

Note: The name of the serial port will change as per the settings of your computer.

6.2.1.4 Editing Serial Port Settings

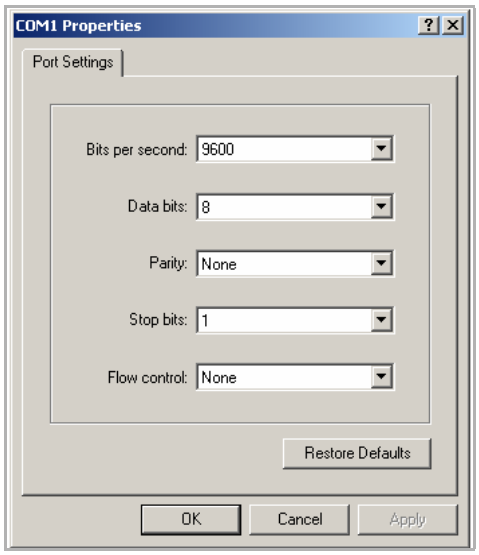


Figure 57. Edit Serial Port Settings

- Edit the serial port settings as follows or click <**Restore Defaults**> to ensure proper communication between the Sensor and your computer.
  - **Bits per second**: 9600
  - **Data bits**: 8
  - **Parity**: None
  - **Stop bits**: 1
  - **Flow control**: None
- Click <**OK**> on the **COM Properties** dialog.
- Press <**Enter**> or <**Space**> on the **HyperTerminal** screen.

6.2.2 *Log in and Change the Default Password*

Log in to the Config Shell using the user name **config** and password **config**. Change the default password using the command **passwd**. You can change the Sensor password using Sensor templates. Refer to section 8.4.4: Sensor Configuration in the Spectraguard Enterprise User Guide for more details.

Recommended; *AirTight recommends that you change the default password for security reasons, although it is not mandatory.*

6.2.3 *Set Server Discovery*

The next step is to set the Server Discovery information. There are two types of Server Discovery.

- Server IP based discovery (preferred)
- Server ID based discovery (deprecated)
- Service Location Protocol (SLP) based discovery (if wifi-security-server service has been configured)

Use the command **set server discovery** to point the Sensor to the correct Server.

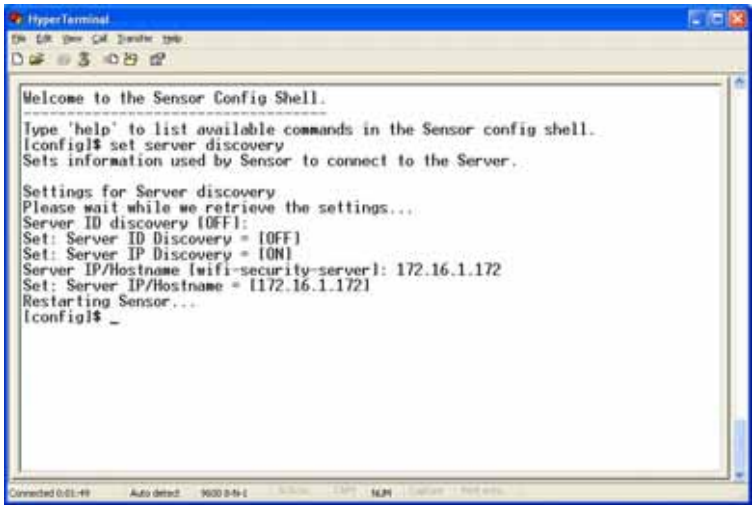


Figure 58. set server discovery command

Note*: If IP/Hostname based discovery is being used and there is more than one Server on the network, then you must enter the IP address of the appropriate Server.*

6.2.4 *Set Sensor Mode*

The next step is to set the mode of the Sensor. There are three possible modes:

- **SO Mode:** This is the **default** mode. In this mode, the Sensor **should be** connected into an **access port** on a switch. It then monitors a **single** VLAN that is configured on that access port. The wireless interface of the Sensor is **enabled**.
- **ND Mode:** This mode needs to be **explicitly configured**. In this mode, the ND **should be** connected into a **trunk port** (802.1Q capable) on a switch. It then monitors **multiple** VLANs that are configured on that trunk port and are chosen by the user using the ND CLI. The wireless interface of the ND is **disabled**. A Sensor in ND mode can **monitor** up to **32** VLANs and **detect** up to **32** VLANs.

- **SNDC Mode:** This mode needs to be **explicitly configured**. In this mode, the Sensor **should be** connected into a **trunk port** (802.1Q capable) on a switch. It then monitors **multiple** VLANs that are configured on that trunk port and are chosen by the user using the ND CLI. The wireless interface of the Sensor is **enabled**. A Sensor in SNDC mode can **monitor** up to **4** VLANs and **detect** up to **4** VLANs.

Use the **set mode** command to set the Sensor mode.

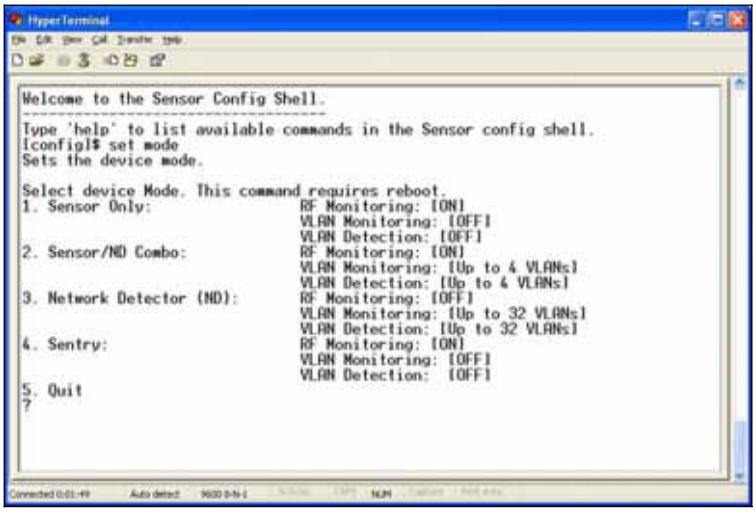


Figure 59. set sensor mode command

6.2.5 *Configure Network Settings*

Once the mode is set, you have to enable the Network Settings.

- **Sensor Only Mode:** For this mode, use the command **set ip config**. This command runs through the current VLAN and the IP config wizard.
- **Network Detector/Sensor/ND Combo Mode:** For this mode, use the command **set vlan config**. This command configures the IP addresses on the ND.

Refer to Chapter 3: Guidelines for Configuring and Installing ND and SNDC in the document 'Network Detector Configuration for SpectraGuard Enterprise_5.7' for further details.

Chapter 7 Setting up the Server Console

The Configuration Wizard guides you through the steps required to set up the system. The system is managed through a Java applet that is launched in the Internet Explorer 5.5+ Web browser. This HTML interface is known as the 'Console or Graphical User Interface (GUI)'. This chapter describes how the Console is launched and setup.

7.1 Logging into the Console

1. On the **Login** screen, type the **Login ID**: admin and the **Password**: admin and click <**Login**> or press <**Enter**>.

Figure 60. Console Login Screen

2. The **End User License Agreement** screen appears as shown in the following figure. Read the agreement carefully and select '**I have read and agree to the Licensing Agreement above'**. Click <**Next**>.

Figure 61. End User License Agreement Screen

7.1.1 Step 1: Starting the Setup Wizard

3. The **Welcome** screen appears as shown in the following figure. This wizard takes you through the steps to help you initialize the system. Click <**Next**> on each screen to proceed to the next step. To go back to a previous step, click <**Previous**>. To exit the setup wizard at any point, click <**Exit**>. You can take a tour of this wizard later through the Console from Administration→Global Tab→System Settings→Wizards and configure the appropriate settings. Click <**Start**>.

Figure 62. System Setup Wizard Welcome Screen

7.1.2 Step 2: Changing your Account Password

4. The **Change Password** screen appears as shown in the following figure. Change your account login password. Specify an email address for the user ***admin*** to be used later to test SMTP Server settings and other email notifications.

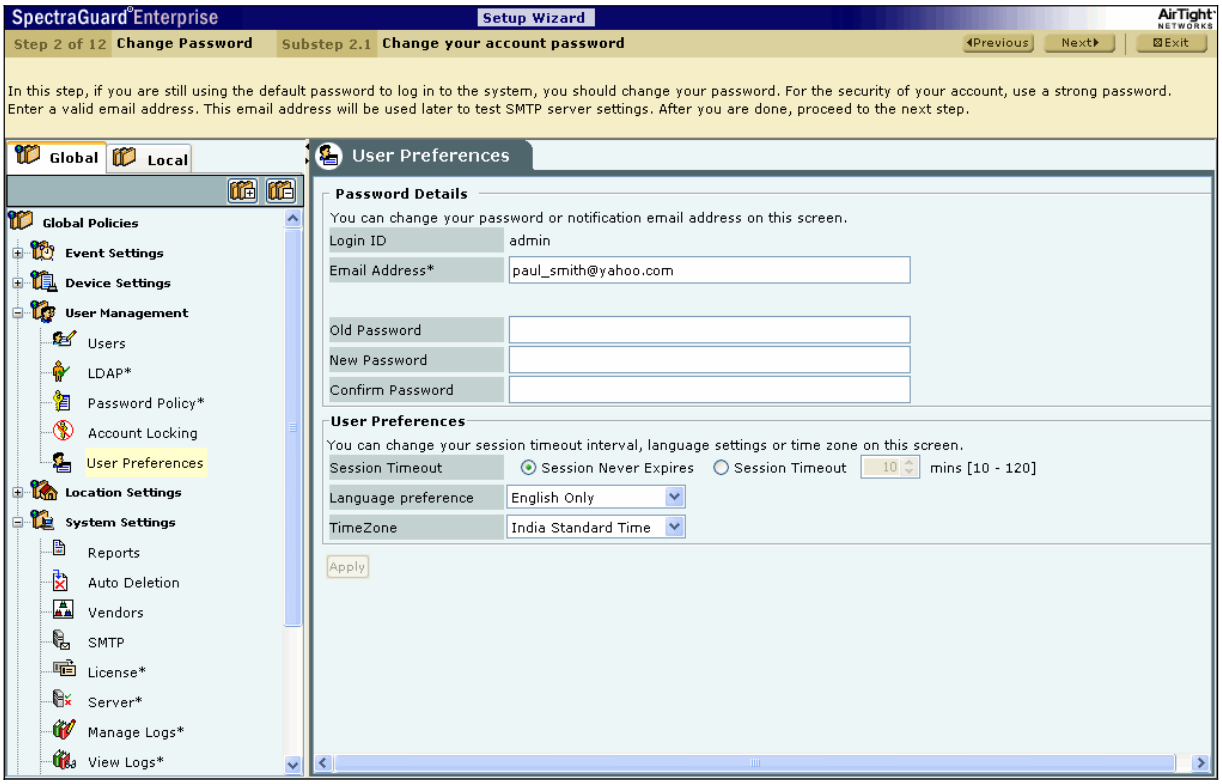


Figure 63. Change Password

Under **Password Details**, you can specify the following:

- Email Address
- Old Password
- New Password
- Confirm Password

Under **User Preferences**, you can change your session timeout interval, language settings, or time zone.

- **Session Timeout:** Enables you to specify the time after which the user is logged out automatically if the system does not detect any activity
  - **Session Never Expires:** Select this checkbox if you do not want the session to expire
  - **Session Timeout**: Enables you to specify the number of minutes after which the system automatically logs out the currently logged in user when there is no activity on the Console for the **Session Timeout** period

  (Minimum: 10 minutes; Maximum: 120 minutes)
- **Language preference:** Select English or Multilingual support from the drop-down list
- **Time Zone:** Select the appropriate time zone for the user

To save the new password and user preferences, click <**Apply**>.

7.1.3 Step 3: Preparing your System for Configuration

5. The **Event Activation** screen appears as shown in the following figure. To avoid transient events during the setup process, de-activate this feature for all locations where changes are to be made. The system prompts you to turn this feature back on at the end of the Setup Wizard. If you exit the Setup Wizard prematurely, you must manually re-activate this feature.

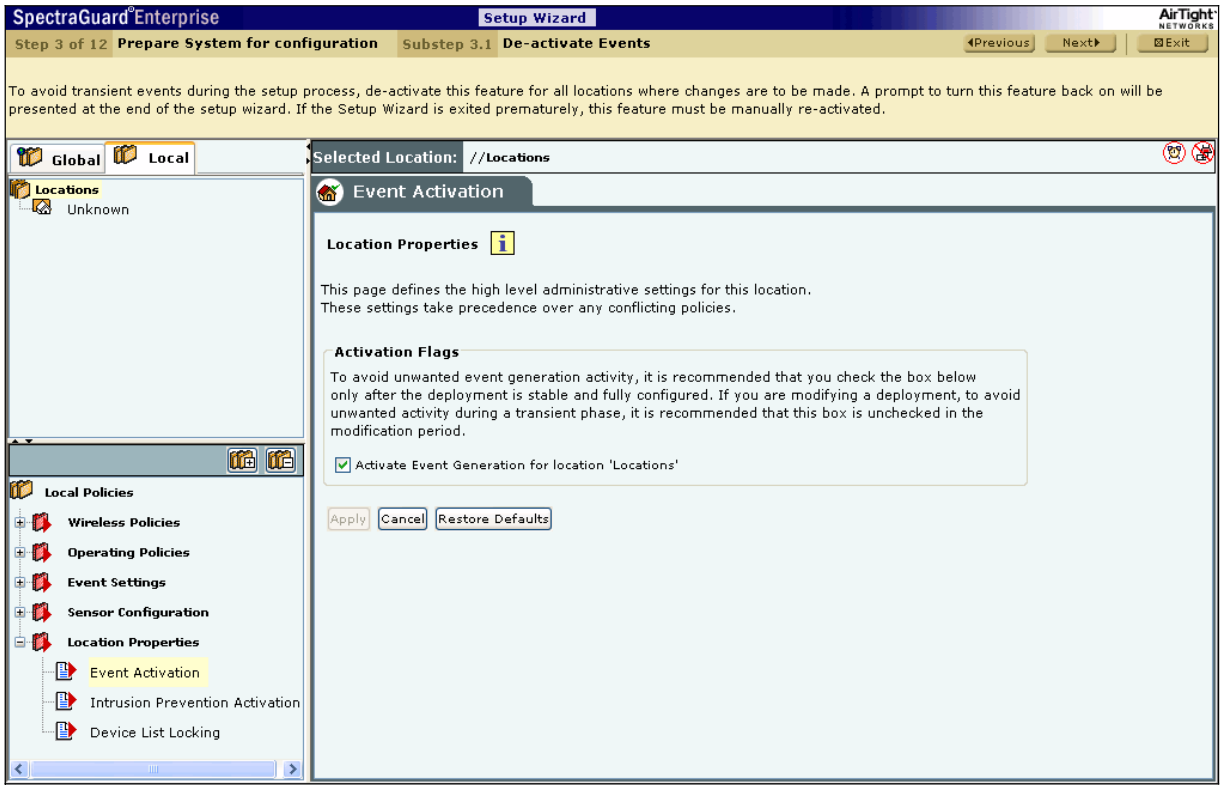


Figure 64. Event De-activation

6. The **Intrusion Prevention Activation** screen appears as shown in the following figure. To avoid unwanted intrusion prevention activity during the setup process, de-activate this feature for all locations where changes are to be made. The system prompts you to turn this feature back on at the end of the Setup Wizard. If you exit the Setup Wizard prematurely, you must manually re-activate this feature. Authorized APs should be in the ***Authorized*** folder before activating intrusion prevention. Their network connectivity icon may show the status as *Wired*, *Unwired*, or *Indeterminate*.

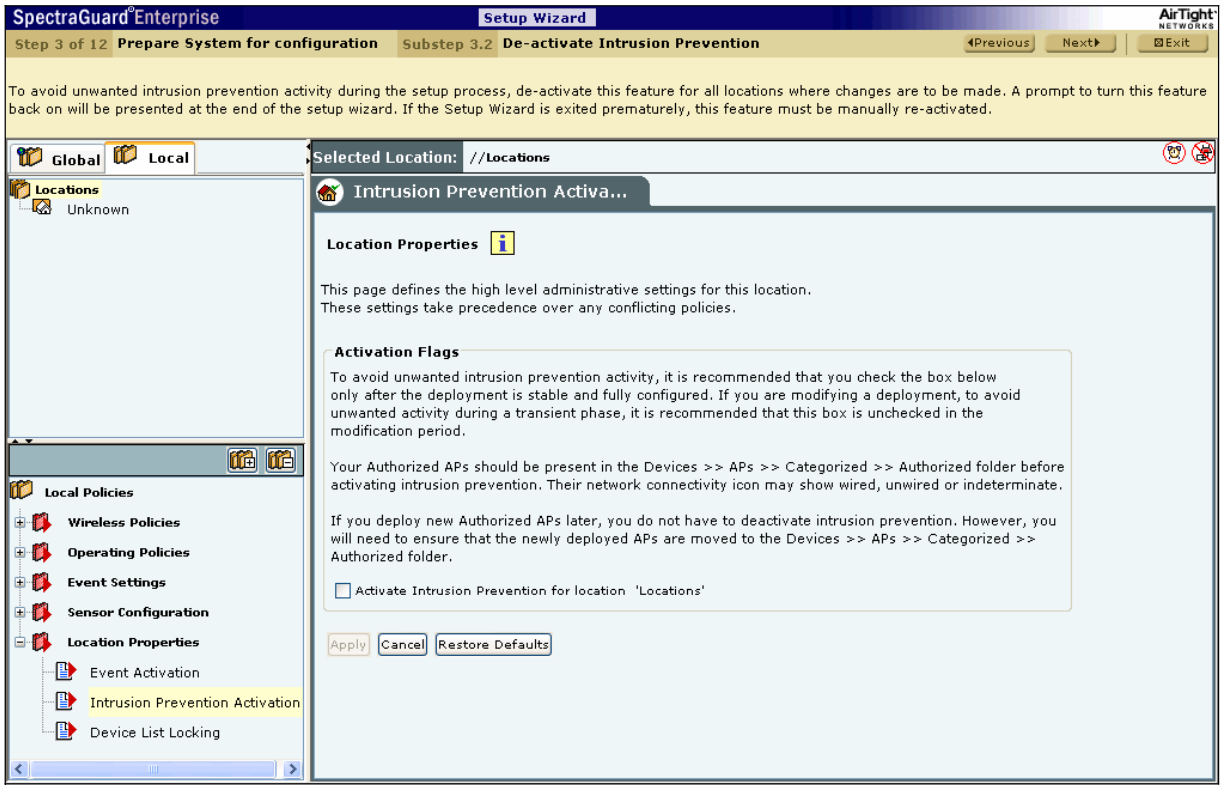


Figure 65. Intrusion Prevention De-activation

7. The **Device List Locking** screen appears as shown in the following figure. If you had previously locked the list of Authorized APs and Clients at a location by checking the two checkboxes **Lock AP List for location '<selected location'>** and **Lock Client List for location '<selected location'>**, you must unlock the lists for all the locations where you expect to add Authorized APs or Clients during the setup wizard. If you lock a particular device list, no more devices of that type can be subsequently automatically **Authorized** for that location. As APs are not automatically moved to the **Authorized** folder, locking the **Authorized AP** list means that no wired APs will be tagged as **Potentially Authorized** at this location; they will become **Potentially Rogue** and may be automatically moved to the **Rogue** folder based on the AP Auto-Classification policy.

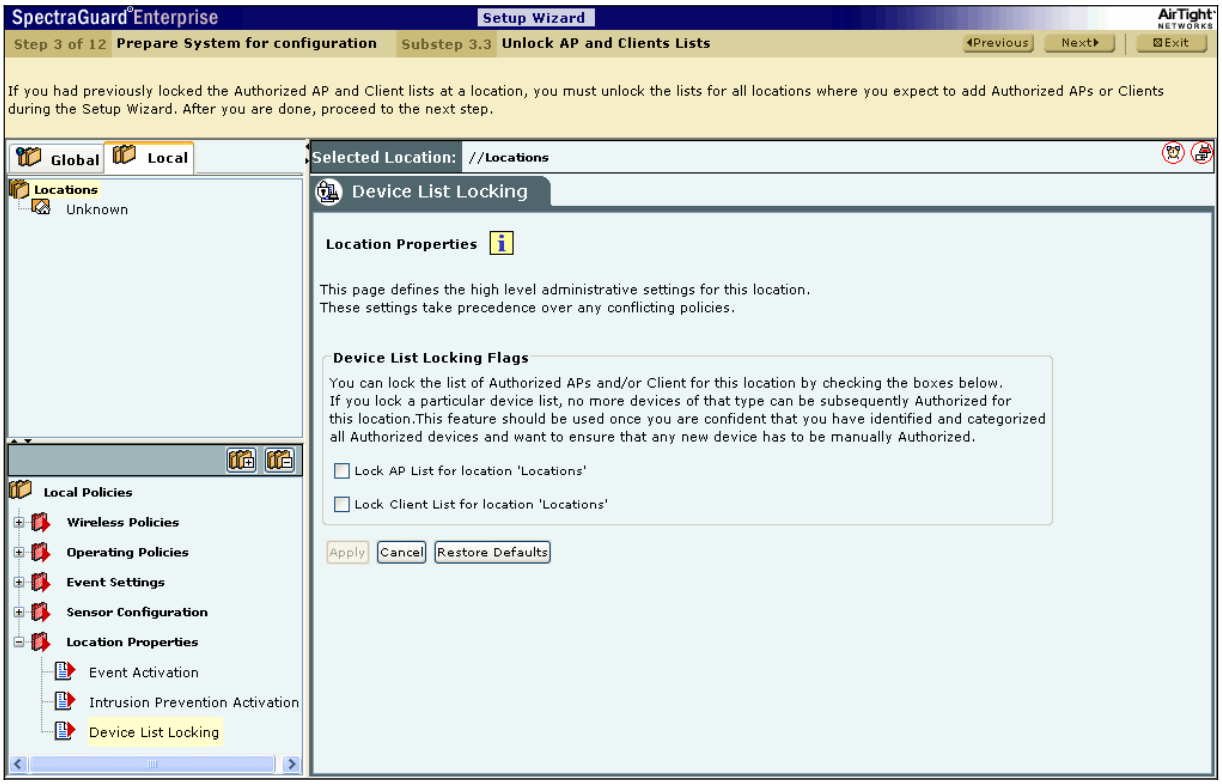


Figure 66. Device List Unlocking

7.1.4 Step 4: Configuring Notification Settings

8. The **SMTP Configuration** screen appears as shown in the following figure. You must set Simple Mail Transfer Protocol (SMTP) Server settings to send notification of events via email. AirTight recommends that you test the SMTP settings before applying the changes. You must have administrator privileges to set these values.

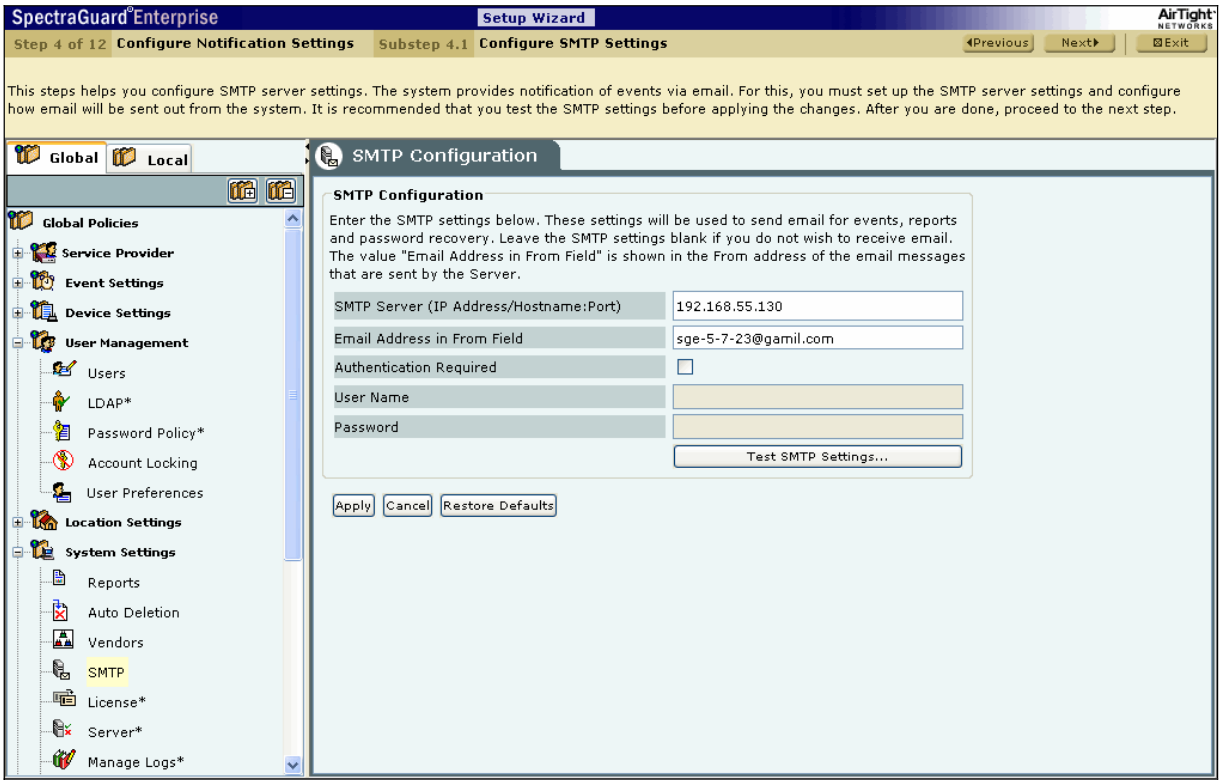


Figure 67. SMTP Configuration

***Note**: If you want the system to notify you by an events email, you need to specify SMTP Server details. The system does not email events by default. If you do not want to receive email for the events, select <**Restore Defaults**> and <**Apply**>.*

SMTP Configuration contains the following options:

- **SMTP Server (IP address/Hostname: Port):** Specifies the IP address or the hostname and the port number of the SMTP Server to be used by the system for sending email alerts.
  (Default: 127.0.0.1:25)

The following are the authentication protocols for SMTP Server:

- PLAIN (For sendmail 8.10 and above)
- LOGIN (For sendmail 8.10 and above)
- NTLM (Windows proprietary authentication method)

- **Email Address in From field:** Specifies the source address from which email alerts are sent.
- **Authentication Required:** If enabled, specifies whether the SMTP Server requires authentication.
  - **Username:** Specifies the user name for SMTP Server authentication.
  - **Password:** Specifies the password for SMTP Server authentication.

To send a test email, click <**Test SMTP Settings**>. This test email will be sent to the email address of the logged in user, in this case user ***admin***.

9. The **Syslog Configuration** screen appears as shown in the following figure. Syslog Configuration allows the system to send events to designated Syslog receivers.

