Extreme AirDefense® Essentials AP Sensor Configuration Guide

9037975-00 Rev AB
October 2023

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, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

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: https://www.extremenetworks.com/support/policies/open-source-declaration/

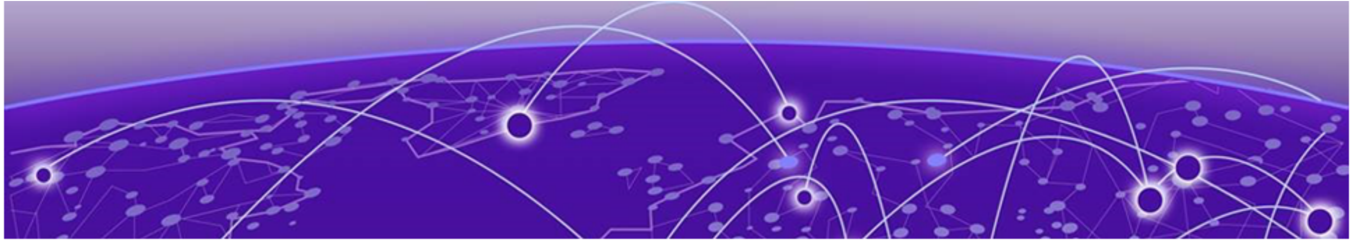
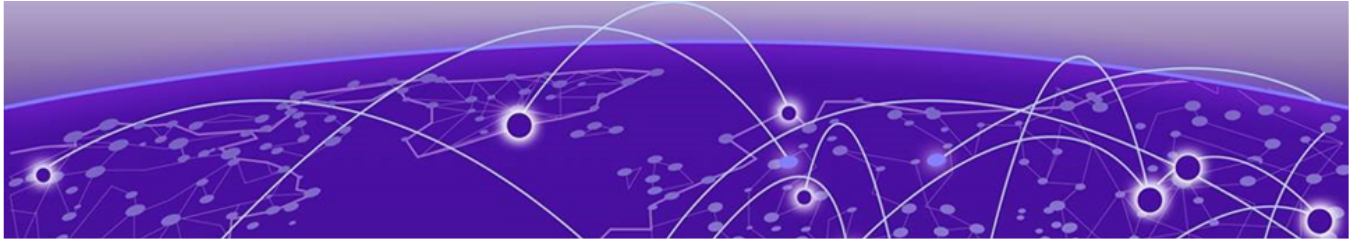


Table of Contents



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product
📝	Note	Useful information or instructions
➡	Important	Important features or instructions
⚠	Caution	Risk of personal injury, system damage, or loss of data
⚠	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed 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 in boldface, for example **Ctrl** 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**
Words in italicized type	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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *`member`*`[`*`member`*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) 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.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

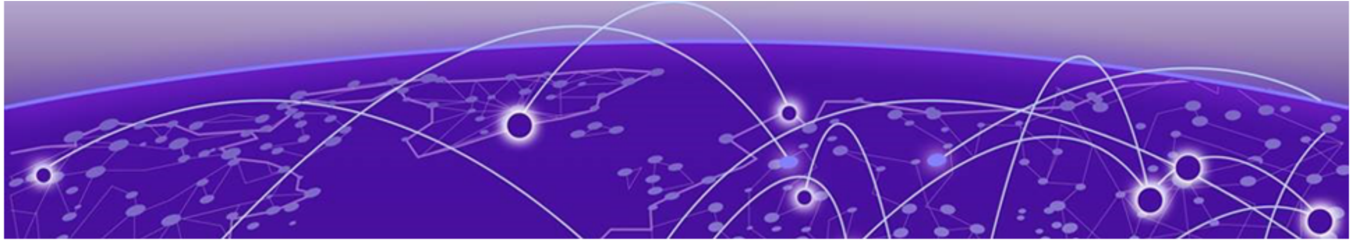
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About this Guide

This guide provides the following:

- An overview and requirements for configuring Extreme AirDefense Essentials AP sensors
- Network Policy procedures for configuring Extreme AirDefense Essentials AP sensors.

