



ExtremeWireless WiNG™ AP-8533 Installation Guide

9035160
August 2017



Copyright © 2024 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>



Table of Contents

| | |
|--|-----------|
| Preface..... | 5 |
| Text Conventions..... | 5 |
| Providing Feedback to Us..... | 6 |
| Getting Help..... | 6 |
| Extreme Networks Documentation..... | 7 |
| Open Source Declarations..... | 7 |
| Overview..... | 8 |
| Package Contents..... | 8 |
| Features..... | 8 |
| AP-8533 Antennas..... | 9 |
| US/Taiwan..... | 9 |
| Canada..... | 10 |
| EU..... | 11 |
| LED Indicators..... | 12 |
| Hardware Installation Instructions..... | 15 |
| Warnings..... | 15 |
| Site Preparation..... | 15 |
| Access Point Placement Guidelines..... | 15 |
| Power Injector System..... | 16 |
| Installing the Power Injector..... | 18 |
| Installing the AP-8533 Access Point..... | 19 |
| Wall Mount Instructions..... | 20 |
| Suspended Ceiling T-Bar Mount Instructions..... | 22 |
| Cabling the Access Point using Power Injector..... | 25 |
| Cabling the Access Point using Power Adapter..... | 26 |
| Configuring the Access Point..... | 27 |
| Configuring using the Typical Setup Wizard..... | 29 |
| Configuring RADIUS Server Users..... | 35 |
| Deriving Access Point IP Address..... | 36 |
| AP-8533 Access Point Specifications..... | 38 |
| Electrical Characteristics..... | 38 |
| Physical Characteristics..... | 38 |
| Radio Characteristics..... | 38 |
| Regulatory Information..... | 40 |
| Bluetooth Wireless Technology..... | 41 |
| Wireless Country Approvals..... | 41 |
| Country Selection..... | 41 |
| Frequency of Operation - IC..... | 41 |
| Industry Canada Statement..... | 41 |

| | |
|--|-----------|
| Avertissement..... | 42 |
| 2.4 GHz Only..... | 42 |
| Warnings for Use of Wireless Devices..... | 42 |
| Potentially Hazardous Atmospheres - Vehicle Installation..... | 42 |
| Potentially Hazardous Atmospheres - Fixed Installations..... | 42 |
| Safety in Aircraft..... | 42 |
| Safety in Hospitals..... | 43 |
| RF Exposure Guidelines..... | 43 |
| Reduce RF Exposure - Use Properly..... | 43 |
| International..... | 43 |
| Europe..... | 44 |
| US and Canada..... | 44 |
| Radio Frequency Interference Requirements..... | 45 |
| Radio Frequency Interference Requirements - FCC..... | 45 |
| Radio Transmitters (Part 15)..... | 45 |
| Canada..... | 46 |
| CE Marking and European Economic Area (EEA)..... | 47 |
| Statement of Compliance..... | 47 |
| Japan (VCCI) - Voluntary Control Council for Interference..... | 47 |
| Korea Warning Statement for Class B ITE..... | 47 |
| Other Countries..... | 48 |
| Australia..... | 48 |
| Brazil (UNWANTED EMISSIONS - ALL PRODUCTS)..... | 48 |
| Chile (Devices with a WLAN Radio)..... | 48 |
| China..... | 49 |
| Hong Kong..... | 49 |
| Mexico..... | 49 |
| S. Korea..... | 49 |
| Taiwan..... | 49 |
| Turkey..... | 50 |
| Ukraine Regulatory Statement..... | 50 |
| Thailand..... | 50 |
| Eurasian Customs Union..... | 50 |
| Waste Electrical and Electronic Equipment..... | 50 |
| TURKISH WEEE Statement of Compliance..... | 50 |
| End-User Software License Agreement..... | 51 |
| Index..... | 63 |
| Glossary..... | 58 |



Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons





| Icon | Notice Type | Alerts you to... |
|---|----------------|--|
|  | General Notice | Helpful tips and notices for using the product. |
|  | Note | Important features or instructions. |
|  | Caution | Risk of personal injury, system damage, or loss of data. |
|  | Warning | Risk of severe personal injury. |
| New! | New Content | Displayed next to new content. This is searchable text within the PDF. |

Table 2: Text Conventions

| Convention | Description |
|--|---|
| Screen displays | This typeface indicates command syntax, or represents information as it appears on the screen. |
| The words enter and type | When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.” |
| [Key] names | Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del] |
| <i>Words in italicized type</i> | Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles. |

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at documentation@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

| | |
|---|--|
| Current Product Documentation | www.extremenetworks.com/documentation/ |
| Archived Documentation (for earlier versions and legacy products) | www.extremenetworks.com/support/documentation-archives/ |
| Release Notes | www.extremenetworks.com/support/release-notes |

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/open-source-declaration/.



Overview

[Package Contents](#) on page 8

[Features](#) on page 8

[AP-8533 Antennas](#) on page 9

[LED Indicators](#) on page 12

The AP-8533 external antenna and internal antenna Access Points are high-tier Access Points for dependable and efficient network performance. The AP-8533 is a tri-radio Wave 2 802.11ac Access Point utilizing one 5GHz 802.11ac radio, one 2.4GHz 802.11n radio and a dual-band unlock 2.4GHz/5GHz 802.11ac radio for sensor functionality. The Access Point's unique WiNG 5 software enables it to function as either a *Standalone Access Point*, an *Adaptive Access Point*, or a *Virtual Controller*.

If new to Access Point technology, refer to the WiNG Access Point System Reference Guide to familiarize yourself with Access Point technology and the feature set supported by the WiNG operating system. The guide is available at www.extremenetworks.com/support/.

This document is written for the qualified network device installer.

Package Contents

An AP-8533 Access Point is available in both external antenna (AP-8533) and internal antenna (AP-8533I) configurations. An AP-8533 ships with the following:

- AP-8533 Access Point
- AP-8533 Installation Guide (this guide)
- Wall mount screws and mounting bracket

Features

An AP-8533 Access Point supports the following feature set:

- Two RJ-45 connectors (GE1/POE and Console)
- Two LED indicators with dual lights for each
- One 2.4GHz 802.11n radio
- One 5GHz 802.11ac radio
- One dual band unlock 2.4GHz/5GHz 802.11ac sensor radio
- One Bluetooth/BLE radio

- Wave 2
- Baud rate: 115200

The GE1/POE accepts 802.3at or 802.3af compliant power from an external source.



Note

When operating in a Gigabit Ethernet environment, CAT-5e or CAT-6 cable is recommended for Gigabit operation. The equipment is to be connected only to PoE networks. ExtremeNetworks does not recommend routing network cables outside.

AP-8533 Antennas

US/Taiwan



Note

Per FCC requirement, the use of the Access Point on UNII-1 of 5GHz band requires installers to input antenna elevation gain during configuration if the AP placement is outdoors. This information can be found in the Extreme Antenna Guide located at www.extremenetworks.com/support/.

An AP-8533 external antenna Access Point supports the following antenna options:

Table 3: Dual Band 2.4 GHz / 5 GHz Wifi Antennas - US/Taiwan

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Elevation Gain | Impedance (Ohms) |
|--------------------|-----------------|--------------------|------------------|----------------|------------------|
| ML-2452-HPAG4A6-01 | Dipole | 4 | 7.3 | 5.7 | 50 |
| ML-2452-APAG2A1-01 | Dipole | 2.7 | 1.7 | N/A | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 6.1 | 4.09 | 50 |
| ML-2452-APA2-01 | Dipole | 3.17 | 4.85 | N/A | 50 |
| ML-2452-PNA5-01R | Panel | 5.5 | 6 | 5.2 | 50 |
| ML-2452-SEC5M4-N36 | Polarized Panel | 6.92 | 7.23 | 3.95 | 50 |
| ML-2452-PTA4M4-036 | Patch | 5 | 6.6 | N/A | 50 |

An AP-8533 internal antenna Access Point supports the following dual band antenna:

Table 4: Dual Band 2.4 GHz / 5 GHz Internal Antennas - US/Taiwan

| Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Elevation Gain (dBi) |
|--------------|--------------------|------------------|--|
| Mono pole | 5.2 | 6.8 | <ul style="list-style-type: none"> • Radio 2:3:4 • Radio 3:4:1 |

Table 5: Single Band 2.4 GHz Bluetooth Antennas - US/Taiwan

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|--------------|--------------------|------------------|
| ML-2452-APA2-01 | Dipole | 3.17 | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 50 |
| ML-2452-PNA7-01R | Panel | 8 | 50 |
| ML-2452-PNL3M3-1 | Panel | 9.7 | 50 |
| ML-2452-PNL9M3-N36 | Panel | 11 | 50 |
| AP-8533 Internal | Mono pole | 7.7 | N/A |

Canada



Note

Per FCC requirement, the use of the Access Point on UNII-1 of 5GHz band requires installers to input antenna elevation gain during configuration if the AP placement is outdoors. This information can be found in Extreme antenna guide located at www.extremenetworks.com/support/.

An AP-8533 external antenna Access Point supports the following dual band antenna options:

Table 6: Dual Band 2.4 GHz / 5 GHz Wifi Antennas - Canada

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|--------------|--------------------|------------------|------------------|
| ML-2452-HPAG4A6-01 | Dipole | 4 | 7.3 | 50 |
| ML-2452-APAG2A1-01 | Dipole | 2.7 | 1.7 | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 6.1 | 50 |
| ML-2452-APA2-01 | Dipole | 3.17 | 4.85 | 50 |
| ML-2452-PNA5-01R | Panel | 5.5 | 6 | 50 |

Table 6: Dual Band 2.4 GHz / 5 GHz Wifi Antennas - Canada (continued)

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|-----------------|--------------------|------------------|------------------|
| ML-2452-SEC5M4-N36 | Polarized Panel | 6.92 | 7.23 | 50 |
| ML-2452-PTA4M4-036 | Patch | 5 | 6.6 | 50 |

An AP-8533 internal antenna Access Point supports the following dual band antenna:

Table 7: Dual Band 2.4 GHz / 5 GHz Internal Antennas - Canada

| Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Impedance (Ohms) |
|--------------|--------------------|------------------|------------------|
| Mono pole | 5.2 | 6.8 | N/A |

Table 8: Single Band 2.4 GHz Bluetooth Antennas - Canada

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|--------------|--------------------|------------------|
| ML-2452-APA2-01 | Dipole | 3.17 | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 50 |
| ML-2452-PNA7-01R | Panel | 8 | 50 |
| ML-2452-PNL3M3-1 | Panel | 9.7 | 50 |
| ML-2452-PNL9M3-N36 | Panel | 11 | 50 |
| AP-8533 Internal | Mono pole | 7.7 | N/A |

EU

**Note**

Per FCC requirement, the use of the Access Point on UNII-1 of 5GHz band requires installers to input antenna elevation gain during configuration if the AP placement is outdoors. This information can be found in the Extreme Antenna Guide located at www.extremenetworks.com/support/.