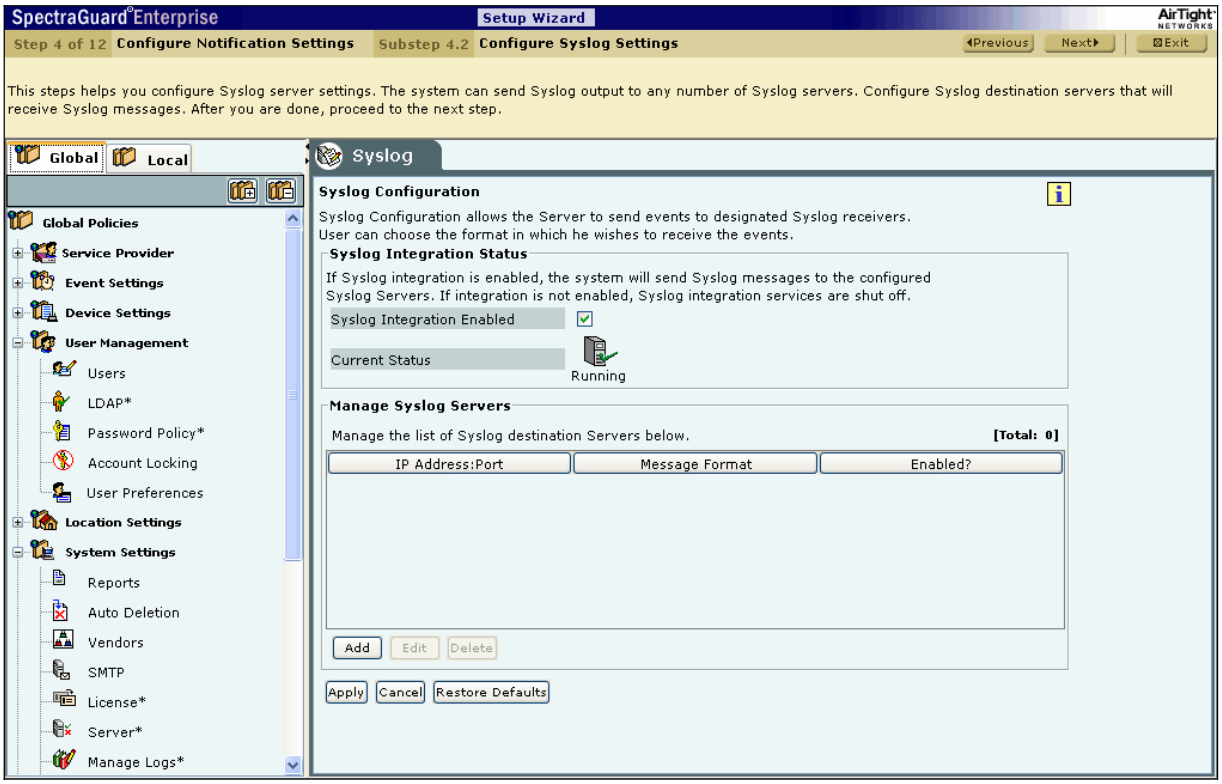


Figure 68. Syslog Configuration

- **Syslog Integration Status:** If Syslog integration is enabled, the system sends messages to the configured Syslog Servers. Else, Syslog integration services are shut off.
  - If you select **Syslog Integration Enabled**, you can manage Syslog Servers. The system ***enables*** Syslog by default.
  - **Current Status:** Displays the **Current Status** of the Syslog Server: ***Running*** or ***Stopped***. An ***Error*** status is shown in one of the following cases:
    - One of the configured and enabled Syslog Servers has a hostname, which cannot be resolved
    - System Server is stopped
    - Internal error, in which case you need to contact Technical Support
- Under **Manage Syslog Severs**, click <**Add**> to open **Syslog Configuration** dialog where you can add Syslog Server details.

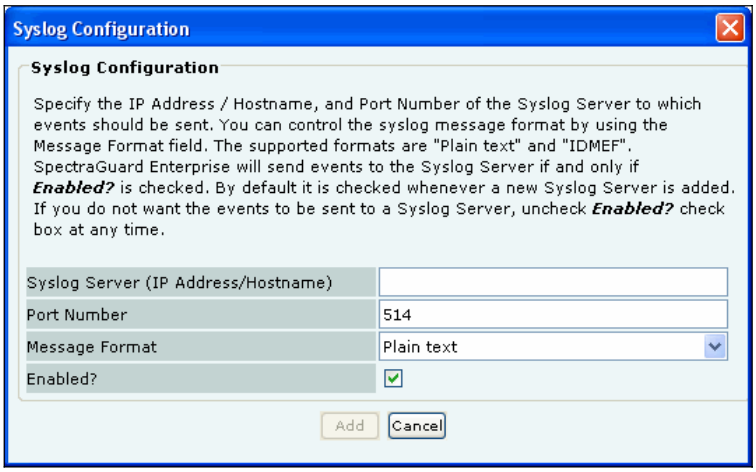


Figure 69. Syslog Configuration Dialog

Syslog Configuration contains the following fields:

- **Syslog Server (IP Address/Hostname):** Specifies the IP address or the hostname of the Syslog Server to which events should be sent.

***Note**: Configured Syslog Servers will use the DNS names and DNS suffixes configured by the user in the Server Initialization and Setup Wizard on the Server Config Shell.*

- **Port Number:** Specifies the port number of the Syslog Server to which the system sends events.
  (Default: 514)
- **Message Format:** Specifies the format in which the event is sent**:** Intrusion Detection Message Exchange Format (IDMEF) or Plain text.
  (Default: Plain text)

***Note**: If you upgrade a Server, pre-5.6 to 5.6, all previously configured Syslog Servers would send events in Plain text Message Format by default. You can select the IDMEF format by editing the Syslog Server settings.*

- **Enabled?:** Specifies if the events are to be sent to this Syslog Server.
  (Default: Enabled)

Click <**Add**> to add the details for a new Syslog Server. Click <**Cancel**> to close the window and discard all changes that were made.

Double-click a row or click <**Edit**> to open **Syslog Configuration** dialog similar to the one shown above. Click <**Save**> to save all settings. Click <**Cancel**> to close the window and discard all changes that were made.

Click <**Delete**> to discard the details of an existing Syslog Server.

10. The **SNMP Configuration** screen appears as shown in the following figure. SNMP Configuration allows the system to send events as SNMP traps to designated SNMP trap receivers. It also allows SNMP managers to query Server operating parameters using IF-MIB, MIB-II, and Host Resources MIB.

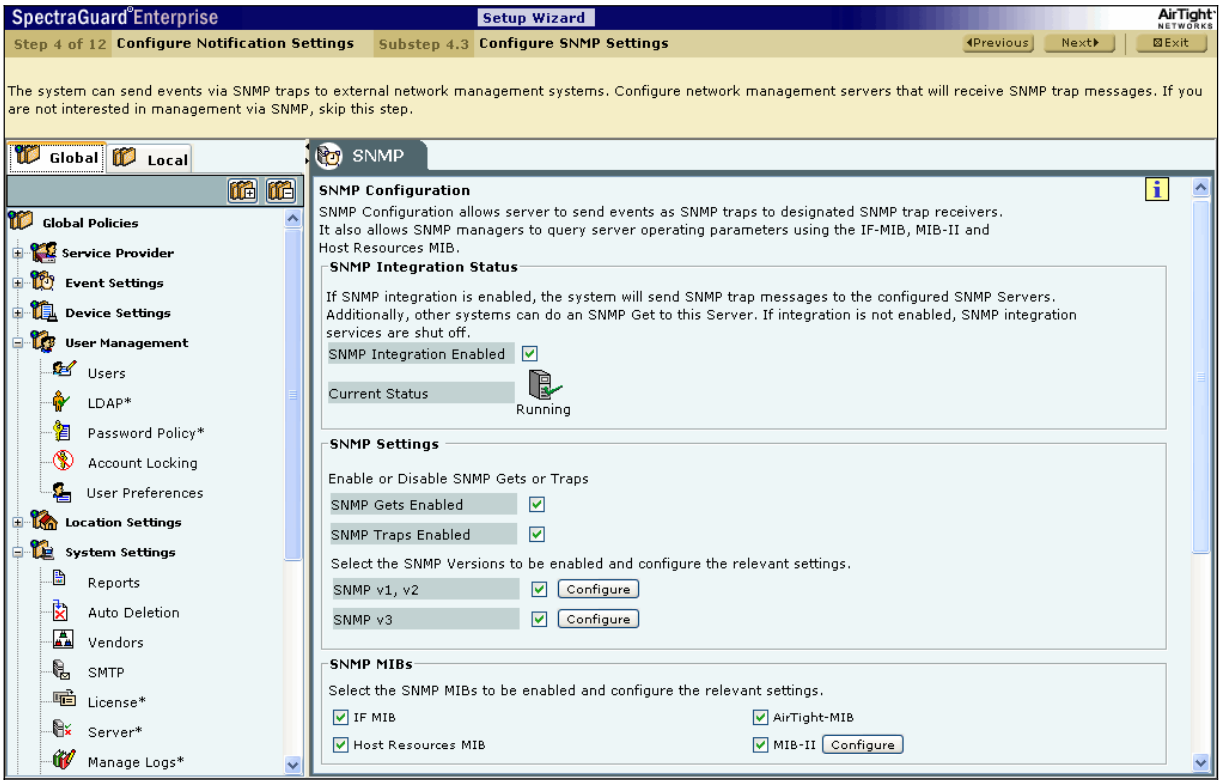


Figure 70. SNMP Configuration

- **SNMP Integration Status:** If SNMP integration is enabled, the system sends SNMP traps to the configured SNMP Servers. Other systems can do an **SNMP Get** to this Server. Else, SNMP integration services are shut off.
  - If you select **SNMP Integration Enabled**, you can edit and manage SNMP Server details. The system ***enables*** SNMP by default.
  - **Current Status:** Displays the **Current Status** of the SNMP Server**:** Running, Error, or Stopped.
- Under **SNMP Settings**, configure SNMP Gets or Traps.
  - **SNMP Gets Enabled:** Allows SNMP managers to query Server-operating parameters using IF-MIB, MIB-II, and Host Resources MIB.
  - **SNMP Traps Enabled:** Allows SNMP traps to be sent to configured SNMP Servers.

Additionally, select the **SNMP versions** to be enabled and configure the relevant settings.

- **SNMP v1, v2:** If selected, specify the **Community String** for the SNMP agent.
  (Default: public)
- **SNMP v3:** If selected, specify the **Engine ID**, **Username**, and **Password**.
  (Default Username: admin; Default Password: password)

- Under **SNMP MIBs**, select the following SNMP MIBs to be enabled and configure the relevant settings.
  - IF MIB
  - Host Resources MIB
  - AirTight-MIB**:** Enables the external SNMP agent to receive traps
  - MIB-II**:** If selected, configure the **System Contact**, **System Name**, and **System Location**.

  (Default System Name: Wifi Security Sever)

Note*: The Internet Assigned Numbers Authority (IANA) assigned Private Enterprise Number for AirTight® Networks, Inc. is 16901.*

- Under **SNMP Trap Destination Servers**, click <**Add**>to open **SNMP Configuration** dialog where you can add SNMP Server details.

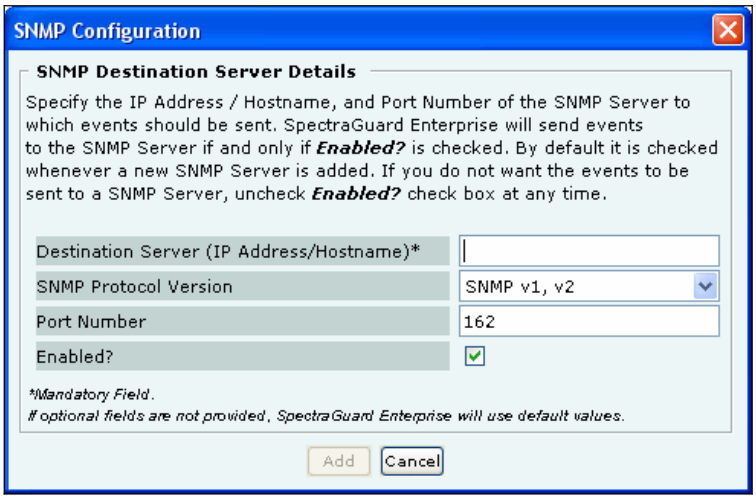


Figure 71. SNMP Configuration Dialog

SNMP Destination Server Details contains the following fields:

- **Destination Server (IP Address/Hostname)*:** Specifies the IP address or the hostname of the SNMP Server to which events should be sent.

***Note**: Configured SNMP Servers will use the DNS names and DNS suffixes configured by the user in the Server Initialization and Setup Wizard on the Server Config Shell.*

- **SNMP Protocol Version:** Specifies the SNMP protocol version for the SNMP agent.
  (Default: SNMP v1, v2)
- **Port Number:** Specifies the port number on the receiving system to which the SNMP trap is sent.
  (Default: 162)
- **Enabled?:** Specifies if the SNMP Server is enabled to receive SNMP traps.
  (Default: Enabled)

***Note**: You must specify a different port number if another application uses the default port.*

Click <**Add**> to add the details for a new SNMP Server.

Double-click a row or select a row and click <**Edit**> to open **SNMP Configuration** dialog similar to the one shown above..
Click <**Save**> to save all settings.

Select a row and click <**Delete**> to discard the details of an existing SNMP Server.

7.1.5 Step 5: Setting up Locations and Sensors

11. The **Locations** screen appears as shown in the following figure. Create a hierarchy of all the locations that the system will monitor and secure by adding location folders and nodes.

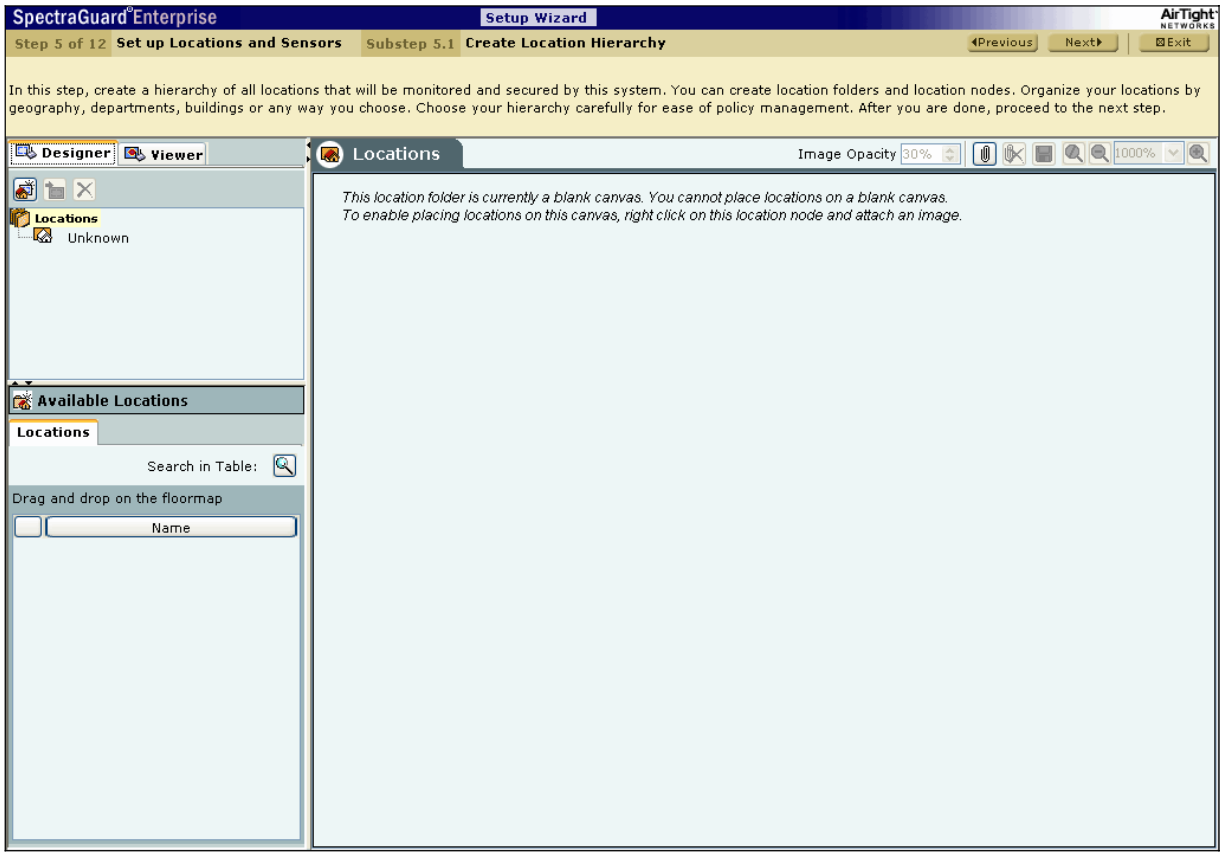


Figure 72. Locations Screen

The **Locations** screen operates in two modes**: Designer** mode and **Viewer** mode. The **Designer** mode is active by default. A location hierarchy of your setup may comprise location folders and location nodes.

- **Location folders** represent organizational components such as buildings, cities, or countries.
  - **Root:** This is the root location. The factory default name for this location is **Locations**. You can rename this location. However, you cannot delete or move this location.
  - **Unknown:** This is the default location folder of the root location. You cannot create, delete, rename, move, or add a location to the **Unknown** folder. When the system detects a new untagged Sensor, it tags this Sensor to the Unknown location folder. In other words, when the location tag of a location-aware entity is not known or cannot be determined, it is tagged to the Unknown folder.
- **Location nodes** represent component details such as a floor in a building. For example, Hawaii Conference Room, Bldg 15–Cubicle G2, or Executive Area.

7.1.5.1 Adding a New Location

Use the following steps to add a location:

a. In the **Location** tree, select the location under which you wish to add a new location.

b. Do one of the following:

- Right-click and from the resulting context-sensitive menu, select **Add New Location**.
- Click the **Add New Location** icon () below the **Designer** mode tab.

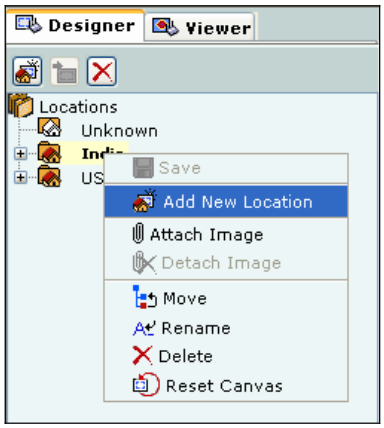


Figure 73. Adding a New Location

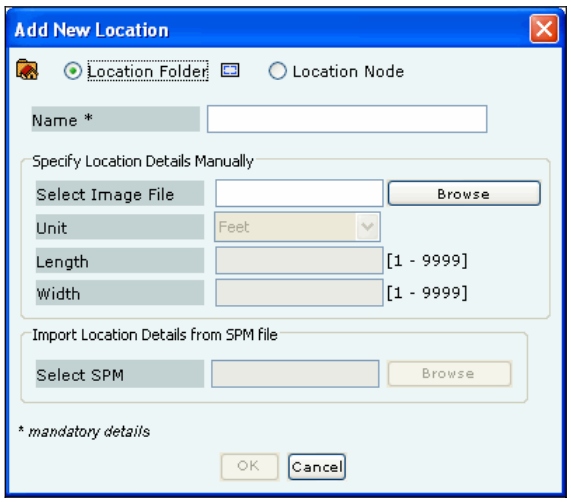


Figure 74. Specifying Location Properties

c. In the **Add New Location** dialog, select the type of location, that is, **Location Folder** or **Location Node**.

d. Enter a name for the new location and optionally enter the following details.

- **Select Image File:** Click <**Browse**> to navigate to the path of the image that you wish to attach to the location folder or node.
- **Unit:** Specify the unit of measurement (feet or meters) for the location node.
- **Length:** Specify the length of the location node.
- **Width:** Specify the width of the location node.
- **Select SPM:** Click <**Browse**> to navigate to the path of the .SPM file that you wish to import from SpectraGuard Planner (Planner) into the new location node.

*Note: **Unit, Length, Width,** and **Select SPM** options are available only for a location node. They are grayed out for a location folder.*

e. Click <**OK**> to create a new location. Alternatively, click <**Cancel**> to avoid creating a new location.

12. The **Sensor Configuration** screen appears as shown in the following figure. This enables you to create different Sensor configuration templates. This allows the user to apply different settings to different Sensors by applying different templates. Each configuration template allows settings for operating region, channels to monitor, channels to defend, antenna configuration, Sensor password, and offline Sensor operation.

    At any location, you can choose a template as a *default template*. This template will be applied to any new Sensor tagged to that location.

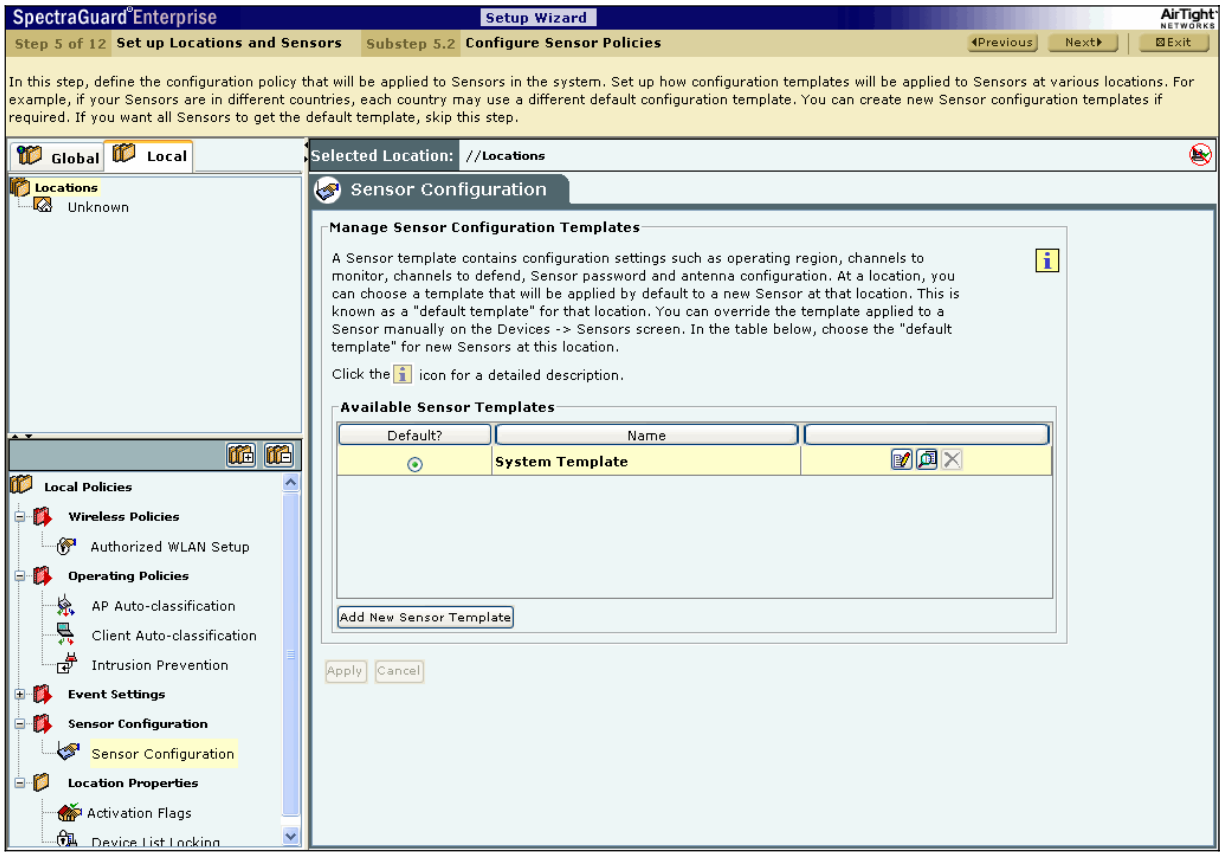


Figure 75. Sensor Configuration

***Note**: Sensors prior to Version 5.2 do not support additional channels (802.11j & Turbo channels), Antenna Port Assignment, and Sensor Password Configuration features. If you apply templates containing these settings to older Sensors, older Sensors will ignore the additional settings.*

Click <**Add New Sensor Template**> to open the **Sensor Configuration Template** dialog.

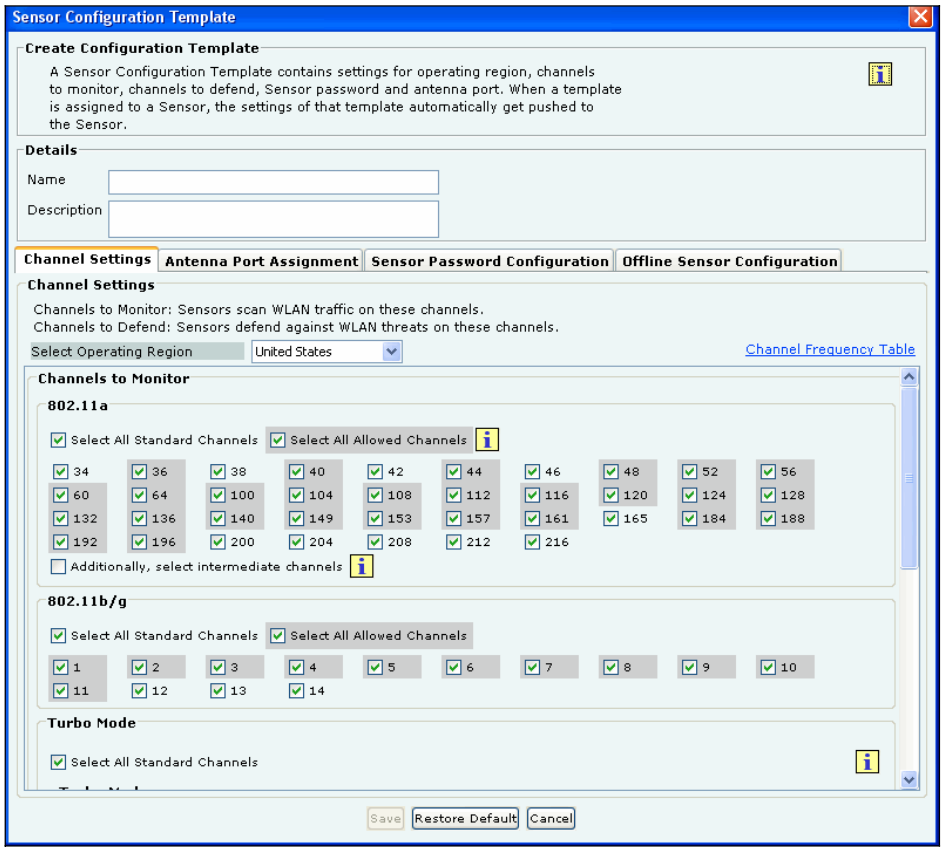


Figure 76. Channel Settings Tab

Under **Create Configuration Template**, specify the following:

- **Name:** Unique name of the Sensor Configuration template (less than 40 characters)
- **Description:** Brief description of the Sensor Configuration template (less than 500 characters)

***Note**: The system stores the default Sensor configuration in a predefined template **System Template**. You **cannot delete** the System Template nor edit its name; it is unique. When a Sensor is added or discovered, it is automatically assigned the configuration settings in this template. You are allowed to edit the configuration settings in the System Template to effect default configuration of their choice.*

Whenever you delete a user-defined Sensor configuration template, all the Sensors associated with that template are assigned the System Template. You can override the template applied to a Sensor manually from the Devices⊙ Sensors tab. If you modify the settings in a template, the new settings are applied to the Sensors to which this template is applied.

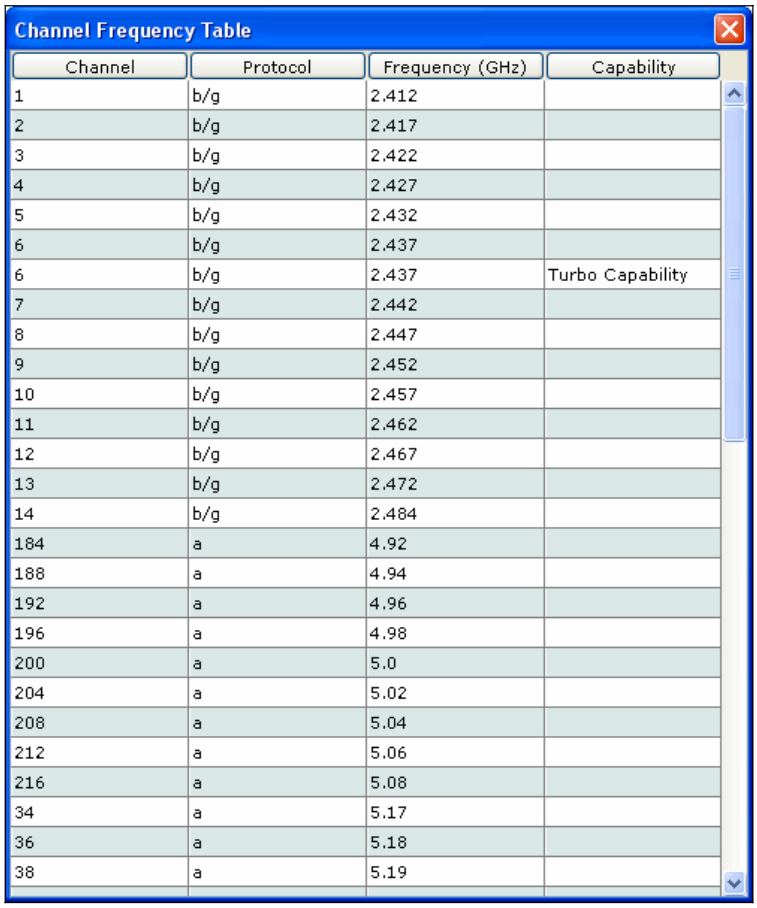
Channel Settings

Channel Settings displays the 802.11a/802.11b/g and Turbo channels on which scanning and defending is enabled/disabled. Sensors scan WLAN traffic on channels specified under **Channels to Monitor** and defend the network against various WLAN threats on channels specified under **Channels to Defend**.

