



Wireless Access Point (WAP) Mini-PIM Installation Guide



Modified: 2019-08-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Wireless Access Point (WAP) Mini-PIM Installation Guide
Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Using the Examples in This Manual	ix
	Merging a Full Example	x
	Merging a Snippet	x
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiv
	Creating a Service Request with JTAC	xiv
Chapter 1	WAP Mini-Physical Interface Module (Mini-PIM)	15
	WAP Mini-Physical Interface Module	15
	Front Panel	16
	WAP Mini-PIM Models	17
	Physical Interface	17
	WAP Mini-PIM Hardware Specifications	18
	WAP Mini-PIM Specifications	18
	Antenna Specifications	18
	Channels and Frequencies Supported on the WAP Mini-PIM	19
Chapter 2	Installation and Configuration	25
	Installing the WAP Mini-PIM in an SRX Series Services Gateway	25
	Configuring the WAP Mini-PIM	28
	Access Point Configuration Overview	28
	Radio Configuration Overview	29
	Virtual Access Point Configuration Overview	30
	Configuring the WAP Mini-PIM	31
	Upgrading the Firmware on the WAP Mini-PIM	33
Chapter 3	Safety and Compliance Information	35
	Regulatory and Safety Information for the WAP Mini-PIM	35
	FCC	35
	FCC Caution	35
	FCC Radiation Exposure Statement	36
	Users Manual of the End Product	36
	Label of the End Product	36
	Industry Canada Statement	37
	CE	39
	Japan Statement	40
	Agency Approvals and Compliance Information	40

List of Figures

Chapter 1	WAP Mini-Physical Interface Module (Mini-PIM)	15
	Figure 1: WAP Mini-PIM Front Panel	16
	Figure 2: WAP Mini-PIM Front Panel LEDs	17
Chapter 2	Installation and Configuration	25
	Figure 3: Installing the WAP Mini-PIM	26
	Figure 4: Attaching the Antennas (Direct Mounting)	26
	Figure 5: Attaching the Antennas Using an Antenna Base (Rack Mounting)	27
	Figure 6: Attaching the Antennas Using an Antenna Base (Wall Mounting)	28

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	xi
	Table 2: Text and Syntax Conventions	xii
Chapter 1	WAP Mini-Physical Interface Module (Mini-PIM)	15
	Table 3: WAP Mini-PIM Front Panel Components	16
	Table 4: WAP Mini-PIM Front Panel LEDs	17
	Table 5: WAP Mini-PIM Models	17
	Table 6: WAP Mini-PIM Hardware Specifications	18
	Table 7: Specifications for the WAP Mini-PIM Antenna	18
	Table 8: Channels Supported on the 2.4 GHz Radio (20 MHz Bandwidth)	20
	Table 9: Channels Supported on the 2.4 GHz Radio (40 MHz Bandwidth)	20
	Table 10: Channels Supported on the 5 GHz Radio (20 MHz Bandwidth)	21
	Table 11: Channels Supported on the 5 GHz Radio (40 MHz Bandwidth)	22
	Table 12: Channels Supported on the 5 GHz Radio (80 MHz Bandwidth)	23
Chapter 2	Installation and Configuration	25
	Table 13: Supported Modes	29

About the Documentation

- Documentation and Release Notes on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xsl;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	- Introduces or emphasizes important new terms. - Identifies guide names. - Identifies RFC and Internet draft titles.	- A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> - RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	- To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. - The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

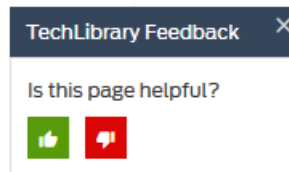
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	- In the Logical Interfaces box, select All Interfaces. - To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

CHAPTER 1

WAP Mini-Physical Interface Module (Mini-PIM)

- [WAP Mini-Physical Interface Module on page 15](#)
- [WAP Mini-PIM Hardware Specifications on page 18](#)
- [Channels and Frequencies Supported on the WAP Mini-PIM on page 19](#)

WAP Mini-Physical Interface Module

The Wireless Access Point (WAP) mini-PIM for SRX devices provides a single box wireless access point solution for retail and small office deployments. The mini-PIM has an embedded Enterprise class wireless system-on-chip (SOC) and supports the 802.11 a, g, ac, and Wave 2 wireless standards.

Key features include:

- 2x2 multiuser—multiple input, multiple output (MU-MIMO), which enables transmission of data to multiple clients simultaneously.
- Dual radios providing concurrent dual bands of 2.4 GHz and 5 GHz—The radios operate in any one of the radio modes, such as 802.11a or 802.11g, specified by the IEEE wireless networking standards. Each radio can be configured independently. The radio mode determines what type of wireless clients can connect to the access point. The radio on the access point can be configured to support just one type of client or a mixed mode, where different types of clients can connect to the radio.
- Up to eight Virtual Access Points (VAPs) per radio—A VAP simulates a physical access point. VAPs allow the wireless LAN to be segmented into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. A single AP is segregated into multiple individual VAPs simulating multiple APs in a single system.

