Installation Guide

SS-300-AT-C-60

3x3 802.11abgn Access Point/Sensor

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

http://www.airtightnetworks.com

Product documentation is being enhanced continuously based on customer feedback. To obtain a latest copy of this document, visit
http://www.airtightnetworks.com/home/support.html

This page has been intentionally left blank.

SS-300-AT-C-60 Access Point/Sensor

Installation Guide

END USER LICENSE AGREEMENT

Please read the End User License Agreement before installing the SS-300-AT-C-60 Access Point/Sensor. The End User License Agreement is available at the following location -.http://www.airtightnetworks.com/fileadmin/pdf/AirTight-EULA.pdf. Installing the SS-300-AT-C-60 Access Point/Sensor constitutes your acceptance of the terms and conditions of the End User License Agreement.

DISCLAIMER

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.

Copyright © 2012 AirTight® Networks, Inc. All Rights Reserved.

AirTight® Networks, The AirTight logo, and SpectraGuard® are registered trademarks of AirTight® Networks. All other products and services are trademarks, registered trademarks, and service marks or registered service marks of their respective owners.

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, 7,440,434, 7,447,184, 7,496,094, 7,536,723, 7,558,253, 7,710,933, 7,751,393, 7,764,648, 7,804,808, 7,856,209, 7,856,656, 7,970,894, 7,971,253, 8,032,939; Australian patent No. 200429804; U.K. patent No. 2410154; Japan patent No. 4639195, and any others listed at www.airtightnetworks.com/patents. More patents pending.

FEDERAL COMMUNICATIONS 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 or more 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.

CAUTION
Any changes or modifications not expressly approved by the guarantee of this device could void the user's authority to operate the equipment.

Labeling requirements
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.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This device is operation in 5.15 – 5.25GHz frequency range, then restricted in indoor use only, Outdoor operations in the 5150~5250MHz is prohibit.

Canada, Industry Canada (IC) Notices
This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information
The radiated output power of the Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.
This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions. (antennas are greater than 20cm from a person's body).

Canada, avis d'Industry Canada (IC)
Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.
Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

Informations concernant l'exposition aux fréquences radio (RF)
La puissance de sortie émise par l'appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l'appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.
Ce périphérique a également été évalué et démontré conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition à des appareils mobiles (les antennes se situent à moins de 20 cm du corps d'une personne).

FCC NOTICE:
To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.
Only the antennas listed below are allowed to be used with the EUT output power.

Antenna List

No.	Manufacturer	Part No.	Peak Gain	NOTE
1.	JOYMAX	JWX-614XRSXX-361	3dBi for 2.4GHz 5dBi for 5.15~5.25GHz 5dBi for 5.725~5.850GHz	External Antenna (Dipole)
2.	MAG.LAYERS	MSA-3810-2G4C1-A36 MSA-3810-2G4C1-A37 MSA-3810-2G4C1-A38 MSA-3810-2G4C1-B3 MSA-3810-2G4C1-B4	4.14dBi for 2.4GHz 2.64dBi for 5.15~5.25GHz 5.72dBi for 5.725~5.850GHz	Internal Antenna (PIFA)

Table of Contents

CHAPTER 1 GETTING STARTED 1

1.1 BEFORE YOU BEGIN 1
1.2 HOW TO GET MORE INFORMATION 1
1.3 CONTACT INFORMATION 1

CHAPTER 2 PACKAGE CONTENTS 2

CHAPTER 3 SS-300-AT-C-60 OVERVIEW 3

CHAPTER 4 INSTALLING SS-300-AT-C60 7

4.1 ZERO CONFIGURATION OF SS-300-AT-C-60 AS SENSOR 7
4.2 CONNECTING SS-300-AT-C-60 7
4.2.1 Mount SS-300-AT-C-60 7
4.2.1.1 Ceiling Mounting 7
4.2.1.2 Wall or Electrical Box Mounting 9
4.2.2 Prerequisites to connect the device to the network 9
4.2.3 Using SS-300-AT-C-60 with PoE 10
4.2.4 Using SS-300-AT-C-60 with power adapter 10

CHAPTER 5 MANUALLY CONFIGURING THE SS-300-AT-C-60 AS SENSOR 12

5.1 INTRODUCTION 12
5.2 CONFIGURING SENSOR THROUGH CONFIG SHELL 12
5.2.1 Invoke HyperTerminal (or minicom) 12
5.2.1.1 Launching HyperTerminal 12
5.2.1.2 Defining a New HyperTerminal Connection 13
5.2.1.3 Specifying HyperTerminal Connection Details 14
5.2.1.4 Editing Serial Port Settings 14
5.2.2 Log in and Change the Default Password 15
5.2.3 Set Server Discovery 15
5.2.4 Set Sensor Mode 15
5.2.5 Configure Network Settings 16
5.2.5.1 Configure IPv6 settings 16
5.2.5.2 How to configure Communication Key or Passphrase 16