An AP-8533 external antenna Access Point supports the following dual band antenna options:

Table 9: Dual Band 2.4 GHz / 5 GHz Wifi Antennas - EU

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|--------------|--------------------|------------------|------------------|
| ML-2452-HPAG4A6-01 | Dipole | 4 | 7.3 | 50 |
| ML-2452-APAG2A1-01 | Dipole | 2.7 | 1.7 | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 6.1 | 50 |
| ML-2452-APA2-01 | Dipole | 3.17 | 4.85 | 50 |
| ML-2452-HPAG5A8-01 | Dipole | 7.5 | 8 | 50 |
| ML-2452-PNA5-01R | Panel | 5.5 | 6 | 50 |
| ML-2452-PNA7-01R | Panel | 8 | 12 | 50 |
| ML-2452-PTA4M4-036 | Patch | 5 | 6.6 | 50 |

An AP-8533 internal antenna Access Point supports the following dual band antenna:

Table 10: Dual Band 2.4 GHz / 5 GHz Internal Antennas - EU

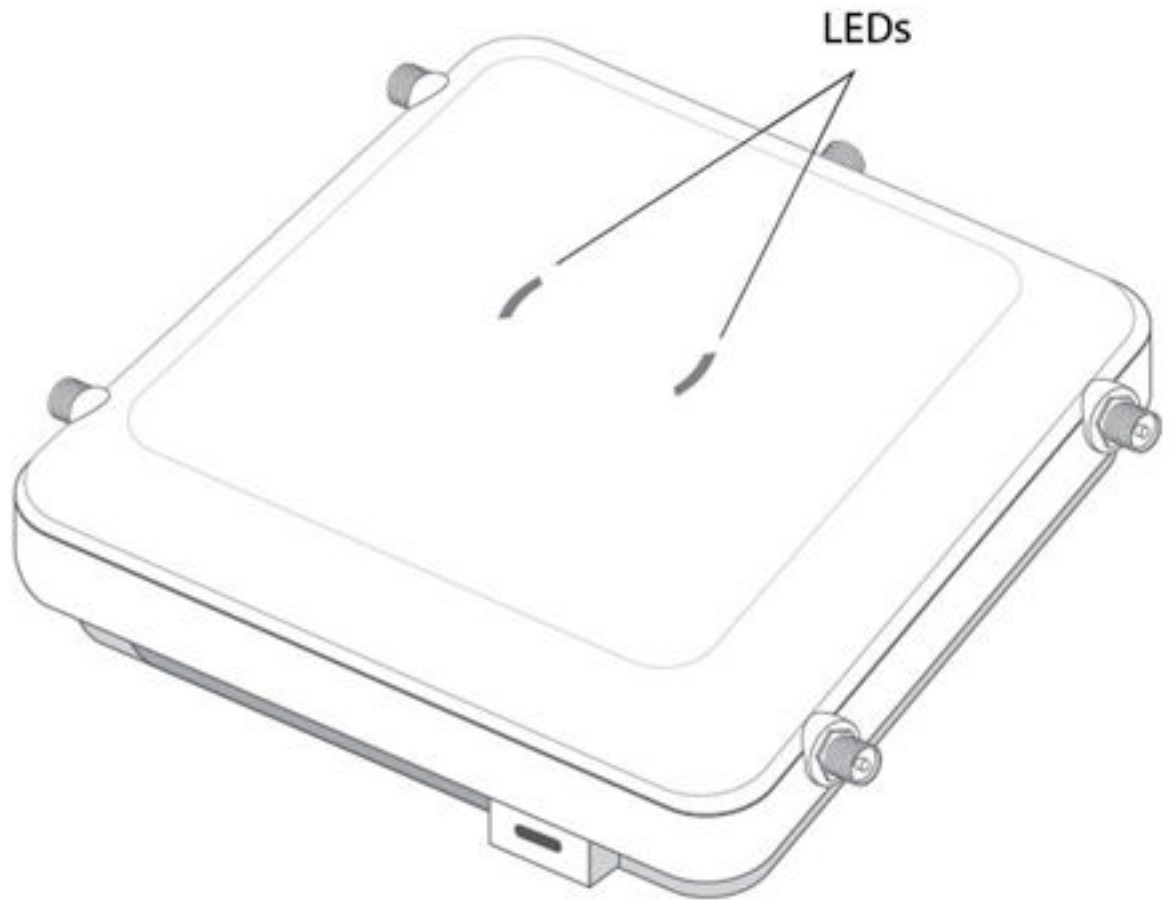
| Antenna Type | 2.4 GHz Gain (dBi) | 5 GHz Gain (dBi) | Impedance (Ohms) |
|--------------|--------------------|------------------|------------------|
| Mono pole | 5.2 | 6.8 | N/A |

Table 11: Single Band 2.4 GHz Bluetooth Antennas - EU

| Part Number | Antenna Type | 2.4 GHz Gain (dBi) | Impedance (Ohms) |
|--------------------|--------------|--------------------|------------------|
| ML-2452-APA2-01 | Dipole | 3.17 | 50 |
| ML-2452-HPA6-01 | Dipole | 5.3 | 50 |
| ML-2452-PNA7-01R | Panel | 8 | 50 |
| ML-2452-PNL3M3-1 | Panel | 9.7 | 50 |
| ML-2452-PNL9M3-N36 | Panel | 11 | 50 |
| AP-8533 Internal | Mono pole | 7.7 | N/A |

LED Indicators

The AP-8533 LED activity indicators are located on the front of the housing and are visible through the enclosure.



The LEDs display error conditions, transmission, and network activity for the 5 GHz 802.11ac (amber) radio, the 2.4 GHz 802.11n (green) radio, sensor radio (white), and the BLE radio (blue).

Table 12: AP-8533 LED Indicators

| State | 5 GHz Activity LED (Amber) | 2.4 GHz Activity LED (Green) | LED (Blue) | LED (White) |
|--------------------------------|--|--|--|--|
| Firmware Update | On | Off | Off | Off |
| Normal Operation | <ul style="list-style-type: none"> If the radio for this is disabled: turned off. If there is activity on this band: Blink interval at 2 times per second. | <ul style="list-style-type: none"> If the radio for this is disabled: turned off. If there is activity on this band: Blink interval at 2 times per second. | N/A | N/A |
| Not Configured | On | On | N/A | N/A |
| Locate AP Mode | LEDs blink in an alternating green, amber, blue and white pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions. | LEDs blink in an alternating green, amber, blue and white pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions. | LEDs blink in an alternating green, amber, blue and white pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions. | LEDs blink in an alternating green, amber, blue and white pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions. |
| Sensor without SS connected | N/A | N/A | N/A | Off |
| Sensor with SS connected | N/A | N/A | N/A | On |
| Air Termination state | N/A | N/A | N/A | Blinking 0.5 seconds in 1 second duty cycle. |
| BT radio disabled | N/A | N/A | Off | N/A |
| BT radio enabled (operational) | N/A | N/A | On | N/A |



Hardware Installation Instructions

[Warnings](#) on page 15

[Site Preparation](#) on page 15

[Access Point Placement Guidelines](#) on page 15

[Power Injector System](#) on page 16

[Installing the AP-8533 Access Point](#) on page 19

Warnings

- Read all installation instructions and site survey reports, and verify correct equipment installation before connecting the AP-8533 Access Point.
- Remove jewelry and watches before installing this equipment.
- Verify any device connected to this unit is properly wired and grounded.
- Verify there is adequate ventilation around the device, and that ambient temperatures meet equipment operation specifications.

Site Preparation

- Consult your site survey and network analysis reports to determine specific equipment placement, power drops, and so on.
- Assign installation responsibility to the appropriate personnel.
- Identify and document where all installed components are located.
- Ensure adequate, dust-free ventilation to all installed equipment.
- Identify and prepare Ethernet and console port connections.
- Verify cable lengths are within the maximum allowable distances for optimal signal transmission.

Access Point Placement Guidelines

For optimal performance, install the Access Point away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other industrial equipment. Signal loss can occur when metal, concrete, walls or floors block transmission.

Install the Access Point in an open area or add Access Points as needed to improve coverage. Antenna coverage is analogous to lighting. Users might find an area lit from far away to be not bright enough. An area lit sharply might minimize coverage and

create dark areas. Uniform antenna placement in an area (like even placement of a light bulb) provides even, efficient coverage.

Install the Access Point at an ideal height of 10 feet from the ground. To maximize the Access Point's radio coverage area, ExtremeNetworks recommends conducting a site survey to define and document radio interference obstacles before installing the Access Point.

Power Injector System

An AP-8533 Access Point can receive power via an Ethernet cable connected to the GE1/POE (LAN) port.

When users purchase a WLAN solution, they often need to place Access Points in obscure locations. In the past, a dedicated power source was required for each Access Point in addition to the Ethernet infrastructure. This often required an electrical contractor to install power drops at each Access Point location. The Power Injector merges power and Ethernet into one cable, reducing the burden of installation and allowing optimal Access Point placement in respect to the intended coverage area.

**Caution**

Using a non-compliant injector, or an injector supporting legacy modes prohibits the AP-8533 from functioning optimally.

**Caution**

Do not plug the AP-PSBIAS-2P3-ATR Power Injector into the Access Point's Console port. Connecting the Power Injector into the console port can damage the port and void the product warranty.

The AP-8533's supported Power Injector (Part No. AP-PSBIAS-2P3-ATR) is a high power POE Injector delivering up to 30 watts. The Access Point can only use a Power Injector when connecting the unit to the Access Point's GE1/POE port. The Power Injector is separately ordered and not shipped with an existing AP SKU.

The Access Point Power Supply (Part No. PWR-BGA48V45W0WW) is not included with the Access Point and is orderable separately as an accessory. If the Access Point is provided both POE power and PWR-BGA48V45W0WW power concurrently, the Access Point will source power from the PWR-BGA48V45W0WW supply only. Disconnecting the AC power from the PWR-BGA48V45W0WW causes the Access Point to re-boot before sourcing power from the POE Power Injector. If the AP is operating using injector supplied power, the AP will not automatically reboot if an AC adapter is connected. The Access Point continues to operate with power supplied from the AC adapter without change to the Access Point operating configuration. If using AC

adapter supplied power and a change to the AP's operating configuration is warranted, the Access Point needs to be manually rebooted.



Caution

The Access Point supports any standards-based compliant power source. However, using the wrong solution (including a POE system used on a legacy Access Point) could either limit functionality or severely damage the Access Point and void the product warranty.

A separate Power Injector is required for each AP-8533 Access Point comprising the network.