- **Under Channel Settings** tab, specify the following:
  - ➢ **Select Operating Region:** Specifies the region: country: of operation. Each region has its own laws governing the use of the unlicensed frequency spectrum for 802.11 communications and Turbo mode. The system automatically selects the channels that are allowed by the regulatory domain in selected region.

  (Default Operating Region: United States)

  - ➢ Click the link **Channel Frequency Table** to view a list of channels, protocols, frequencies, and capabilities.



Channel Frequency Table

Channel	Protocol	Frequency (GHz)	Capability
1	b/g	2.412	
2	b/g	2.417	
3	b/g	2.422	
4	b/g	2.427	
5	b/g	2.432	
6	b/g	2.437	
6	b/g	2.437	Turbo Capability
7	b/g	2.442	
8	b/g	2.447	
9	b/g	2.452	
10	b/g	2.457	
11	b/g	2.462	
12	b/g	2.467	
13	b/g	2.472	
14	b/g	2.484	
184	a	4.92	
188	a	4.94	
192	a	4.96	
196	a	4.98	
200	a	5.0	
204	a	5.02	
208	a	5.04	
212	a	5.06	
216	a	5.08	
34	a	5.17	
36	a	5.18	
38	a	5.19	

Figure 77. Channel Frequency Table

- **Channels to Monitor:** Specifies the channels to be used by Sensors to monitor WLAN traffic.
  - Select the checkbox **Select All Standard Channels** to select a superset of all the channels. For 802.11a, the standard sets of channels are 184 – 216 and 34 - 165. By default, this checkbox is selected.
  - Select the checkbox **Select All Allowed Channels** to select all the allowed channels in the selected operating region. By default, this checkbox is selected.
  - Select the checkbox **Additionally, select intermediate channels** *for 802.11 a only* to select the channels between the allowed channels that are non-allowed in the selected operating region. Selecting the option helps the system detect devices operating on illegal channels. For 802.11a, the intermediate channels are 185, 186, 187, 35, 37, and so on. By default, this checkbox is deselected.
- **Turbo Mode:** Certain Atheros Chipset based devices use wider frequency bands on certain channels in 802.11 b/g and 802.11a band of channels. The system is capable of monitoring channels that support Turbo Mode of operation and detecting any unauthorized communication on these channels. You can select specific or all channels to monitor wireless activity on Turbo channels. There are ten Turbo channels in ***a-mode***. These channels are 40, 42, 48, 50, 56, 58, 152, 153, 160, and 161. There is only one Turbo channel in ***b/g-mode*** i.e. 6.
- **Channels to Defend:** Specifies the channels to be used by Sensors to defend WLAN traffic to protect your network against various WLAN threats.

Note*: It is mandatory that channels selected for defending be selected for scanning. If a channel is selected for defending and is not already selected for scanning, the system automatically selects that channel for scanning as well. If you deselect a channel from* ***Channels to Monitor****, then this channel is also deselected from* ***Channels to Defend*** *section.*

Antenna Port Assignment

Antenna connectivity setting is an advanced setting and should be used with utmost care. This setting allows you to provide

additional information about the type of antennas connected to the Sensor. You need to change this setting only if you use Sensors that allow you to connect antennas.

Applying a template with a particular antenna setting to a Sensor with incompatible antenna connection can result in a loss of system functionality leading to higher security risks. You should not change the Antenna Connectivity Settings for a template that is already applied to a group of Sensors or is a Default Sensor template. If you need to change these settings, you should save the changes as a new template first, then change the antennas settings as required, save the template and apply it to a group of Sensors which have the same antenna settings as specified in the template.

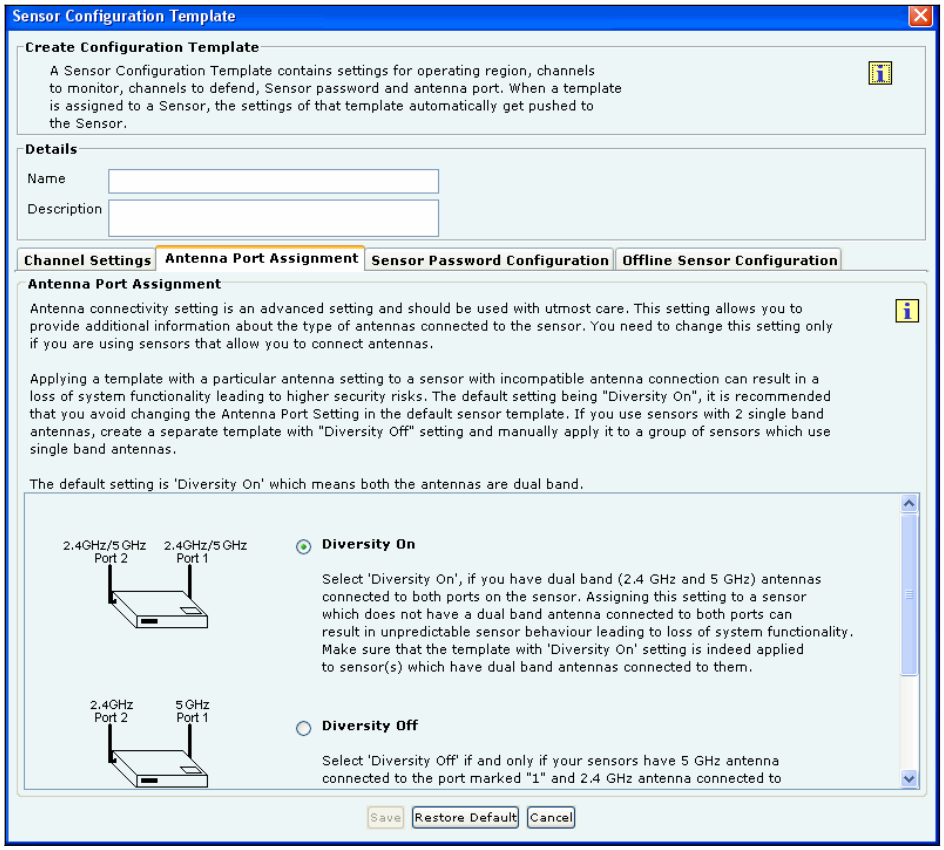


Figure 78. Antenna Port Assignment Tab

- Under **Antenna Port Assignment** tab
  - Select **Diversity On** or **Diversity Off**
    - **Diversity On:** This is the default setting, which means both the antennas are dual band. Select this option if you have a dual band (2.4 GHz and 5 GHz) antenna connected to both the ports on the Sensor. Assigning this setting to a Sensor which does not have a dual band antenna connected to both ports, can result in unpredictable Sensor behavior leading to loss of system functionality. Make sure that the template with "Diversity On" setting is indeed applied to Sensor(s), which have dual band antenna connected to them.
    - **Diversity Off:** Select this option **if and only if** your Sensors have a 5 GHz antenna connected to Port 1 and a 2.4 GHz antenna connected to Port 2. The figure in the **Antenna Port Assignment** tab shows how to locate the ports to ensure that the *single band* antennas are correctly connected. Assigning this setting to a Sensor that does not have *single band* antennas connected as mentioned above can result in unpredictable Sensor behavior leading to loss of system functionality. Make sure that the template with Diversity Off setting is indeed applied to Sensor(s) that have two different *single band* antennas supporting 2.4 GHz and 5 GHz frequency bands and connected as mentioned above.

Sensor Password Configuration

Sensor Password setting allows you to manage the password for user *config* on the Sensor Command Line Interface (CLI). By

defining a password in the Sensor template, you can manage the password for a group of Sensors without having to change it on each Sensor separately. Type a new password or click <**Restore Default**> to change the current password settings. If you choose <**Restore Default**>, then the password setting will be the same as that in the System Template.

***Note**: If a Sensor template contains a blank password, then the Sensors, to which this template is assigned, retain their existing password. Factory setting of the System Template contains a blank password.*

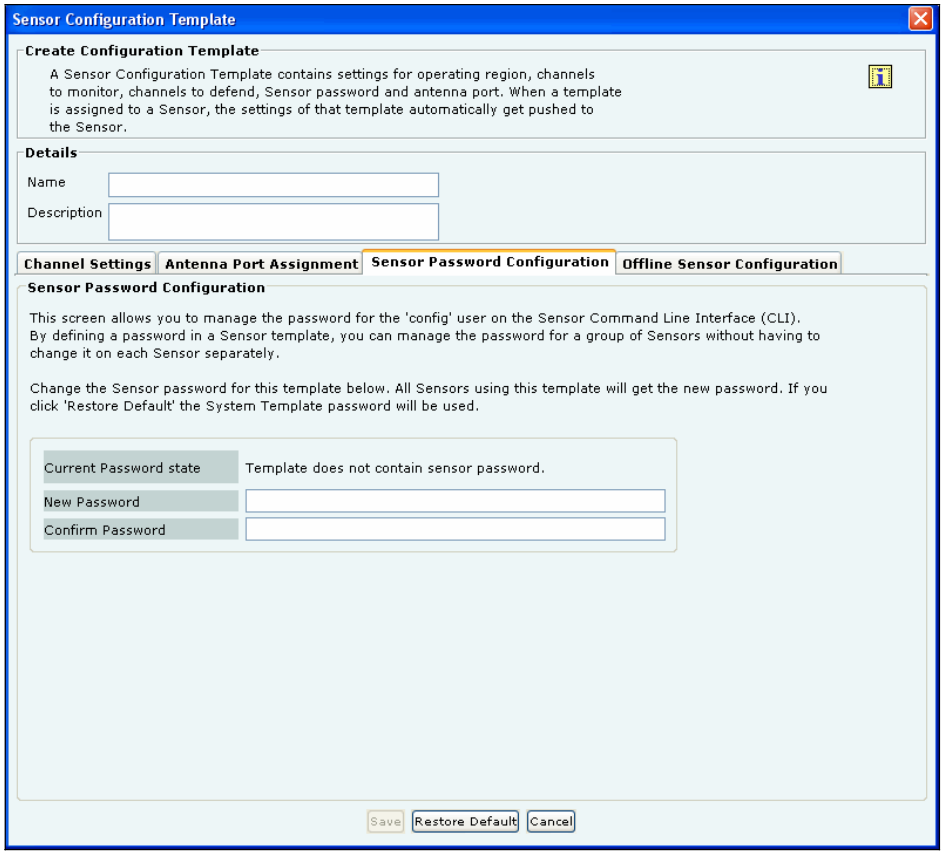


Figure 79. Sensor Password Configuration Tab

- Under **Sensor Password Configuration** tab specify the following
  - **Current Password state:** Specifies that the new password must be the same as the one specified in the System Template.
  - **New Password:** Enter the new password to be assigned as user 'config' password for all Sensors associated with the Sensor template being edited.
  - **Confirm Password:** Reenter the password to help confirm the new password before saving.

Offline Sensor Configuration

This feature provides some security coverage even when there is no connectivity between a Sensor and the Server. The Sensor provides some classification and prevention capabilities when it is disconnected from the Server. The Sensor also raises events, stores them, and sends them back to the Server on reconnection.

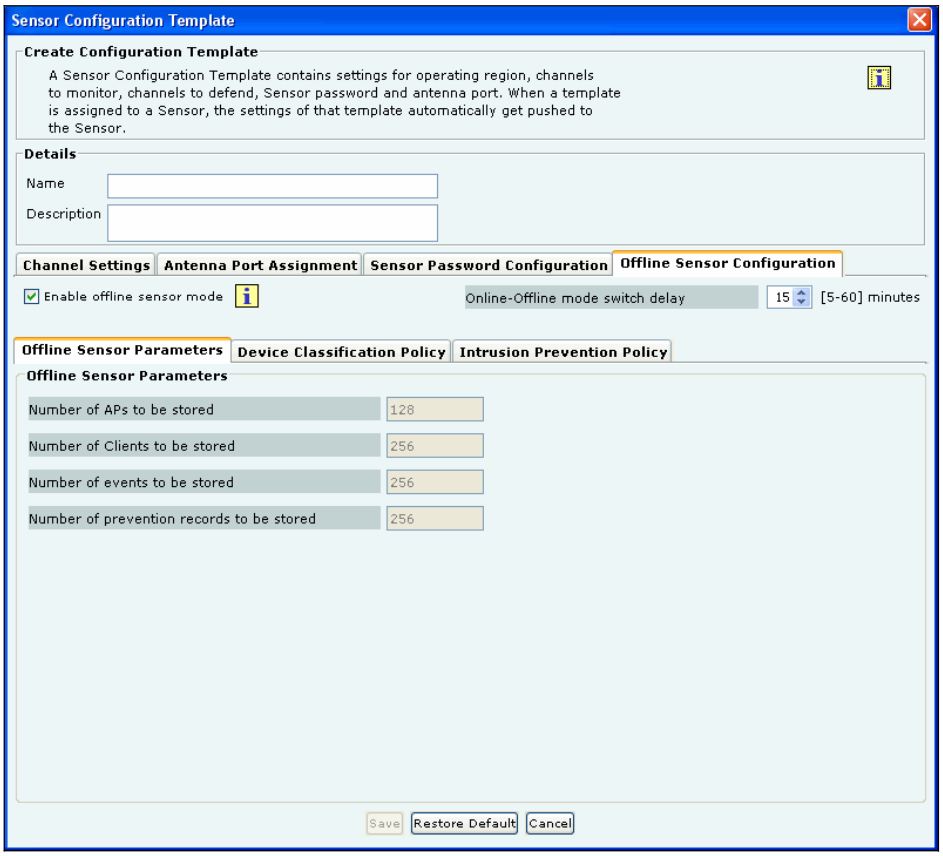
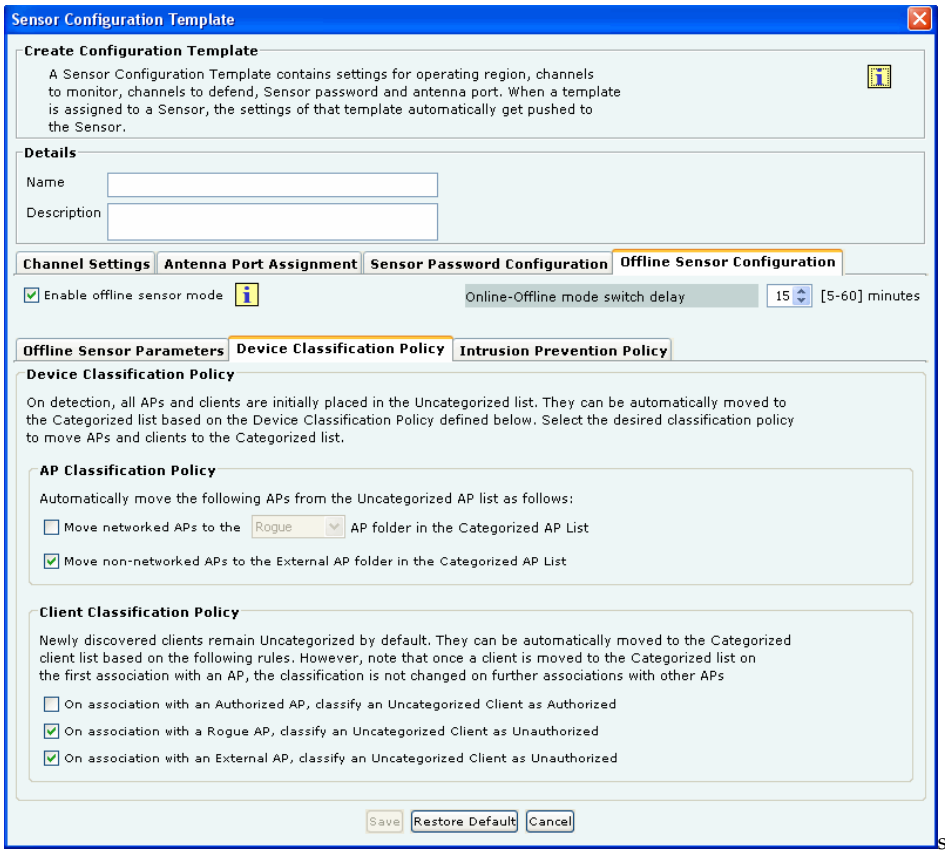


Figure 80. Offline Sensor Configuration Tab

- **Enable offline Sensor mode:** Select this checkbox to enable the offline Sensor mode. When this mode is enabled, the Sensor continues to detect and classify devices, raise event alerts, and prevent ongoing threats. *(Default: Selected)*
- **Online-Offline mode switch delay:** Specify the time after which, if the Sensor does not receive any communication from the Server and **Enable offline Sensor mode** is enabled, the Sensor switches to the offline mode. *(Minimum: 5 minutes; Maximum: 60 minutes; Default: 5 minutes)*
- Under **Offline Sensor Parameters** tab, you can view the following:
  - **Number of APs to be stored**: Number of APs that the Sensor will continue to detect in Offline mode *(Default: 128)*
  - **Number of Clients to be stored**: Number of Clients that the Sensor will continue to detect in Offline mode *(Default: 256)*
  - **Number of events to be stored**: Number of events that the Sensor will continue to raise in Offline mode *(Default: 256)*
  - **Number of prevention records to be stored**: Number of prevention records that the Sensor will continue to store in Offline mode to prevent ongoing threats *(Default: 256)*



sue

Figure 81. Offline Sensor Configuration: Device Classification Policy Tab

- Under **Device Classification Policy** tab specify the desired classification policies to move APs and Clients from the **Uncategorized** list to the **Categorized** list:
  - Under **AP Classification Policy**, select one or more options to enable the system automatically move APs from the Uncategorized AP list to the Categorized AP list:
    - Move networked APs to the Rogue or Authorized AP folder in the Categorized AP List
    - Move non-networked APs to the External AP folder in the Categorized AP List
  - Under **Client Classification Policy**, select one or more options to enable the system automatically classify Clients based on their associations with APs:
    - On association with an Authorized AP, classify an Uncategorized Client as Authorized
    - On association with a Rogue AP, classify an Uncategorized Client as Unauthorized
    - On association with an External AP, classify an Uncategorized Client as Unauthorized

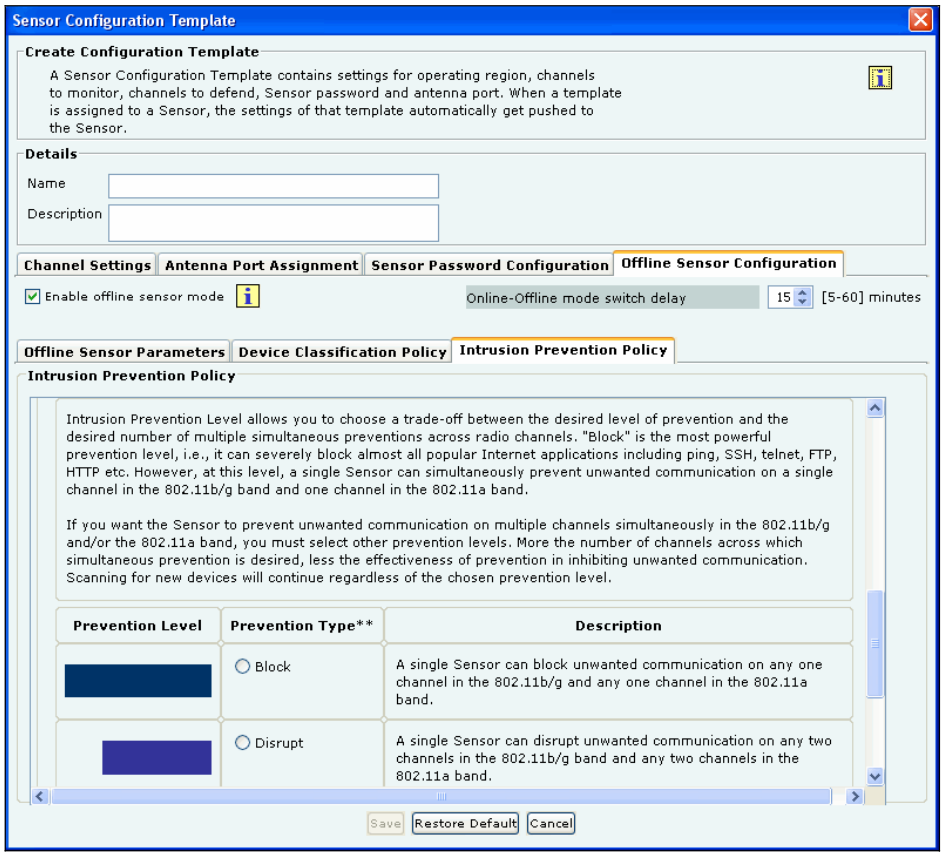


Figure 82. Offline Sensor Configuration: Intrusion Prevention Policy Tab

- Under **Intrusion Prevention Policy** tab enable intrusion prevention against the following threats:
  - **Rogue APs**
    - APs categorized as Rogue
    - Uncategorized APs that are connected to the network
  - **Misconfigured APs**
    - APs categorized as Authorized but using no security mechanism (Open)
    - APs categorized as Authorized but using weak security mechanism (WEP)
  - **Client Mis-associations**
    - Authorized Client connections to APs categorized as External
  - **Unauthorized Associations**
    - Unauthorized Client connections to APs categorized as Authorized
  - **Adhoc Connections**
    - Authorized Clients participating in any adhoc network
  - **Honeypot/Evil Twin APs**
    - Authorized Client connection to Honeypot/Evil Twin APs

Additionally, specify the intrusion prevention level that allows you to choose a trade-off between the desired level of prevention and the desired number of multiple simultaneous preventions across radio channels. You can choose either of the following prevention levels:

- Block
- Disrupt
- Interrupt
- Degrade

Refer to the section Intrusion Prevention Level for more details.

Click <**Save**> to save all settings.

Click the icon to edit an existing Sensor template. When an existing Sensor template is edited a **Confirmation – Save** dialog appears indicating the modifications, by selecting the tabs that were modified. You are allowed to uncheck a tab if you wish to cancel those modifications. Click <**OK**> to save the changes for the selected tab.

---

*Note: **Name** and **Description** of the Sensor template are automatically saved.*

Click <**Save As**> to save the Sensor template with a different name without modifying the original template.

Click <**Restore Default**> to revert to the System Template. The system enables you to select tabs to control the settings that will be restored to the default values. If you click <**Restore Default**> on the System Template, parameters under the selected tabs are restored to their factory default settings. A **Confirmation – Restore Default** dialog appears with a list of tabs selected, for which default settings will be applied.

***Important**: The system has the ability to scan and defend on 4.920-4.980 GHz and 5.470-5.725 GHz channels in US/Canada and IEEE 802.11j channels 4.920-4.980 GHz and 5.040-5.080GHz channels in Japan.*

Click the icon to view an existing Sensor template. Click the icon to delete an existing Sensor template.

13. The **Import Sensor List** screen appears as shown in the following figure. Importing a Sensor list is an efficient alternative to manually moving Sensors to the desired locations while setting up the system. The successfully imported Sensors are automatically tagged to the chosen locations when they connect to the Server.

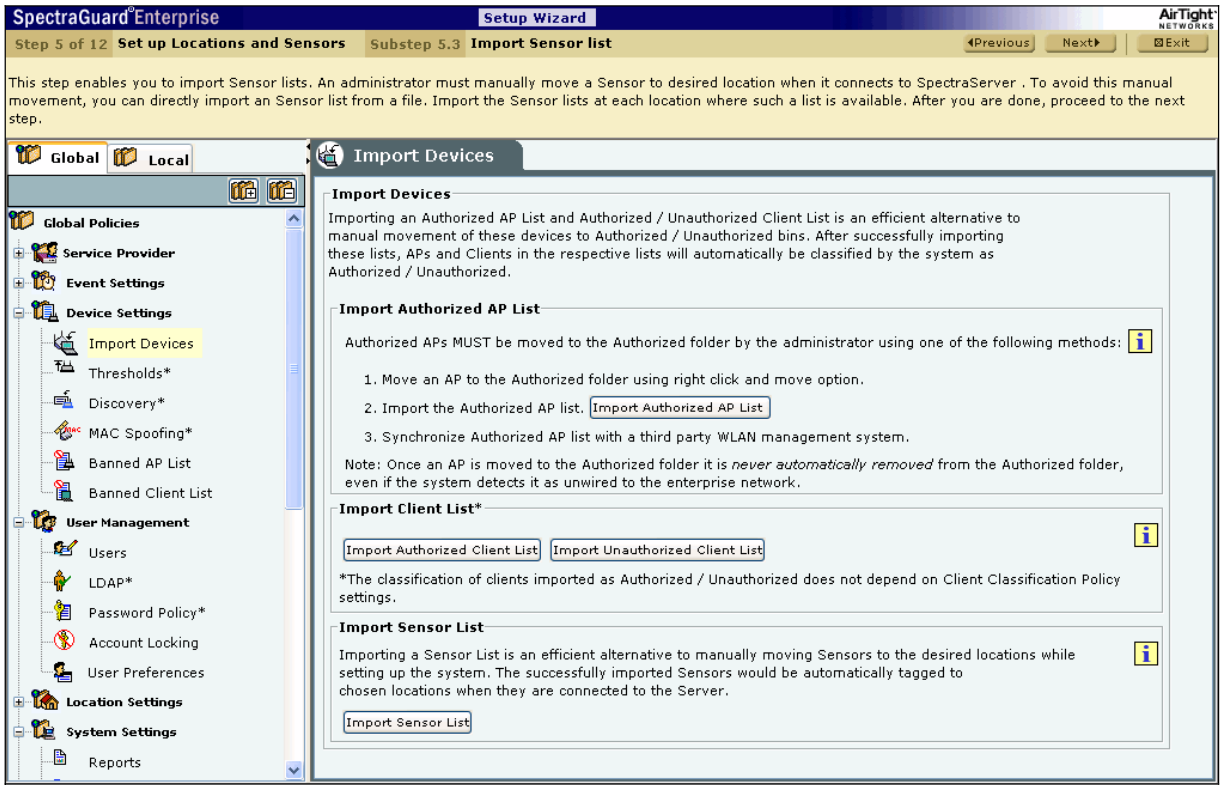


Figure 83. Import Devices - Sensors

Under **Import Sensor List**, click <**Import Sensor List**> to open **Import Sensor List** dialog.

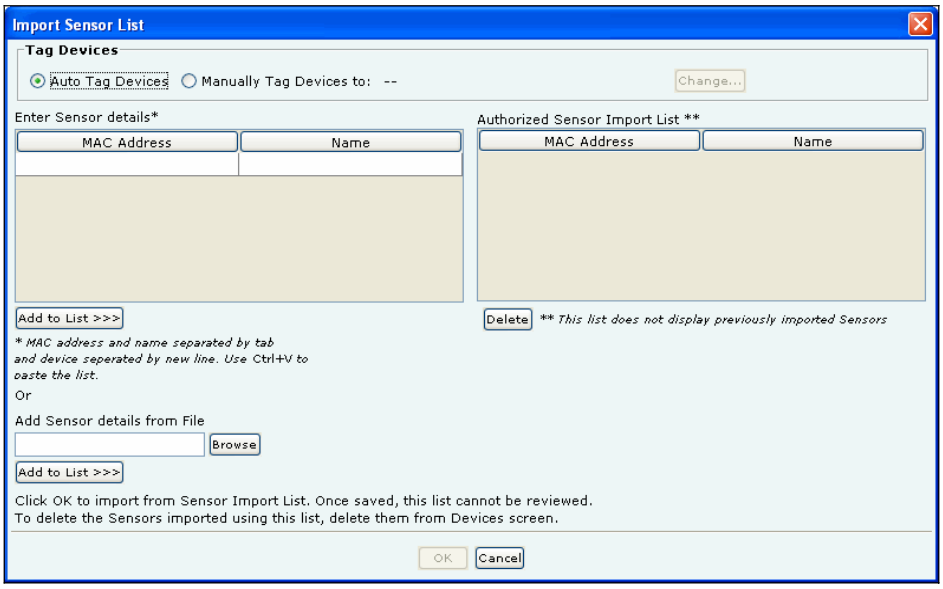


Figure 84. Import Sensor List

In the **Import Sensor List** dialog:
Under **Tag Devices**, select one of the following:

- **Auto Tag Devices:** To automatically tag the Sensor to the corresponding location.
- **Manually Tag Devices to::** Click <**Change**> to manually tag the Sensor to the desired location.

Under **Enter Sensor details**

- To add a Sensor's details, type the Sensor's MAC address and Name and click <**Add to List>>>**>.
- To add a Sensor's details from a file, click <**Browse**>. On the **Select Sensor_Device_List_File** dialog, select the .txt file from the desired location and click <**Open**>. Then click <**Add to List>>>**>.

Under **Authorized Sensor Import List**

- To delete a Sensor's details, select the corresponding row and click <**Delete**>.