You can configure up to 8 VAPs on each radio.

- Software configurable transmit power—The access point allows for configuration of transmit power for each radio. Transmit power assignment is done on a percentage basis. By default, the access point assigns 100 percent power to each radio at startup to give maximum coverage and potentially reduce the number of access points required.
- Wireless security for client authentication—The access point supports the following authentication methods:

- Wi-Fi Protected Access (WPA) Personal, that includes Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) with preshared key authentication.
- WPA Enterprise, that includes AES-CCMP and TKIP with RADIUS server authentication.
- MAC authentication, where wireless clients are allowed or denied network access based on their MAC address.

The WAP mini-PIM is supported on the SRX320, SRX340, SRX345, and SRX550M devices and can coexist with the other mini-PIMs supported on these devices.

Front Panel

Figure 1 on page 16 shows the front panel of the WAP mini-PIM.

Figure 1: WAP Mini-PIM Front Panel

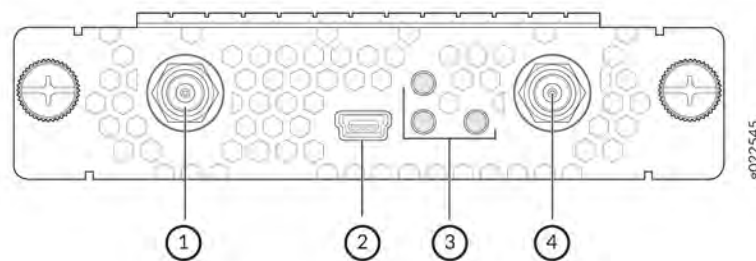


Table 3 on page 16 lists the components on the front panel.

Table 3: WAP Mini-PIM Front Panel Components

Sl. No.	Component	Description
1, 4	Antenna connectors	Two Reverse Polarity SubMiniature version A (RP-SMA) connectors
2	Console	Mini-USB Type-B port for monitoring and troubleshooting
3	LEDs	Indicate the status of the mini-PIM at a glance

Figure 2 on page 17 shows the front panel LEDs.

Figure 2: WAP Mini-PIM Front Panel LEDs

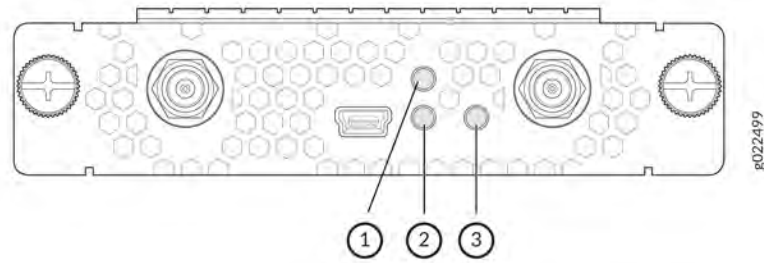


Table 4: WAP Mini-PIM Front Panel LEDs

Sl. No.	Component	Description
1	2.4 GHz	• Solid green—2G WLAN connection is established • Blinking green—Data activity
2	5 GHz	• Solid green—5G WLAN connection is established • Blinking green—Data activity
3	STATUS	• Solid green—The mini-PIM is operational • Blinking green—Powering on or running diagnostics

WAP Mini-PIM Models

There are three models based on the regional wireless standards.

Table 5: WAP Mini-PIM Models

Model	Supported Region	Notes
SRX-MP-WLAN-US	United States	This model is based on the wireless standards supported in the United States. The country code is fixed and cannot be changed.
SRX-MP-WLAN-IL	Israel	This model is based on the wireless standards supported in Israel. The country code is fixed and cannot be changed.
SRX-MP-WLAN-WW	Other countries	You can set the country code using the command, set wlan access-point <i>ap-name</i> access-point-options country <i>country code</i>

Physical Interface

The physical interface for the WAP mini-PIM uses the name `wl-x/0/0`, where `x` identifies the slot on the services gateway where the mini-PIM is installed. You can insert the mini-PIM in any of the mini-PIM slots on the services gateway.

WAP Mini-PIM Hardware Specifications

WAP Mini-PIM Specifications

Table 6 on page 18 provides the hardware specifications for the mini-PIM.

Table 6: WAP Mini-PIM Hardware Specifications

Description	Value
Dimensions(H x W x L)	0.79 in. x 3.70 in. x 5.29 in. (2.0 cm x 9.4 cm x 13.43 cm)
Weight	0.29 lb (0.13 kg)
Form factor	Mini-PIM
Connector type	RP-SMA
Environmental operating temperature	32° F through 104° F (0° C through 40° C)
Storage temperature	-40° F through 158° F (-40° C through 70° C)
Relative humidity	5% to 90% noncondensing

Antenna Specifications

The mini-PIM supports two multi-band swivel-mount dipole antennas, which can be rotated 360°. You can rotate the antennas and select the angle at which the signal strength is high. Table 7 on page 18 lists the specifications for the antenna.