Prerequisites and Limitations

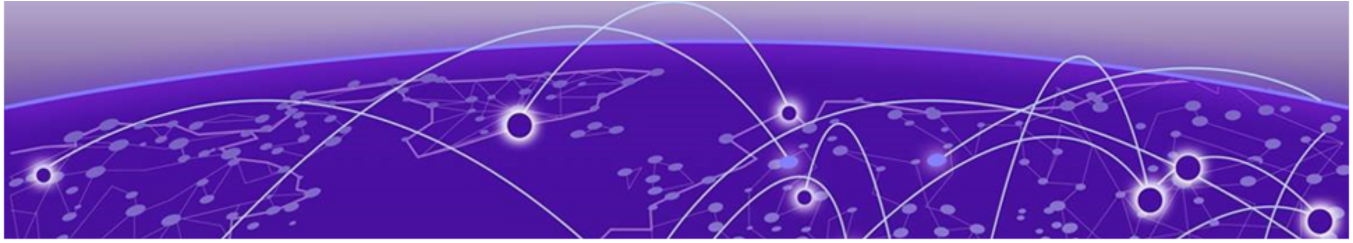
This document provides the information required to perform an Extreme AirDefense Essentials AP sensor configuration.

You must be familiar with accessing and performing basic functions in ExtremeCloud IQ and Extreme AirDefense Essentials. For more information, see the following product documentation:

- ExtremeCloud IQ
- Extreme AirDefense Essentials

You need the following before you begin:

- An ExtremeCloud IQ account with Pilot license for access to Extreme AirDefense Essentials services
- An ExtremeCloud IQ supported AP model that is connected to the cloud and assigned a working network policy.

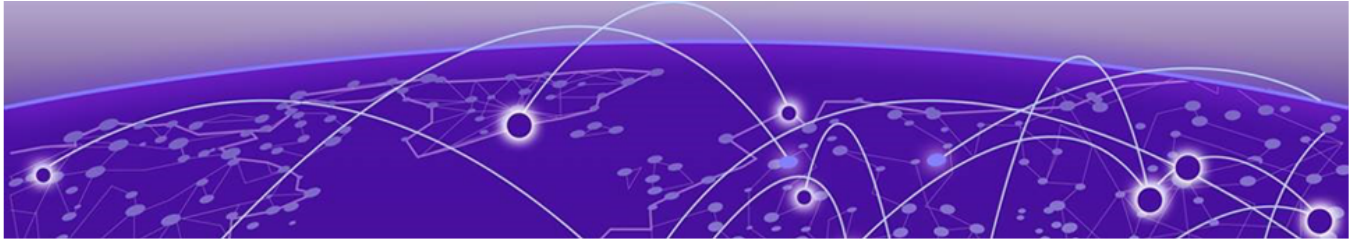


Introduction to Extreme AirDefense Essentials AP Sensor Configuration

This document provides the work flow of procedures required to configure Extreme AirDefense Essentials with AP sensors:

- Enable Extreme AirDefense Essentials on the ExtremeCloud IQ account
- Configure a Network Policy for Extreme AirDefense Essentials managed APs to operate as an Extreme AirDefense Essentials sensor in ExtremeCloud IQ
- Create and assign a WIPS Policy in ExtremeCloud IQ to the Network Policy used by the AP sensor.

For more information, see Network Policy Configuration for Sensor Mode.



Sensor Mode Overview

When configuring AP models to operate as sensors, there are two sensor mode types:

- Dedicated
- Radio-Share

Note

- Sensor mode is not user-selectable and is determined by the AP model.
- If an AP has a radio designed to operate as a full-time sensor, then that particular radio can only operate in dedicated sensor mode.
- Some AP models have radios that only operate as full time sensors, for example the AP410i/e.
- If an AP model does not have a radio designed to operate as a full-time sensor, that AP model can only operate in radio-share sensor mode.

Dedicated Sensor Mode

For APs operating as dedicated sensors, the individual dedicated sensor radio in the AP cannot service clients. The sensor radio scans full-time and senses on all available channels.

On some AP models, enabling the radio designed for dedicated sensing disables a frequency spectrum (2.4, 5, 6 GHz) for wireless client service. For example, an AP4000 disables the 6Ghz spectrum for client service on the third radio when you enable dedicated sensing.