CHAPTER 6 SS-300-AT-C-60 CONFIG SHELL COMMANDS 17

CHAPTER 7 SS-300-AT-C-60 TROUBLESHOOTING 19

CHAPTER 8 APPENDIX A: SERVER SENSOR MUTUAL AUTHENTICATION 21

Table of Figures

FIGURE 1. SS-300-AT-C-60 PACKAGE CONTENTS 2
FIGURE 2. FRONT PANEL OF SS-300-AT-C-60 3
FIGURE 3. REAR PANEL OF SS-300-AT-C-60 5
FIGURE 4. SIDE PANEL OF SS-300-AT-C-60 6
FIGURE 5. ATTACHING THE METAL SLIDER 8
FIGURE 6. CLIPPING THE METAL CEILING-BRACKET 8
FIGURE 7. SLIDING THE MOVABLE SECTION 8
FIGURE 8. FINAL POSITIONING OF THE SENSOR 9
FIGURE 9. HOLES FOR INSERTING SCREWS 9
FIGURE 10. POWER UP AND CONNECT SS-300-AT-C-60 USING POE 10
FIGURE 11. POWER UP SS-300-AT-C-60 10
FIGURE 12. CONNECT SS-300-AT-C-60 TO THE NETWORK 11
FIGURE 13. CONNECTING SS-300-AT-C-60 TO YOUR COMPUTER USING A SERIAL CABLE 12
FIGURE 14. OPENING HYPERTERMINAL 13
FIGURE 15. DEFINE A NEW HYPERTERMINAL CONNECTION FOR SENSOR 13
FIGURE 16. SPECIFY HYPERTERMINAL CONNECTION DETAILS 14
FIGURE 17. EDIT SERIAL PORT SETTINGS FOR SENSOR SS-300-AT-C-60 15
FIGURE 18. SET SERVER DISCOVERY COMMAND 15
FIGURE 19. SET SENSOR MODE COMMAND FOR SS-300-AT-C-60 16

Chapter 1 Getting Started

1.1 Before You Begin

Thank you for purchasing SS-300-AT-C-60 from AirTight® Networks, Inc. The SS-300-AT-C-60 is a 3x3 802.11abgn Access Point / Sensor.

Please read the EULA before installing the SS-300-AT-C-60. Installing the sensor 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 package contents and explains how to mount and configure the SS-300-AT-C60. This guide contains the following chapters:

- **Package Contents:** Lists the components included in the system package.
- **SS-300-AT-C-60 Overview:** Provides an overview of sensor.
- **Installing the device:** Describes how to connect and install SS-300-AT-C-60.
- **Manually Configuring the device:** Describes how to configure SS-300-AT-C-60 through the config shell.
- **Config Shell Commands:** Lists a pre-defined set of commands that allow you to configure and view the status of the sensors.
- **Troubleshooting:** Provides troubleshooting tips while installing the 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 SS-300-AT-C-60 device package. SS-300-AT-C-60 is a 3x3 802.11abgn Access Point / Sensor. It can function either as an AP or as a sensor depending on how it is configured.
Please ensure that the following items are included in the SS-300-AT-C-60 device 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.

The contents of the SS-300-AT-C-60 package are as follows:

- SS-300-AT-C-60
- Mounting Bracket and Accessories

Figure 1. SS-300-AT-C-60 Package Contents

Chapter 3 SS-300-AT-C-60 Overview

This chapter provides an overview of the SS-300-AT-C-60 and describes in detail about the following.

- Front panel of SS-300-AT-C-60
- Rear panel of SS-300-AT-C-60

SS-300-AT-C-60 is a 802.11n access point/sensor device with a Cisco compatible console port. It has five external antenna ports- three at the top and two at the bottom. It is a dual radio device capable of acting as an access point or a sensor. The top three antennas are for radio1 and the bottom two antennas are for radio2.

The front panel of the SS-300-AT-C-60 has LEDs that indicate the working of the device.

Figure 2. Front Panel of SS-300-AT-C-60

***Note**: LED5, that is not visible in the zoomed-in view in the above figure, is not in use. Only LED1, LED2, LED3 and LED4 are in use.*

The following table indicates various device states using the LEDs on the device, when the device is in AP mode.

Table 1. LED details for SS-300-AT-C-60 in AP mode

LED1 or Power	LED2 or WLAN1	LED3 or WLAN2	LED4 or LAN	Description
Solid Green	Any	Any	Solid Green	The AP is receiving power and is working normally. The AP is connected to the Server.
Solid Green	Off	Slow Blink	Slow Blink	The AP upgrade is in progress.
Solid Orange	Any	Any	Solid Green	The AP is unable to get Ethernet link.
Solid Orange	Any	Any	Fast Blink	The AP did not receive a valid IP address via the DHCP.
Solid Orange	Any	Any	Slow Blink	The AP is unable to connect to the Server.
Off	Off	Off	Off	The AP is not powered on or it is in the process of starting up.

WLAN1 and WLAN2 LEDs will blink when there is activity on the respective radios.

The following table indicates various device states using the LEDs on the device, when the device is in sensor mode.