To import Sensors from the **Sensor Import List**, click <**OK**>.

***Note**: When you import Sensors from a list, you can delete these Sensors only from the **Devices** screen.*

14. The **Devices→Sensors** screen appears as shown in the following figure. Sensors proactively scan the network and generate events. Sensors communicate event information to the system. This screen guides you to move all the Sensors from the **Unknown** location to their correct locations.

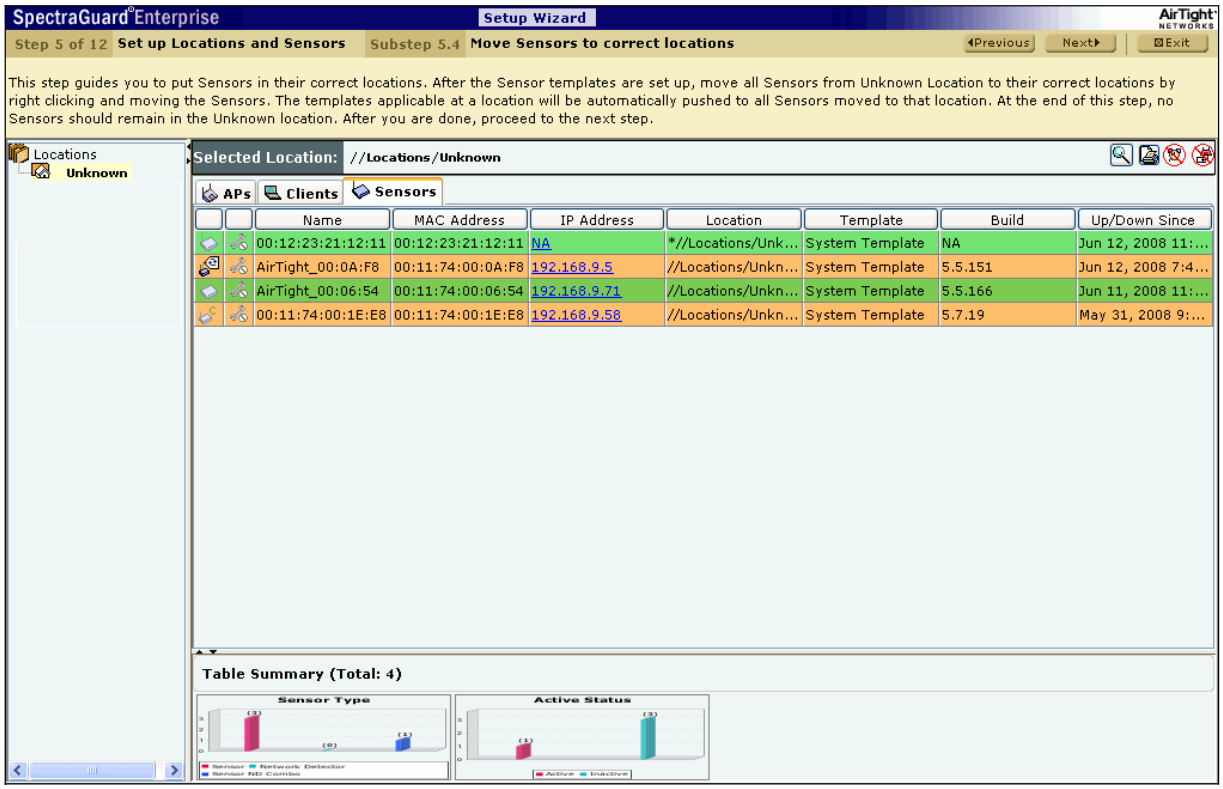


Figure 85. Devices Screen – Sensors

Right-click a Sensor row to move a Sensor. Select **Change Location** from the resultant context-sensitive menu to manually tag the Sensor to the desired location.

15. The **Locations** screen appears as shown in the following figure. Create a visual view of your deployment by attaching pictures and floormaps to locations.

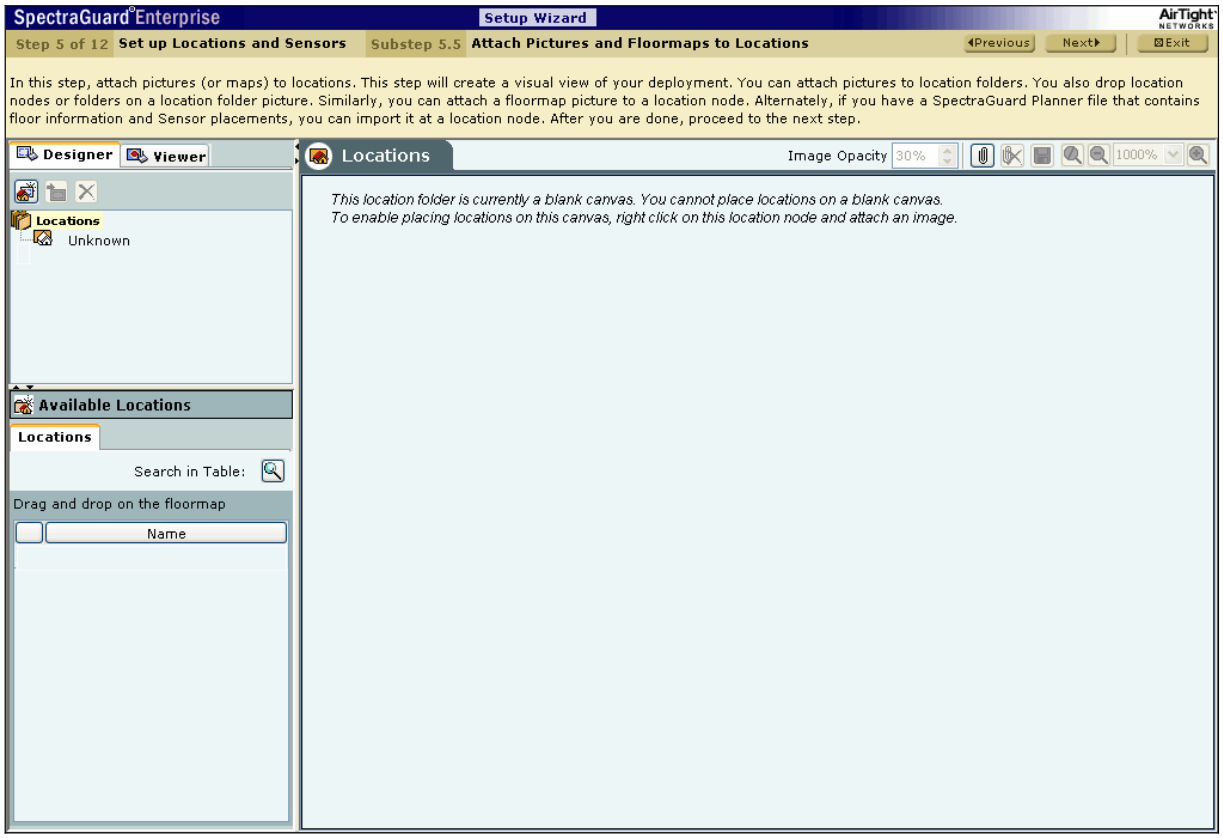


Figure 86. Locations Screen

7.1.5.2 Attaching an image

Use the following steps to attach an image:

a. In the **Location** tree, select the location to which you wish to attach an image.

b. Do one of the following:

- Right-click and from the resulting context-sensitive menu, select **Attach Image**.
- Click the **Attach Image on floor** icon ( ) in the right corner.

c. On the **Select an image file to attach to attach over a planned location** dialog, browse to the appropriate image and then click <**Open**>.

7.1.5.3 Placing Locations on a Location Folder with an Attached Image

The system enables you to place locations on a location folder that has an attached image. This helps you identify the physical position of each of the locations. The locations placed on the attached image are indicated by colored circles. A green circle indicates that the location is **Secure**, while a red circle indicates that the location is **Vulnerable**.

Use the following steps to place locations on the attached image and view their details:

a. In the **Location** tree, select a location folder.

b. Under **Available Locations**, drag and drop the required locations on the attached image.

c. To view details about the location hold the mouse cursor over the colored circle.

d. To go to a particular location placed on the image, do one of the following:

- Click the colored circle representing the location.
- Point to colored circle representing the location, right-click and select **Jump to this location**.

***Note**: You can traverse to a particular location node by following step d until you reach the desired location node.*

7.1.5.4 Importing a Planner file into a Location Node

The system enables you to specify a layout for each location node using a blank canvas, a layout image, or a .SPM file exported from Planner. Use the following steps to import a Planner file:

a. In the **Location** tree, select the location node into which you wish to import the .SPM file and then right-click.

b. Do one of the following:

- From the resulting context-sensitive menu, select **Import Location**.
- Click the **Import Location** icon ( ) below the **Viewer** mode tab.

c. In the **Select SpectraGuard Planner (.spm) File** dialog, browse to the appropriate Planner exported .SPM file and then click <**Open**>.

16. The **Locations** screen appears as shown in the following figure. You can place Sensors on the floormaps by dragging and dropping them. If you have imported an SPM file from Planner that contains floor information and Sensor placements, Sensors contained in that file will be placed automatically.

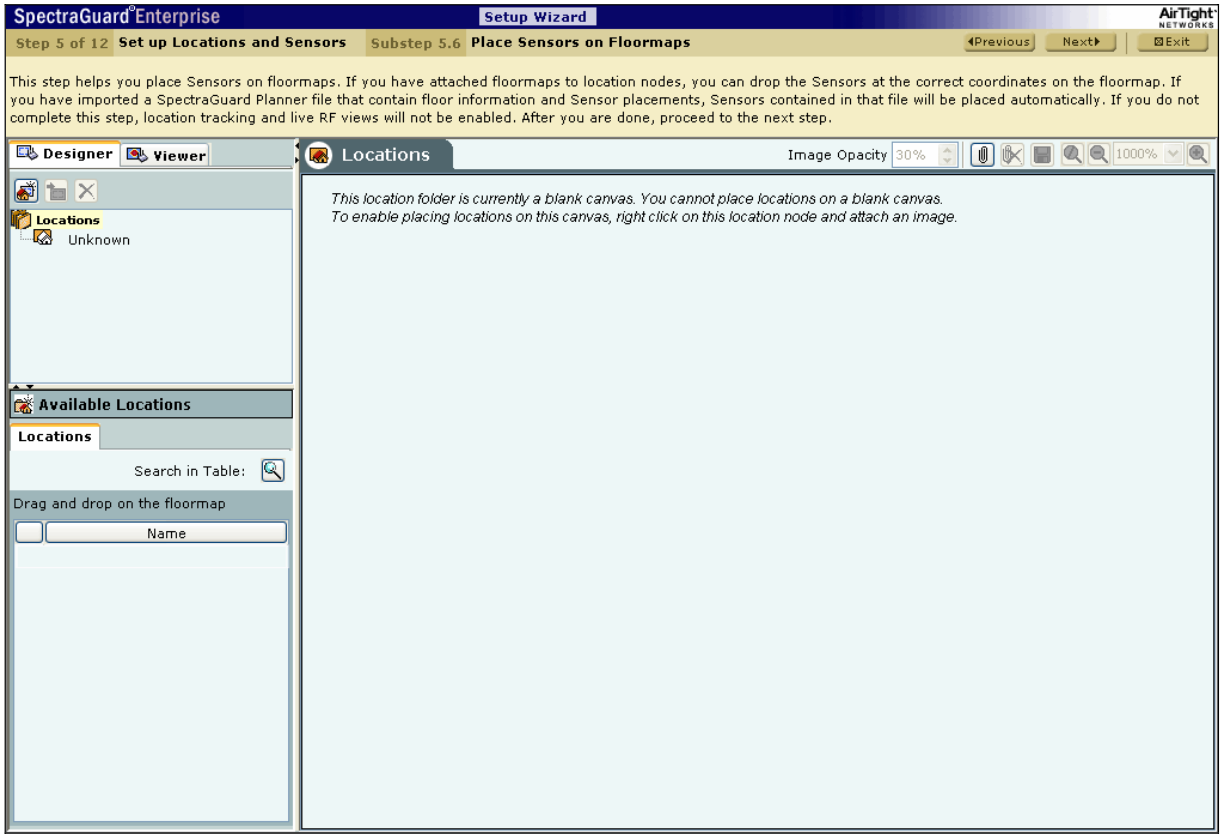


Figure 87. Placing Sensors on the Floormap

You must complete this step to view live RF coverage maps for a location node and perform on-floor location tracking of visible 802.11 devices. Use the following steps to place Sensors on the floormap:

a. In the **Location** tree, select a location node.

b. Under **Available Devices**, select the **Sensors** tab, then drag and drop the Sensors on your floormap.

7.1.6 Step 6: Classifying APs

17. The **Authorized WLAN Setup** screen appears as shown in the following figure. On this screen, specify Authorized AP details using SSID templates to suit different locations.

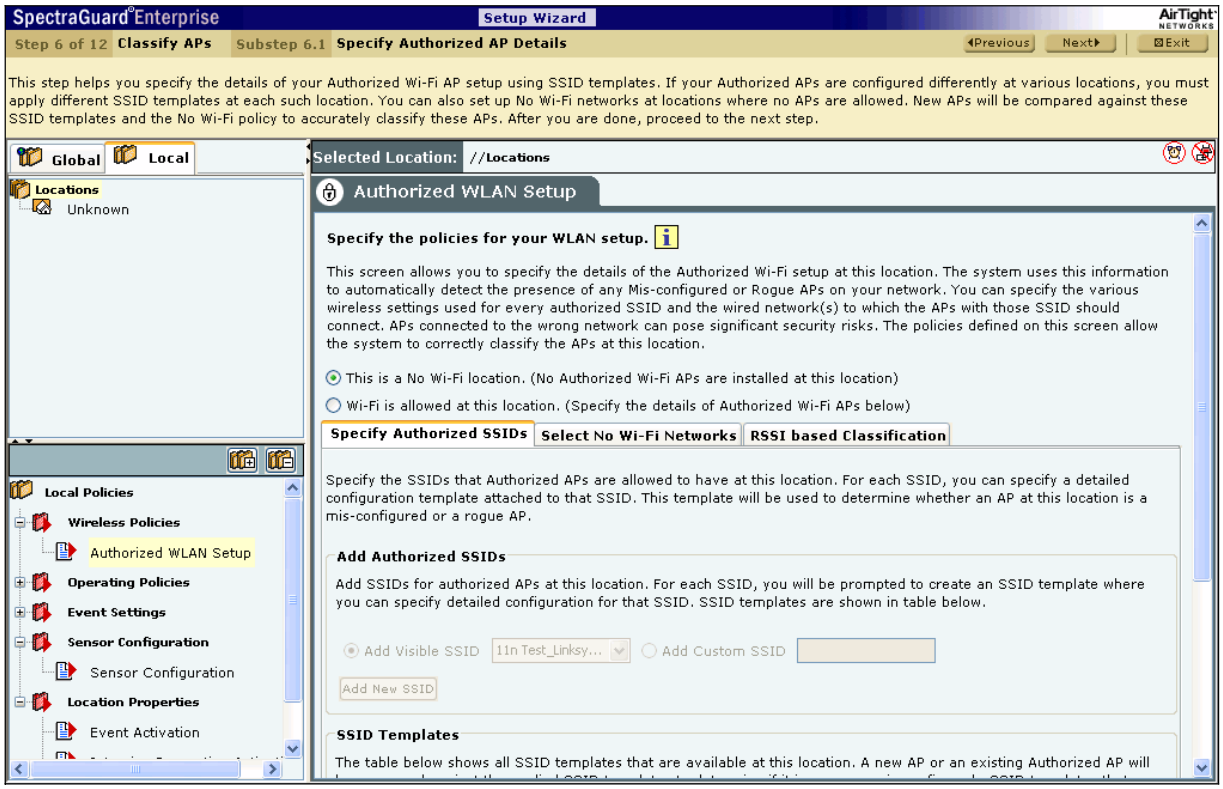


Figure 88. Authorized WLAN Setup

Select one of the following to characterize a particular location:

- **This is a No Wi-Fi location:** If no Authorized Wi-Fi APs are installed at this location. If you configure a location as a no Wi-Fi location, the **Specify Authorized SSID** section is grayed out.
- **Wi-Fi is allowed at this location:** To specify the details of the Authorized Wi-Fi APs in this location.

7.1.6.1 Specify Authorized SSIDs

Under this tab, specify the Authorized SSIDs at this location. For each SSID, you can specify the detailed configuration. This per SSID configuration is called an SSID template.

Creating a Configuration Template for an Authorized 802.11 SSID

Add Authorized SSIDs allows you to create an SSID template in one of the following ways:

- **Add Visible SSID:** To create an SSID template from a list of visible SSIDs. The visible SSID list is built using the data received from Sensors.
- **Add Custom SSID:** To create a template using a user-defined SSID.

Click <**Add New**> to create a new SSID template. The **Template for an Authorized 802.11 SSID** dialog appears where you can select multiple items in some fields.

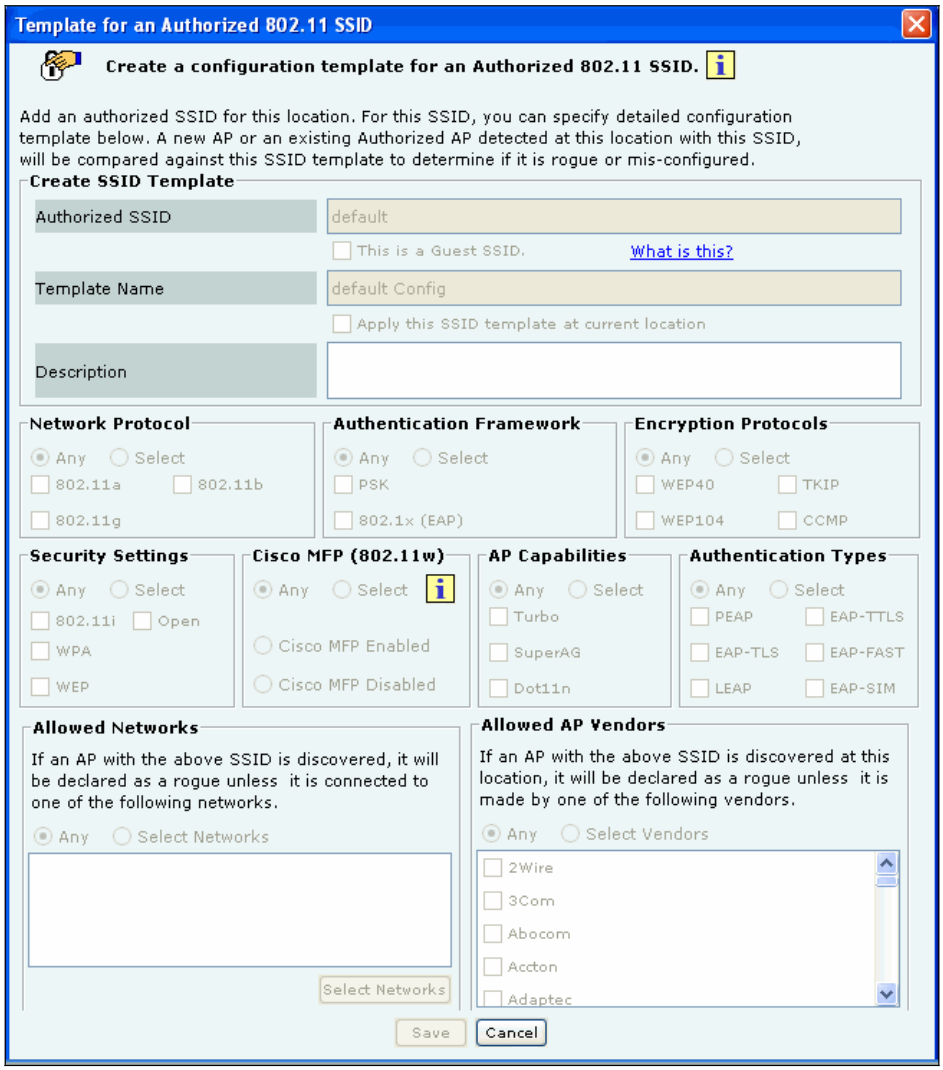


Figure 89. Creating a Configuration Template for an Authorized SSID

- **Create SSID Template** allows you to specify the details for creating a new SSID as follows:
  - **Authorized SSID:** Displays the name of the SSID that you have added earlier
  - **This is a Guest SSID:** Select this option if this SSID is a Guest SSID used to provide Wi-Fi connectivity to visitors and guests. Though APs with Guest SSID are *Authorized*, they may be treated differently than APs that are used by employees for corporate access. Making an SSID as Guest allows you to specify additional classification and prevention policies related to Guest SSIDs. Refer to the sections Client Auto-Classification and Intrusion Prevention Policy in the SpectraGuard Enterprise User Guide for more details on classifying Guest SSIDs
  - **Template Name:** Name of the SSID template
  - **Apply this SSID template at current location:** Select this option to apply this SSID template to the current location. The WLAN policy at a location consists of SSID templates applied at that location. If the template is not applied at this location, it will not be a part of the WLAN policy
  - **Description:** Write a short description to help identify the SSID template
- **Network Protocol** allows you to select the allowed 802.11 protocols for the SSID:
  - **Any:** Allow APs with any network protocol for this SSID
  - **Select:** Specify the 802.11 protocol on which the system allows the APs connected to the network to operate– 802.11 a, 802.11 b, and 802.11g
- **Authentication Framework** allows you to select the security framework for the SSID:

  - **Any:** Allow APs with any authentication framework to connect to the system
  - **Select:** Specify the authentication framework–PSK and 802.1x (EAP). The authentication framework is only applicable if the template supports WPA/WPA2 and 802.11i privacy

- **Encryption Protocols** allows you to select the allowed encryption protocols for the SSID:
  - **Any:** Allow APs with any encryption protocol for this SSID
  - **Select:** Specify the encryption protocols–WEP40, WEP108, TKIP, and CCMP. TKIP and CCMP are available only if the template supports WPA/WPA2 and 802.11i privacy

- **Security Settings** allows you to select the security protocol(s) for the SSID:
  - **Any:** Allow APs with any security settings to connect
  - **Select:** Specify the privacy mechanism–Open, WEP, WPA, and 802.11i for the APs connected to the SSID

- **Cisco MFP** allows you to make classification decisions on Cisco Management Frame Protection(MFP) capability if **802.11i** checkbox is selected under **Security Settings:**
  - **Any**: Policy does not check for MFP; both Cisco MFP enabled and disabled APs are classified as *Authorized*
  - **Select**: Policy checks for MFP
    - **Cisco MFP Enabled:** Select to classify only Cisco MFP supporting APs as *Authorize*d APs
    - **Cisco MFP Disabled:** Select to classify non-Cisco MFP supporting APs as *Authorized* APs

- **AP Capabilities** allows you to select the additional capabilities that Authorized APs may have. If you select any of these advanced capabilities, the classification logic allows APs with and without these capabilities. Select one of the following:
  - **Any:** Allow APs with any special capability for this SSID
  - **Select:** Specify if the AP uses any Turbo/Super techniques used by Atheros to get higher throughputs–Turbo, SuperAG, and Dot11n (802.11n)

- **Authentication Types** allows you to select the allowed authentication types that Clients can use. Authentication types do not determine the classification of APs, but are used to raise an event if a Client is authenticated via a non-allowed authentication type. The system raises this event only if the system sees authentication protocol handshake frames.
  - **Any:** Allow Clients with any authentication type for this SSID
  - **Select:** Specify the authentication types that Clients can use (only if 802.1x is selected)–PEAP, EAP-TLS, LEAP, EAP-TTLS, EAP-FAST, and EAP-SIM Selection is allowed

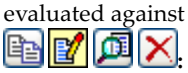
- **Allowed Networks** allows you to select the networks where Authorized APs with this SSID are connected:
  - **Any:** Allow APs with this SSID to connect to any network
  - **Select Networks:** Specify the networks where Authorized APs with this SSID are connected. You can either choose from networks that are discovered automatically by the system or add new networks that are not yet discovered by the system
    - Click <**Select Networks**> to open **Allowed Networks for SSID** dialog where you can move a network from **Networks Monitored by the System** to **Allowed Networks for this SSID** and add or delete networks.

- Under **Allowed AP Vendors**, select one of the following:
  - **Any:** Allow APs manufactured by any vendor to connect to the system
  - **Select Vendors:** Select the manufacturer of the AP with the specified SSID. If an AP with the specified SSID is discovered at this location, the system declares it as a Rogue, unless one of the manufacturers listed manufactures it.

SSID Templates

A policy is collection of SSID templates attached to that location. You can apply an SSID template from the parent or create it locally; if you wish to customize the WLAN policy for that location. Other templates may be available to be attached but are not part of the WLAN policy and will not be used for AP classification.

The **SSID Templates** section lists the SSID templates that are available at a particular location. You must apply the templates from the available list to create the WLAN policy at that location. A new AP or an existing Authorized AP is compared against the applied SSID templates to determine if it is a Rogue or Mis-configured AP. The SSID templates created at other locations can be applied to a selected location but cannot be edited or deleted. The edit and delete operations are possible only at the location where the template is created. The table shows the following details:

- **SSID:** Name of the SSID
- **Guest SSID?:** Indicates if it is a Guest SSID
- **Template Name:** Name of the SSID template
- **Apply Here?:** Enables you to apply the SSID template to the selected location. New and existing Authorized APs are evaluated against all applied SSID templates to determine if they are Rogue or Mis-configured.
-  : Click these icons to perform the following:
  - Copy the selected SSID template to another location.
  - Edit the SSID template. This option is enabled only at the location where the template was created.
  - View the SSID template.
  - Delete the template. This option is enabled only at the location where the template was created and only if the template is not applied at any other child locations of the location where it was created.

7.1.6.2 Select Wi-Fi Networks

This section allows you to specify the list of networks at the selected location where no Wi-Fi APs are allowed to be connected. The No Wi-Fi Networks list at a location takes precedence over the list of networks in SSID templates applied at that location. In other words, if a network is included in a location's no Wi-Fi list and happens to be in the list of networks in one or more applied SSIDs at that location, the network will be still treated as a no Wi-Fi network.

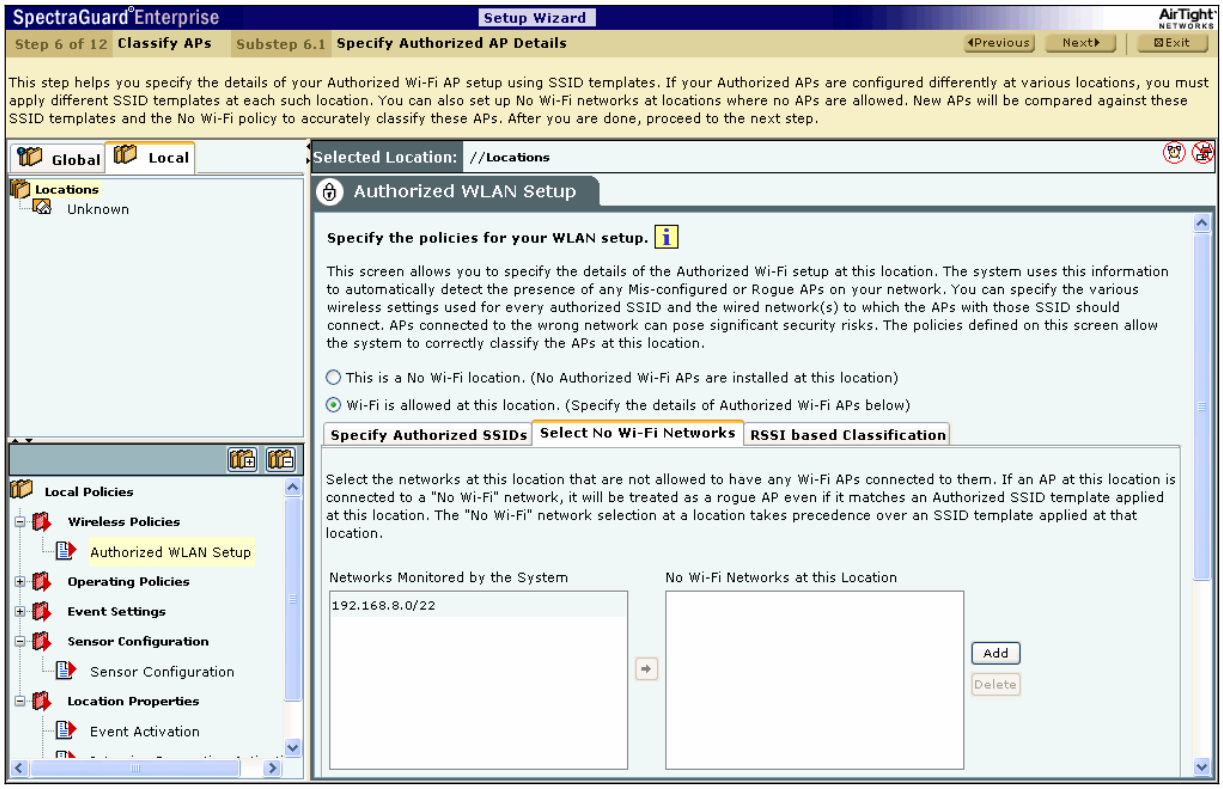


Figure 90. No-Wi-Fi Networks

- **Networks Monitored by the System:** Specifies the networks monitored by the system.
- **No Wi-Fi Networks at this Location:** Specifies the networks to which no Wi-Fi AP should be connected at the selected location.