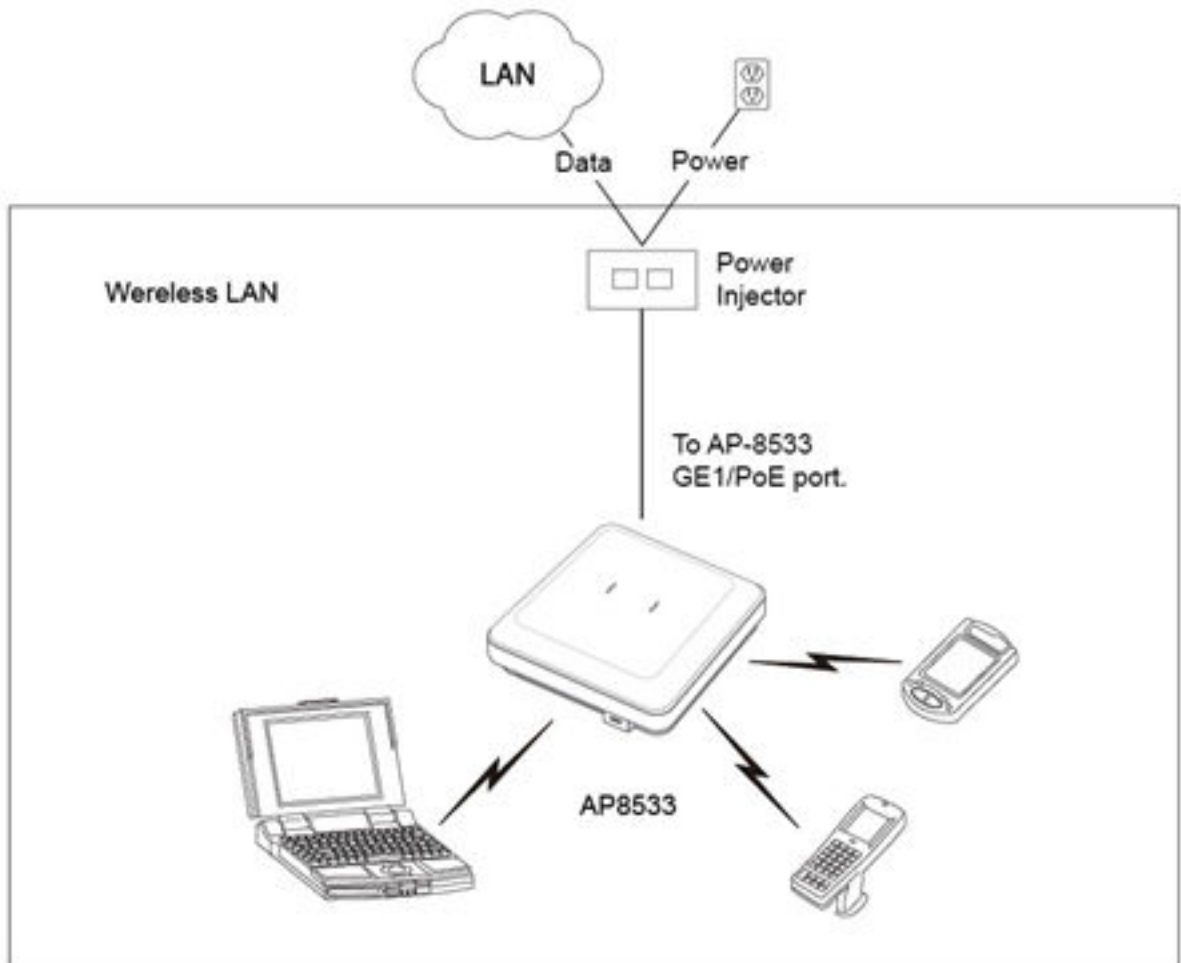


Table 13: AP-8533 Power Management

| AP-8533 | 3af | 3at |
|---------|-----|-----|
| Radio 1 | 3x3 | 4x4 |
| Radio 2 | 2x4 | 4x4 |
| Radio 3 | 1x1 | 3x3 |
| BLE | ON | ON |

Table 13: AP-8533 Power Management (continued)

| AP-8533 | 3af | 3at |
|---------|-----|-----|
| GE1 | ON | ON |
| GE2 | ON | ON |

Installing the Power Injector

About This Task

The Power Injector can be installed free standing, on an even horizontal surface, or wall mounted using the Power Injector's wall mounting key holes. The following guidelines should be adhered to before cabling the power injector to an ethernet source and an access point:

- Do not block or cover airflow to the Power Injector.
- Keep the Power Injector away from excessive heat, humidity, vibration and dust.
- The Power Injector isn't a repeater, and does not amplify the Ethernet signal.
- For optimal performance, ensure the Power Injector is placed as close as possible to the data port.



Caution

To avoid problematic performance and restarts, disable POE from a wired switch port connected to an Access Point if mid-span power sourcing equipment (PSE) is used between the two, regardless of the manufacturer of the switch.



Caution

Ensure AC power is supplied to the Power Injector using an AC cable with an appropriate ground connection approved for the country of operation.

To install the Power Injector to an Ethernet data source and an Access Point:

Procedure

1. Connect the Power Injector to an AC outlet (110VAC to 220VAC).
2. Connect an RJ-45 Ethernet cable between the Power Injector Data & Power Out connector and the Access Point's GE1/POE port.
3. Connect an RJ-45 Ethernet cable between the network data supply (host) and the Power Injector Data In connector.



Note

Ensure the cable length from the Ethernet source (host) to the Power Injector and Access Point does not exceed 100 meters (333 ft).

The Power Injector has no On/Off power switch. The Injector receives power and is ready for device connection and operation as soon as AC power is applied. Refer to the Installation Guide shipped with the Power Injector for a description of the device's LEDs.

Installing the AP-8533 Access Point

About This Task

Before installing an AP-8533 Access Point, verify the following:

- You are using the correctly rated power solution for the AP-8533 (either the AP-PSBIAS-2P3-ATR Power Injector or the PWR-BGA48V45W0WW external power supply).
- Do not to install the AP-8533 in wet or dusty areas.
- Verify the environment has a continuous temperature range between 32°F to 122°F or 0°C to 50°C.

An AP-8533 Access Point mounts either on a wall (with M 3.5 x 0.6 x 23 MM pan head screws and mounting bracket or equivalent) or on a suspended ceiling T-bar.

To prepare for the installation:

Procedure

1. Match the part number on the purchase order with the part numbers in the packing list and on the case of the Access Point.
2. Verify the contents of the box include the intended AP-8533 Access Point, and the included hardware matches the package contents (see [AP-8533 Package Contents](#)).

Table 14: Test

| Part Number | Description |
|-------------------|--|
| AP-8533-68SB30-US | AP-8533 Tri Radio 802.11AC Wave 2 Access Point, Dedicated Sensor, BLE, Internal Antenna 2XGE, US Version |
| AP-8533-68SB30-WR | AP-8533 Tri Radio 802.11AC Wave 2 Access Point, Dedicated Sensor, BLE, Internal Antenna 2XGE, International Version - WR |
| AP-8533-68SB30-EU | AP-8533 Tri Radio 802.11AC Wave 2 Access Point, Dedicated Sensor, BLE, Internal Antenna 2XGE, EU version |
| AP-8533-68SB40-US | AP-8533 Tri Radio 802.11AC Wave 2 Access Point Dedicated Sensor, BLE, External Antenna 2XGE, US version |
| AP-8533-68SB40-WR | AP-8533 Tri Radio 802.11AC Wave 2 Access Point Dedicated Sensor, BLE, External Antenna 2XGE, International version -WR |
| AP-8533-68SB40-EU | AP-8533 Tri Radio 802.11AC Wave 2 Access Point Dedicated Sensor, BLE, External Antenna 2XGE, EU version |

3. Review site survey and network analysis reports to determine the location and mounting position for the AP-8533 Access Point.

4. Connect a CAT-5 or better Ethernet cable to a compatible 802.3at or 802.3af power source and run the cable to the installation site. Ensure there is sufficient slack on the cable to perform the installation steps.

**Note**

When operating in a Gigabit Ethernet environment, CAT-5e or CAT-6 cable is recommended for Gigabit operation.

Wall Mount Instructions

A wall mount deployment requires hanging the AP-8533 with the provided mounting bracket and two screws. The AP-8533 can be mounted on to any plaster, wood or cement wall surface using the provided mounting bracket.

The hardware required to install the AP-8533 on a wall consists of:

- Two wide-shoulder Phillips pan head self-tapping screws (M3.5 x 0.6 x 23 mm)
- Mounting bracket

Optional customer provided installation tools include:

- Phillips head screw driver, or drill and drill bit

Wall Mounting Procedure - New Installation

This section describes a new AP-8533 installation with no previous Access Point existing on the intended wall surface.

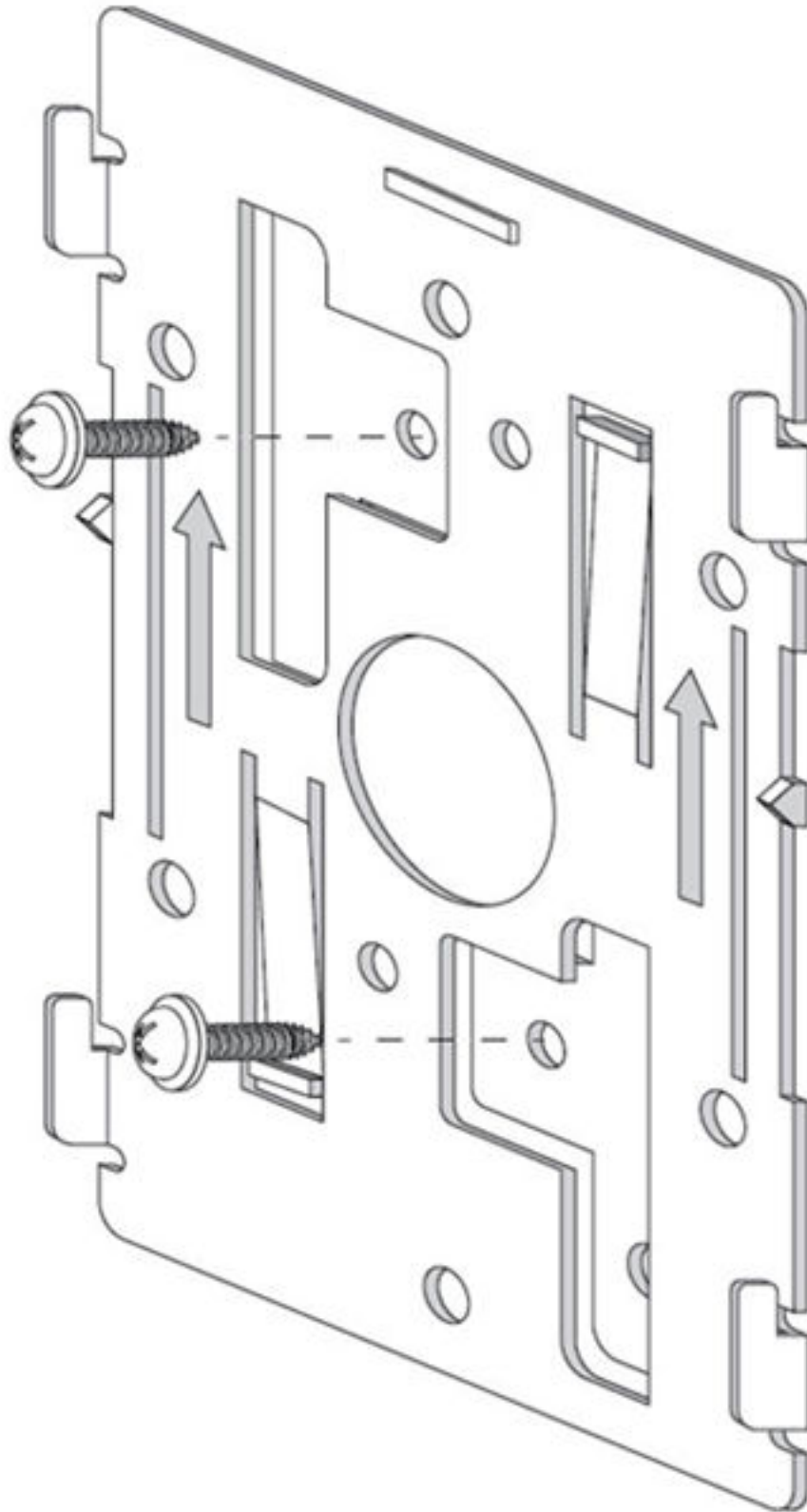
Procedure

1. Place the mounting bracket against the wall.
2. Mark the screw hole locations depending on the intended deployment orientation of the unit.