Table 2. LED details for SS-300-AT-C-60 in sensor mode

LED1 or Power	LED2 or WLAN1	LED3 or WLAN2	LED4 or LAN	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	Fast Blink	Solid Green	The Sensor is performing troubleshooting on 802.11a/n.
Solid Green	Solid Green	Slow Blink	Solid Green	The Sensor is performing intrusion prevention on 802.11a/n.
Solid Green	Fast Blink	Solid Green	Solid Green	The Sensor is performing troubleshooting on 802.11b/g/n.
Solid Green	Fast Blink	Fast Blink	Solid Green	The Sensor is performing troubleshooting on 802.11b/g/n and 802.11a/n.
Solid Green	Fast Blink	Slow Blink	Solid Green	The Sensor is performing troubleshooting on 802.11b/g/n and intrusion prevention on 802.11a/n.
Solid Green	Slow Blink	Solid Green	Solid Green	The Sensor is performing intrusion prevention on 802.11b/g/n.
Solid Green	Slow Blink	Fast Blink	Solid Green	The Sensor is performing intrusion prevention on 802.11b/g/n and troubleshooting on 802.11a/n.
Solid Green	Slow Blink	Slow Blink	Solid Green	The Sensor is performing intrusion prevention on 802.11b/g/n and 802.11a/n.
Solid Green	Off	Slow Blink	Slow Blink	The Sensor upgrade is in progress.
Solid Orange	Any	Any	Solid Green	The Sensor is unable to get Ethernet link.
Solid Orange	Any	Any	Fast Blink	The Sensor did not receive a valid IP address via the DHCP.
Solid Orange	Any	Any	Slow Blink	The Sensor is unable to connect to the Server.
Solid Orange	Solid Green	Any	Any	There is an error on 802.11a/b/g/n interfaces.
Solid Orange	Any	Solid Green	Any	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.

The following table indicates various device states using the LEDs on the device, when the device is in AP/sensor combo mode, that is one radio is configured to function as an AP and the other radio is configured to function as a sensor.

Table 3. LED details for SS-300-AT-C-60 in AP/sensor combo mode

LED1 or Power	LED2 or WLAN1	LED3 or WLAN2	LED4 or LAN	Description
Solid Green	Solid Green	Any	Solid Green	The AP-Sensor is receiving power and is working normally. The AP-Sensor is connected to the Server.
Solid Green	Fast Blink	Any	Solid Green	The Sensor is performing Troubleshooting on 802.11a/b/g/n
Solid Green	Slow Blink	Any	Solid Green	The Sensor is performing Prevention on 802.11a/b/g/n
Solid Green	Off	Slow Blink	Slow Blink	The AP upgrade is in progress.
Solid Orange	Any	Any	Solid Green	The AP is unable to get Ethernet link.
Solid Orange	Any	Any	Fast Blink	The AP did not receive a valid IP address via the DHCP.

Solid Orange	Any	Any	Slow Blink	The AP is unable to connect to the Server.
Off	Off	Off	Off	The AP is not powered on or it is in the process of starting up.

WLAN2 LED will blink when there is activity on the AP radio.

Note: *If no channels are specified for monitoring and prevention on the sensor radio, the respective LED will have no activity and it will not glow.*

The rear panel of the SS-300-AT-C-60 has two Ethernet ports -LAN 1 and LAN 2, that enables the device to be connected to the wired LAN through a switch or a hub and provides the power for the device using 802.3af standard.

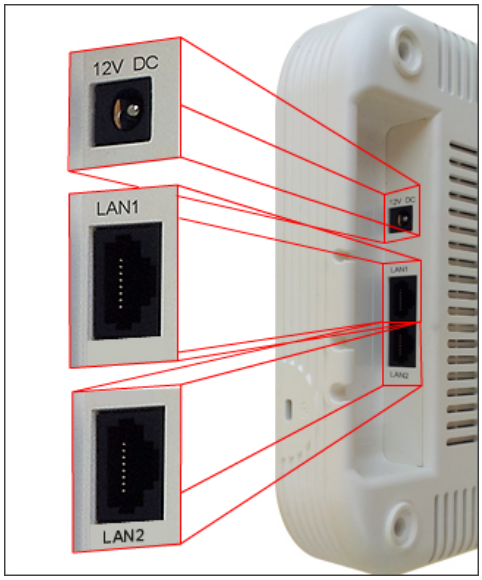

Figure 3. Rear Panel of SS-300-AT-C-60

Table 4. Rear Panel Port Settings for SS-300-AT-C-60

Port	Description	Connector Type	Speed / Protocol
Ethernet (LAN1)	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
Ethernet (LAN2)	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

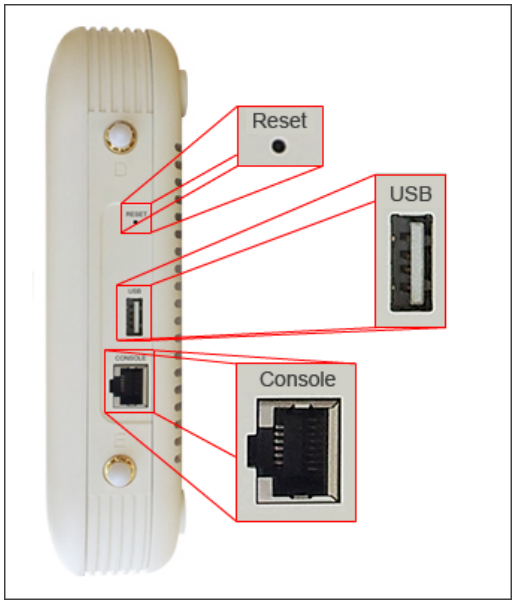

Figure 4. Side Panel of SS-300-AT-C-60

The side panel has the following ports:

- **Serial port:** Connects the SS-300-AT-C-60 device to serial terminal emulation programs such as Hyper Terminal for Windows or minicom for Linux.
- **USB port:** Connects the SS-300-AT-C-60 device to a USB device.
- **Reset switch:** Resets the SS-300-AT-C-60 device to factory defaults. To reset the SS-300-AT-C-60 device, press the **Reset** switch and power cycle (remove the power cable once and connect it back again) the device, until all LEDs blink green. Pressing <**Reset**> while the device 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.
  - Device mode is changed to **Sensor Only**.
  - If **static IP** was configured on the device, the **IP** is **erased** and **DHCP mode** is **set**.