You can move a network from **Networks Monitored by the System** to **No Wi-Fi Networks at this Location**.

Click <**Add**> to enter a new network address to add a *No Wi-Fi* network at the selected location.

7.1.6.3 RSSI based Classification

APs are further classified based on the RSSI value that the Sensors receive. If the signal strenth exceeds a maximmum threshold, the Sensor appropriately clssifies the AP. Airtight ***higly*** recommends that you turn ***on*** network connectivity based

classification as it is the most reliable mechanism to classify wireless devices when most of your network is monitored using Sensors and NDs.

Under **RSSI Threshold**, select one or both (recommend) of the following checkboxes:

- **Pre-classify APs with signal strength stronger than threshold as Rogue or Authorized APs** to specify the threshold RSSI value based on which the system further classifies APs.
- **Pre-classify APs connected to monitored subnet as Rogue or Authorized APs** to classify APs based on their network connectivity.

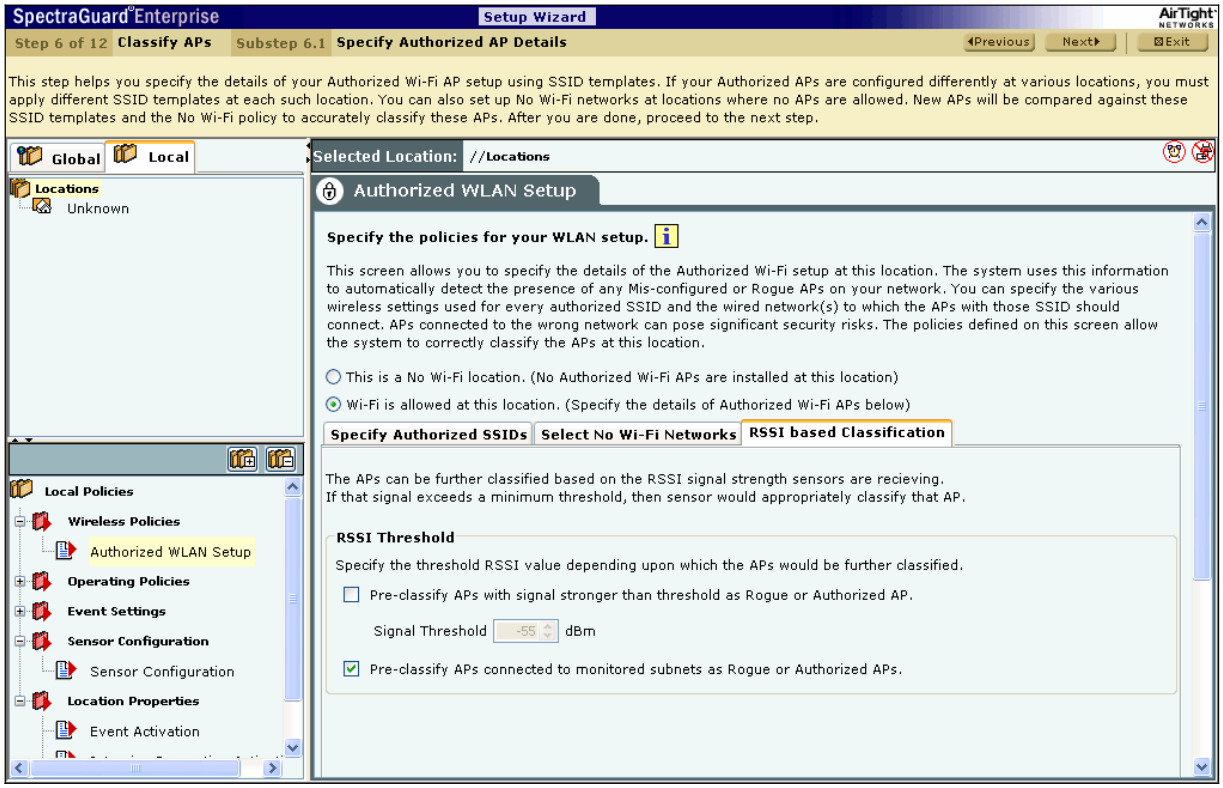


Figure 91. RSSI based Classification

18. The **AP Auto-classification** screen appears as shown in the following figure. It enables you to specify the AP classification policy for different AP categories.

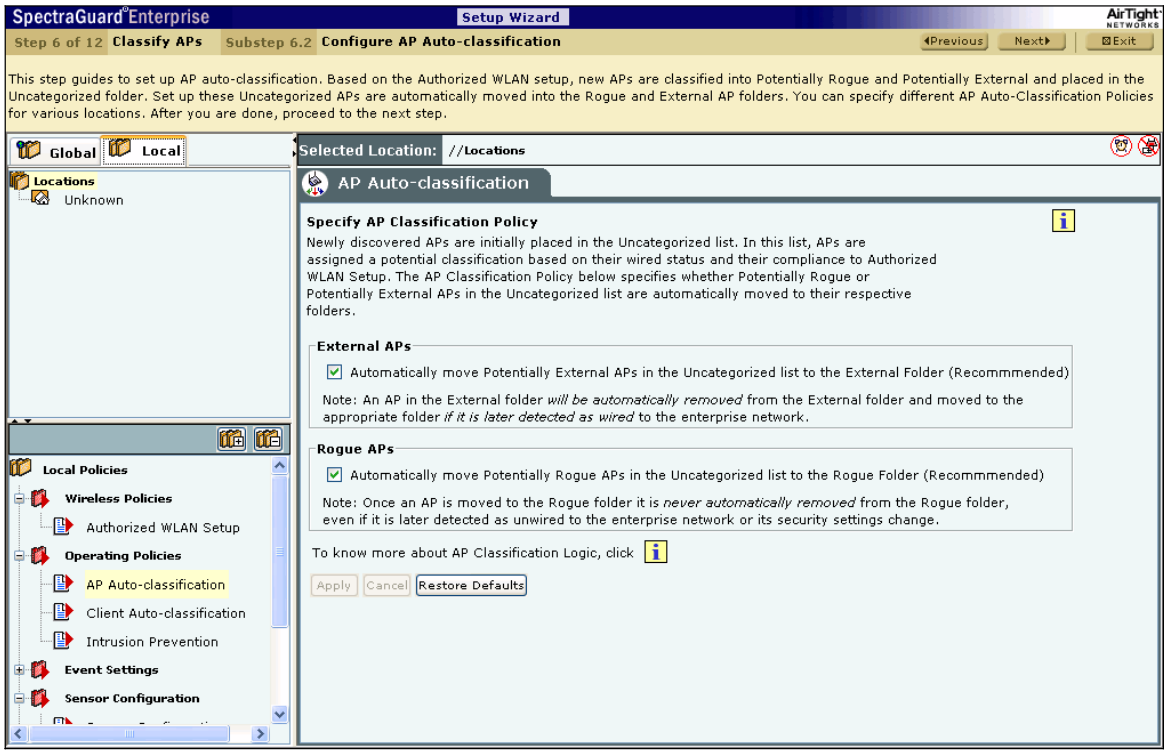


Figure 92. AP Auto-Classification Policy

Under **External APs**, AirTight recommends that you select **Automatically move Potentially External APs in the Uncategorized list to the External Folder**. The system automatically removes an AP from the ***External*** folder and moves it to an ***appropriate*** AP folder if it later detects that the AP is wired to the enterprise network.

Under **Rogue APs**, AirTight recommends that you select **Automatically move Potentially External APs in the Uncategorized list to the Rogue Folder**.

***Note**: Once you move an AP to the **Rogue** folder, the system never automatically removes it from the Rogue folder, even if it later detects that the AP is unwired from the enterprise network or its security settings have changed.*

---

19. The **Import Devices** screen appears as shown in the following figure. Importing an **Authorized AP List** is an efficient alternative to manual movement of these APs into the **Authorized** bin. After successfully importing these lists, the system automatically classifies the APs in the respective lists as **Authorized**.

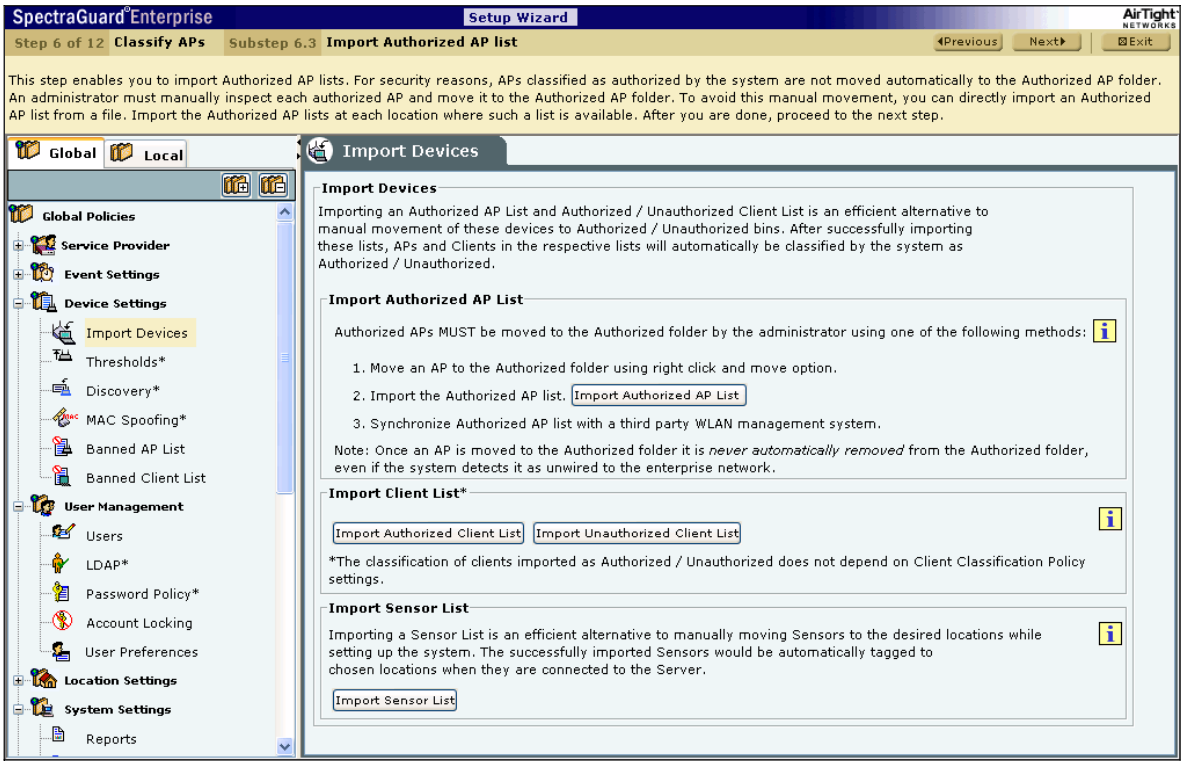


Figure 93. Import Devices – APs

You can move Authorized APs to the Authorized folder using one of the following methods:

- Move an AP to the Authorized folder using right click and **Move** option
- Import the Authorized AP list
- Synchronize with an AP Management Server

***Note**: Once you move an AP to the **Authorized** folder, the system **never** automatically removes it from the **Authorized** folder, even if it later detects that the AP is **unwired** from the enterprise network.*

Under **Import AP List**, click <**Import Authorized AP List**> to open **Import Authorized AP List** dialog.

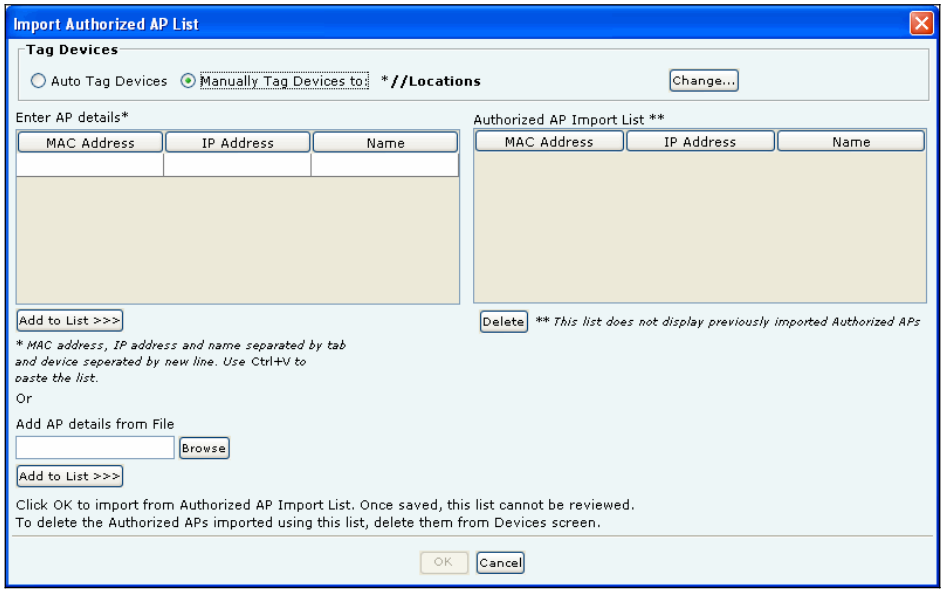


Figure 94. Import Authorized AP List

In the **Import Authorized AP List** dialog:
Under **Tag Devices**, select one of the following:

- **Auto Tag Devices:** To automatically tag the AP to the corresponding location.
- **Manually Tag Devices to::** Click <**Change**> to manually tag the AP to the desired location.

Under **Enter AP details**

- To add an AP's details, type the AP's MAC address, IP Address, and Name and click <**Add to List>>>**>.
- To add an AP's details from a file, click <**Browse**>. On the **Select Authorized AP_Device_List_File** dialog, select the .txt file from the desired location and click <**Open**>. Then click <**Add to List>>>**>.

Under **Authorized AP Import List**

- To delete an AP's details, select the corresponding row and click <**Delete**>.

To import Authorized APs from the **Authorized AP Import List**, click <**OK**>.

***Note**: When you import APs from a list, policy settings in the Setup Wizard do not affect these APs.*

20. The **Devices→APs** screen appears as shown in the following figure. The system enables you to inspect, confirm, and re-classify a device, which is, move a device to a different folder based on fresh information.

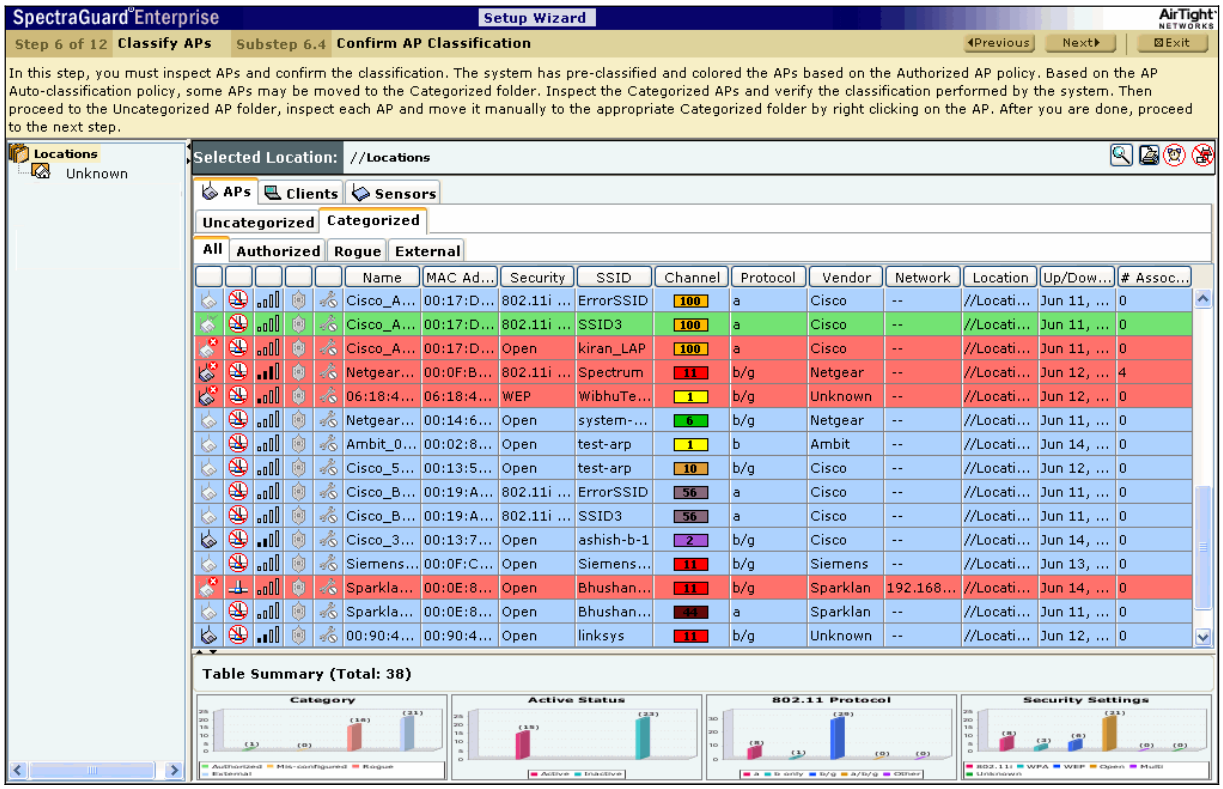


Figure 95. Devices Screen – APs

Use the following steps to move an AP to a specific folder:

a. In the AP list, right click the desired AP row.
b. From the resulting context sensitive menu, select **Move to…**.
c. Click the desired category to which you want to move the AP.

***Note**: If you move an AP placed on a floormap, an **Error** dialog appears.*

21. The **Locations** screen appears as shown in the following figure. The system enables you to place APs on the floormap to view live RF coverage maps for a location node and perform on-floor location tracking of visible 802.11 devices.

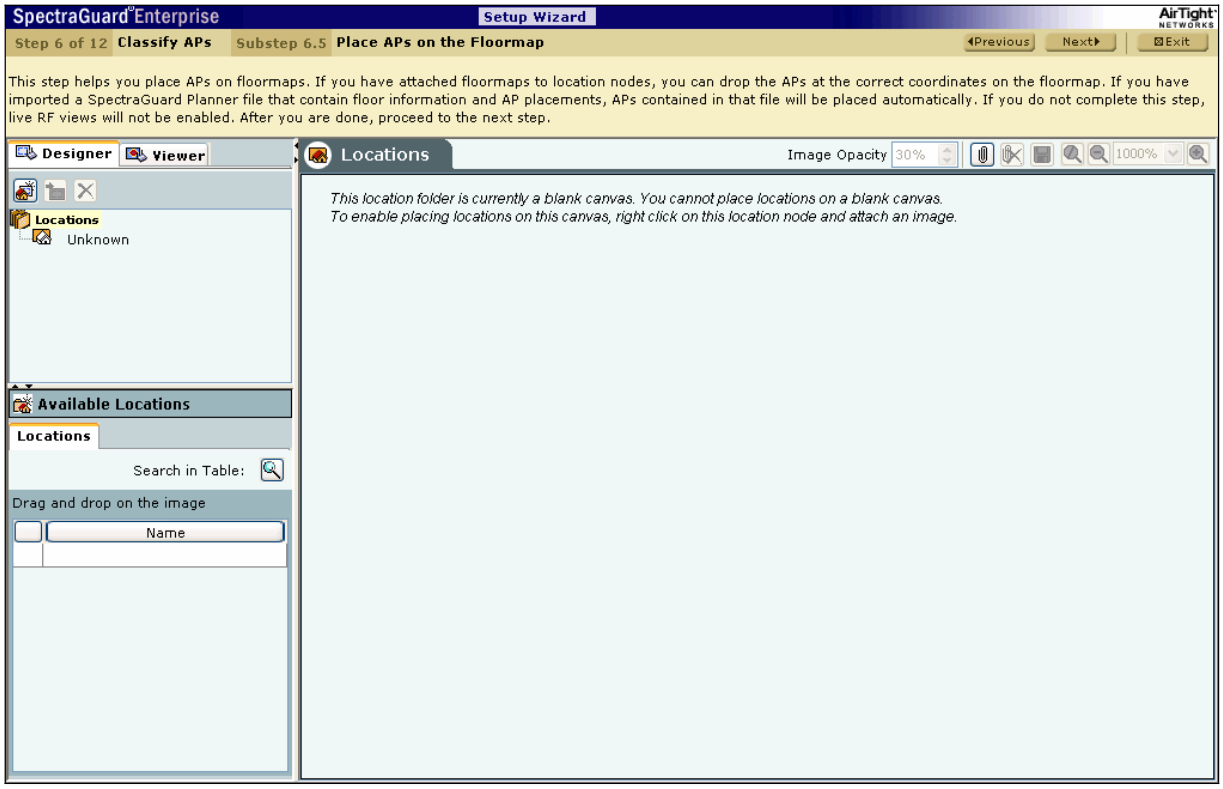


Figure 96. Locations Screen

Use the following steps to place APs on the floormap:

a. In the **Location** tree, select a location node.

b. Under **Available Devices**, select the **APs** tab, then drag and drop the APs on your floormap.

7.1.7 Step 7: Classifying Clients

22. The **Client Auto-classification** screen appears as shown in the following figure. It determines how Clients are classified upon initial discovery and subsequent associations with APs.

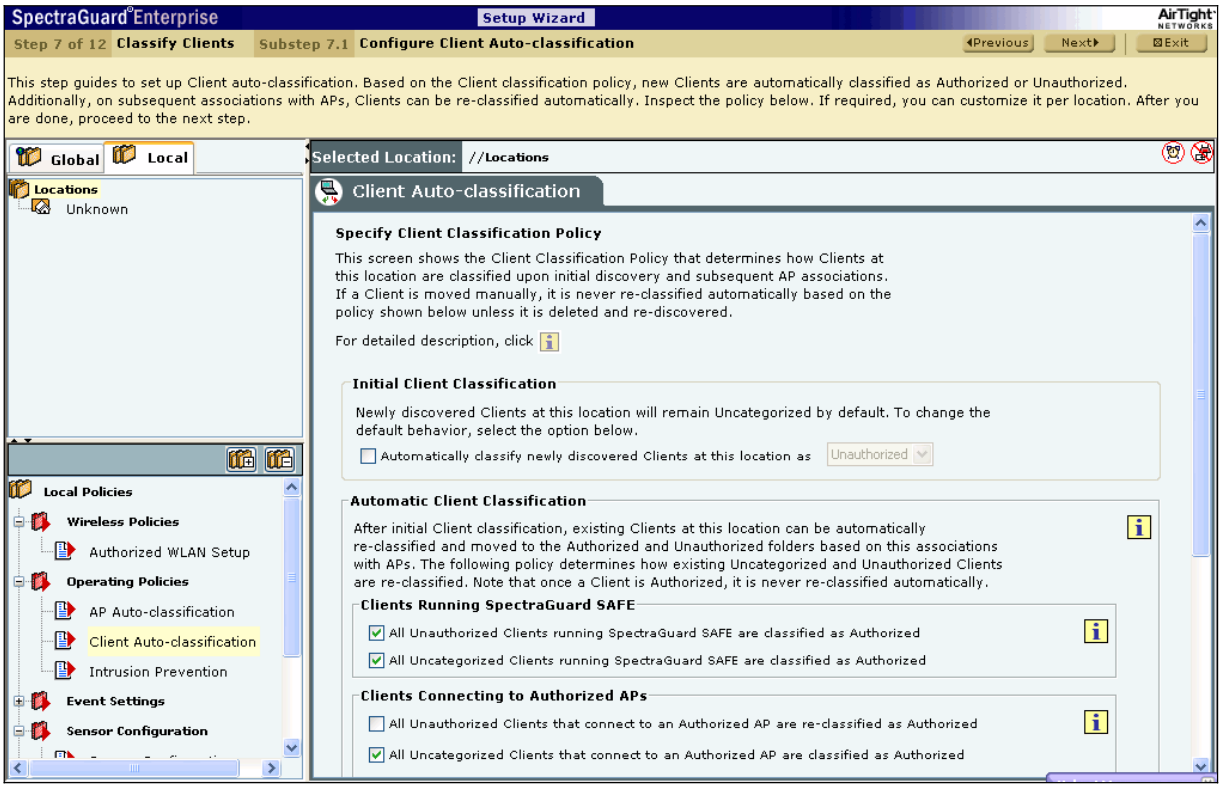


Figure 97. Client Auto-Classification Policy

Under **Initial Client Classification**, specify if newly discovered Clients at a particular location, which are **Uncategorized** by default should be classified as *Authorized* or *Unauthorized*.

Under **Automatic Client Classification**, select one or more options to enable The system automatically re-classify **Uncategorized** and **Unauthorized** Clients based on their associations with APs. You can categorize the following types of Clients.

- **Clients running SAFE**
  - All Unauthorized Clients running SpectraGuard SAFE are classified as Authorized
  - All Uncategorized Clients running SpectraGuard SAFE are classified as Authorized
- **Clients connecting to Authorized APs**
  - All Unauthorized Clients that connect to an Authorized AP are re-classified as Authorized
  - All Uncategorized Clients that connect to an Authorized AP are classified as Authorized

You can select the following **Exceptions**

- Do not re-classify a Client connecting to a Guest AP as Authorized
- Do not re-classify a Client connecting to a Mis-configured AP as Authorized
- Do not re-classify a Client as Authorized if its wireless data packets are not detected on the wired network

- **Clients connecting to External or Rogue APs**
  - All Uncategorized Clients that connect to an External AP are classified as Unauthorized
  - All Uncategorized Clients that connect to a Rogue AP are classified as Unauthorized
  - All Uncategorized Clients that connect to a Potentially External AP are classified as Unauthorized
  - All Uncategorized Clients that connect to a Potentially Rogue AP are classified as Unauthorized

23. The **Import Devices** screen appears as shown in the following figure. Importing an **Authorized** or **Unauthorized Clients List** is an efficient alternative to manual movement of these devices into the **Authorized/Unauthorized** bins. After successfully importing these lists, the system automatically classifies the Clients in the respective lists as **Authorized/Unauthorized**.

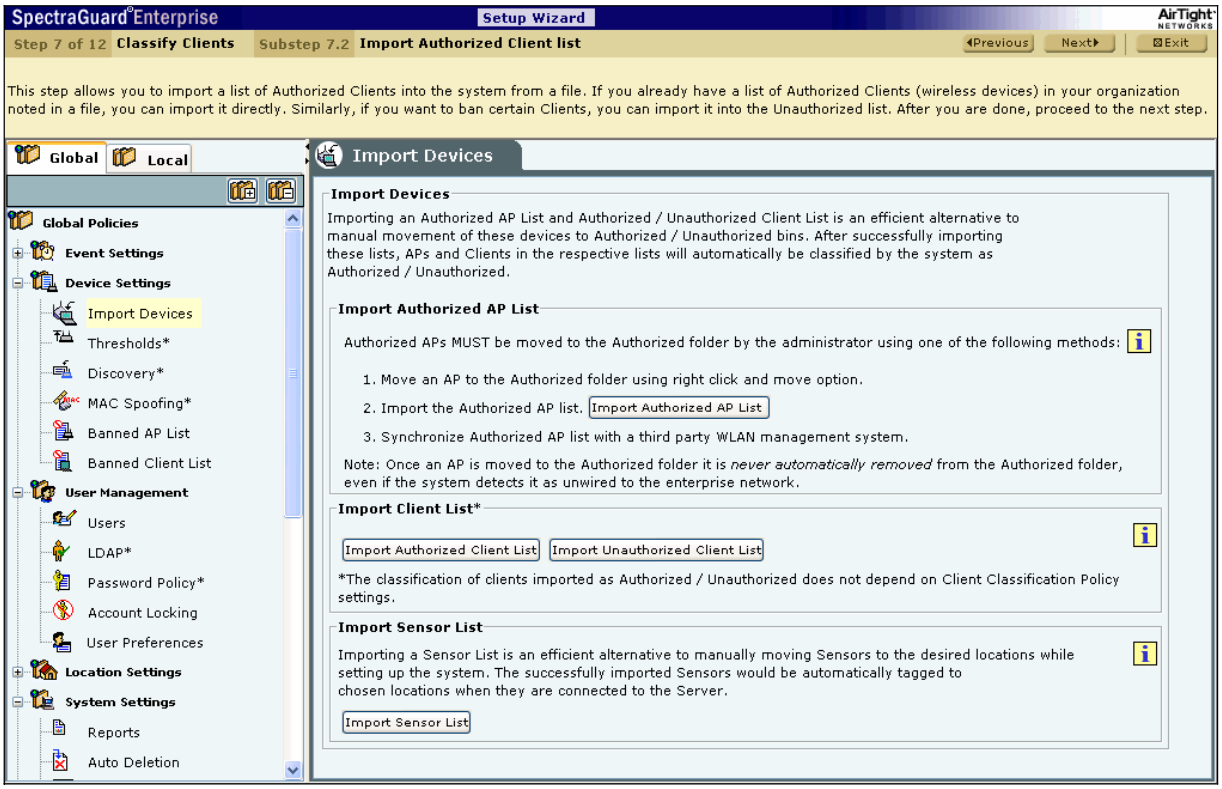


Figure 98. Import Devices – Clients

In the **Import Devices** dialog, under **Import Client List**, click <**Import Authorized Client List**> to open **Import Authorized Client List** dialog and/or click <**Import Unauthorized Client List**> to open **Import Unauthorized Client List** dialog.