**Note**

When pre-drilling a hole, the recommended hole size is 4mm (0.16in).

3. At each point, drill a hole in the wall and attach the mounting bracket.



4. Place the access point on the mounting bracket.
5. To cable the access point using the Power Injector solution (AP-PSBIAS-2P3-ATR), see [Cabling the Access Point using Power Injector](#) on page 25.
6. To cable the access point using the approved AP-8533 power supply (PWR-BGA48V45W0WW), see [Cabling the Access Point using Power Adapter](#) on page 26.
7. Verify the access point is receiving power by observing the LEDs are lit or flashing. For more information on AP-8533 LED behavior, see [LED Indicators](#).

The access point is ready to configure.

**Caution**

If not using an AP-PSBIAS-2P3-ATR Power Injector, ensure only the AP-8533's designated power supply (PWR-BGA48V45W0WW) is used to supply power to the Access Point. Using an incorrectly rated power supply could damage the Access Point and void the product warranty. Do not actually connect to the power source until the cabling portion of the installation is complete.

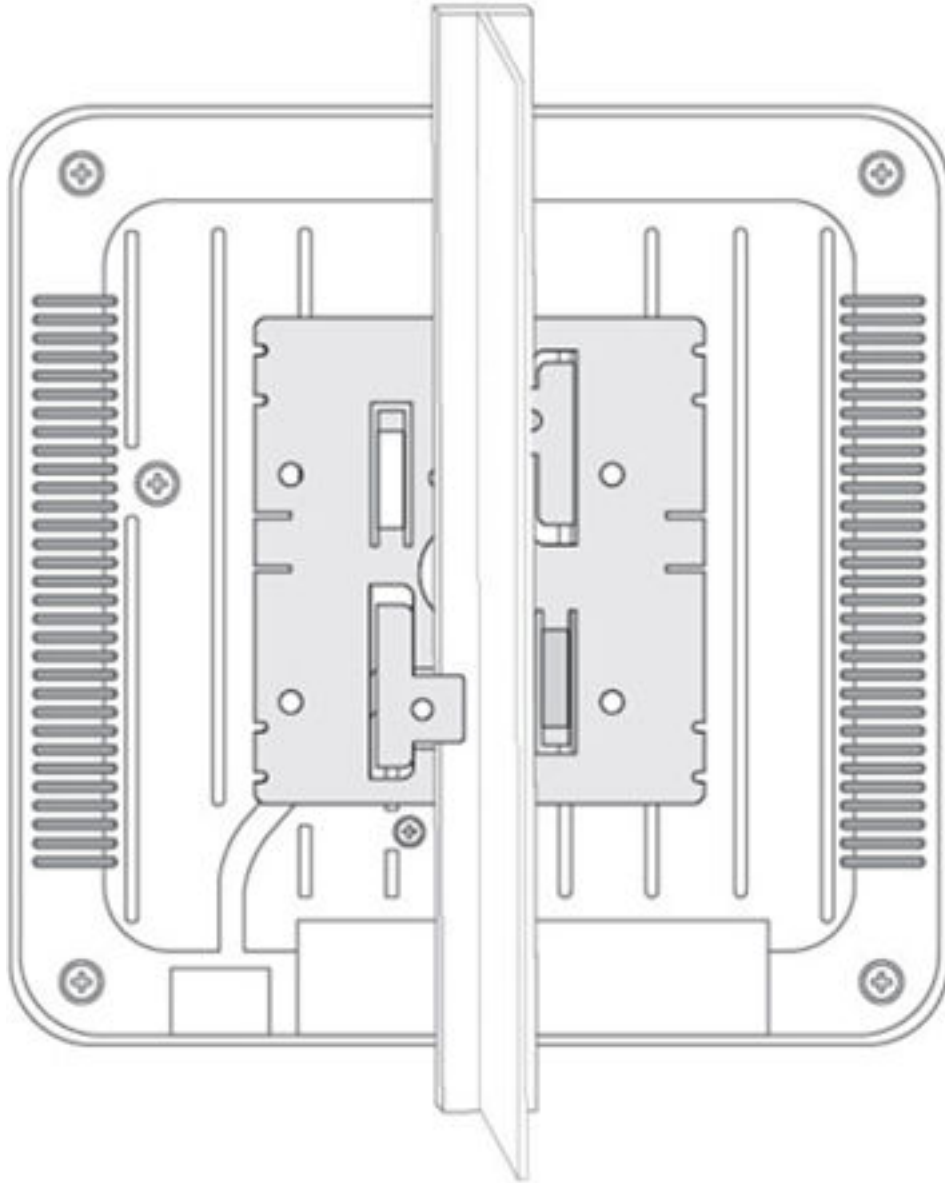
Suspended Ceiling T-Bar Mount Instructions

About This Task

Ceiling mount requires holding the AP-8533 up against the T-bar of a suspended ceiling grid and twisting the unit on to the T-bar. If deploying the AP-8533 on a sculpted ceiling TBar, the Access Point mounting kit (Part No. KT-135628-01) can optionally be used as well.

Procedure

1. Install the mounting bracket on the T-bar, then attach the mounting bracket using the mounting slots on the Access Point.



2. To cable the access point using the Power Injector solution (AP-PSBIAS-2P3-ATR), see [Cabling the Access Point using Power Injector](#) on page 25.

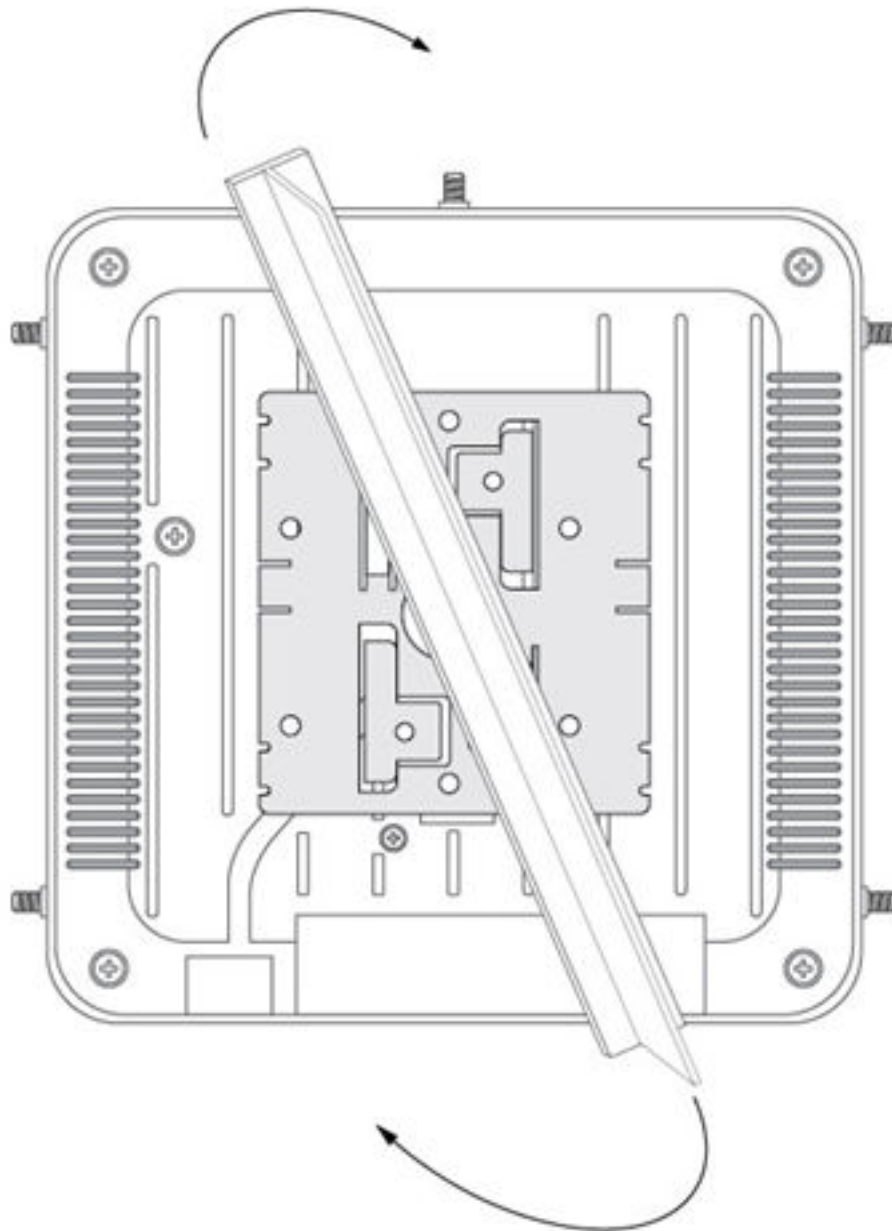
3. To cable the access point using the approved AP-8533 power supply (PWR-BGA48V45W0WW), see [Cabling the Access Point using Power Adapter](#) on page 26.

**Caution**

If not using an AP-PSBIAS-2P3-ATR Power Injector, ensure only the AP-8533's designated power supply (PWR-BGA48V45W0WW) is used to supply power to the Access Point. Using an incorrectly rated power supply could damage the Access Point and void the product warranty. Do not actually connect to the power source until the cabling portion of the installation is complete.

4. Verify the unit has power by observing the LEDs.
For more information on AP-8533 LED behavior, see [LED Indicators](#).
5. Align the bottom of the ceiling T-bar with the back of the Access Point.
6. Orient the Access Point chassis by its length and the length of the ceiling T-bar.
7. Rotate the Access Point chassis 45 degrees clockwise.
8. Push the back of the Access Point chassis on to the bottom of the ceiling T-bar.

9. Rotate the Access Point chassis 45 degrees counter-clockwise. The clips click as they fasten to the T-bar.



The Access Point is ready to configure.

Cabling the Access Point using Power Injector

About This Task

For Power Injector installations:

Procedure

1. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the Power Injector Data & Power Out connector and the Access Point's GE1/POE port.
2. Connect a RJ-45 CAT5e (or CAT6) Ethernet cable between the network data supply (host) and the Power Injector Data In connector.
3. Ensure the cable length from the Ethernet source (host) to the Power Injector and Access Point does not exceed 100 meters (333 ft).