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

Note: *For SS-300-AT-C-60, the user is expected to press and hold the reset switch while a power-cycle for 30 seconds (actually takes 26 seconds for the reset to complete).*

Table 5. Side Panel Port Settings for SS-300-AT-C-60

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
USB	Connects the SS-300-AT-C-60 device to a USB device		
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 SS-300-AT-C60

When the SS-300-AT-C-60 functions as a WIPS sensor, it monitors your network and communicates with the Server to guard your corporate network against over-the-air attacks.

When the SS-300-AT-C-60 functions as an access point(AP), clients can connect to your corporate network in wireless mode through the APs.
The SS-300-AT-C-60 must be plugged to your corporate network to perform the above operations.

As a WIPS sensor, SS-300-AT-C-60 can be configured in one of the following two modes:

- **Sensor Mode:** This is the default mode. 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. Similarly, a SS-300-AT-C-60 can monitor up to 16 VLANs.
- **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. A SS-300-AT-C-60 can monitor upto 100 VLANs.

Important: *To prevent abuse and intrusion by Non-authorized 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.*

4.1 Zero Configuration of SS-300-AT-C-60 as Sensor

Zero configuration is supported if the following conditions are satisfied:

- The device is in 'Sensor' 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 device 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

4.2 Connecting SS-300-AT-C-60

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

4.2.1 Mount SS-300-AT-C-60

Take a configured SS-300-AT-C-60, that is, make sure that the device is given a static IP or the settings have been changed for DHCP. Note the MAC address and the IP address of the device in a safe place before it is installed in a hard-to-reach location. The MAC address of the device is printed on a label at the bottom of the product.

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

4.2.1.1 Ceiling Mounting

Use the mounting bracket to install the SS-300-AT-C-60 on the ceiling.
To mount the device:

1. Attach the metal slider to the back of the device using the two small screws. The slider should still be able to slide after the screws are tightened.

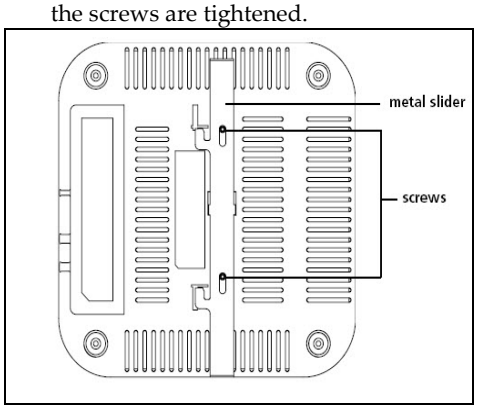

Figure 5. Attaching the Metal Slider

Make sure that the slide is left in the same position as shown above.
Clip the metal ceiling bracket to a suitably-located ceiling tile separator.

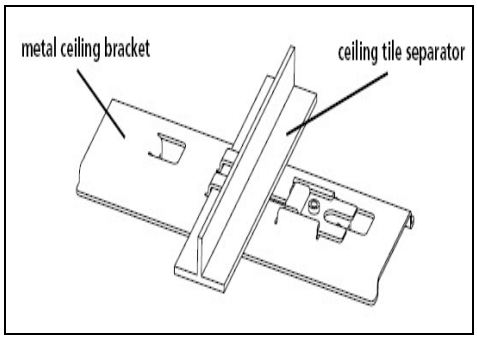

Figure 6. Clipping the Metal Ceiling-bracket

Slide the movable section into place and tighten the screw (found underneath) to secure it

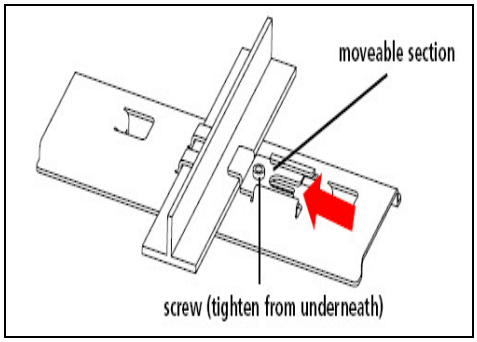

Figure 7. Sliding the movable section

Position the device such that the two tabs from the ceiling bracket locate in the slots in the device (A), then slide the slider across to lock the device to the bracket (B).

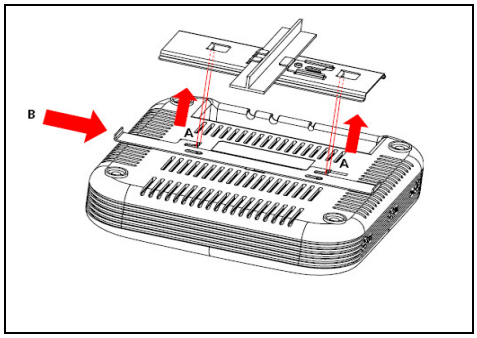

Figure 8. Final positioning of the Sensor

4.2.1.2 Wall or Electrical Box Mounting

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

1. Following these guidelines, screw the mounting bracket to a wall or electrical box (NEMA enclosure):
   - 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.