Table 7: Specifications for the WAP Mini-PIM Antenna

Specification	Value
Part number	EDA-1713-25GR2-A3 (Vendor: MAG.LAYERS)
Operating frequency range	• 2.4~2.5 GHz • 5.15~5.85 GHz
Impedance	50 ohm
Voltage Standing Wave Ratio (VSWR)	2 (maximum)
Return loss	10 dB (maximum)
Radiation	Omnidirectional
Peak gain	5dBi +/-0.5

Table 7: Specifications for the WAP Mini-PIM Antenna (continued)

Specification	Value
Polarization	Linear
Operating temperature	–4° F (–20° C) to 149° F (65° C)
Connector type	RP-SMA

Channels and Frequencies Supported on the WAP Mini-PIM

The WAP mini-PIM supports channel bandwidths of 20 MHz, 40 MHz, and 80 MHz. You can configure the bandwidth by using the command **set wlan access-point *ap-name* radio [1|2] radio-option channel bandwidth *bandwidth***



NOTE: You can configure the 80 MHz channel bandwidth only on the 5 GHz radio.

The default channel bandwidth is 20 MHz. Setting the bandwidth to 40 MHz or 80 MHz reduces the number of available channels for use.

[Table 8 on page 20](#) and [Table 9 on page 20](#) list the channels supported on the 2.4 GHz radio.

Table 8: Channels Supported on the 2.4 GHz Radio (20 MHz Bandwidth)

Band	Channel Number	Center Frequency (MHz)
2400~2483.5 MHz	1	2412
	2	2417
	3	2422
	4	2427
	5	2432
	6	2437
	7	2442
	8	2447
	9	2452
	10	2457
	11	2462
	12	2467
	13	2472

Table 9: Channels Supported on the 2.4 GHz Radio (40 MHz Bandwidth)

Band	Channel Number	Center Frequency (MHz)
2400~2483.5 MHz	3	2422
	4	2427
	5	2432
	6	2437
	7	2442
	8	2447
	9	2452
	10	2457
	11	2462

Table 10 on page 21 through Table 12 on page 23 list the channels supported on the 5 GHz radio.

Table 10: Channels Supported on the 5 GHz Radio (20 MHz Bandwidth)

Band	Channel Number	Frequency
5150~5250 MHz	36	5180
	40	5200
	44	5220
	48	5240
5250~5350 MHz	52	5260
	56	5280
	60	5300
	64	5320

Table 10: Channels Supported on the 5 GHz Radio (20 MHz Bandwidth) (continued)

Band	Channel Number	Frequency
5470~5725 MHz	100	5500
	104	5520
	108	5540
	112	5560
	116	5580
	120	5600
	124	5620
	128	5640
	132	5660
	136	5680
	140	5700
5725~5850 MHz	144	5720
	149	5745
	153	5765
	157	5785
	161	5805
	165	5825

Table 11: Channels Supported on the 5 GHz Radio (40 MHz Bandwidth)

Band	Channel Number	Frequency
5150~5250 MHz	38	5190
	46	5230
5250~5350 MHz	54	5270
	62	5310

Table 11: Channels Supported on the 5 GHz Radio (40 MHz Bandwidth) (continued)

Band	Channel Number	Frequency
5470~5725 MHz	102	5510
	110	5550
	118	5590
	126	5630
	134	5670
5725~5850 MHz	142	5710
	151	5755
	159	5795

Table 12: Channels Supported on the 5 GHz Radio (80 MHz Bandwidth)

Band	Channel Number	Frequency
5150~5250 MHz	42	5210
5250~5350 MHz	58	5290
5470~5725 MHz	106	5530
	122	5610
5725~5850 MHz	138	5690
	155	5775

CHAPTER 2

Installation and Configuration

- Installing the WAP Mini-PIM in an SRX Series Services Gateway on page 25
- Configuring the WAP Mini-PIM on page 28
- Upgrading the Firmware on the WAP Mini-PIM on page 33

Installing the WAP Mini-PIM in an SRX Series Services Gateway

To install the WAP Mini-PIM in a services gateway:



NOTE: You can install only one Mini-PIM in a services gateway. The Mini-PIM can be installed in any of the Mini-PIM slots on the services gateway.

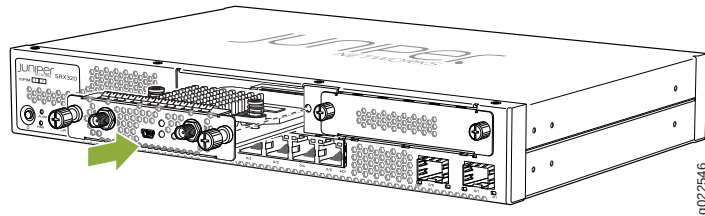
1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the grounding point on the back of the services gateway.
2. Power off the services gateway by briefly pressing the **Power** button on the front panel. Wait for the **Power** LED to turn off before proceeding. Disconnect the services gateway from the power source.
3. Remove the blank mini-PIM installed on the services gateway:
 - a. Loosen the screws on the faceplate of the blank Mini-PIM.
 - b. Grasp the screws on each side and remove the blank Mini-PIM.
4. Remove the mini-PIM from the electrostatic bag.
5. Grasp the screws on each side of the mini-PIM faceplate and align the notches in the connector at the rear of the mini-PIM with the notches in the mini-PIM slot in the services gateway.