The Power Injector has no On/Off power switch. The Power Injector receives power as soon as AC power is applied.

Cabling the Access Point using Power Adapter

About This Task

For standard power adapter (non Power Injector) and line cord installations:

Procedure

1. Connect a RJ-45 Ethernet cable between the network data supply (host) and the Access Point's GE1/POE port.
2. Verify the power adapter is correctly rated according to the country of operation.
3. Connect the power supply line cord to the power adapter.
4. Attach the power adapter cable into the power connector on the Access Point.
5. Attach the power supply line cord to a power supply.



Configuring the Access Point

[Configuring using the Typical Setup Wizard](#) on page 29

[Configuring RADIUS Server Users](#) on page 35

[Deriving Access Point IP Address](#) on page 36

You can access the AP-8533 management functions once it is installed and powered on.

About This Task

Procedure

1. Derive the IP address for the access point.
2. Point the Web browser to the Access Point's IP address.

The following login screen displays:



3. Enter the default username `admin` in the **Username** field.
4. Enter the default password `admin123` in the **Password** field.

- Click **Login** to load the management interface.



Note

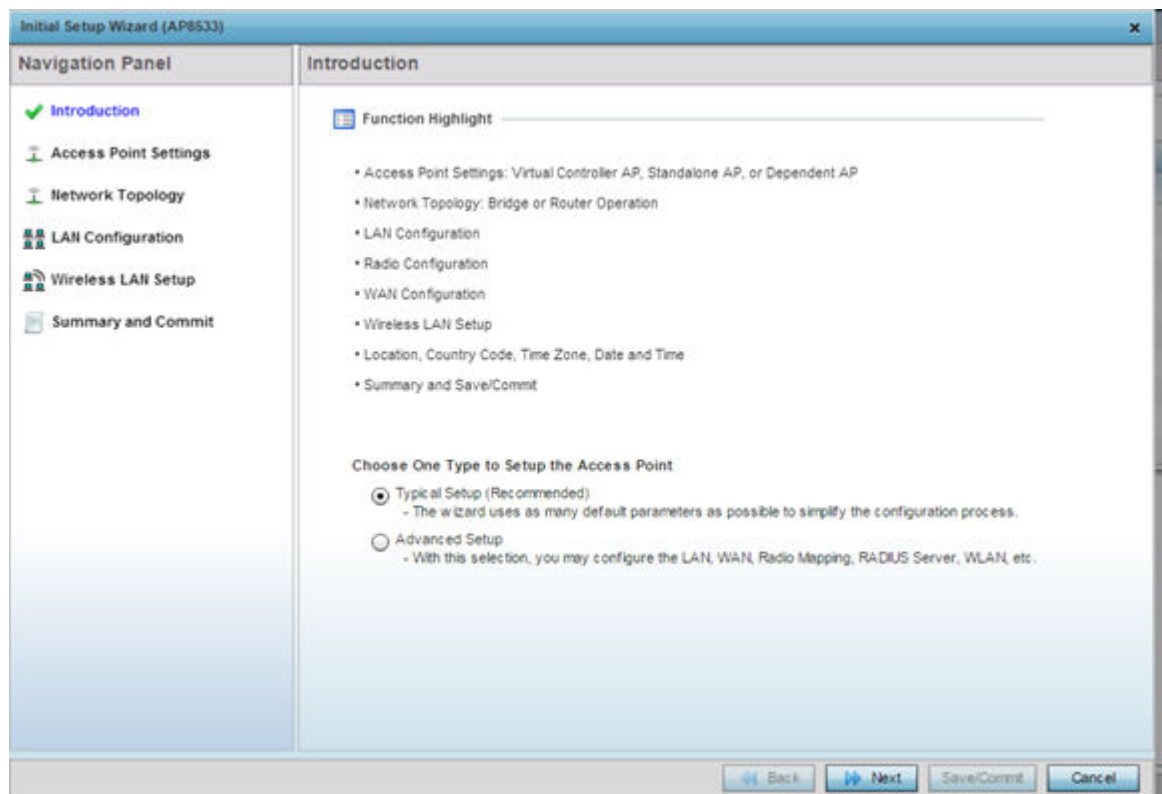
When logging in for the first time, you're prompted to change the password to enhance device security in subsequent logins.



Note

If you get disconnected when running the wizard, you can connect again with the Access Point's actual IP address (once obtained) and resume the wizard.

If this is the first time the management interface has been accessed, the Initial Setup Wizard automatically displays.



Note

The **Initial Setup Wizard** displays the same pages and content for each Access Point type supported. The only difference being the number of radios configurable by Access Point, as models vary.

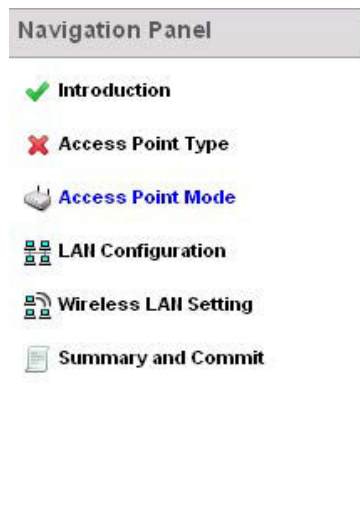
The **Introduction** screen displays the various actions that can be performed using the wizard under the **Function Highlight** field.

- Use the **Choose One type to Setup the Access Point** field options to select the type of wizard to run.

The **Typical Setup** is the recommended wizard. This wizard uses the default parameters for most of the configuration and sets a working network with the least amount of manual configuration.

The **Advanced Setup** is for administrators who prefer more control over the different configuration parameters. A few more configuration screens are available for customization when the Advanced Setup wizard is used.

The **Navigation Panel** for the Typical Setup Wizard displays the basic configuration options.



A green checkmark to the left of an item in the **Navigation Panel** defines the task as having its minimum required configuration set correctly. A red X defines a task as still requiring at least one parameter to be defined correctly.

- Click **Save/Commit** within each page to save the updates made to that page's configuration or click **Next** to proceed to the next page listed in the **Navigation Panel** without saving your updates.



Note

While you can navigate to any page in the **Navigation Panel**, you cannot complete the Initial AP Setup Wizard until each task in the **Navigation Panel** has a green checkmark.

Configuring using the Typical Setup Wizard

About This Task

For the purposes of this guide, use the Typical Setup (Recommended) option to simplify the process of getting the Access Point up and running quickly with a minimum number of changes to the Access Point's default configuration.

For information on using the Access Point's Advanced Setup option, refer to the WiNG Access Point System Reference Guide to familiarize yourself with the

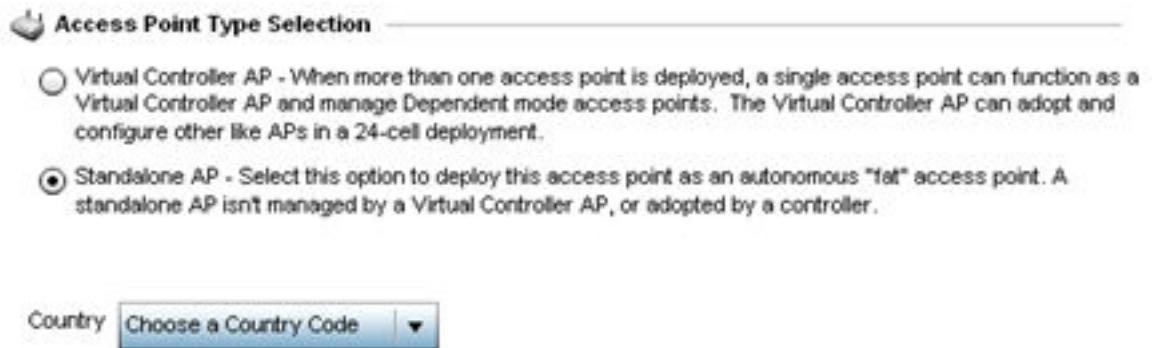
feature set supported by the WiNG operating system. The guide is available at www.extremenetworks.com/support/.

To configure the Access Point using the Typical Setup Wizard:

Procedure

1. Click **Typical Setup** from the **Choose One type to Setup the Access Point** field on the **Initial Setup** Wizard.

The **Typical Setup Wizard** displays the Access Point Settings screen to define the Access Point's Standalone versus Virtual Controller AP functionality. This screen also enables selection of the country of operation for the Access Point.



Access Point Type Selection

Virtual Controller AP - When more than one access point is deployed, a single access point can function as a Virtual Controller AP and manage Dependent mode access points. The Virtual Controller AP can adopt and configure other like APs in a 24-cell deployment.

Standalone AP - Select this option to deploy this access point as an autonomous "fat" access point. A standalone AP isn't managed by a Virtual Controller AP, or adopted by a controller.

Country



Note

The professional installer should refer to the WiNG Access Point System Reference Guide for detailed information on how to set the Access Point's transmit power, antenna gain and channel in respect to the deployment country's unique regulatory requirements.

2. Select an Access Point type.



Note

If wanting to adopt the Access Point to a controller or service platform, use the controller or service platform's resident UI to connect to the Access Point, provision its configuration and administrate the Access Point's configuration.



Note

If designating the Access Point as a Standalone AP, it's recommended the Access Point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without encountering problems.

3. Select the country code of the country where the Access Point is deployed.

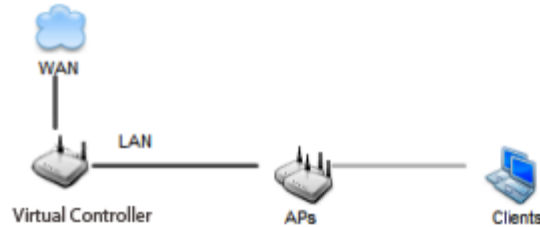
Selecting a proper country is a critical task while configuring the Access Point, as it defines the correct channels of operation and ensures compliance to the regulations of the selected country. This field is only available for the Typical Setup Wizard.

- Click Next to set the Access Point's network mode.

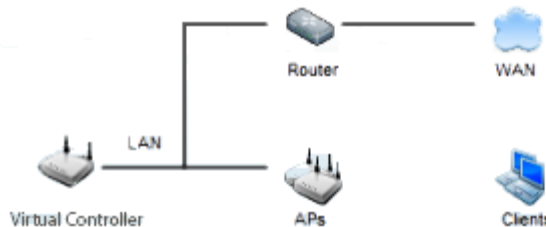
The Typical Setup Wizard displays the **Network Topology** screen to define how the Access Point manages network traffic.

 **Network Topology**

- Router Mode - the access point routes traffic between the wireless network and the Internet or corporate network (WAN).



- Bridge Mode - In Bridge Mode, the access point depends on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger density network. Thus, select Bridge Mode when deploying this access point with numerous peer APs supporting clients on both the 2.4 and 5GHz radio bands.



- Choose an Access Point Mode from the available options.

Router mode is recommended in a deployment supported by just a single Access Point. Bridge Mode is recommended when deploying this Access Point with numerous peer Access Points supporting clients on both the 2.4GHz and 5GHz radio bands.