In the **Import Authorized/Unauthorized Client List** dialog:
Under **Tag Devices**, select one of the following:

- **Auto Tag Devices:** To automatically tag the AP to the corresponding location.
- **Manually Tag Devices to::** Click <**Change**> to manually tag the AP to the desired location.

Under **Enter Client details**

- To add a Client's details, under **Enter Client details**, type the Client's MAC Address, IP Address, and Name and click <**Add to List>>>**>.
- To add a Client's details from a file, click <**Browse**>. On the **Select Authorized/Unauthorized Client_Device_List_File** dialog, select the .txt file from the desired location and click <**Open**>. Then click <**Add to List>>>**>.

Under **Authorized/Unauthorized Client Import List**

- To delete a Client's details, select the corresponding row and click <**Delete**>.

To import Authorized/Unauthorized Clients from the **Authorized/Unauthorized Client Import List**, click <**OK**>.

***Note**: When you import Clients from a list, policy settings in the Setup Wizard do not affect these Clients.*

24. The **Devices→Clients** screen appears as shown in the following figure. The system enables you to inspect, confirm, and re-classify a device, which is, move a device to a different folder based on fresh information.

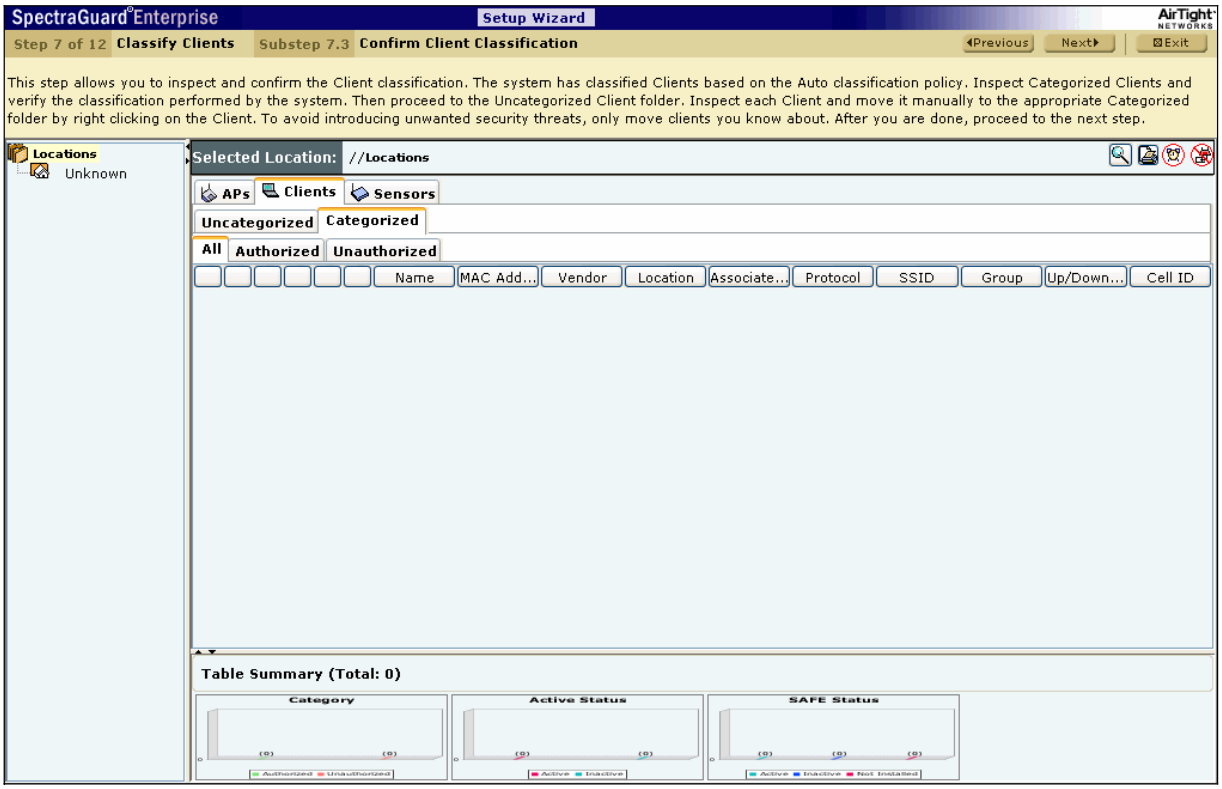


Figure 99. Devices Screen – Clients

Use the following steps to move a Client to a specific folder:

a. In the Client list, right click the desired Client row.
b. From the resulting context sensitive menu, select **Move to…**.
c. Click the desired category to which you want to move the Client.

7.1.8 Step 8: Configuring Intrusion Prevention Policy

25. The **Intrusion Prevention** screen appears as shown in the following figure.

7.1.8.1 Intrusion Prevention Policy

The Intrusion Prevention policy determines the wireless threats against which the system protects the network automatically. The system automatically moves such threat-posing APs and Clients to quarantine. The system can protect against multiple threats simultaneously based on the selected Intrusion Prevention Level.

If the Server quarantines an AP or Client based on the Intrusion Prevention policy, the **Disable Auto-quarantine** option ensures that the system will not automatically quarantine this AP or Client (regardless of the specified Intrusion Prevention policies).

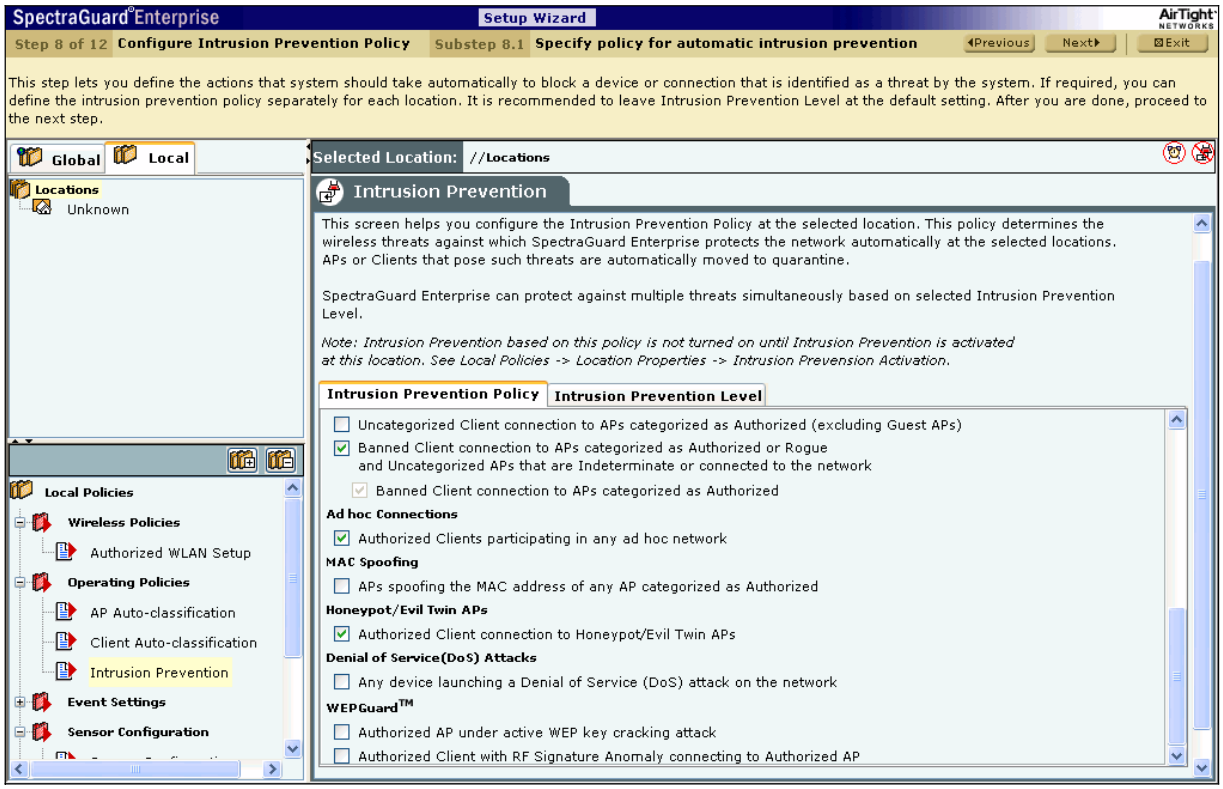


Figure 100. Intrusion Prevention Policy

You can enable intrusion prevention against the following threats:

- **Rogue APs:** APs that are connected to your network but not authorized by the administrator; an attacker can gain access to your network through the Rogue APs. You can also automatically quarantine Uncategorized Indeterminate and Banned APs connected to the network.
- **Mis-configured APs:** APs that are authorized by the administrator but do not conform to the security policy; an attacker can gain access to your network through misconfigured APs. This could happen if the APs are reset, tampered with, or if there is a change in the security policy.
- **Client Mis-association:** Authorized Clients that connect to Rogue or External (neighboring) APs; corporate data on the Authorized Client is under threat due to such connections. AirTight recommends that you provide automatic intrusion prevention against Authorized Clients that connect to External APs.
- **Unauthorized Associations:** Unauthorized and Banned Clients that connect to Authorized APs; an attacker can gain access to your network through Authorized APs if the security mechanisms are weak. Unauthorized or Uncategorized Client connections to an Authorized AP using a Guest SSID are not treated as unauthorized associations.
- **Ad hoc Connections:** Peer-to-peer connections between Clients; corporate data on the Authorized Client is under threat if it is involved in an ad hoc connection.
- **MAC Spoofing:** An AP that spoofs the wireless MAC address of an Authorized AP; an attacker can launch an attack through a MAC spoofing AP.
- **Honeypot/Evil Twin APs:** Neighboring APs that have the same SSID as an Authorized AP; Authorized Clients can connect to Honeypot/Evil Twin APs. Corporate data on these Authorized Clients is under threat due to such connections.
- **Denial of Service (DoS) Attacks:** DoS attacks degrade the performance of an official WLAN.
- **WEPGuard ™:** Active WEP cracking tools allow attackers to crack the WEP key and gain access to confidential data in a matter of minutes or even seconds. Compromised WEP keys are used to gain entry into the authorized WLAN by spoofing the MAC address of an inactive Authorized Client.

7.1.8.2 Intrusion Prevention Level

The system can prevent any unwanted communication in your 802.11 network. It provides you various levels of prevention-blocking mechanisms of varying effectiveness. Intrusion Prevention Level enables you to specify a trade-off between the desired level of prevention and the desired number of multiple simultaneous preventions across radio channels.

The greater the number of channels across which simultaneous prevention is desired, the lesser is the effectiveness of prevention in inhibiting unwanted communication. Scanning for new devices continues regardless of the chosen prevention level.

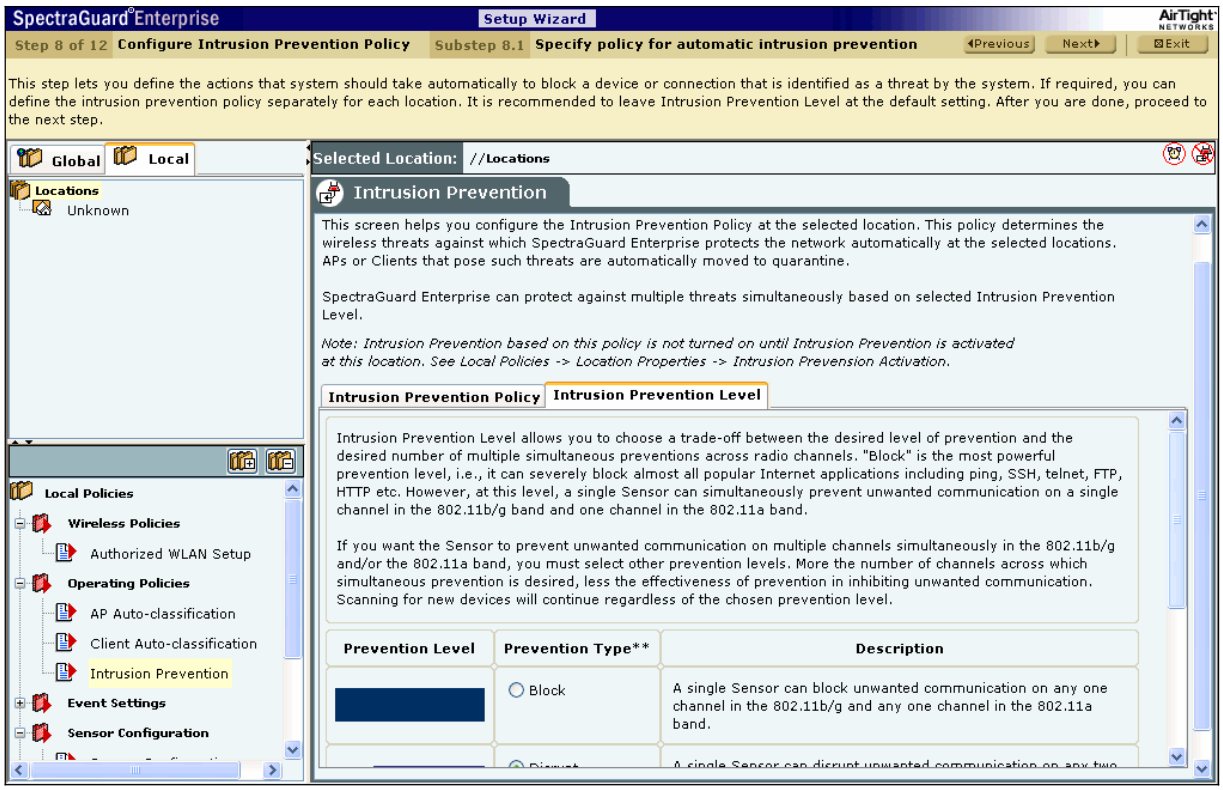


Figure 101. Intrusion Prevention Level

You can select the following prevention levels:

- **Block:** A single Sensor can block unwanted communication on any one channel in the 802.11b/g band and any one channel in the 802.11a band.
- **Disrupt:** A single Sensor can disrupt unwanted communication on any two channels in the 802.11b/g band and any two channels in the 802.11a band.
- **Interrupt:** A single Sensor can interrupt unwanted communication on any three channels in the 802.11b/g band and any three channels in the 802.11a band.
- **Degrade:** A single Sensor can degrade the performance of unwanted communication on any four channels in 802.11b/g band and any four channels in the 802.11a band.

Block is the most powerful prevention level, that is, it can severely block almost all popular Internet applications including ping, SSH, telnet, FTP, HTTP, and the like. However, at this level, a single Sensor can simultaneously prevent unwanted communication on only one channel in the 802.11b/g band and one channel in the 802.11a band. If you want the Sensor to prevent unwanted communication on multiple channels simultaneously in the 802.11 b/g and/or the 802.11a band, you must select other prevention levels.

Note: ***Prevention Type*** *determines the blocking strength to prevent communication from unwanted APs and Clients. The system can prevent multiple APs and Clients on each channel. Prevention Type is not applicable for Denial of Service (DoS) attacks or ad hoc networks. You must select a lower blocking level to prevent devices on more channels. Choosing a lower blocking level means that some packets from the blocked device may go through.*

7.1.9 Step 9: Configuring Events and Reports

26. The **Event Configuration** function screen of the Event Settings appears as shown in the following figure.

7.1.9.1 Security

Security enables you to view events related to security and that pose a threat to your network.

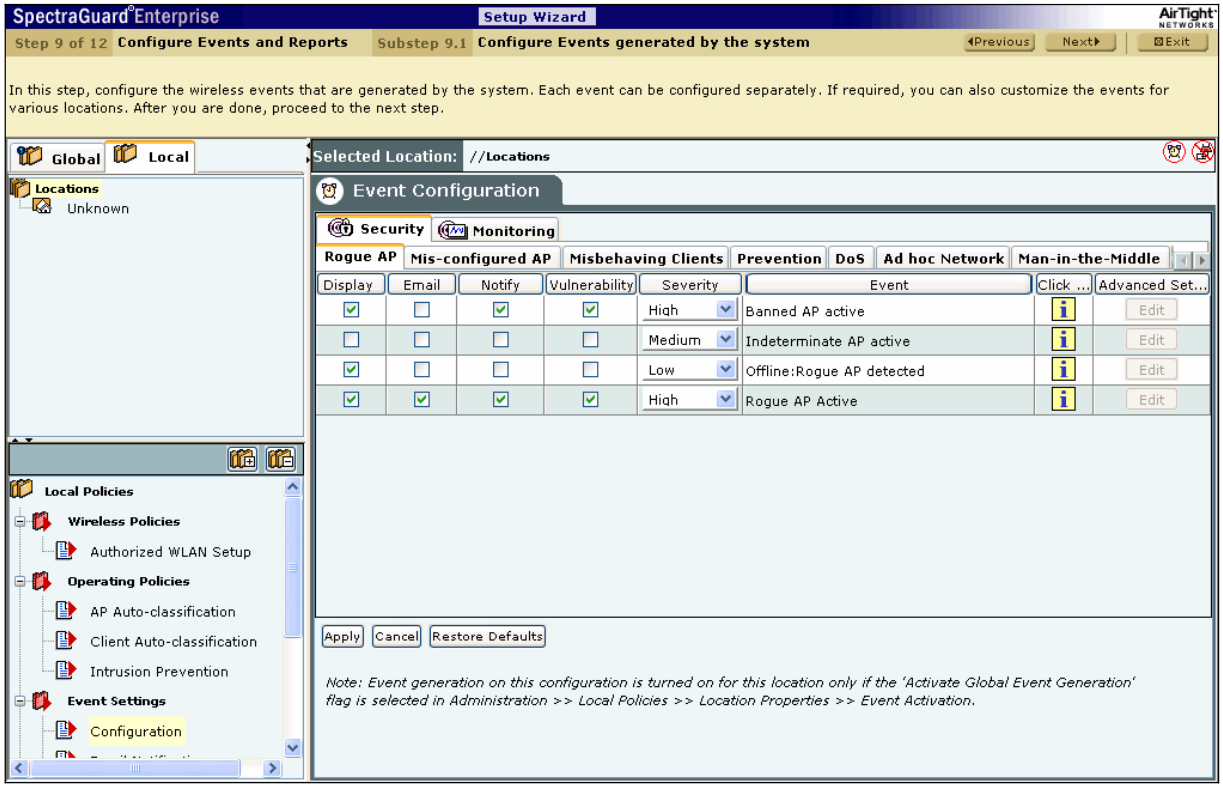


Figure 102. Event Configuration – Security

Security is further divided into the following:

- Rogue AP
- Mis-Configured AP
- Misbehaving Clients
- Prevention
- DoS
- Ad hoc Network
- Man-in-the-Middle
- MAC Spoofing
- Reconnaissance
- System

7.1.9.2 Monitoring

Monitoring enables you to view events related to the monitoring of your network and that are informational in nature.

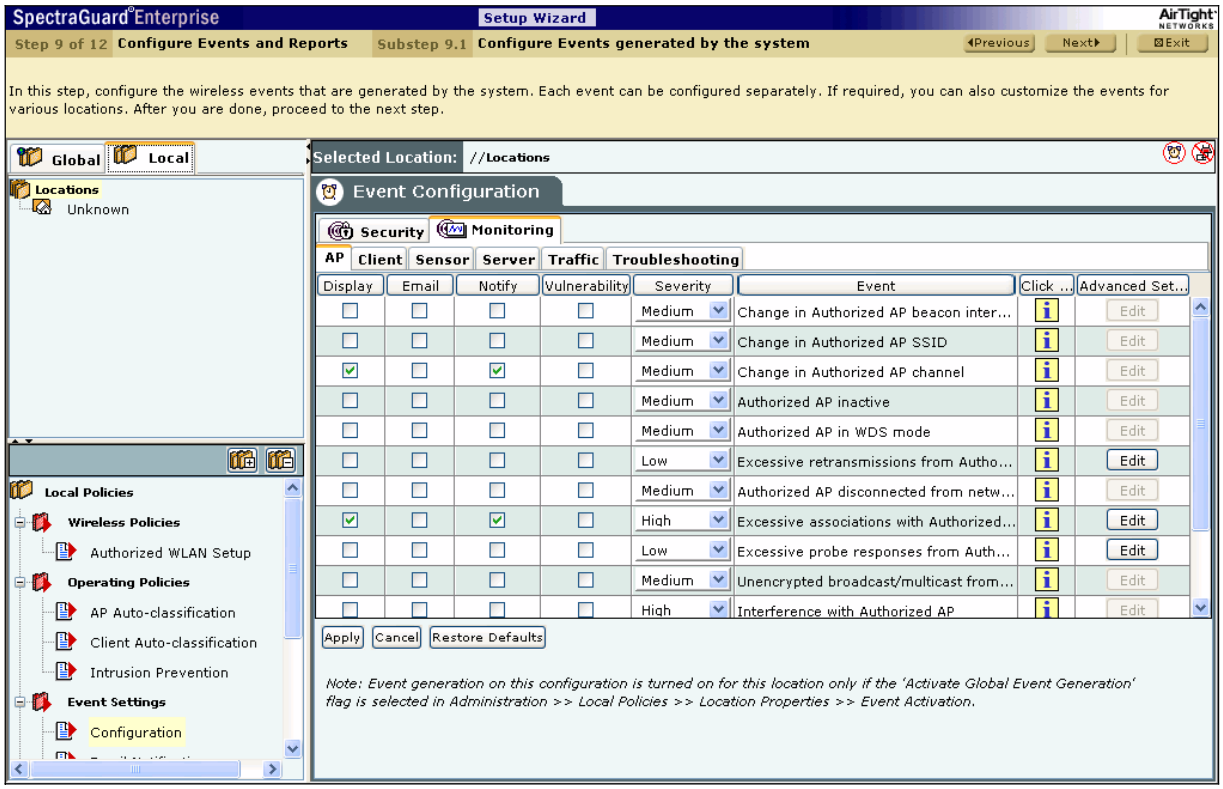


Figure 103. Event Configuration – Monitoring

Monitoring is further divided into the following:

- AP
- Client
- Sensor
- Server
- Traffic
- Troubleshooting

Once you select any of the above categories and sub-categories, a list of related events appears.

The events list displays the following columns:

- **Display:** Select the checkboxes that correspond to the types of events that you want to appear in the main **Events** screen.
- **E-mail:** Select the checkboxes that correspond to the types of events for which you want emails notifications sent to all users whose email addresses you have configured in the **Administration→Event Settings→Email Notification**.
- **Notify:** Select the checkboxes that correspond to the types of events for which you want notifications sent to external agents such as SNMP, Syslog, ArcSight, and OPSEC.
- **Vulnerability:** Select checkboxes to indicate which events make the system **Vulnerable**. The **Security Scorecard** shows **Vulnerable** status if any events of the selected type occur.
- **Severity:** Select the severity of each event as **High**, **Medium**, or **Low**. This function helps you to organize events in the most useful way.
- **Event:** Provides a short description of each event.
- **Click…:** Click to view a detailed description of the corresponding event category.
- **Advanced Settings:** Click <**Edit**> to open the **Event Advanced Settings** dialog and change the configuration parameters of the corresponding event category. <**Edit**> is disabled when the event has no configuration parameters.

*Note: The parameters in the **Event Advanced Settings** dialog changes according to the settings for the selected event.*

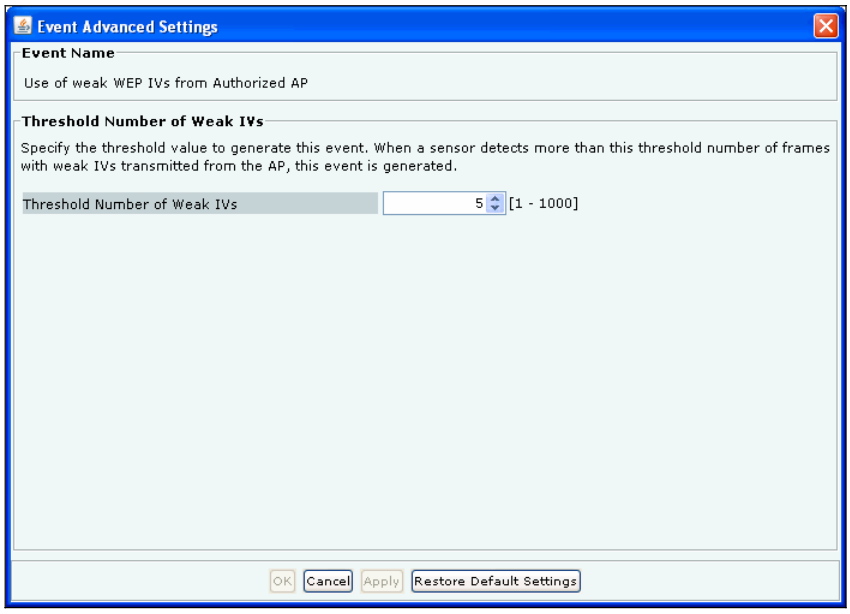


Figure 104. Event Advanced Settings

27. The **Email Notification** screen appears as shown in the following figure. The **Email Notification** node enables you to select the email addresses that should be notified when an event occurs at a particular location. You can select from the email addresses of system users or add a custom email address.

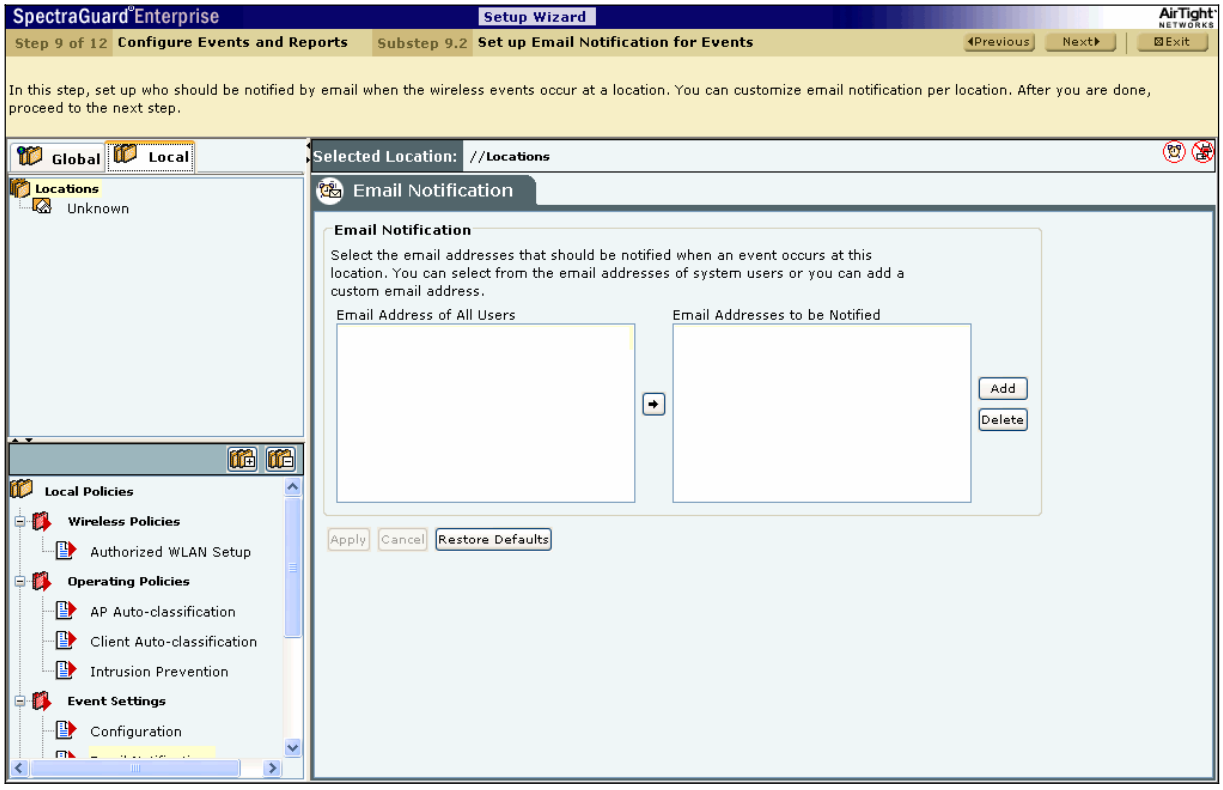


Figure 105. Email Notification

Click <**Add**>to open **Custom Email Address for Notification** dialog where you can add a new email address.