CAUTION: Slide the mini-PIM straight into the slot to avoid damaging the components on the mini-PIM.

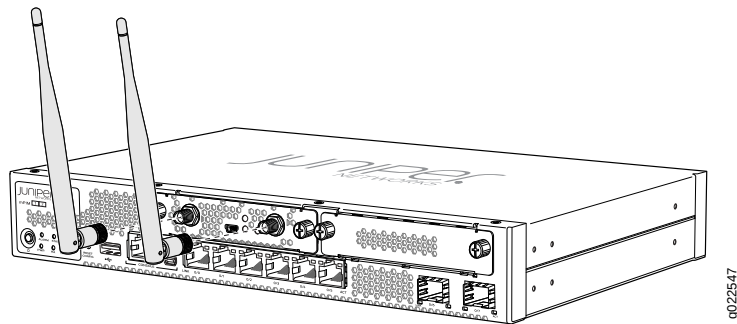
6. Slide the mini-PIM in until it lodges firmly in the services gateway. See [Figure 3 on page 26](#).

Figure 3: Installing the WAP Mini-PIM



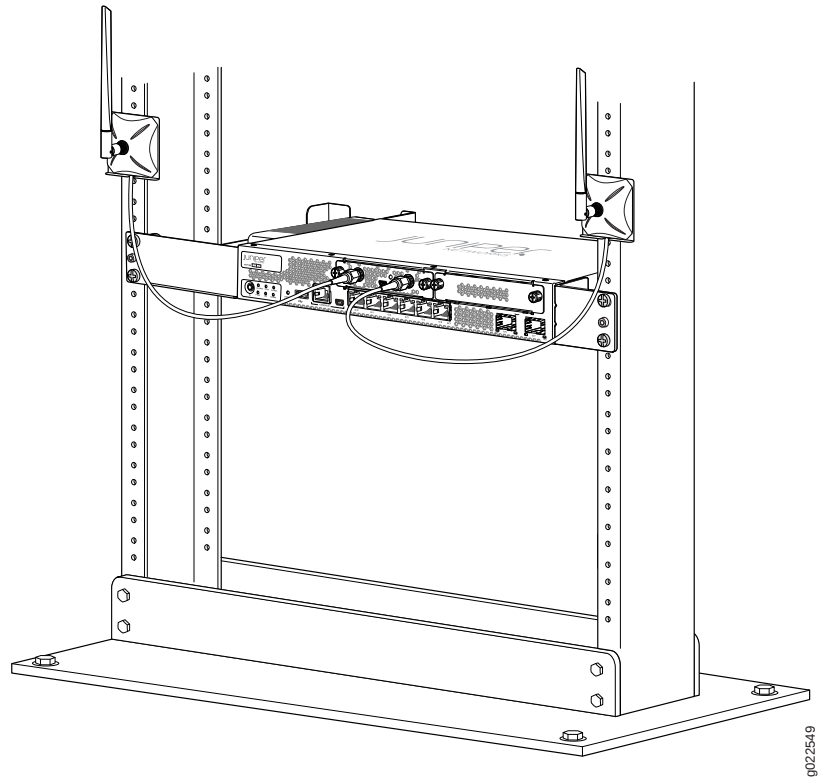
7. Using a 1/8-in. (3-mm) flat-blade (–) screwdriver, tighten the screws on each side of the Mini-PIM faceplate.
8. Attach the antennas to the front panel. You can attach the antenna by using one of the following methods:
 - Direct mounting—Attach the antennas to the RP-SMA connectors on the front panel of the mini-PIM.

Figure 4: Attaching the Antennas (Direct Mounting)