Note

When Bridge Mode is selected, WAN configuration cannot be performed and the Typical Setup Wizard does not display the WAN configuration screen.

6. Click **Next**.

The Typical Setup Wizard displays the LAN Configuration screen to set the Access Point's LAN interface configuration.

LAN Configuration

Please configure interface settings for LAN (VLAN 1) which will be used by wireless clients

Use DHCP [What is this?](#)

Static IP Address/Subnet [What is this?](#) 192.168.13.23 / 24 *

DHCP Server

Use on-board DHCP server to assign IP addresses to wireless clients

Range: 192.168.0.100 -- 192.168.0.200

Default Gateway: 192.168.0.1

Domain Name Server (DNS)

DNS Forwarding

Primary DNS: . . .

Secondary DNS: . . .

7. Set the following DHCP and Static IP Address/Subnet information for the LAN interface:

Use DHCP

Select the checkbox to enable an automatic network address configuration using the Access Point's DHCP server.

Static IP Address/Subnet

Enter an IP Address and a subnet for the Access Point's LAN interface. If Use DHCP is selected, this field is not available.

Define the following DHCP Server and Domain Name Server (DNS) resources, as those fields will become enabled on the bottom portion of the screen.

Use on-board DHCP server to assign IP addresses to wireless clients

Select the checkbox to enable the Access Point's DHCP server to provide IP and DNS information to requesting clients on the LAN interface.

Range

Enter a starting and ending IP Address range for client assignments on the LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.

Default Gateway

Define a default gateway address for use with the default gateway. This is a required parameter.

DNS Forwarding

Select this option to allow a DNS server to translate domain names into IP addresses. If this option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.

Primary DNS

Enter an IP Address for the main Domain Name Server providing DNS services for the Access Point's LAN interface.

Secondary DNS

Enter an IP Address for the backup Domain Name Server providing DNS services for the Access Point's LAN interface.

- Click **Next**.

The **Typical Setup** Wizard displays the **Wireless LAN Setup** screen to set the an Access Point's WLAN 1 and WLAN 2 configuration.

The screenshot shows the 'WLAN 1 Configuration' screen. At the top, there are two tabs: 'WLAN 1' and 'WLAN 2'. Below the tabs, the title 'WLAN 1 Configuration' is displayed with a wireless LAN icon. The main configuration area includes:

- SSID:** A text input field containing 'WLA_01', followed by a 'What is this?' link and a star icon.
- WLAN Type:** Three radio button options:
 - No Authentication and No Encryption [What is this?](#)
 - Captive Portal Authentication and No Encryption [What is this?](#)
 - PSK authentication, WPA2 encryption [What is this?](#)

- Set the following WLAN1 configuration parameters:

SSID

Configure the SSID for the WLAN.

WLAN Type

Configure encryption and authentication settings to protect the data and user integrity of WLAN 1.

No Authentication and No Encryption

Configures a network without any user authentication or data encryption. This means any data transmitted through the network is in plain text. Any device between end points can see the information transmitted. This is the least secure of all network configurations.

Captive Portal Authentication and No Encryption

Uses a RADIUS server to authenticate users before allowing them on to the network. Once on the network, no encryption is used for the data transmitted

through the network. Select this option to use a Web page (either internally or externally hosted) to authenticate users before access is granted to the network.

PSK authentication, WPA2 encryption




Configures a network that uses PSK authentication and WPA2 encryption.

Select this option to implement a pre-shared key that must be correctly shared between the Access Point and requesting clients.

10. Click **Next**.

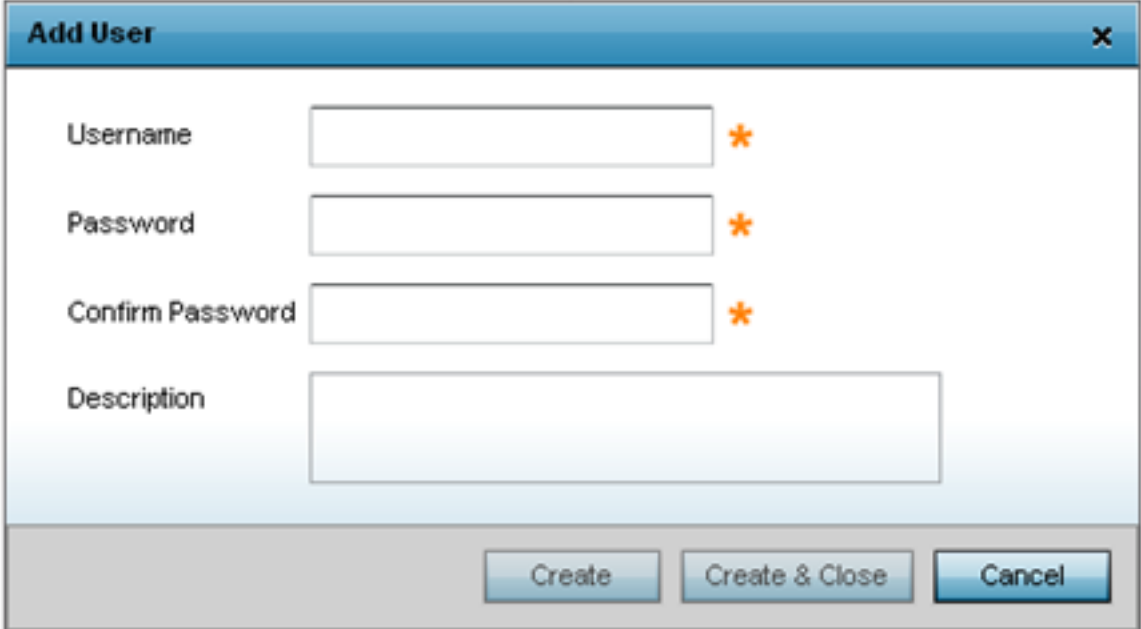
The **Typical Setup Wizard** displays the **RADIUS Server Configuration** screen if required. See [Configuring RADIUS Server Users](#) to configure the users for the onboard RADIUS server.

Otherwise, the **Typical Setup Wizard** displays the **Summary and Commit** screen to summarize the screens (pages) and settings updated using the Typical Setup Wizard.

| | | |
|---|-------------------------------|-------|
|  | Access Point Type Page | _____ |
| Access Point Type | Standalone AP | |
| | | |
|  | Networking Mode Page | _____ |
| Networking Mode | Router Mode | |
| | | |
|  | LAN Configuration Page | _____ |
| LAN Configuration Type | Static IP Address/Subnet | |
| VLAN ID for the LAN Interface | 1 | |
| Static IP Address/Subnet | 192.168.13.23/24 | |
| | | |
|  | WAN Configuration Page | _____ |
| WAN Configuration Type | Use DHCP | |
| Port to External | GE1 Port | |
| | | |
|  | WLAN Configuration | _____ |

11. If the configuration displays as intended, click **Save/Commit** to implement these settings to the Access Point's configuration.

2. Click **Add User** to display the dialog to enter user information to add to the RADIUS server user database.



The screenshot shows a dialog box titled "Add User" with a close button (X) in the top right corner. The dialog contains four input fields: "Username", "Password", "Confirm Password", and "Description". Each of the first three fields has an orange asterisk to its right, indicating they are required. At the bottom of the dialog, there are three buttons: "Create", "Create & Close", and "Cancel".

3. Enter the following user information:
 - Username - Provide a user name to authenticate the user.
 - Password - Provide a password to authenticate the user.
 - Confirm Password - Confirm the password by entering the same password entered in the Password field.
 - Description - Provide a description to identify the user created in the RADIUS server database.
4. Click **Create** to create the entry in the RADIUS server database and add another user. Select **Create & Close** to create an entry in the RADIUS server database and close the Add User dialog.
5. Click **Modify User** within the RADIUS Server Configuration screen to modify information for an existing user
The Username cannot be modified with this dialog.
6. Click **Delete User** on the RADIUS Server Configuration screen to remove information for an existing user.
7. Click **Yes** to verify the removal.
8. Click **Cancel** to revert to the last saved configuration.

Deriving Access Point IP Address

About This Task

The Access Point's IP address is optimally provided using DHCP. A zero config IP address can also be derived if DHCP resources are unavailable. Using zero config, the last two octets in the IP address are the decimal equivalent of the last two bytes in the Access Point's hardcoded MAC address.

For example: MAC address - 00:C0:23:00:F0:0A

Zero-config IP address - 169.254.240.10

To derive the Access Point's IP address using its MAC address:

Procedure

1. Open the Windows calculator by selecting Start > All Programs > Accessories > Calculator. This menu path may vary slightly depending on your version of Windows.
2. With the Calculator displayed, select View > Scientific. Select the Hex radio button.
3. Enter a hex byte of the Access Point's MAC address. For example, F0.
4. Select the Dec radio button.
The calculator converts F0 into 240.
5. Repeat steps 3 and 4 for the last Access Point MAC address octet.



AP-8533 Access Point Specifications

Electrical Characteristics

| | |
|-----------------------------|--|
| Operating Current & Voltage | <ul style="list-style-type: none"> • 48 VDC, 0.5A (AUX input voltage) • 48VDC PWR-BGA48V45W0WW Power Supply • 48VDC, 0.5A (POE) • 802.3at AP-PSBIAS-2P3-ATR Power Injector |
|-----------------------------|--|

Physical Characteristics

| | |
|------------------------------|--|
| Dimensions | <ul style="list-style-type: none"> • 8.25 in. L x 8.25 in. W x 1.8 in. H • 210 mm L x 210 mm W x 46 mm H |
| Weight | 3.0 lbs/1.37 kg |
| Operating Temperature | 32° F to 122° F/0° C to 50° C* |
| Storage Temperature | -40° F to 158° F/-40° C to 70° C |
| Operating Humidity | 95% RH non-condensing |
| Operating Altitude (maximum) | 13,000 ft @ 28C |
| Storage Altitude (maximum) | 30,000 ft @ 12C |
| Electrostatic Discharge | ESD to ±12KV air and ±8KV contact |

Radio Characteristics

| | |
|----------------------|--|
| Data Rates Supported | <ul style="list-style-type: none"> • 802.11b/g: 1,2,5.5,11,6,9,12,18,24,36,48 and 54 Mbps • 802.11a: 6,9,12,18,24,36,48, and 54 Mbps • 802.11n: MCS 0-31 up to 600Mbps • 802.11ac: MCS 0-9 up to 1.733Gbps |
| Wireless Medium | <ul style="list-style-type: none"> • Direct Sequence Spread Spectrum (DSSS) • Orthogonal Frequency Division Multiplexing (OFDM) • Spatial multiplexing (MIMO) |

| | |
|---------------------------|--|
| Network Standards | <ul style="list-style-type: none">• IEEE 802.11a/b/g/n/ac, Wave 2• 802.11d and 802.11i WPA2• WMM and WMM-UAPSD |
| Transmit Power Adjustment | 1 dB increments |



Regulatory Information

- [Bluetooth Wireless Technology](#) on page 41
- [Wireless Country Approvals](#) on page 41
- [Frequency of Operation - IC](#) on page 41
- [Warnings for Use of Wireless Devices](#) on page 42
- [RF Exposure Guidelines](#) on page 43
- [Radio Frequency Interference Requirements](#) on page 45
- [CE Marking and European Economic Area \(EEA\)](#) on page 47
- [Statement of Compliance](#) on page 47
- [Japan \(VCCI\) - Voluntary Control Council for Interference](#) on page 47
- [Korea Warning Statement for Class B ITE](#) on page 47
- [Other Countries](#) on page 48
- [Waste Electrical and Electronic Equipment](#) on page 50
- [TURKISH WEEE Statement of Compliance](#) on page 50
- [End-User Software License Agreement](#) on page 51

This guide applies to the following Model Numbers: AP-8533, AP-8533I.