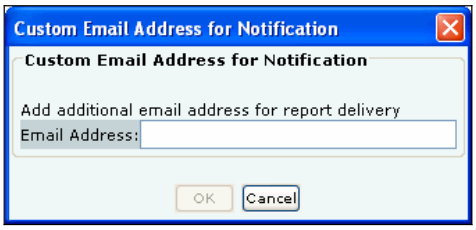


Figure 106. Email Configuration Dialog

Click <**OK**> to add the new email address.

Select an email address and click <**Delete**> to delete an existing email address. You can delete multiple email addresses using click-and-drag or using the <**Shift**> + <**Down Arrow**> keys and then clicking <**Delete**>.

28. The **Reports** screen appears as shown in the following figure. The system enables you to use reports generated by the system and create custom reports. You can schedule email delivery of a Shared report. You can select one time delivery or recurring delivery.

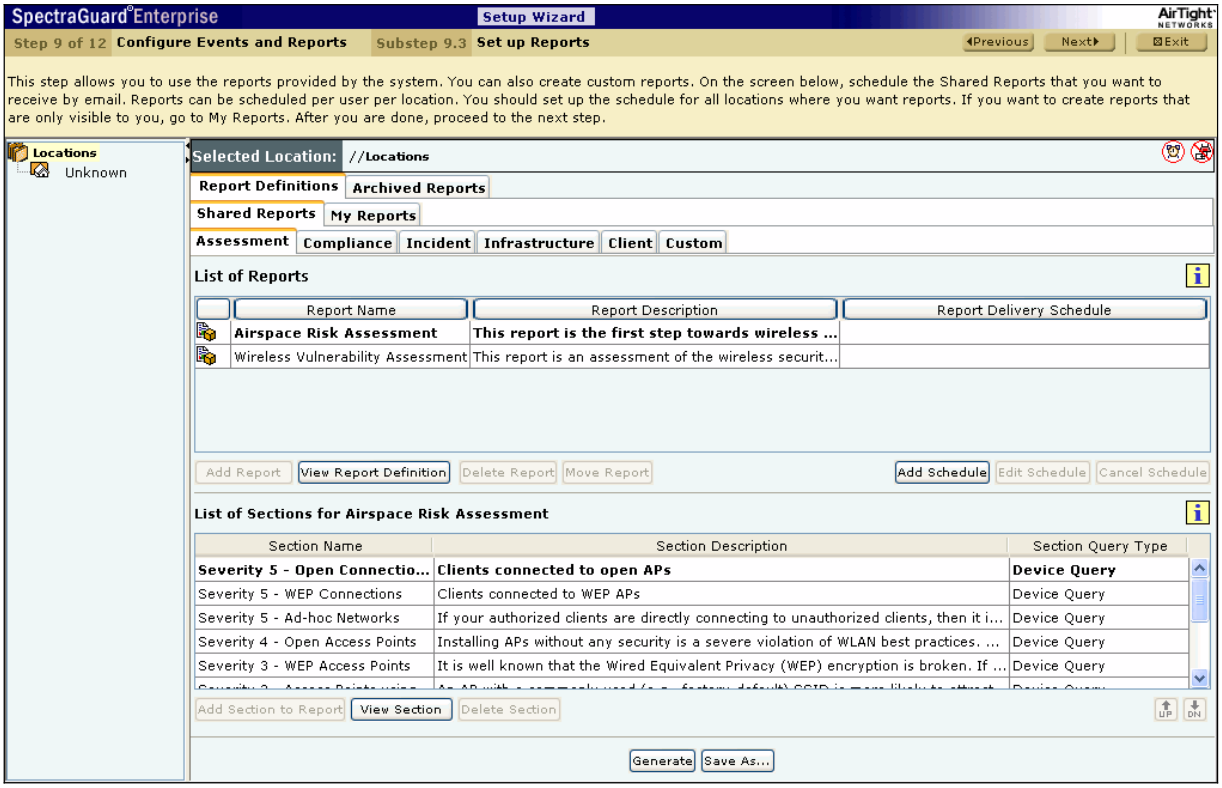


Figure 107. Reports Screen

7.1.9.3 Adding a Report

The system enables you to define customized reports so that you can view precise details that you require. Use the following steps to add a report:

a. Select the tab **My Reports**.

b. Under **List of Reports**, click <**Add Report**>.

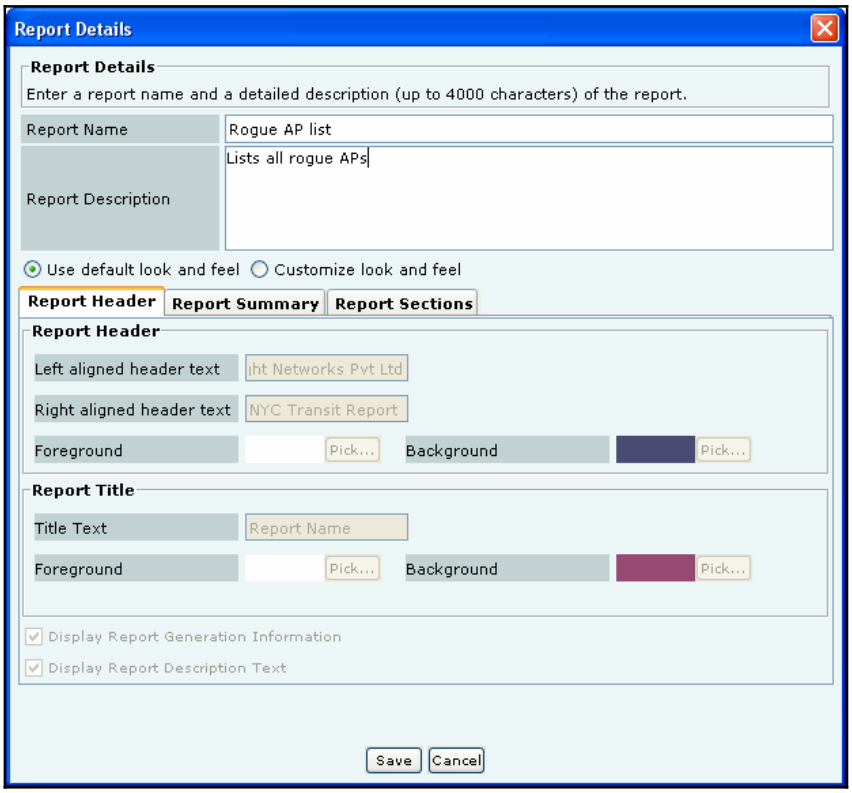


Figure 108. Report Details Screen

c. On the **Report Details** dialog, under **Report Name**, enter a unique, user-friendly name for the report.
d. Under **Report Description**, enter brief notes to help identify the report.
e. Click **Use default look and feel**, to retain the default text, title, and colors for the reports.
f. Alternatively, click **Customize look and feel**, to customize the appearance of the report.
g. Select the **Report Header** tab.
   - Under **Report Header**, specify the following parameters to be customized in the generated report:
     - **Title Text:** Specify the text that should appear in the header on the left side.
     - **Text on Right:** Specify the text that should appear in the header on the right side.
     - Click <**Pick…**> and select the **Foreground** and **Background** colors for the Report Header.
   - Under **Report Title**, specify the following parameters to be customized in the generated report:
     - **Title Text:** Specify a title that appears below the header on the left side. The Report Description follows this title.
     - Click <**Pick…**> and select the **Foreground** and **Background** colors for the Report Title.
   - Select the checkbox, **Display Report Generation Information** to view the following information below the Report Title
     - Duration for which the report is generated
     - Location for which the report is generated
     - User who generated the report
     - Date and time when the report is generated
   - Select the checkbox, **Display Report Description Text** to view a detailed description of the report.
h. Select the **Report Summary** tab.

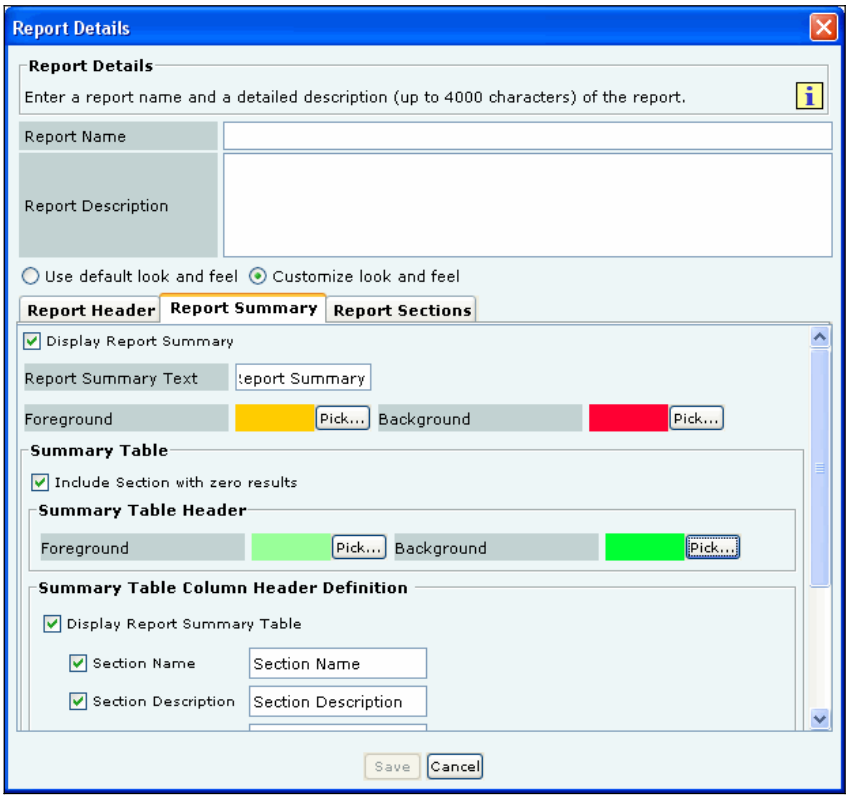


Figure 109. Report Details Screen showing Report Summary Tab

- De-select the checkbox, **Display Report Summary** if you do not wish to view the Report Summary in a tabular form.
- Alternatively, select the checkbox, **Display Report Summary** to customize parameters in the Report Summary table in the generated report.
  - Specify the **Report Summary Text** that should appear as the Report Summary table heading.
  - Click <**Pick…**> and select the **Foreground** and **Background** colors for the Report Summary table heading.
- Under **Summary Table**, select the checkbox, **Include Section with zero results** to view sections in which the result count is zero.
- Under **Summary Table Header**, click <**Pick…**>, select the **Foreground**, and **Background** colors for the Report Summary table row header.
- Under **Summary Table Column Header Definition**, select the checkbox, **Display Report Summary Table** to customize the following column names in the Report Summary table in the generated report.
  - Section Name
  - Section Description
  - Query Type
  - Result Count
  - Jump to
- Under **Summary Charts**, select a radio button to view the charts in the desired format.

i. Select the **Report Sections** tab.

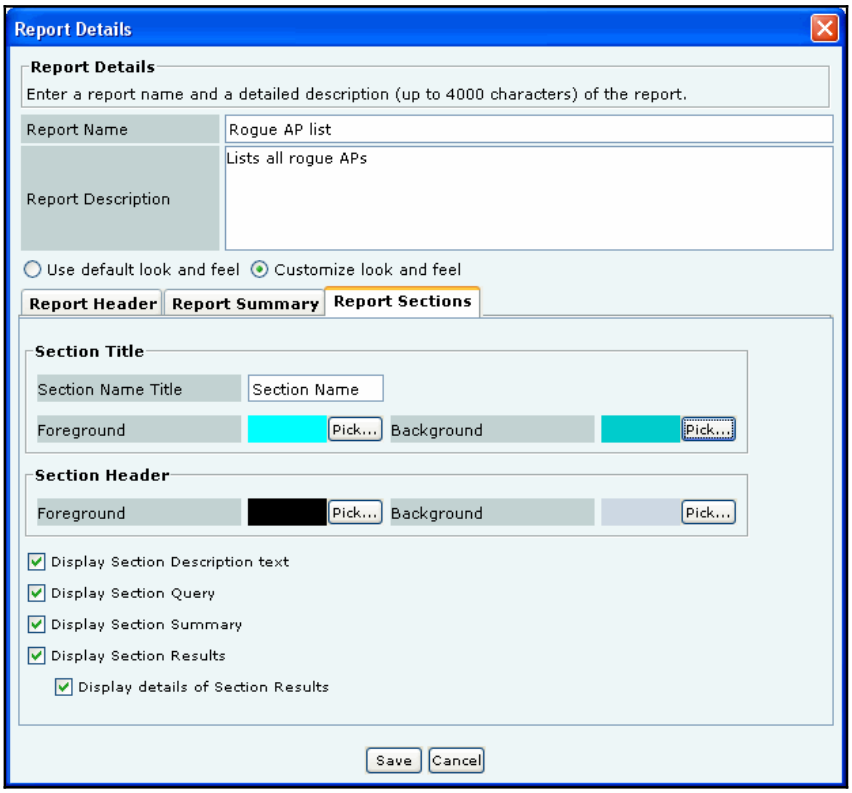


Figure 110. Report Details Screen showing Report Sections Tab

- Under **Section Title**, specify the following parameters to be customized in the generated report:
  - **Section Name Title:** Specify the text that should appear as a common heading for all the Section Names.
  - Click <**Pick…**> and select the **Foreground** and **Background** colors for the Section Name Title.
- Under **Section Header**, specify the following parameters to be customized in the generated report:
  - Click <**Pick…**>, select the **Foreground**, and **Background** colors for the table row headers in the Section Summary and Section Results sections.
  - Select **Display Section Description** text to view a brief description for each section of the report.
  - Select **Display Section Query** to view all the constraints specified in the database query for that section.
  - Select **Display Section Summary** to view a graphical and tabular at-a-glance view of the results of the section.
  - Select **Display Section Results** to view all the entries in the database that satisfy the constraints specified by the section query.
    - Select **Display details of Section Results** to view additional details for each entry in the **Section Results** table.

j. To add the report to the **List of Reports**, click <**Save**>. The new report appears under the **List of Reports** table.

7.1.9.4 Adding a Section to a Report

A report consists of one or more sections. Each section is a query to the database. The system then searches its database for those records that satisfy the conditions that you impose. Use the following steps to add a section to a report:

a. From the **List of Reports** table, select the report to which you need to add a section.

b. Click <**Add Section to Report**>.

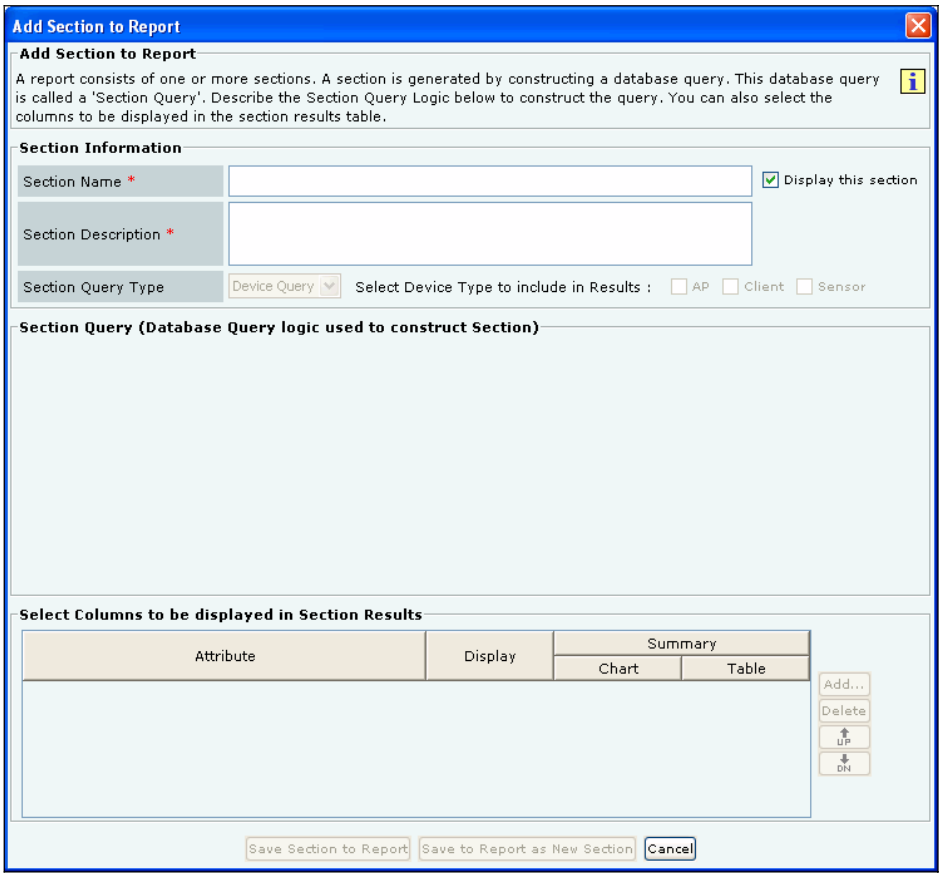


Figure 111. Adding a Section to a Report

c. On the **Add Section to Report** dialog, enter a **Section Name** and a **Section Description** for the newly added section.
d. Select the checkbox **Display this section** to view this section in the generated report.
e. Under **Section Query Type**, select **Device**, **Event**, or **SAFE** as the query type.
f. Select any combination of the **AP**, **Client**, and **Sensor** checkboxes to include these device types in the report. These checkboxes are not available for a **SAFE** query.
g. Describe the **Section Query** construction logic by selecting the following:
   - A column from **Select Column**
   - A condition from **Select Condition**
   - An object for the query, which you can select or enter
h. Optionally, select one or more Boolean connectors (**OR** or **AND**) to join two or more queries. Click <**Delete**> to delete a query.
i. Under **Select Columns to be displayed in Section Results**, do the following.
   - Click <**Add**> to view a list of attributes and select an attribute.
   - Select the checkbox **Display** to view the selected attribute in the generated report.
   - Under **Summary**, you can choose to do the following:
     - Select the type of chart from the drop-down list to view a graph for the selected attribute.
     - Select the checkbox **Table** to view a tabulated count for the selected attribute.

Note: *Pie charts are not visible in an HTML report. You can view pie charts only in a PDF report.*

   - Select an attribute and click <**Delete**> to delete that attribute.
   - Select an attribute and click <**Up**> or <**Down**> to organize the attributes that appear as columns in the **Section Results** table of the generated report.

j. To save the section to an existing report, click <**Save Section to Report**>. To save the section with a new name, click <**Save to Report as New Section**>.

7.1.9.5 Creating a Report Schedule

Use the following steps to schedule email delivery of a report:

a. From the **List of Reports** table, select the report that you want to schedule.

b. Click <**Add Schedule**>. The **Generation and Delivery Options for Selected Location** dialog appears.

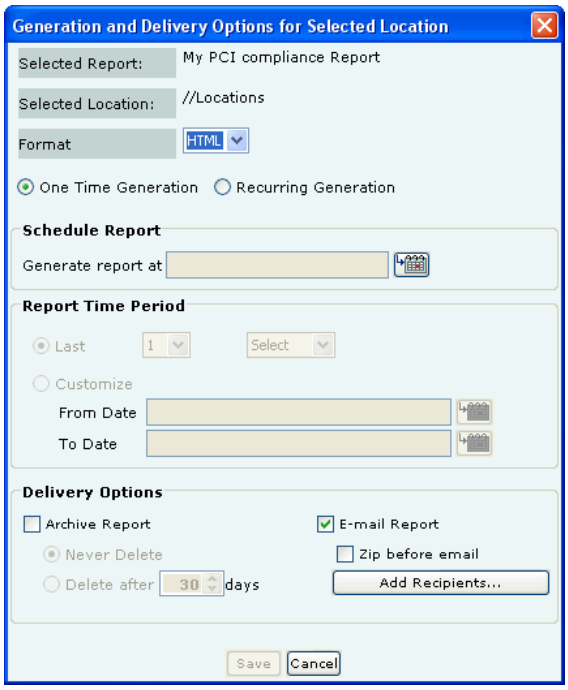


Figure 112. Scheduling a Report for One Time Delivery

c. From the **Format** drop-down list, select the output type for the report, that is, HTML, XML, or PDF.

***Note**: The system does not support PDF report generation on older versions of IE (versions lower than 7.0).*

d. Select either **One Time Generation** or **Recurring Generation**.

- To schedule a report for **One Time Generation**, perform the following:
  - Under **Schedule Report**, click the calendar icon to specify the date and the time on which to generate the report.
  - Under **Report Time Period**, customize the duration for which the report should be generated by doing either of the following:
    - Select **Last** and then the number of hours, days, or months before the report delivery time.
    - Select **Customize** and then the exact date and time in **From Date** and **To Date** fields.

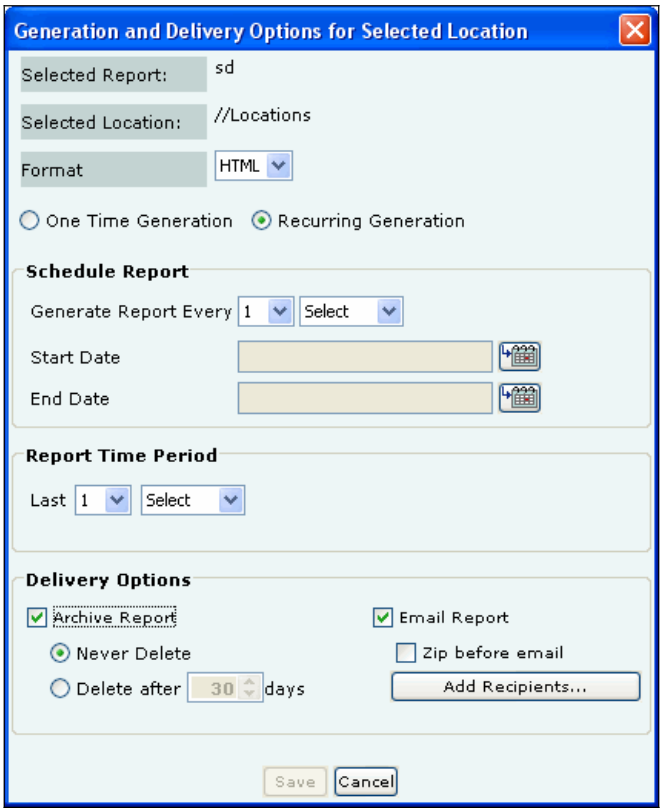


Figure 113. Scheduling a Report for Recurring Generation

- To schedule a report for **Recurring Generation**, perform the following:
  - Under **Schedule Report**, from the **Generate Report Every** drop-down list, select the number of hours, days, or months over which to deliver the report.
  - Click the calendar icon next to **Start Date** to select the start date and time for the report.
  - Click the calendar icon next to **End Date** to select the end date and time for the report. The **End Date** must be greater than the **Start Date**. The system automatically selects the **End Date** and **Time** from the **Start Date**.
  - Under **Report Time Period**, customize the duration for which the report should be generated by selecting **Last** and then the number of hours, days, or months before the report delivery time.

e. Under **Delivery Options**, perform the following:
- Select **Archive Report** and then choose the following:
  - **Never Delete** to retain the report forever
  - **Delete after 'n' days** to delete the report after the specified number of days
- Select **Email Report** to email a copy of the report to the selected user(s).
  - Select **Zip before email** to compress the report before emailing it.

f. Click <**Add Recipients**> to open **Report Delivery** dialog. Here, you can do the following:
- Select one or more email addresses under **System Users** and then click→ to move the chosen email address(s) to **Recipients**. The system delivers scheduled reports to the users under **Recipients**.
- Click <**Add**> to open **Additional Email Addresses** dialog where you can specify a custom email address for a non-system user who will receive a scheduled report. In this dialog, you can add multiple email addresses one at a time.

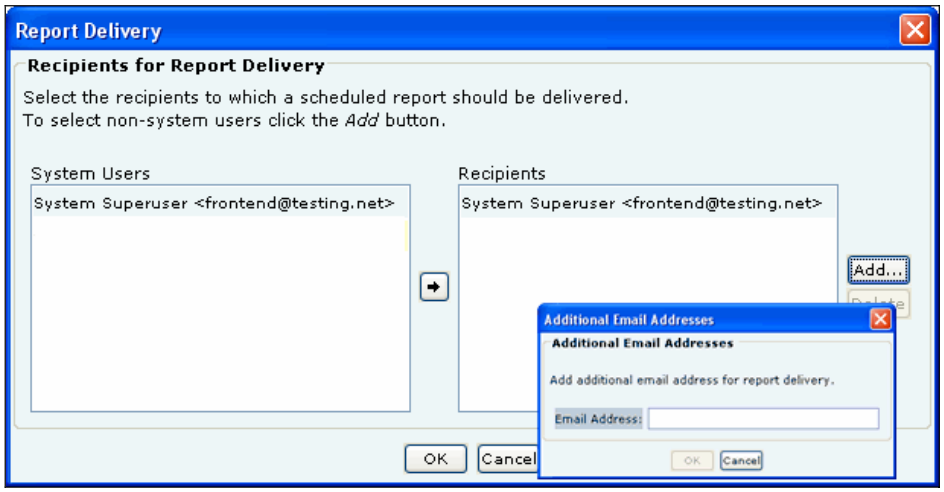


Figure 114. Specifying Additional Email Addresses for Report Delivery

g. Click <**OK**> to close the **Additional Email Addresses** dialog.
h. Click <**OK**> to close the **Report Delivery** dialog.
i. To schedule the report, click <**Save**>.

7.1.10 Step 10: Calibrating Location Tracking

29. The **Locations** screen appears as shown in the following figure. Calibrate your system for accurate location tracking.

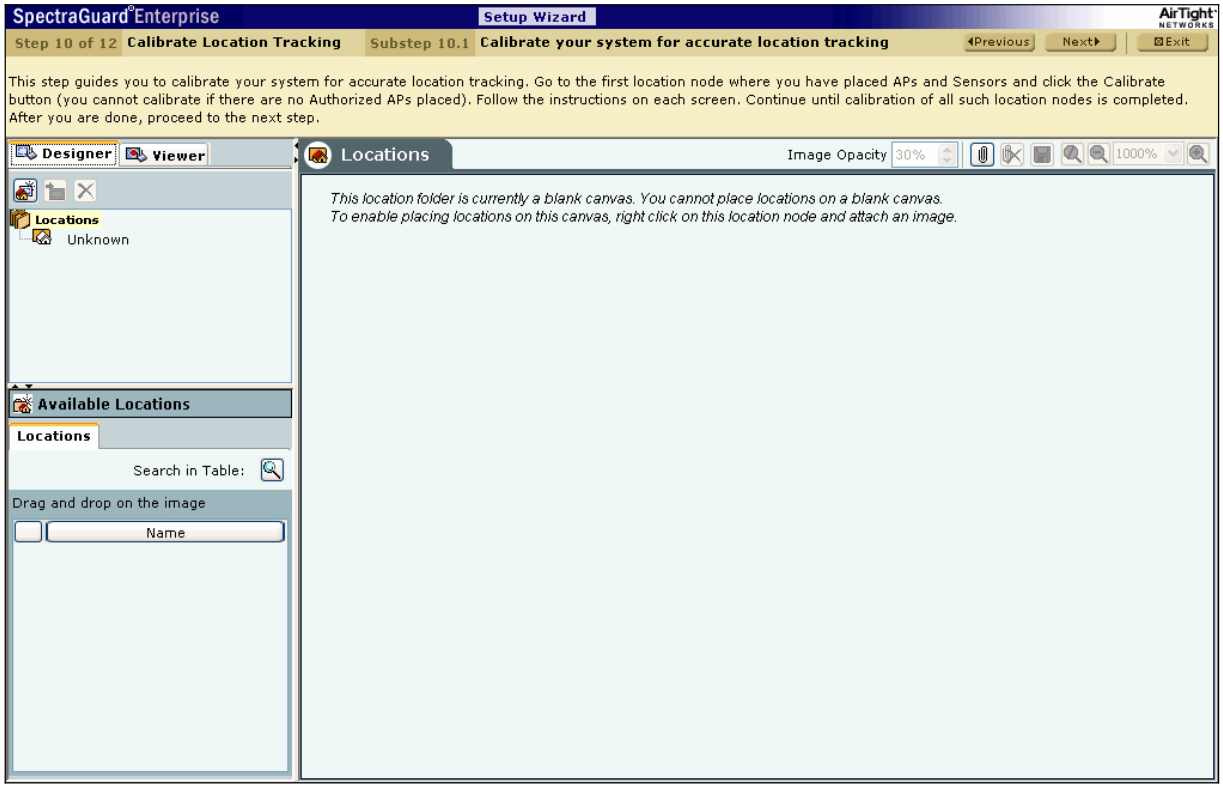


Figure 115. Locations Screen – Calibration

Calibration helps in tuning RF parameters used by the system to compare the AP and Sensor predictions to actual observations. The system has a robust calibration technique that also allows manual intervention in case of discrepancy. Use the following steps to calibrate RF views:

a. Place devices on the floormap.
b. Select the **Viewer** tab.
c. Select one of the AP or Sensor views.
d. Generate the desired RF Coverage map by clicking <**Calibration**>.
e. To improve predictions, fine-tune the **Min. Signal Decay Constant** and the **Max. Signal Decay Constant**.