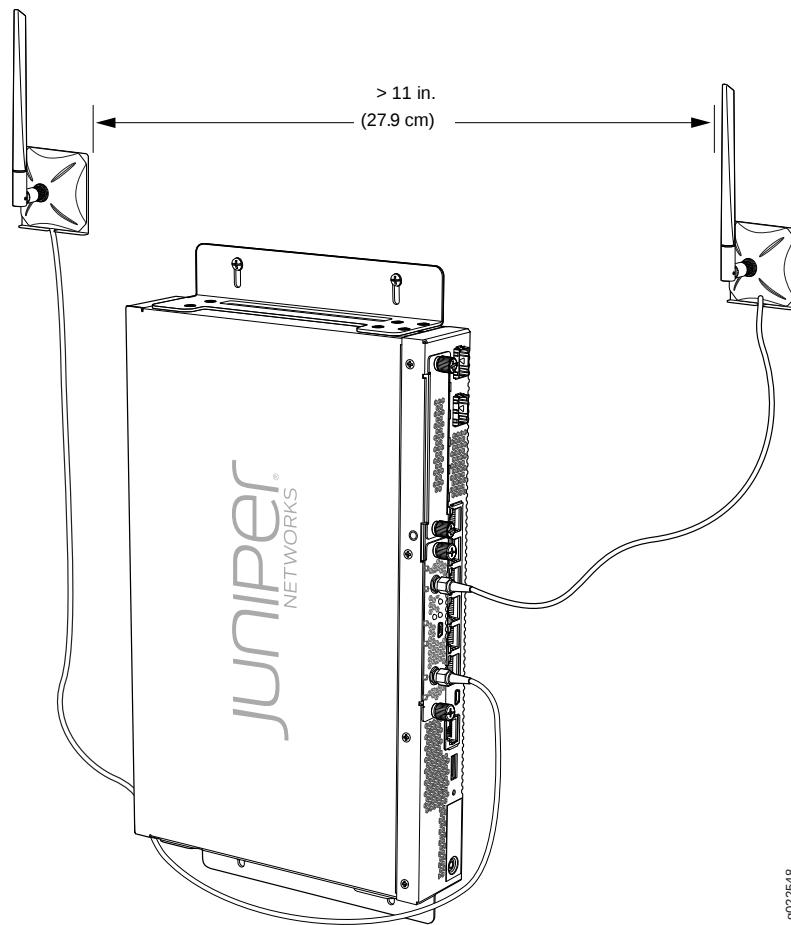
- Using an antenna base—Attach the antennas to the antenna base. Connect the cables from each antenna base to the RP-SMA connectors on the front panel.

Figure 5: Attaching the Antennas Using an Antenna Base (Rack Mounting)



For SRX320 Services Gateways, which can be mounted on a wall, the antennas can be mounted as shown in [Figure 6 on page 28](#).

Figure 6: Attaching the Antennas Using an Antenna Base (Wall Mounting)



9. Power on the services gateway.

Related Documentation

Configuring the WAP Mini-PIM

- [Access Point Configuration Overview on page 28](#)
- [Radio Configuration Overview on page 29](#)
- [Virtual Access Point Configuration Overview on page 30](#)
- [Configuring the WAP Mini-PIM on page 31](#)

Access Point Configuration Overview

Before proceeding with the configuration, configure the network settings on the SRX Series device and connect the device to your network. For details, see the Hardware Guide for your SRX Series device.

Configure the following options for the Access Point (AP):

- Name for the AP
- Interface—The interface name for the AP is denoted as wl-x/0/0, where x is the slot on the services gateway in which the interface module is installed.
- Country code—The country code setting identifies the regulatory domain in which the access point operates. The country code affects the radio modes, list of channels, and radio transmission power that the access point can support. Make sure you select the correct code for the country in which the access point operates so that the access point complies with the regulations in that country.
- Location
- MAC address

Radio Configuration Overview

The mini-PIM supports dual radios, each of which can be configured independently. A radio can operate in any one of the radio modes specified by IEEE wireless networking standards such as 802.11a, 802.11g, or 802.11n. The radio mode determines what type of wireless clients can connect to the access point. You can configure the radio to support only one type of wireless client or a mixed mode, where different types of clients can connect to the radio.

Radios on the access point are enabled by default. You can disable a radio. When a radio is disabled, the access point does not send messages to the connected wireless clients.

Configure the following options for each radio:

- Channel number—If you select auto, then the access point chooses the channel automatically.
- Mode—The radio mode determines the types of wireless clients that can connect to the access point. You can configure the radio to support only one type of wireless client or a mixed mode, where different types of clients can connect to the radio.

[Table 13 on page 29](#) lists the modes supported on each radio.

Table 13: Supported Modes

Radio	Supported Modes
Radio 1 (5.0 GHz)	• an—802.11a and 802.11n clients operating on 5 GHz frequency can connect to the access point • ac—Only 802.11ac Wave 1 clients can connect to the access point • an+ac—802.11a, 802.11n and 802.11ac clients operating on 5 GHz frequency can connect to the access point
Radio 2 (2.4 GHz)	• gn—802.11g, and 802.11n clients operating in 2.4 GHz frequency can connect to the access point. This is the default mode for this radio.

- Bandwidth—Radio 1 supports 20 MHz, 40 MHz, and 80 MHz bandwidths, whereas Radio 2 supports only 20 MHz and 40 MHz bandwidths.
- Transmit power—You can configure transmit power on a per radio basis. By default, the access point assigns 100% power to each radio at startup.

To increase capacity of the network, place access points closer together and reduce the value of the transmit power. This helps reduce overlap and interference among access points. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.

Virtual Access Point Configuration Overview

A virtual access point (VAP) simulates a physical access point. VAPs allow the wireless LAN to be segmented into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. A single AP is segregated into multiple individual virtual APs simulating multiple APs in a single system.