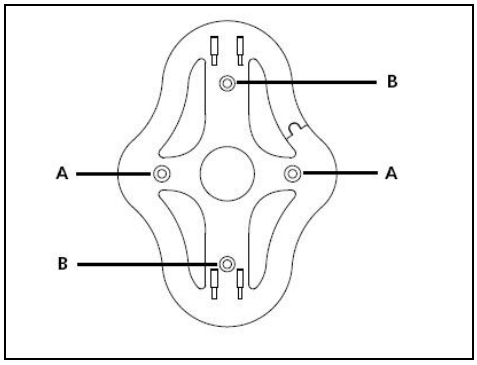

Figure 9. Holes for inserting screws

Connect the Ethernet cable (for power and network connection) to the LAN port on the back of the device.
To mount the SS-300-AT-C-60 device onto the mounting bracket, insert the mounting-bracket tabs into the slots on the back of the AP.

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

A SS-300-AT-C-60 device can be powered on by 802.3af Class 0 Power Over Ethernet of Nominal input voltage 48V DC. You can connect the device to the network using PoE or a power adapter.

4.2.2 Prerequisites to connect the device to the network

1. Ensure that the Server is already running on your network.
2. Add the DNS entry 'wifi-security-server' on all DNS Servers. This entry should point to the IP address of the Server.
3. Ensure that DHCP is running on the subnet to which the device will be connected.

4. ***Important:*** *If DHCP is not enabled on a subnet, Sensors cannot connect to that subnet with zero configuration. If the DNS entry is not present on the DNS servers or you do not have the DHCP server running on the subnet, you need to configure the sensor manually. Refer to Manually Configuring SS-300-AT-C-60 as Sensor for details on manual configuration of Sensor.*

4.2.3 Using SS-300-AT-C-60 with PoE

To power on, and connect SS-300-AT-C-60 to the network using PoE, do the following.

1. Connect one end of the network interface cable to the Ethernet port at the rear of the SS-300-AT-C-60 device.
2. Connect the other end of the network interface cable to the Ethernet jack that provides PoE power.

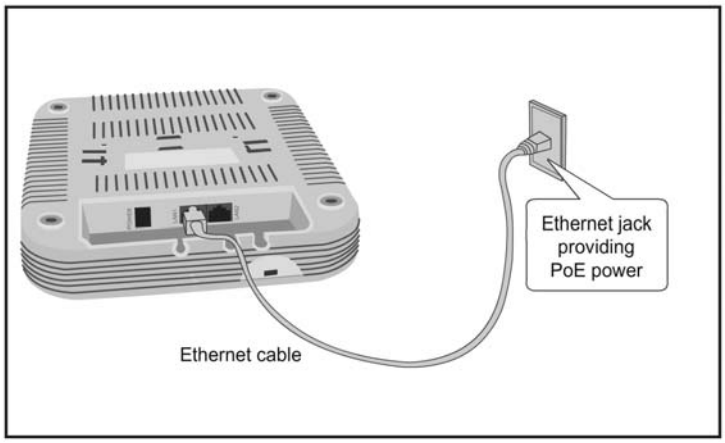

Figure 10. Power up and connect SS-300-AT-C-60 using PoE

4.2.4 Using SS-300-AT-C-60 with power adapter

To power up the device, perform the following steps:

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

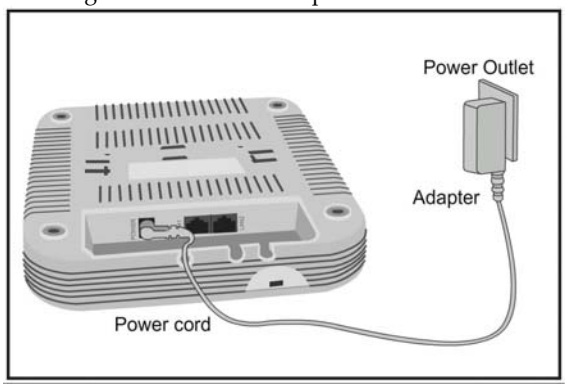

Figure 11. Power up SS-300-AT-C-60

Wait for two minutes!
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.

To connect SS-300-AT-C-60 to the network, perform the following steps:

1. Ensure that DHCP is running on the subnet to which the SS-300-AT-C-60 device will be connected.
2. Connect one end of the Network Interface cable to the Ethernet port (LAN1) at the rear of the SS-300-AT-C-60 device
3. Connect the other end of the Network Interface cable to an Ethernet jack that is connected to the desired subnet.

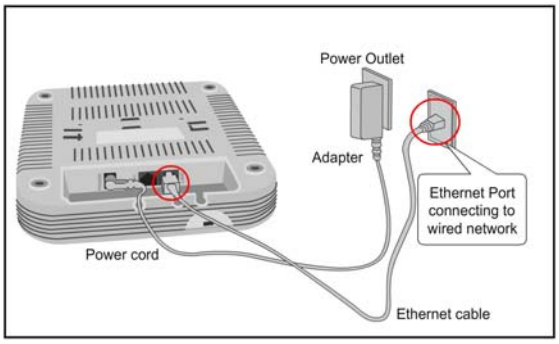

Figure 12. Connect SS-300-AT-C-60 to the network

Wait for two minutes!

Check the Status LEDs on the device. If all LEDs glow green, then the device is operational and connected to the SpectraGuard® Enterprise server.