***Note**: **Min. Signal Decay Constant** specifies the amount of signal loss that is acceptable for regions close to the transmitter (Sensor). **Max. Signal Decay Constant** specifies the amount of signal loss that is acceptable for regions away from the transmitter. Signal loss is directly proportional to the signal decay constants.*

---

f. Change the values of the **Signal Decay Slope (Beta)** and the **Signal Decay Inflection (Alpha)**. The system uses these parameters when computing the RF and defines the region around the transmitter that is unobstructed.

***Note**: When you change the values of **Min. Signal Decay Constant**, **Max. Signal Decay Constant**, **Signal Decay Slope (Beta)**, and **Signal Decay Inflection (Alpha)** the RF view and Location Tracking for unobstructed regions is affected. In the obstructed regions, only Location Tracking is affected, RF view is not affected.*

---

g. Click <**Update Graph**> to view your selection against the predicted values.

***Important**: The **Predicted value** curve should overlap the **Observed value** curve as much as possible.*

---

h. Click <**Calibrate**> to complete calibration if you have adjusted the parameters manually such that the two curves are parallel (but not coinciding).
i. Click <**Apply**> to commit your changes.

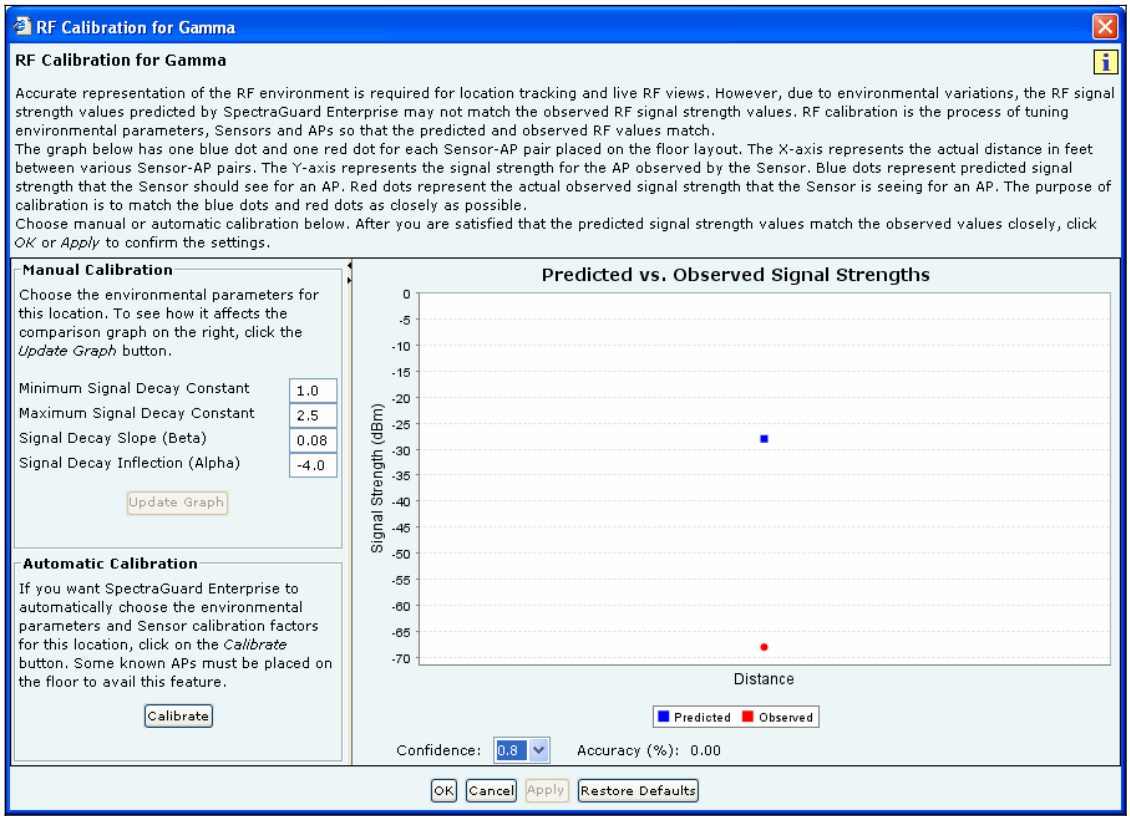


Figure 116. RF Calibration Dialog

7.1.11 Step 11: Locking the System Configuration

30. The **Event Activation** screen appears as shown in the following figure. If the system configuration is not confirmed, you need to go back to the previous steps and complete any additional configuration. Otherwise, in this step, you can turn on events. The system will become completely operational after activating intrusion prevention.

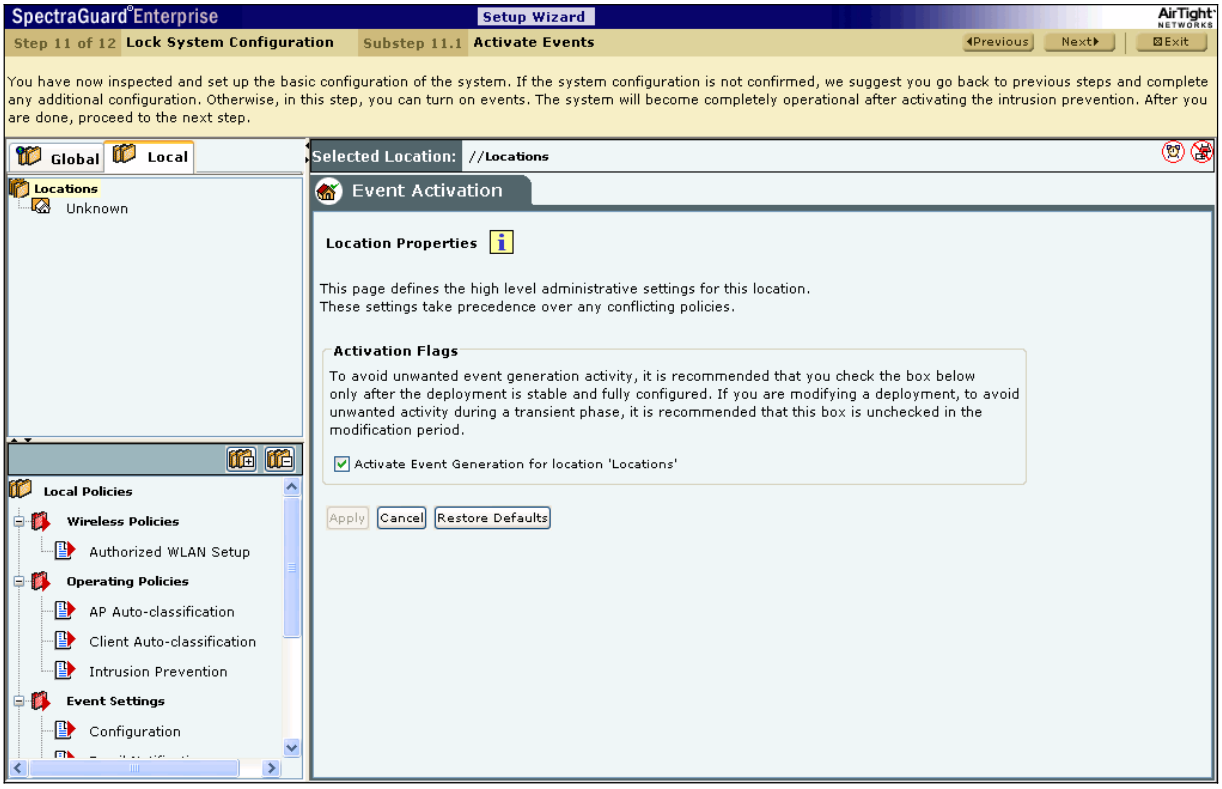


Figure 117. Event Activation

31. The **Intrusion Prevention Activation** screen appears as shown in the following figure. If the system configuration is not confirmed, you need to go back to the previous steps and complete any additional configuration. Otherwise, in this step, you can turn on intrusion prevention. This makes the system operational.

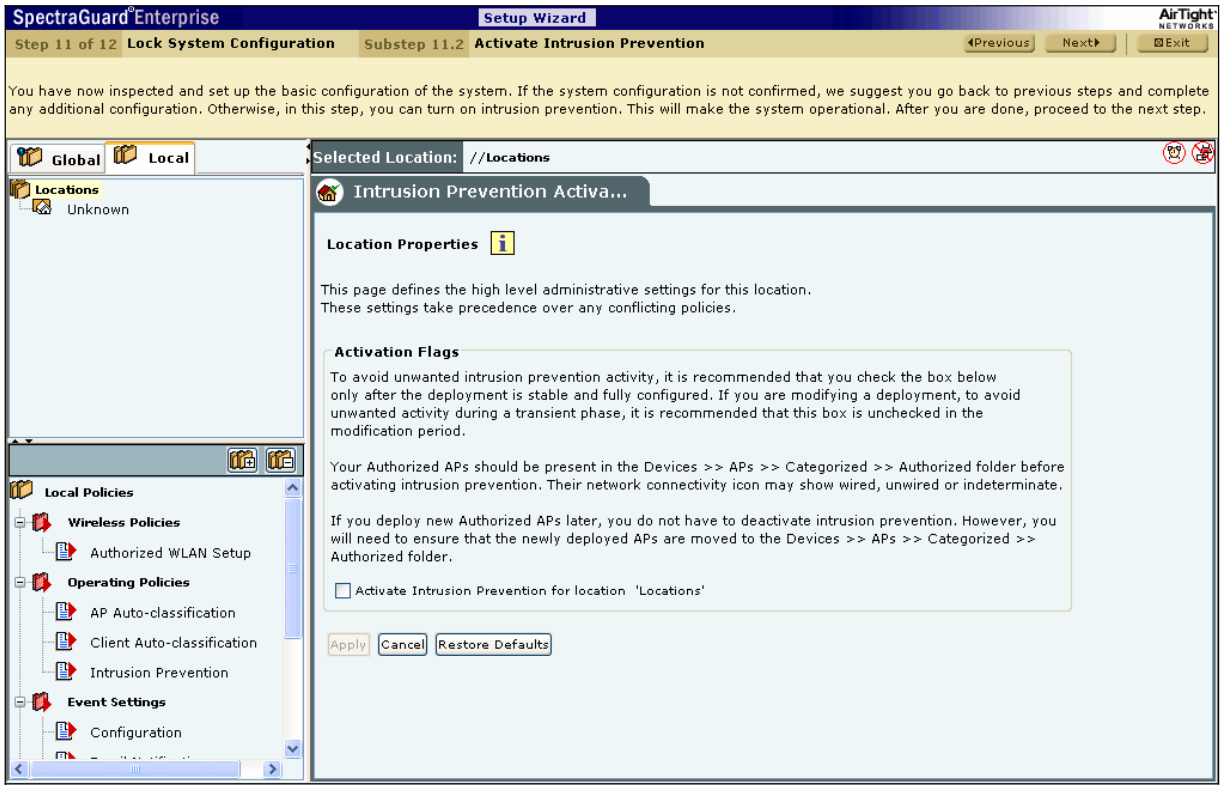


Figure 118. Intrusion Prevention Activation

32. The **Device List Locking** screen appears as shown in the following figure. If you had previously unlocked the list of Authorized APs and Clients at a location by de-checking the two checkboxes **Lock AP List for location '<selected location'>** and **Lock Client List for location '<selected location'>**, you may lock the lists for all locations where you do not expect more authorized APs or Clients to be added. AirTight recommends that you lock the AP list. If your Clients are authorized automatically, do not lock the Client lists. Any new device added after the list is locked has to be manually moved to the **Authorized** category.

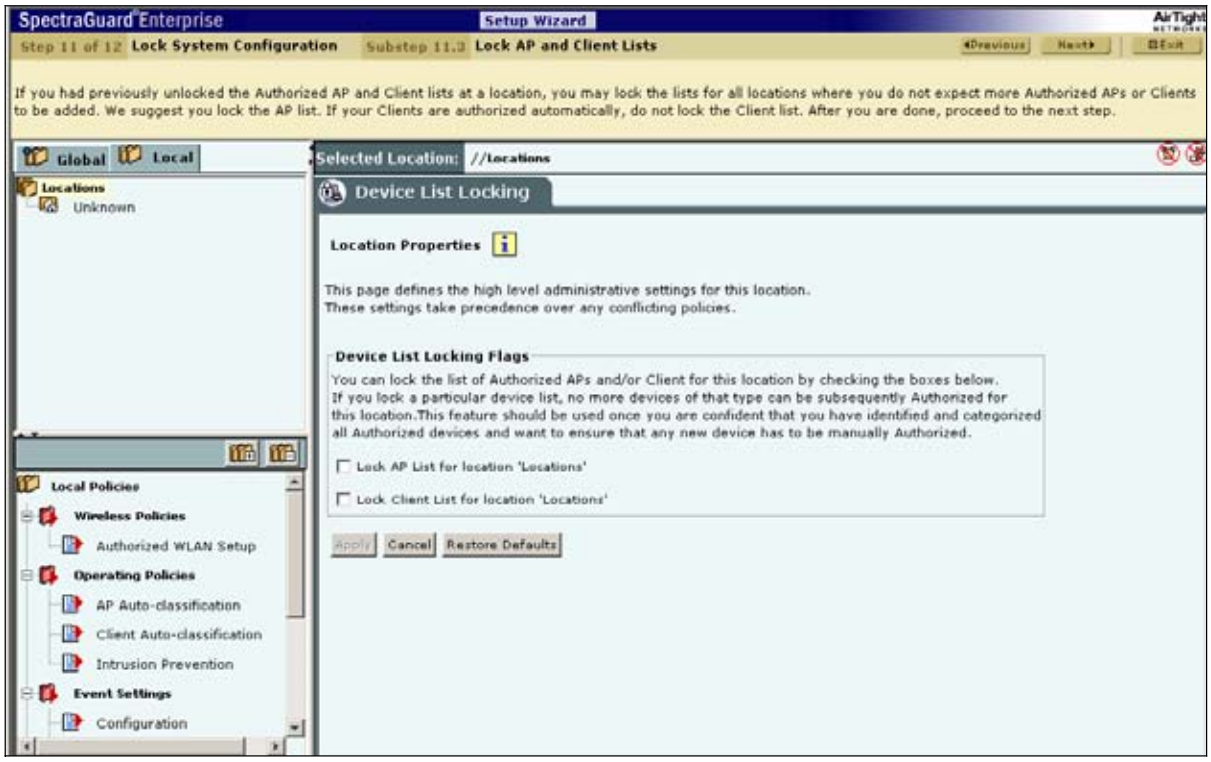


Figure 119. Device List Locking

7.1.12 Step 12: Completion of Setup Wizard

33. This marks the completion of the setup wizard. The **Dashboard** screen appears as shown in the following figure. The Server is configured to protect your network against wireless threats.

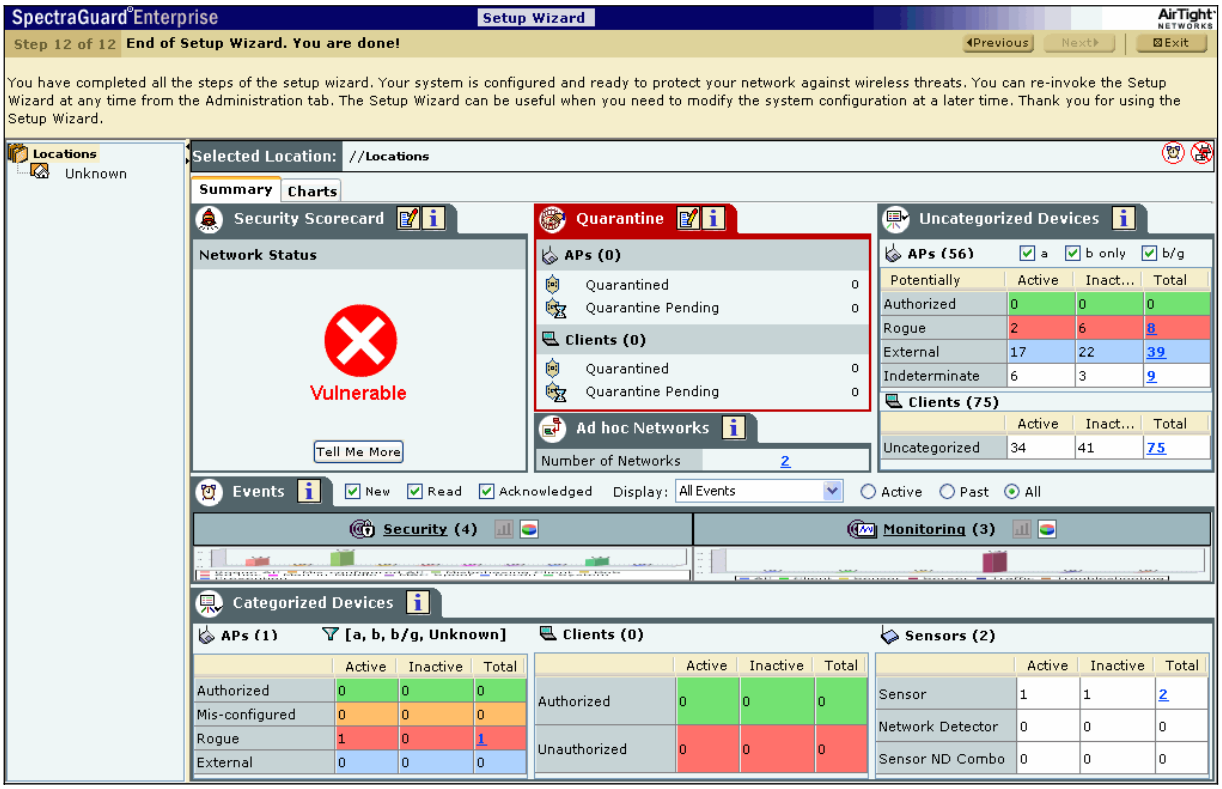


Figure 120. Dashboard Screen

Chapter 8 Config Shell Commands

8.1 Server Config Shell Commands

This chapter describes the commands in the Server Config Shell used to reconfigure or maintain the Server after running the Server Configuration Wizard. Some commands display the status of the Server.

Database Commands	
Command	**Description**
db backup	Backs up the database to the Remote Server specified by you
db clean	Resource clean-up without disruption of services
db maintain	Resource clean-up after temporary shutting down of services
db reset	Resets the database to factory defaults but maintains network settings
db restore	Restores the database from a previous backup on a Remote Server

get Commands	
Command	**Description**
get allowed ip	Displays the list of IP addresses or subnets that are allowed to access this device
get cert	Generates a self-signed certificate
get certreq	Generates a Certificate Signing Request (CSR)
get date	Displays the current time zone, date, and time on the Server
get debug	Creates a debug information 'tarball' file; this file can be used for debugging purposes
get ha	Displays High Availability (HA) Cluster configuration and service status
get ha help	Displays detailed High Availability (HA) setup help
get interface	Displays the Network and HA Interface speed and mode
get locationinfo	Extracts information about location hierarchy, imported images, and signal strength for all devices seen by Sensor
get log config	Displays the configuration of the logger
get monitoring	Displays the number of days that the system should keep the data for all performance monitoring charts
get network	Displays the Network Interface (eth0) configuration including the IP Address, Subnet mask, Gateway, DNS Address, and DNS Prefix
get opsec log	Displays the log messages generated by OPSEC API
get route	Displays the routing table

get sensor list	Displays a list of Sensors and NDs
get server config	Displays the complete Server configuration which includes the Server ID, Server Version, Server Build, MAC address of the Network and HA Interface, Server Mode, Server Time Zone, Date and Time Settings, WLSE Integration Settings, Settings of Network Interfaces, and Server Processes
get server check	Runs a Server consistency check and display the results. If any fatal item fails, a failure result is recorded
get serverid	Displays the Server ID
get ssh	Displays the status of the SSH Server
get status	Displays the status of Server processes
get support	Displays settings that control how, when, where, and what support information is to be sent
get version	Displays the version and build information of all the Server components

set Commands	
Command	**Description**
set allowed ip	Sets the list of IP addresses or subnets that are allowed to access this device
set cert	Installs a signed SSL certificate issued for the request generated using 'get certreq'
set date	Sets the current time zone, date, and time information on the Server; the Server needs to be rebooted for the date/time information to take effect
set dbserver	Starts/Stops the Database Server
set erase	Configures the backspace key
set ha	Enables or disables High Availability (HA) service
set interface	Sets the Network and HA Interface speed and mode
set log config	Sets the configuration of the logger
set monitoring	Sets the number of days that the system should keep the data for all performance monitoring charts
set network	Sets the Network Interface (eth0) configuration including the IP Address, Subnet mask, Gateway, DNS Address, and DNS Prefix
set route	Allows addition/deletion of routing table entries
set server	Starts/Stops the Application Server
set serverid	Sets the Server ID
set ssh	Starts/Stops the SSH access to the Server
set support	Sets up how, when, where, and what support information is to be sent
set webserver	Starts/Stops the Web Server

Other Commands	
Command	**Description**
exit	Exits the config shell session
help	Displays help for all the commands
passwd	Allows the admin to change the config shell password
ping<Hostname/IP Address>	Pings a host
reboot	Reboots the Server
reset factory	Resets the Server to the factory defaults/out of the box status
reset password gui	Sets the Graphical User Interface (GUI) password for the user 'admin' to the factory default 'admin'
shutdown	Shuts down the Server gracefully
traceroute	Shows the route to a host
upgrade	Upgrades the Server using the specified upgrade bundle from an HTTP location

8.2 Sensor Config Shell Commands

get Commands	
Command	**Description**
get ap	Displays all the currently visible APs
get interface	Displays Network Interface speed and mode
get ip config	Displays the IP information
get log	Displays the log information as it is created
get log config	Displays the configuration of the logger
get mode	Displays the mode in which the Sensor is currently configured
get rf	Displays if RF monitoring for a Sensor is 'ON' or 'OFF'
get serial num	Displays the Board Number
get server discovery	Displays the Server discovery/setting information
get status	Displays the current running status of all the components
get version	Displays the version and build information of all the components
get vlan config	Displays the VLAN information (set info and dynamic info)
get vlan id	Displays the VLAN IDs seen by the ND
get vlan status	Displays the VLAN status information
get model	Displays the Sensor Model

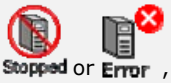
set Commands	
Command	**Description**
set erase	Sets the erase character to ^H
set interface	Sets Network Interface speed and mode
set ip config	Runs through the current VLAN and IP config wizard
set server discovery	Sets the Server discovery information
set vlan config	Sets multiple VLAN monitoring to 'ON' or 'OFF'
set mode	Sets the mode to Sensor, Sensor/ Network Detector Combo, Network Detector, or Sentry

Other Commands	
Command	**Description**
exit	Exists the Sensor config Shell session
help	Displays help for all commands
help set	Displays help for 'set' commands
help get	Displays help for 'get' commands
help other	Displays help for 'other' commands
passwd	Changes the config Shell password
ping	Pings a host. Usage: ping <IP_address/host_name> e.g. ping 192.168.1.246
reboot	Reboots the Sensor
restart	Restarts the Sensor application
reset factory	Resets the Sensor to 'out of the box' status
upgrade	Upgrades the Sensor manually from a given IP address

Chapter 9 Troubleshooting

9.1 Server Troubleshooting

Problem	Solution
After changing the IP address of the Server, the computer used to configure the Server gets disconnected.	The subnet mask of the computer used to configure the Server may not be the same as that of the Server. Change the subnet mask of the computer so that it is in the same subnet as the Server.
On typing 'https:// wifi-security-server' in the IE 5.5 browser, the 'Login' screen does not appear even after adding a DNS entry 'wifi-security-server' for the Server.	The Default gateway and Preferred DNS Server settings of the computer used to access the Server Console may be incorrect. Ensure that the Default gateway and Preferred DNS Server settings of the computer used to access the Server Console match the Server settings.
On rebooting the Server, the get network command does not show an IP address.	The IP address that you have assigned to the Server conflicts with some other IP address on the network. Change the IP address of the Server using the set network command.
No Sensors connect to the Server after setting the Server ID.	The Server ID used by the Server may be used by another Server on the network. Verify that no other Server with the Server ID set for the Server is running on the network. Change the Server ID using the set serverid command.
No connection to the Server	Check if the Server is powered on. If the Server is not powered on, switch it on. Else, check the IP Address or the DNS Name on the Server Config Shell. Important: Please ensure that you have used the correct IP Address or the DNS name to connect to the Server. If the IP Address or the DNS name is correct, try pinging other computers on the network from the Server Config Shell interface. If the problem still exits, reset the Server and attempt to reconnect to the Server.
The Console reports "Java Runtime Environment Detection" not installed message.	Follow the instructions provided on the Console to install the Java Runtime Environment.
Unable to log into the Console.	If you are logging in for the first time, refer to the Initializing section for the default Login Name and Password. Try recovering the password using the Recover option in the Forgot Password? section of the Login Screen.
The Console has frozen (Clicks do not work).	Close the browser and try connecting to the Server in another window. If you cannot connect to the Server, follow the steps listed in Problem 1 of this table.

No events are being reported or the device status is stale (not updated).	Check the status of the Server on the Administration screen.  If the Current Status field shows , click the Start Server button in the Server Status section.
No Sensor is connected to the Server.	Check the status of the Server on the Administration screen.  If the Current Status field shows , click the Start Sever button in the Server Status section.  If the Current Status field shows , refer to the Sensors Troubleshooting section for the solution.
Server response time is high.	Restart the Console. If the problem persists, run the db clean command from the Server Config Shell.

9.2 Sensor Troubleshooting

Symptoms	Diagnosis	Solution
LED1: Solid Orange LED2: Fast Blink	The Sensor did not receive a valid IP address via the DHCP.	The DHCP Server is unreachable. Restore the connectivity to the DHCP Server or set a static IP address via the HTTP interface or the Config Shell CLI.
LED1: Solid Orange LED2: Slow Blink	Unable to connect to the Server.	Ensure that the Server is running and is reachable from the network to which the Sensor is attached. If there is a firewall or a router with ACLs enabled between the Sensor and the Server, ensure that the traffic is allowed on UDP port 3851. If utilizing the Server ID based discovery, ensure that multicast is enabled on the network. Alternatively, if utilizing the Server IP based discovery, ensure that the DNS name 'wifi-security-server' has been correctly entered on the DNS Server. Also ensure that the DNS Server IP addresses are either correctly configured on the Sensor, or are provided by the DHCP Server.
LED1: Solid Orange LED2: Solid Green	The Ethernet cable is loose. It is probably disconnected from the network.	Ensure that the Ethernet cable is connected.
LED1: Solid Orange LED3: Solid Green	An error on the 802.11 interface has occurred.	Contact support@airtightnetworks.com for more details.
LED1: Solid Orange LED4: Solid Green	A fatal Software error has occurred.	Contact support@airtightnetworks.com for more details.