VAPs allow different security mechanisms for different clients on the same access point. VAPs also provide better control over broadcast and multicast traffic, which can help avoid a negative performance impact on a wireless network. Each VAP is identified by a configured Service Set Identifier (SSID) and a unique Basic Service Set Identifier (BSSID). The AP supports multiple VLANs, which can be distributed across VAPs and radios.

Each virtual access point can be independently enabled or disabled with the exception of VAP 0 on each radio. VAP 0 is the physical radio interface and is always enabled. To disable operation of VAP 0, the radio itself must be disabled. VAP 0 is assigned to the BSSID of the physical radio interface. *Reviewer: Please confirm if this is accurate.*

A VAP is configured on a per-radio basis. You can configure up to 8 VAPs per radio. Configure the following options for each VAP:

- Description (maximum length is 64)
- SSID value for the VAP. The maximum length is 32. The SSID value can include only letters, numerals, and the special characters . - _ @ #.
- VLAN ID for the VAP. The value can range from 1 to 4094. The default value is 1.
- The maximum number of clients that can connect to the VAP. The value can range from 1 to 127.
- Security for the AP. The AP supports several types of authentication methods that are used by clients to connect to the access point. Each of these methods and their associated parameters is configurable on a per VAP basis. By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN. You configure secure wireless client access for each VAP.
- None—The data transferred between clients and the access point is not encrypted. This method allows clients to associate with the access point without any authentication.

- Wi-Fi Protected Access (WPA) Enterprise—A Wi-Fi Alliance standard that uses RADIUS server authentication with Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) cipher suites. This mode allows for use of high security encryption along with centrally managed user authentication. Both WPA and WPA2 standards are supported.
- Wi-Fi Protected Access (WPA) Personal—A Wi-Fi Alliance standard that uses preshared key authentication with Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) and Temporal Key Integrity Protocol (TKIP) cipher suites. Both WPA and WPA2 standards are supported.

Configuring the WAP Mini-PIM

To configure the WAP interface module:

1. Configure the access point settings:

- a. Configure the interface:

```
user@host# set wlan access-point name interface wl-x/0/0
```

- b. Set the country code (applicable only for SRX-MP-WLAN-WW models):



NOTE: You cannot set the country code for the SRX-MP-WLAN-US and SRX-MP-WLAN-IL models.

If you do not set the country code for the SRX-MP-WLAN-WW models, the interface module considers the country code as US.

```
user@host# set wlan access-point name access-point-options country country-code
```

- c. Set the location:

```
user@host# set wlan access-point name location location
```

- d. Configure the MAC address:

```
user@host# set wlan access-point name mac-address mac-address
```

- e. Commit the configuration:

```
user@host# commit
```

2. Configure the radio settings. Note that radio 1 operates at 5.0 GHz and radio 2 operates at 2.4 GHz.



NOTE: Applying changes to radio settings can cause the access point to stop and restart system processes. If this happens, wireless clients that are connected to the access point will temporarily lose connectivity. We recommend that you change radio settings when WLAN traffic is low.

- a. Configure the radio mode:

```
user@host# set wlan access-point name radio [1|2] radio-options mode [can|an|gn]
```

- b. Configure the channel number and bandwidth. The default channel bandwidth is 20 MHz.

```
user@host# set wlan access-point name radio [1|2] radio-options channel number number channel bandwidth [20|40|80]
```

- c. Configure the transmit power:

```
user@host# set wlan access-point name radio [1|2] radio-options transmit-power percent
```

- d. Commit the configuration:

```
user@host# commit
```

3. Configure the virtual access point (VAP) settings.

- a. Enter an ID and description for the VAP:

```
user@host# set wlan access-point name virtual-access-point id description
```

- b. Enter the SSID value:

```
user@host# set wlan access-point name virtual-access-point id ssid ssid
```

- c. Configure the security authentication method for the VAP. You can select any of the following options:

- None-The data transferred between clients and the access point is not encrypted. Clients can associate with the access point without any authentication.

```
user@host# set wlan access-point name virtual-access-point id security none
```

- wpa-enterprise-The device authenticates through an 802.1X-compliant RADIUS server

```
user@host# set wlan access-point name virtual-access-point id security wpa-enterprise cipher-suites[ccmp|tkip-ccmp] radius-server ip-address radius-port port radius-key secret-key wpa-version [v1-v2|v2]
```

- wpa-personal-The device uses preshared keys (PSKs) or a passphrase for authentication and encryption. Keys are stored on the device and on all wireless clients. You do not need to configure a separate authentication server.

```
user@host# set wlan access-point name virtual-access-point id security wpa-personal cipher-suites[ccmp|tkip-ccmp] key[ascii|hex] key wpa-version [v1-v2|v2]
```

- d. Specify the upload and download rate limits:

```
user@host# set wlan access-point name virtual-access-point id upload-limit upload-limit-rate download-limit download-limit-rate
```

- e. Specify the maximum number of clients that can be connected to the VAP:

```
user@host# set wlan access-point name virtual-access-point id maximum-stations
number
```