All Extreme Networks devices are designed to be compliant with the rules and regulations in the locations they are sold and will be labeled as required. Any changes or modifications to Extreme Networks equipment, not expressly approved by Extreme Networks could void the user's authority to operate the equipment. Extreme Networks devices are professionally installed, the Radio Frequency Output Power will not exceed the maximum allowable limit for the country of operation.

Antennas: Use only the supplied or an approved replacement antenna. Unauthorized antennas, modifications, or attachments could cause damage and may violate regulations.

This device is only to be used with an Extreme Networks Wireless Switch. For use only with Extreme Networks approved and UL Listed mobile computers, Extreme Networks approved, and UL Listed/Recognized battery packs.



Caution

Do NOT attempt to charge damp/wet mobile computers or batteries. All components must be dry before connecting to an external power source.

Declared maximum operating temperature: 50°C.

Bluetooth Wireless Technology

This is an approved Bluetooth® product. For more information or to view the End Product Listing, visit <https://www.bluetooth.org/tpg/listings.cfm>.

Wireless Country Approvals

**Note**

This section is applicable only to WW/WR configurations.

Regulatory markings are applied to the device signifying the radio(s) are approved for use in the following countries and continents: United States, Canada, Japan, China, South Korea, Australia, Europe and Taiwan.

Please refer to the Declaration of Conformity (DoC) for details of other country markings. This is available at: www.extremenetworks.com

**Note**

Europe includes, Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Operation of the device without regulatory approval is illegal.

Country Selection

Select only the country in which you are using the device. Any other selection will make the operation of this device illegal.

Country Roaming

This device incorporates the International Roaming feature (IEEE802.11d) which will ensure the product operates on the correct channels for the particular country of use.

Frequency of Operation - IC

5 GHz Only

Industry Canada Statement:



Caution

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-Channel mobile satellite systems. High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Avertissement

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

2.4 GHz Only

The available channels for 802.11bg operation in the US are Channels 1 to 11. The range of channels is limited by firmware.

Warnings for Use of Wireless Devices



Caution

Observe all warning notices with regard to the usage of wireless devices.

Potentially Hazardous Atmospheres - Vehicle Installation

You are reminded of the need to observe restrictions on the use of radio devices in fuel depots, chemical plants etc. and areas where the air contains chemicals or particles (such as grain, dust, or metal powders).

Potentially Hazardous Atmospheres - Fixed Installations

You are reminded of the need to observe restrictions on the use of radio devices in fuel depots, chemical plants etc. and areas where the air contains chemicals or particles such as grain, dust, or metal powders.

Safety in Aircraft

Switch off your wireless device whenever you are instructed to do so by airport or airline staff. If your device offers a 'flight mode' or similar feature, consult airline staff as to its use in flight.

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

Wireless devices transmit radio frequency energy and may affect medical electrical equipment.

Wireless devices should be switched off wherever you are requested to do so in hospitals, clinics, or healthcare facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

Pacemakers

Pacemaker manufacturers recommended that a minimum of 15cm (6 inches) be maintained between a handheld wireless device and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with independent research and recommendations by Wireless Technology Research.

Persons with Pacemakers:

- Should ALWAYS keep the device more than 15cm (6 inches) from their pacemaker when turned ON.
- Should not carry the device in a breast pocket.
- Should use the ear furthest from the pacemaker to minimize the potential for interference.
- If you have any reason to suspect that interference is taking place, turn OFF your device.

Other Medical Devices

Consult your physician or the manufacturer of the medical device, to determine if the operation of your wireless product may interfere with the medical device.

RF Exposure Guidelines

Reduce RF Exposure - Use Properly

Only operate the device in accordance with the instructions supplied.

International

The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices. For information on

"International" human exposure to electromagnetic fields refer to [#unique_40/unique_40_Connect_42_SECTION_DOC_EU](#).

The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices.

Europe

Remote and Standalone Antenna Configurations

To comply with EU RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop or similar configurations must operate with a minimum separation distance of from all persons.

US and Canada

Co-located Statement

To comply with FCC RF exposure compliance requirement, the antenna used for this transmitter must not be co-located or operating in conjunction with any other transmitter/antenna except those already approved in this filling.

To satisfy US and Canadian RF exposure requirements, a transmitting device must operate with a minimum separation distance of or more from a person's body.

Pour satisfaire aux exigences Américaines et Canadiennes d'exposition aux radiofréquences, un dispositif de transmission doit fonctionner avec une distance de séparation minimale de ou plus de corps d'une personne.

Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance between the radiator and your body.

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de de distance entre la source de rayonnement et votre corps.

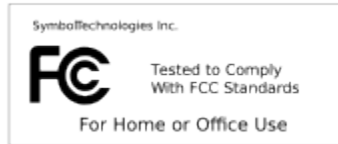
Remote and Standalone Antenna Configurations

To comply with FCC RF exposure requirements, Antennas that are mounted externally must be professionally installed at a fixed location and operate with a minimum distance of from all persons.

To comply with FCC Antenna requirements, the Antenna must be adjusted such that the RF emission lobes are below 30 degrees elevation.

Radio Frequency Interference Requirements

Radio Frequency Interference Requirements - FCC



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.

Radio Transmitters (Part 15)

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.

The equipment shall be subject to professional engineering personnel to install and configure, it just can be used, and may not be sold directly to the general consumer.

Based on 20 cm separation distance to assess the amount of electromagnetic exposure(MPE).

MPE limit 1mW/cm²; Test result is 0.39207 mW/cm²

When using this device, it is recommended to have a separation distance of 20 cm.

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

Canada

For RLAN Devices

The use of 5 GHz RLANs, for use in Canada, have the following restrictions:

- Restricted Band

This device complies with RSS 247 of Industry Canada. 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.

Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Label Marking: The Term "IC:" before the radio certification only signifies that Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

The maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.


In compliance with respective local regulatory law, the AP software provides professional installers the option to configure the antenna type and antenna gain for approved antennas.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (identifier le dispositif par son numéro de certification ou son numéro de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Refer to the Antennas information of this guide for a listing of the 2.4 and 5 GHz antennas initially approved for use with the this AP model.

CE Marking and European Economic Area (EEA)

| | |
|---|--|
|  | WARNING: This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. |
|---|--|

The use of 2.4 GHz RLANS, for use through the EEA, have the following restrictions:

- Maximum radiated transmit power of 100 mW EIRP in the frequency range
- Italy requires a user license for outside usage.

Bluetooth® Wireless Technology for use throughout the EEA has the following restrictions:

- Maximum radiated transmit power of 100 mW EIRP in the frequency range 2.400 - 2.4835 GHz.

Statement of Compliance

Extreme Networks hereby declares that this radio equipment is in compliance with Directive 2011/65/EU and 1999/5/EC or 2014/53/EU (2014/53/EU supersedes 1999/5/EC from 13th June 2017). A Declaration of Conformity may be obtained from www.extremenetworks.com.

Japan (VCCI) - Voluntary Control Council for Interference

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

5.25GHz屋内使用規定 or この製品は屋内においてのみ使用可能です

Korea Warning Statement for Class B ITE

| 기종별 | 사용자안내문 |
|--|---|
| B급 기기 (가정용 방송통신기기) | 이 기기는 가정용 (B급) 으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다. |
| Class B (Broadcasting Communication Device for Home Use) | This device obtained EMC registration mainly for home use (Class B) and may be used in all areas. |

Other Countries

Australia

Use of 5 GHz RLANS in Australia is restricted in the following band: .

Brazil (UNWANTED EMISSIONS - ALL PRODUCTS)

Regulatory declarations for AP-8533I, AP-8533 - BRAZIL

For more information consult the website www.anatel.gov.br.

Nota: A marca de certificação se aplica ao Transceptor, modelo AP-8533. Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário. Para maiores informações sobre ANATEL consulte o site: www.anatel.gov.br.

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Este produto está homologado pela Anatel, de acordo com os procedimentos regulamentados pela Resolução nº242/2000 e atende aos requisitos técnicos aplicados, incluindo os limites de exposição da Taxa de Absorção Específica referente a campos elétricos, magnéticos e eletromagnéticos de radiofrequência, de acordo com as Resoluções nº 303/2002 e 533/2009.

Chile (Devices with a WLAN Radio)

This device complies with the Resolution Not 403 of 2008, of the Undersecretary of telecommunications, relating to electromagnetic radiation.

Este equipo cumple con la Resolución No 403 de 2008, de la Subsecretaria de telecomunicaciones, relativa a radiaciones electromagnéticas.

will comply with Chile's Resolution 755, part j.1) which states that the device is set to operate in the following bands for indoor use only with maximum radiated power not greater than 150 mW:

- 2.400 hasta 2.483,5 MHz
- 5.150 hasta 5.250 MHz
- 5.250 hasta 5.350 MHz
- 5.725 hasta 5.850 MHz

as well as that band 5150-5250 MHz will be restricted to the indoor use and the maximum radiated power density does not exceed 7.5 mW / MHz in any 1 MHz band and 0.1875 mW / 25 kHz in any 25 kHz band.

Conforme a Resolución 755 parte j.1), se ajustará el dispositivo a operar en interiores en las siguientes bandas con una potencia máxima radiada no superior a 150 mW:

- 2.400 hasta 2.483,5 MHz
- 5.150 hasta 5.250 MHz
- 5.250 hasta 5.350 MHz
- 5.725 hasta 5.850 MHz

Además, de acuerdo con Resolución 755, para la banda 5150-5250 MHz la operación del equipo estará restringida al interior de inmuebles y la densidad de potencia radiada máxima no supera 7,5 mW/MHz en cualquier banda de 1MHz y 0.1875 mW/25 kHz en cualquier banda de 25 kHz.

China



Hong Kong

In accordance with HKTA1039, the band is for indoor operation only.

Mexico

Restrict Frequency Range to: .

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

S. Korea

For a radio equipment using , the following two expression should be displayed:

Taiwan

臺灣
 本設備符合國家通訊傳播委員會
 第十二條
 規定之無線電設備之技術規格，其設計、公司、商標或名稱均不得與國家標
 記、商標或名稱相同或相似。
 第十四條
 本設備不得對其他無線電設備造成有害干擾，且應能忍受其他無線電設備之
 有害干擾。本設備之操作不得對其他無線電設備造成有害干擾。
 或本設備之操作不得對其他無線電設備造成有害干擾。
 或本設備之操作不得對其他無線電設備造成有害干擾。

電磁洩露量MP目標值1mW/cm²，本產品符合標準電磁干擾人體：40cm

Turkey

Bu cihaz Türkçe karakterlerin tamamını ihtiva eden ETSI TS 123.038 V8.0.0 (veya sonraki sürümün kodu) ve ETSI TS 123.040 V8.1.0 (veya sonraki sürümün kodu) teknik özelliklerine uygundur.