Log on to the SpectraGuard® Enterprise server through SSH. Run the 'get sensor list' command. You will see a list of all Sensors that are recognized by the SpectraGuard® Enterprise 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 SS-300-AT-C-60 as Sensor for details*

Chapter 5 Manually Configuring the SS-300-AT-C-60 as Sensor

Important: *If the installation in InstallingSS-300-AT-C-60 was successful, stop! You do not need to configure the device manually.*

5.1 Introduction

Manual configuration of SS-300-AT-C-60 as a Sensor is typically required in the following cases:

- Device needs to be configured in ND mode.
- Sensor Only (SO) devices cannot connect to the SpectraGuard® Enterprise server through zero configuration. The DNS entry for the SpectraGuard® Enterprise 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.

5.2 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.

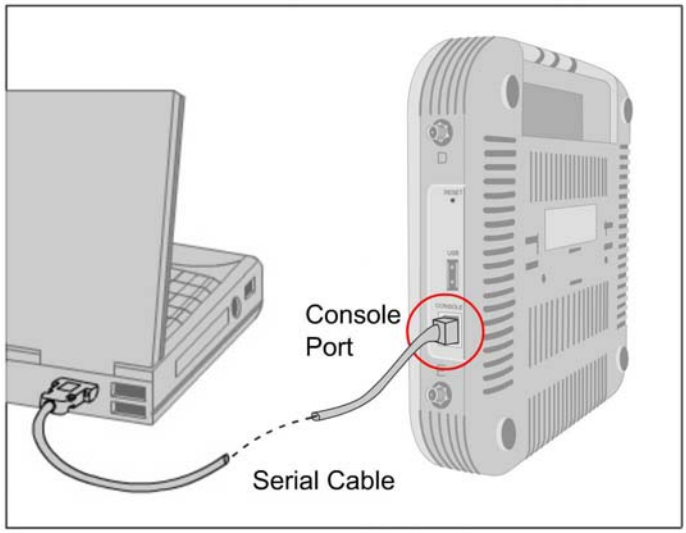

Figure 13. Connecting SS-300-AT-C-60 to your computer using a Serial Cable

The steps to configure the Sensor manually are as follows:

1. Invoke Hyper Terminal (or minicom)

Log in and change the default password
Set Server Discovery
Set Sensor Mode
Set Network Settings for that Sensor Mode

The above steps are explained in detail below.