Note

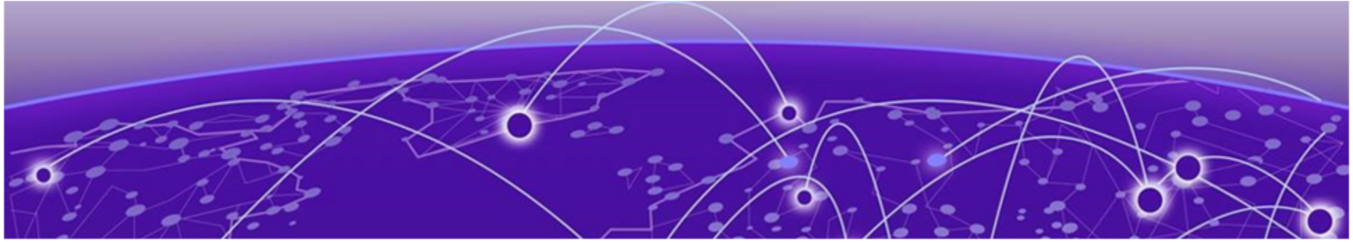
Dedicated sensors scan all available channels, so no need to configure all dedicated sensor capable APs as sensors. How many and which AP models to configure as dedicated sensors is out of scope for this document. For assistance, contact your Extreme Networks® professional services provider.

Radio-Share Sensor Mode

For APs operating as radio-share sensors, AP radios can service the wireless clients as usual. All radios configured for radio-share mode (one or both can be selected) also perform security scans on the same channels that the radios are operating for client service.

Additionally, radio-share sensors only analyze wireless traffic for connected wireless clients. Radio-share sensors scanning coverage is reduced compared to dedicated sensors.

A best-practice is to configure all radio-share AP models to operate as radio-share sensors to sense as many channels as possible.



Network Policy Configuration for Sensor Mode

This chapter contains the following details:

- Modifying a Network Policy to configure an AP model sensor radio to operate as a sensor
- Creating and adding a WIPS Policy to the Network Policy
- Updating the AP with the new configuration.

The WIPS Policy

The WIPS policy defines the following types of WIPS solution for the sensors to send data:

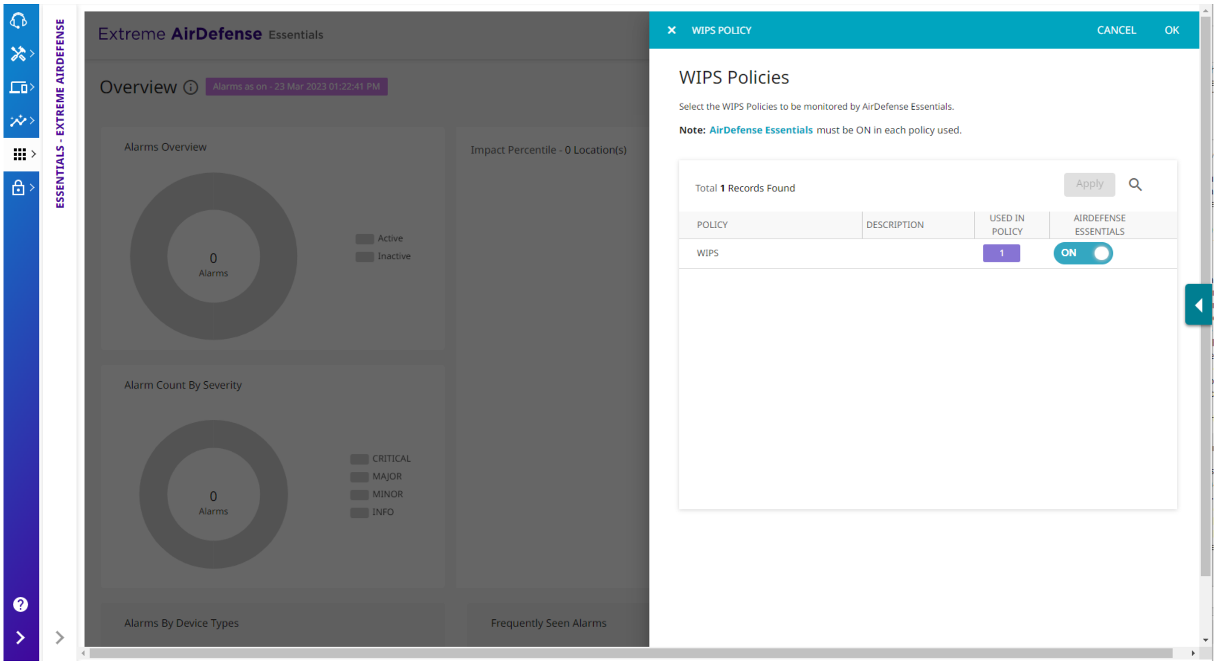
- AirDefense Enterprise - The AirDefense Enterprise option includes the server address and the AirDefense server port for sensors to connect
- Extreme AirDefense Essentials
- Legacy ExtremeCloud IQ.

WIPS Policies for Extreme AirDefense Essentials

To access Extreme AirDefense Essentials, the WIPS Policy must be enabled for Extreme AirDefense Essentials in ExtremeCloud IQ.