- f. Commit the configuration:

```
user@host# commit
```

See Also •

Upgrading the Firmware on the WAP Mini-PIM

To upgrade the firmware on the Mini-PIM, using the CLI:

1. Identify the currently installed firmware version and new firmware version available for upgrade:

```
user@host > show system firmware
```

Part	Type	Tag	Current version	Available version	Status
FPC 1					
PIC 0	MWAP_FW	1	1.1.2	0	OK
Routing Engine 0	RE BIOS	0	3.1	3.6	OK
Routing Engine 0	RE BIOS Backup	1	3.1	3.6	OK

- a. If the **Available Version** field in the output does not list any information, it indicates that the device is not running the latest jfirmware. Proceed to Step 2 to download and upgrade to the latest jfirmware.
 - b. If the **Available Version** field in the output lists the firmware version, proceed to Step 4.
2. Download the appropriate jfirmware version from <https://www.juniper.net/support/downloads/?p=junos-srx#sw:>



NOTE: Ensure that the Junos OS version installed on the device is the same as the jfirmware version or higher. To know the Junos OS version, issue the `show version` command.

```
user@host > request system software add var/tmp/jfirmware-<version>-signed.tgz
```

3. Verify the new firmware version available:

```
user@host > show system firmware
```

The version is displayed under the **Available Version** field in the output.

4. Upgrade the firmware on the device:

```
user@host > request system firmware upgrade pic pic-slot <pic-slot-number> fpc-slot  
<fpc-slot-number>
```

5. Verify the successful completion of the firmware upgrade. The status should show **Upgraded Successfully**.

```
user@host > show system firmware
```

6. Take the FPC offline and then bring it online:

- a. Take the FPC offline:

```
user@host > request chassis pic pic-slot <pic-slot-number> fpc-slot  
<fpc-slot-number> offline
```

- b. Verify that the FPC is offline:

```
user@host > show chassis fpc pic-status <fpc-slot-number>
```

```
user@host > show chassis fpc pic-status 2
```

- c. Bring the FPC online:

```
user@host > request chassis pic pic-slot <pic-slot-number> fpc-slot  
<fpc-slot-number> online
```

- d. Verify that the FPC is online:

```
user@host > show chassis fpc pic-status <fpc-slot-number>
```

```
user@host > show chassis fpc pic-status 2
```

Slot 2	Online	FPC
PIC 0	Online	WAP for US mPIM

7. Verify that the firmware is upgraded to the latest version:

```
user@host > show system firmware
```

Related •
Documentation

CHAPTER 3

Safety and Compliance Information

- [Regulatory and Safety Information for the WAP Mini-PIM on page 35](#)
- [Agency Approvals and Compliance Information on page 40](#)

Regulatory and Safety Information for the WAP Mini-PIM

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 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

FCC Caution

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

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

For products available in the USA/Canada markets, only channels 1–11 can be operated. Selection of other channels is not possible.

FCC Radiation Exposure Statement

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

This module is intended for OEM integrator. This module is only FCC authorized for the specific rule parts listed on the grant, and that the host product manufacturer is responsible for compliance to any other FCC rules that apply to the host not covered by the modular transmitter grant of certification. The final host product still requires Part 15 Subpart B compliance testing with the modular transmitter installed. Additional testing and certification may be necessary when multiple modules are used.

Users Manual of the End Product

In the users manual of the end product, the end user has to be informed to keep at least 20 cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied.

The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

This device complies with Part 15 of 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.

Label of the End Product

The final end product must be labeled in a visible area with the following " Contains TX FCC ID: QZEMPWAPUS ".

This device complies with Part 15 of 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.

Industry Canada Statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- For product available in the USA/Canada market, only channels 1–11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

- Dynamic Frequency Selection (DFS) for devices operating in the bands 5250–5350 MHz, 5470–5600 MHz and 5650–5725 MHz.

Sélection dynamique de fréquences (DFS) pour les dispositifs fonctionnant dans les bandes 5250–5350 MHz, 5470–5600 MHz et 5650–5725 MHz.

- This device and its antenna(s) must not be co-located with any other transmitters except in accordance with IC multi-transmitter product procedures. Referring to the multi-transmitter policy, multiple-transmitter(s) and module(s) can be operated simultaneously without reassessment permissive change.

Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

- The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

les dispositifs fonctionnant dans la bande 5150–5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

- The maximum antenna gain permitted for devices in the bands 5250–5350 MHz and 5470–5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.

le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250–5350 MHz et 5470–5725 MHz doit se conformer à la limite de p.i.r.e.

- The maximum antenna gain permitted for devices in the band 5725–5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate.

le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725–5850 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

- For indoor use only.

Pour une utilisation en intérieur uniquement

- This radio transmitter [4558A-MPWAPUS] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Cet émetteur radio [4558A-MPWAPUS] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes énumérés ci-dessous, avec le gain maximal admissible indiqué. Les types d'antenne non inclus dans cette liste et dont le gain est supérieur au gain maximal indiqué pour l'un des types répertoriés ne sont strictement pas autorisés pour une utilisation avec cet appareil.