5.2.1 Invoke HyperTerminal (or minicom)

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

5.2.1.1 Launching HyperTerminal

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

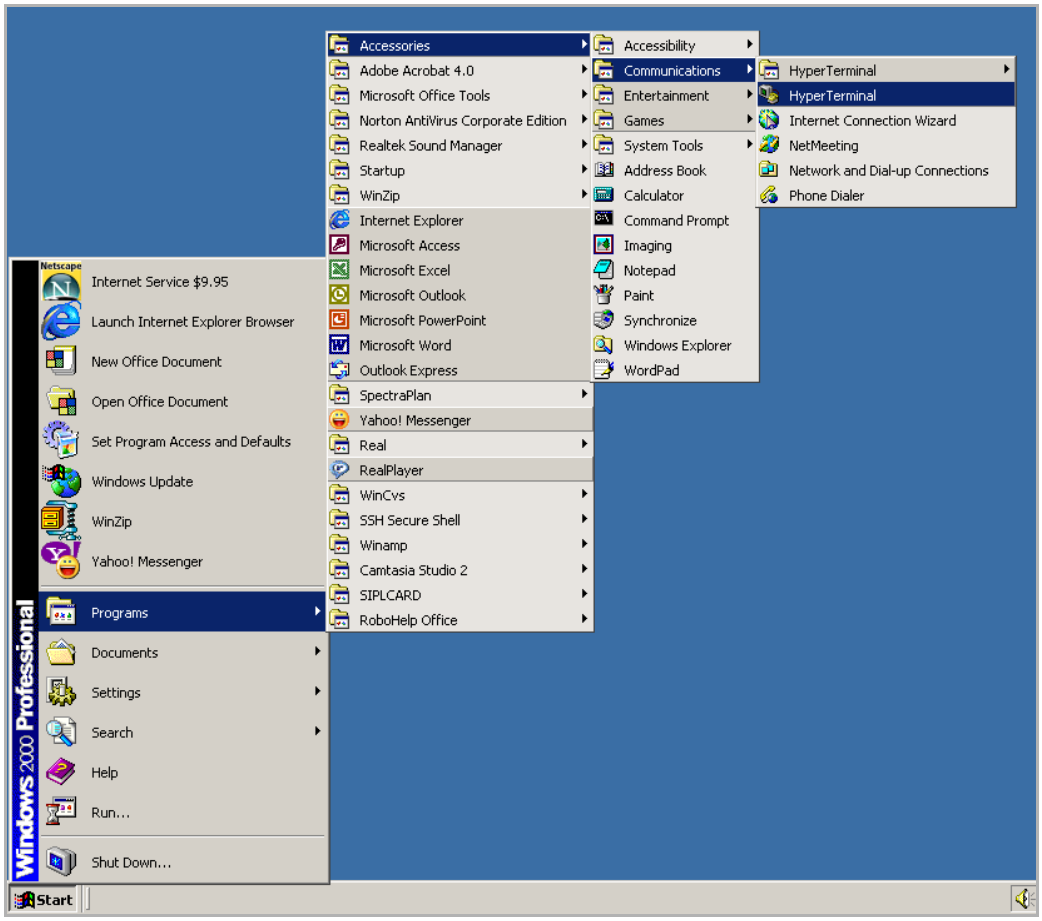

Figure 14. Opening HyperTerminal

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

5.2.1.2 Defining a New HyperTerminal Connection

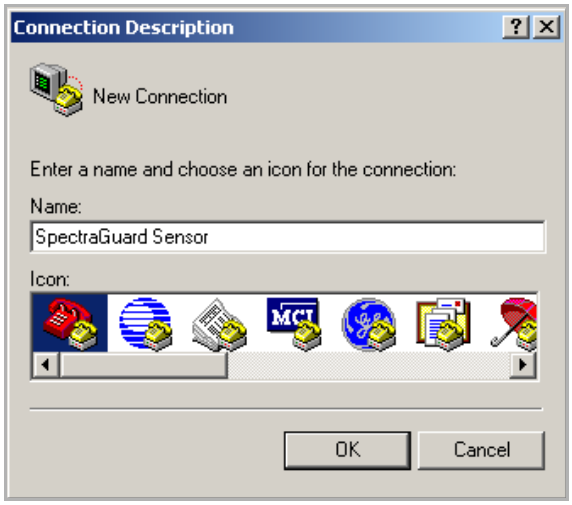

Figure 15. Define a New HyperTerminal Connection for Sensor

- 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.

5.2.1.3 Specifying HyperTerminal Connection Details

Figure 16. 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.*

5.2.1.4 Editing Serial Port Settings

Sensor SS-300-AT-C-60

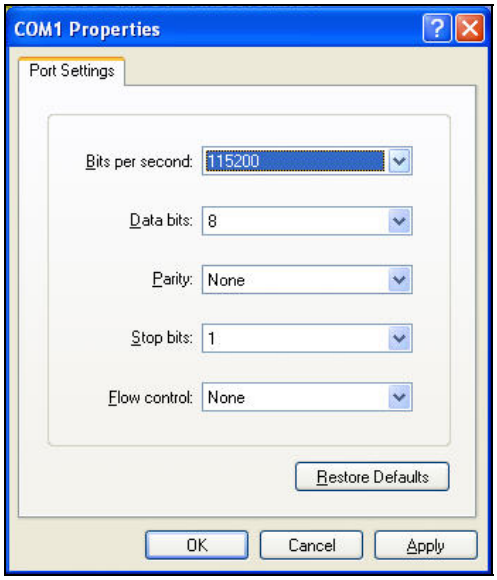

Figure 17. Edit Serial Port Settings for Sensor SS-300-AT-C-60

- Edit the serial port settings as follows or click <**Restore Defaults**> to ensure proper communication between the Sensor and your computer.
  - **Bits per second**: 115200
  - **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.

5.2.2 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.*

5.2.3 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.

```
[config]$ set server discovery
Sets information used by Sensor to connect to the Server.

Settings for Server discovery
Please wait while we retrieve the settings...
Select Server Discovery Settings:
1. Server ID Discovery
2. Server IP/DNS Discovery
3. SLP Discovery
Select Option [2]: 2
Set: Server ID Discovery = [OFF]
Set: Server IP/DNS Discovery = [ON]
Set: SLP Discovery = [OFF]
Primary Server IP/Hostname [192.168.55.141]: 192.168.55.141
Set: Primary Server IP/Hostname = [192.168.55.141]
Secondary Server IP/Hostname [kjkj]: 192.168.55.142
Set: Secondary Server IP/Hostname = [192.168.55.142]

Restarting Sensor...
```

Figure 18. 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.*

5.2.4 Set Sensor Mode

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

- **Sensor Mode:** This is the **default** mode. In this mode, the device **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**. Similarly, an SS-300-AT-C-60 can monitor upto 16 VLANs.
- **ND Mode:** This mode needs to be **explicitly configured**. In this mode, the device **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 SS-300-AT-C-60 functioning as a WIPS sensor can detect and monitor upto 100 VLANs.
- Use the **set mode** command to set the device mode for SS-300-AT-C-60.

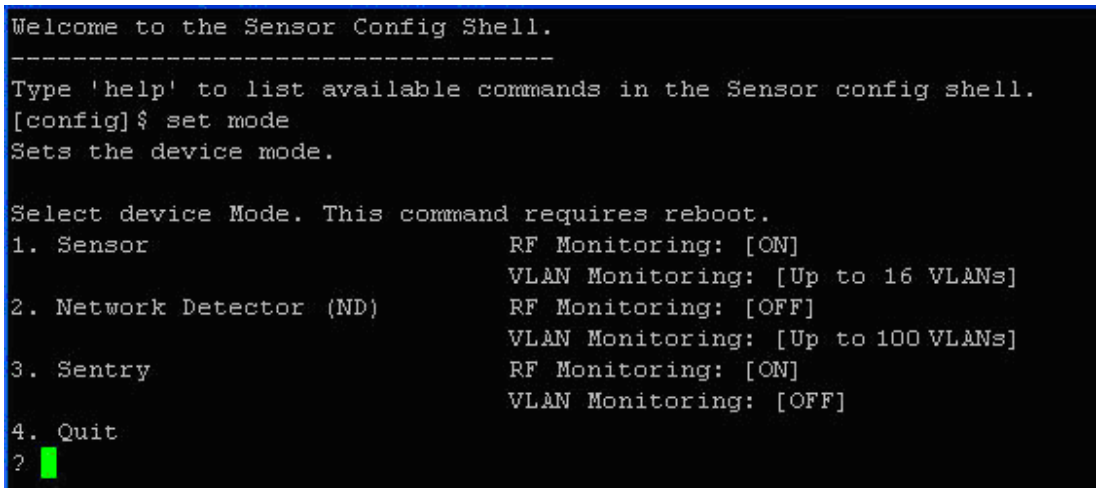

Figure 19. set sensor mode command for SS-300-AT-C-60

5.2.5 Configure Network Settings

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

Network Detector/Sensor 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 in the document 'Network Detector Configuration for SpectraGuard Enterprise_6.7 Update 1 ' for further details.