Ukraine Regulatory Statement

Дане обладнання відповідає вимогам технічного регламенту №1057, № 2008 на обмеження щодо використання деяких небезпечних речовин в електричних та електронних пристроях.

Thailand

เครื่องโทรคมนาคมและอุปกรณ์นี้ มีความสอดคล้องตามข้อกำหนดของ กททช.

Eurasian Customs Union



Waste Electrical and Electronic Equipment



In accordance with Directive 2012/19/EU of the European Parliament on waste electrical and electronic equipment (WEEE):

1. The symbol above indicates that separate collection of electrical and electronic equipment is required.
2. When this product has reached the end of its serviceable life, it cannot be disposed of as unsorted municipal waste. It must be collected and treated separately.
3. It has been determined by the European Parliament that there are potential negative effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment.
4. It is the users' responsibility to utilize the available collection system to ensure WEEE is properly treated.

For information about the available collection system, please contact Extreme Environmental Compliance at Green@extremenetworks.com.

TURKISH WEEE Statement of Compliance

EEE Yönetmeliğine Uygundur

For terminals that support Turkish characters in SMS Release 8 services, the following statement should be printed on the packages and manual of the device:

This device conforms to technical specification in ETSI TS 123.038 V8.0.0 (or the code of any subsequent release) and ETSI TS 123.040 V8.1.0 (or the code of any subsequent release) which contain all Turkish characters.

Bu cihaz Türkçe karakterlerin tamamını ihtiva eden ETSI TS 123.038 V8.0.0 (veya sonraki sürümün kodu) ve ETSI TS 123.040 V8.1.0 (veya sonraki sürümün kodu) teknik özelliklerine uygundur.

End-User Software License Agreement

This document is an agreement (“Agreement”) between You, the end user, and Extreme Networks, Inc., on behalf of itself and its Affiliates (“Extreme”) that sets forth your rights and obligations with respect to the “Licensed Materials”. BY INSTALLING SOFTWARE AND/ OR THE LICENSE KEY FOR THE SOFTWARE (“License Key”) (collectively, “Licensed Software”), IF APPLICABLE, COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE AND/OR ANY OF THE LICENSED MATERIALS UNDER THIS AGREEMENT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE(S) AND THE LIMITATION(S) OF WARRANTY AND DISCLAIMER(S)/LIMITATION(S) OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY (IF APPLICABLE) TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND/OR LICENSED MATERIALS AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT TO ARRANGE FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. “Affiliates” means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. “Server Application” means the software application associated to software authorized for installation (per License Key, if applicable) on one or more of Your servers as further defined in the Ordering Documentation. “Client Application” shall refer to the application to access the Server Application. “Network Device” for purposes of this Agreement shall mean a physical computer device, appliance, appliance component, controller, wireless access point, or virtual appliance as further described within the applicable product documentation, which includes the Order Documentation. “Licensed Materials” means the Licensed Software (including the Server Application and Client Application), Network Device (if applicable), Firmware, media embodying software, and the accompanying documentation. “Concurrent User” shall refer to any of Your individual employees who You provide access to the Server Application at any one time. “Firmware” refers to any software program or code embedded in chips or other media. “Standalone” software is software licensed for use independent of any hardware purchase as identified in the Ordering Documentation. “Licensed Software” collectively refers to the software, including Standalone software, Firmware, Server Application, Client Application or other application licensed with conditional use parameters as defined in the Ordering Documentation. “Ordering Documentation” shall mean the applicable price quotation, corresponding purchase order, relevant invoice, order acknowledgment, and accompanying documentation or specifications for the

products and services purchased, acquired or licensed hereunder from Extreme either directly or indirectly.

2. **TERM.** This Agreement is effective from the date on which You accept the terms and conditions of this Agreement via click-through, commence using the products and services or upon delivery of the License Key if applicable, and shall be effective until terminated. In the case of Licensed Materials offered on a subscription basis, the term of “licensed use” shall be as defined within Your Ordering Documentation.
3. **GRANT OF LICENSE.** Extreme will grant You a non-transferable, non-sublicensable, nonexclusive license to use the Licensed Materials and the accompanying documentation for your own business purposes subject to the terms and conditions of this Agreement End-User Software License Agreement AP-7562 Installation Guide 54 applicable licensing restrictions, and any term, user server networking device, field of use, or other restrictions as set forth in Your Ordering Documentation. If the Licensed Materials are being licensed on a subscription and/or capacity basis, the applicable term and/or capacity limit of the license shall be specified in Your Ordering Documentation. You may install and use the Licensed Materials as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. **YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.**
4. **LICENSE TYPES**
 - **Single User, Single Network Device.** Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials as bundled with a single Network Device as identified by a unique serial number for the applicable Term, if and as specified in Your Ordering Documentation, or any replacement for that network device for that same Term, for internal use only. A separate license, under a separate License Agreement, is required for any other network device on which You or another individual, employee or other third party intend to use the Licensed Materials. A separate license under a separate License Agreement is also required if You wish to use a Client license (as described below).
 - **Single User, Multiple Network Device.** Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials with a defined amount of Network Devices as defined in the Ordering Documentation.
 - **Client.** Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Materials on your server and allow the specific number of Concurrent Users as ordered by you and is set forth in Your Ordering Documentation. A separate license is required for each additional Concurrent User.
 - **Standalone.** Software or other Licensed Materials licensed to You for use independent of any Network Device.
 - **Subscription.** Licensed Materials, and inclusive Software, Network Device or related appliance updates and maintenance services, licensed to You for

use during a subscription period as defined in Your applicable Ordering Documentation.

- Capacity. Under the terms of this license, the license granted to You by Extreme authorizes You to use the Licensed Materials up to the amount of capacity or usage as defined in the Ordering Documentation.
5. **AUDIT RIGHTS.** You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, Extreme reserves the right to charge You for all reasonable expenses related to such audit in addition to any other liabilities and overages applicable as a result of such noncompliance, including but not limited to additional fees for Concurrent Users, excess capacity or usage over and above those specifically granted to You. From time to time, the Licensed Materials may upload information about the Licensed Materials and the associated usage to Extreme. This is to verify the Licensed Materials are being used in accordance with a valid license and/or entitlement. By using the Licensed Materials, you consent to the transmission of this information.
 6. **RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS.** Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, End-User Software License Agreement AP-7562 Installation Guide 55 or reverse engineer the Licensed Materials, including the Licensed Software, or to translate the Licensed Materials into another computer language. The media embodying the Licensed Materials may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.
 7. **TITLE AND PROPRIETARY RIGHTS**
 - a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell,

lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

- b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.
8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme' exclusive property, and You shall use all commercially reasonable efforts to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme' prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so. You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the End-User Software License Agreement AP-7562 Installation Guide 56 Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Materials on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.
9. MAINTENANCE AND UPDATES. Except as otherwise defined below, updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide updates, modifications, or enhancements, or maintenance and support services for the Licensed Materials to You. If you have purchased Licensed Materials on a subscription basis then the applicable service terms for Your Licensed Materials are as provided in Your Ordering Documentation. Extreme will perform the maintenance and updates in a timely and professional manner, during the Term of Your subscription, using qualified and experienced personnel. You will cooperate in good faith with Extreme in the performance of the support services including, but not limited to, providing Extreme with: (a) access to the Extreme Licensed Materials (and related systems); and (b) reasonably requested assistance and information. Further information about the applicable maintenance and updates terms can be found on Extreme's website at www.extremenetworks.com/company/legal/terms-of-support

10. **DEFAULT AND TERMINATION.** In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
- a. Immediately after any termination of the Agreement, Your licensed subscription term, or if You have for any reason discontinued use of Licensed Materials, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Materials, including an Licensed Software, from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
 - b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. **EXPORT REQUIREMENTS.** You are advised that the Licensed Materials, including the Licensed Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Licensed Materials, including the Licensed Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The Licensed Materials (i) were developed solely at private expense; (ii) contain “restricted computer software” End-User Software License Agreement AP-7562 Installation Guide 57 submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.
13. **LIMITED WARRANTY AND LIMITATION OF LIABILITY.** Extreme warrants to You that (a) the initially-shipped version of the Licensed Materials will materially conform to the Documentation; and (b) the media on which the Licensed Software is recorded will be free from material defects for a period of ninety (90) days from the date of delivery to You or such other minimum period required under applicable law. Extreme does not warrant that Your use of the Licensed Materials will be error-free or uninterrupted. NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR

FIRM ARE VOID. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS. Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
15. FREE AND OPEN SOURCE SOFTWARE. Portions of the Software (Open Source Software) provided to you may be subject to a license that permits you to modify these portions and redistribute the modifications (an Open Source License). Your use, modification and redistribution of the Open Source Software are governed by the terms and conditions of the applicable Open Source License. More details regarding the Open Source Software and the applicable Open Source Licenses are available at www.extremenetworks.com/services/SoftwareLicensing.aspx. Some of the Open Source software may be subject to the GNU General Public License v.x (GPL) or the Lesser General Public Library (LGPL), copies of which are provided with the Licensed Materials End-User Software License Agreement AP-7562 Installation Guide 58 and are further available for review at www.extremenetworks.com/services/SoftwareLicensing.aspx, or upon request as directed herein. In accordance with the terms of the GPL and LGPL, you may request a copy of the relevant source code. See the Software Licensing web site for additional details. This offer is valid for up to three years from the date of original download of the software.
16. GENERAL
- a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
 - b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
 - c. You represent that You have full right and/or authorization to enter into this Agreement.
 - d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme' assignees, licensors, and licensees.

- e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
- f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
- g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
- h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.

6480 Via Del Oro

San Jose, CA 95119, USA

Tel: +1 408-579-2800

Toll-free: +1 888-257-3000



Glossary

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *[IBSS \(Independent Basic Service Set\)](#)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management

systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at <http://www.extremenetworks.com/product/data-center-connect/>.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. (See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the *Extreme Management Center* software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at <http://www.extremenetworks.com/product/extreme-access-control/>.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at <http://www.extremenetworks.com/product/extremeanalytics/>.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at <http://www.extremenetworks.com/product/management-center/>.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at <http://www.extremenetworks.com/product/extremecloud/>.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at <http://www.extremenetworks.com/products/switching-routing/>.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at <http://www.extremenetworks.com/products/wireless/>.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at <http://www.extremenetworks.com/product/extremexos-network-operating-system/>.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token

Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2).
(See also [EAP-TLS/EAP-TTLS](#).)

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)



Index

C

conventions
 notice icons 5
 text 5

D

documentation
 feedback 6
 location 7

G

guidelines, RF Exposure 43

O

Open Source Declaration 7

R

requirements, RF Interference 45

S

support, *see* technical support

T

technical support
 contacting 6