Antenna Information:

Model Name	Antenna Type	Connector	Gain (dBi)	Remark
EDA-1713-25G R2-A3	Dipole Antenna	Reversed-SMA	5.5	2.4 GHz
EDA-1713-25G R2-A3	Dipole Antenna	Reversed-SMA	5.5	5 GHz

- IC Radiation Exposure Statement

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

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 20 cm de distance entre la source de rayonnement et votre corps.

- IMPORTANT NOTE

This module is intended for OEM integrator. The OEM integrator is responsible for the compliance to all the rules that apply to the product into which this certified RF module is integrated. Additional testing and certification may be necessary when multiple modules are used.

NOTE IMPORTANTE:

Ce module est destiné à l'intégrateur OEM. L'intégrateur OEM est responsable de la conformité à toutes les règles applicables au produit dans lequel ce module RF certifié est intégré. Des tests et une certification supplémentaires peuvent être nécessaires lorsque plusieurs modules sont utilisés.

- USERS MANUAL OF THE END PRODUCT

In the users manual of the end product, the end user has to be informed to keep at least 20 cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the IC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied.

MANUEL UTILISATEUR DU PRODUIT FINAL:

Dans le manuel d'utilisation du produit final, l'utilisateur final doit être informé de la nécessité de maintenir une distance d'au moins 20 cm avec l'antenne pendant l'installation et l'utilisation du produit final. L'utilisateur final doit être informé que les consignes d'IC relatives à l'exposition aux fréquences radioélectriques pour un environnement non contrôlé peuvent être satisfaites.

The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. Operation is subject to the following two conditions: (1) this device may not cause harmful interference (2) this device must accept any interference received, including interference that may cause undesired operation.

L'utilisateur final doit également être informé du fait que tout changement ou modification non expressément approuvé par le fabricant pourrait annuler son droit d'utiliser cet équipement. Son utilisation est soumise aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférences nuisibles (2) cet appareil doit accepter toutes les interférences reçues, y compris celles pouvant entraîner un fonctionnement indésirable.

- LABEL OF THE END PRODUCT

The final end product must be labeled in a visible area with the following " Contains IC: 4558A-MPWAPUS ".

The Host Model Number (HMN) must be indicated at any location on the exterior of the end product or product packaging or product literature which shall be available with the end product or online.

ETIQUETTE DU PRODUIT FINAL

Le produit final doit être étiqueté de manière visible dans la zone "Contient le composant IC: 4558A-MPWAPUS".

Le numéro de modèle de l'hôte (HMN) doit être indiqué à n'importe quel endroit à l'extérieur du produit final ou de l'emballage du produit final ou de la documentation sur le produit, qui doit être disponible avec le produit final ou en ligne.

CE

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

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80)

The frequency and the maximum transmitted power in EU are listed below:

- 2412-2472 MHz: 19.99 dBm
- 5180-5240 MHz: 22.97 dBm

- 5260-5320 MHz: 22.91 dBm
- 5500-5700 MHz: 28.16 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.



AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK

Japan Statement

5 GHz band (W52, W53): Indoor use only

Agency Approvals and Compliance Information

The interface module complies with the following standards:

- Safety
 - CAN/CSA-C22.2 No. 60950-1 Information Technology Equipment - Safety
 - CAN/CSA C22.2 No. 62368-1-2014, Audio/Video, Information and Communication Technology Equipment – Safety
 - UL 60950-1 (2nd Edition) Information Technology Equipment - Safety
 - UL 62368-1, Audio/Video, Information and Communication Technology Equipment – Safety
 - IEC 60950-1: 2005/ A2:2013 Information Technology Equipment - Safety (All country deviations): CB Scheme
 - IEC 62368-1: 2014 Audio/Video, Information and Communication Technology Equipment – Safety CB Scheme
 - EN 60950-1: 2006/ A2:2013 Information Technology Equipment
- EMC Emissions
 - EN55022 / CISPR22
 - EN55032/CISPR 32
 - CFR 47 Part 15
 - ICES003
 - VCCI-V-3
 - AS/NZS CISPR22
 - AS/NZS CISPR 32

- AS/NZS 2772.2
- AS/NZS 4268
- EN300-386
- EN61000-3-2
- EN61000-3-3
- EN61000-6-1
- United States
 - FCC 15.247 (2.4 GHz and 5 GHz)
 - FCC 15.407 (5 GHz) and DFS
 - FCC RF Exposure calculation
- Canada
 - IC RSS-102 and RSS-247 (2.4Ghz and 5.8Ghz) and DFS
- Europe
 - ETSI EN 300 328 (2.4 GHz)
 - ETSI EN 300 893 (5GHz) and DFS
 - EN 50385, EN 50665, and EN 62311 RF exposure
 - ETSI EN 301 489-1
 - ETSI EN 301 489-17
- EMC Immunity
 - EN55024/CISPR24
 - EN300-386