5.2.5.1 Configure IPv6 settings

SS-300-AT-C-60 is IPv6 capable. Use the command **set ipv6 config** to configure advanced options such as DHCP settings, auto negotiation and manual configuration.

***Note**: IPv6 settings are not supported in the SS-200-AT sensorsHow to configure Communication key or Passphrase*

5.2.5.2 How to configure Communication Key or Passphrase

To configure the communication key or passphrase kindly refer to Appendix A: Mutual Authentication for details.

Chapter 6 SS-300-AT-C-60 Config Shell Commands

The following tables detail the SS-300-AT-C-60 config shell commands.

Table 1. get commands

get Commands	
Command	**Description**
get ap	Displays all the currently visible APs
get interface	Displays Network Interface speed and mode
get ip config (deprecated)	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 listing of VLANs which are configured for monitoring by ND or Sensor
get vlan id	Displays listing of all VLANs which can be detected by ND or Sensor
get vlan status	Displays status of VLANs which are configured for monitoring by ND or Sensor
get model	Displays the Sensor Model
get antenna	Displays antenna configuration (Internal/ External)

Table 2. set commands

set Commands	
Command	**Description**
set erase	Sets the erase character to ^H.
set interface	Sets Network Interface properties like auto negotiation, speed, and duplex settings.
set ip config	Runs through the current VLAN and IP config wizard.
set server discovery	Sets the Server discovery information.

set vlan config	Configures list of VLANs and their network settings, to be monitored by ND or Sensor.
set ipv6 config	Sets IPv6 network settings.
set mode	Sets the mode to Sensor,Network Detector, or Sentry.
set communication key	Sets the Sensor-Server shared secret. You need to enter a hexadecimal value, of length 32, as the shared secret. It can be used instead of the 'set communication passphrase' command. Use this command if you are comfortable working with hexadecimals.
set communication passphrase	Sets the Sensor-Server shared secret. You need to enter a character string, of length between 10 and 127, as the shared secret. The string is internally converted to hexadecimal format. It can be used instead of the 'set communication key' command.

Table 3. Miscellaneous commands

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 <Hostname/IP address>	Pings a host. Usage: ping <IP_address/host_name> e.g. ping 192.168.1.246
ping6 <IPv6 address or hostname>	Pings an IPv6 host Usage: ping6 <IPv6_address/host_name>
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 7 SS-300-AT-C-60 Troubleshooting

Following are the troubleshooting guidelines for SS-300-AT-C-60 in AP mode.

Symptoms	Diagnosis	Solution
LED1: Solid Orange LED4: Fast Blink	The AP 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 LED4: Slow Blink	Unable to connect to the Server.	Ensure that the Server is running and is reachable from the network to which the AP is attached. If there is a firewall or a router with ACLs enabled between the AP 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 AP, or are provided by the DHCP Server. It is also possible that the AP is unable to connect to the Server because it has failed to authenticate with the Server. If this is the case, there will be an 'Authentication failed for AP's event raised on the Server. Refer to the Event for recommended action.
LED1: Solid Orange LED4: 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	A fatal Software error has occurred.	Contact support@airtightnetworks.com for more details.

Following are the troubleshooting guidelines for SS-300-AT-C-60 in sensor mode.

Symptoms	Diagnosis	Solution
LED1: Solid Orange LED4: 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 LED4: 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. It is also possible that the Sensor is unable to connect to the Server because it has failed to authenticate with the Server. If this is the case, there will be an 'Authentication failed for Sensor's event raised on the Server. Refer to the Event for recommended action.
LED1: Solid Orange LED4: Solid Green	The Ethernet cable is loose. It is probably disconnected from the network.	Ensure that the Ethernet cable is connected.
LED1: Solid Orange LED2: Solid Green	An error on the 802.11 interface has occurred.	Contact support@airtightnetworks.com for more details.
LED1: Solid Orange LED3: Solid Green	A fatal Software error has occurred.	Contact support@airtightnetworks.com for more details.

Chapter 8 Appendix A: Server Sensor Mutual Authentication

The Sensor-Server communication begins with a mutual authentication step in which the Sensor and Server authenticate each other using a shared secret. Sensor-Server communication takes place only if this authentication succeeds.

Once authentication succeeds, a session key is generated. All communication between the Sensor and Server from this point on is encrypted using the session key.

The Sensor and Server are shipped with the same default value of the shared secret. The CLI commands are provided on both Server and Sensor for changing the shared secret.

Note: *Once the shared secret (communication key) is changed on the Server, all Sensors connected to the Server will automatically be setup to use the new communication key. Sensors that are not connected to the Server at this time will need to be setup with the same communication key for them to be able to communicate with this Server.*

Note: *While the Server is backward compatible, that is, pre version 6.7 Update 1 Sensors can connect to a version 6.7 Update 1 Server, this is not recommended. Once all Sensors have been upgraded to version 6.7 Update 1, the* ***set sensor legacy authentication*** *CLI command can be used to disable older Sensors from connecting to the Server.*