1. From the Extreme AirDefense Essentials overview view, select the **Settings** icon located beside the **More Insights?** button.

   The **WIPS Policies** window opens, where you can select the policies for Wireless Threat Detection.



✕ WIPS POLICY CANCEL OK

WIPS Policies

Select the WIPS Policies to be monitored by AirDefense Essentials.

Note: AirDefense Essentials must be ON in each policy used.

Total **1** Records Found Apply

POLICY	DESCRIPTION	USED IN POLICY	AIRDEFENSE ESSENTIALS
WIPS		1	ON

Figure 1: Extreme AirDefense Essentials WIPS Policies

2. Select the WIPS Policies that are used in Extreme AirDefense Essentials and select **Apply** then **Ok**.

Log in and Select the Network Policy

Perform these steps to log in to ExtremeCloud™ IQ and select the network policy.

1. Log into ExtremeCloud IQ.
2. In the main navigation bar, select ⚒
3. Select Network Policies.
4. Select a network policy in use by a managed AP that supports Extreme AirDefense® Essentials sensor functionality.
5. Select ✎
6. Select 2 Wireless.

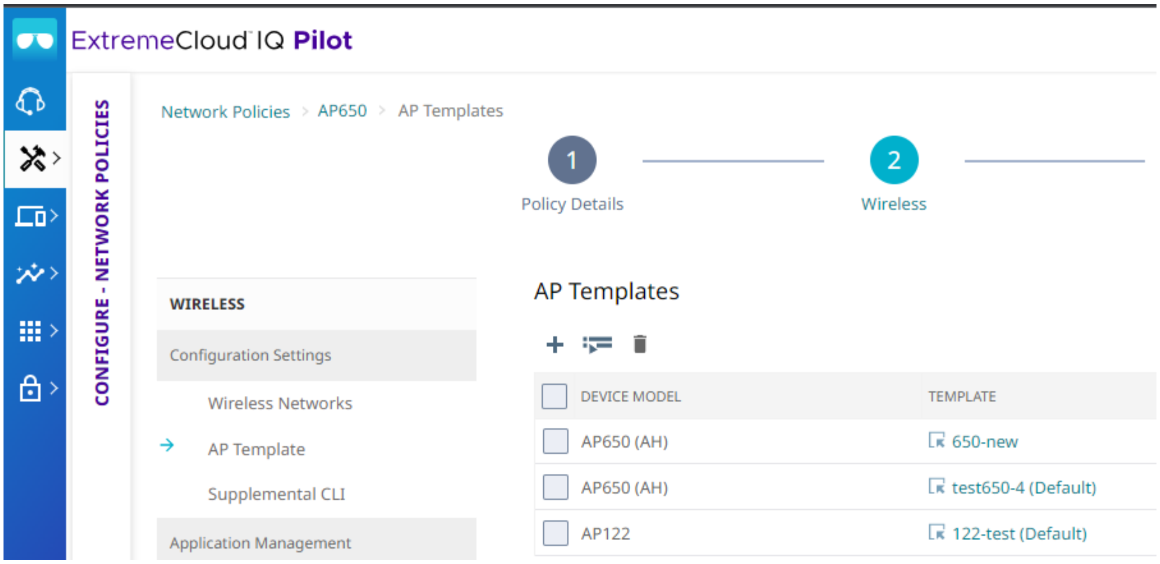
Continue to the next procedure in the series, Configure the AP Template on page 14.

Configure the AP Template

Complete the procedure, Log in and Select the Network Policy on page 13.

Perform these steps to edit an AP template for AP sensor use.

1. From the **WIRELESS → Configuration Settings** navigation list, select **AP Template**



AP Templates

DEVICE MODEL	TEMPLATE
AP650 (AH)	650-new
AP650 (AH)	test650-4 (Default)
AP122	122-test (Default)

2. Select an AP template from the **Template** column to modify.
3. In the **Device Template** view, select **Wireless Interfaces**.
4. Select **WIFI2.**
5. Select the **Radio Status** and toggle it **ON**.
6. Select **Save Template** to confirm the changes.

> **Note**
> Radios that support sensor functionality vary depending on the AP model. For details, see the AP Model Data Sheet for specifications from the WI-FI Access Points

Continue to the next procedure in the series, Apply a WIPS policy to the Network Policy on page 14.

Apply a WIPS policy to the Network Policy

Ensure you have completed the following procedures in sequence:

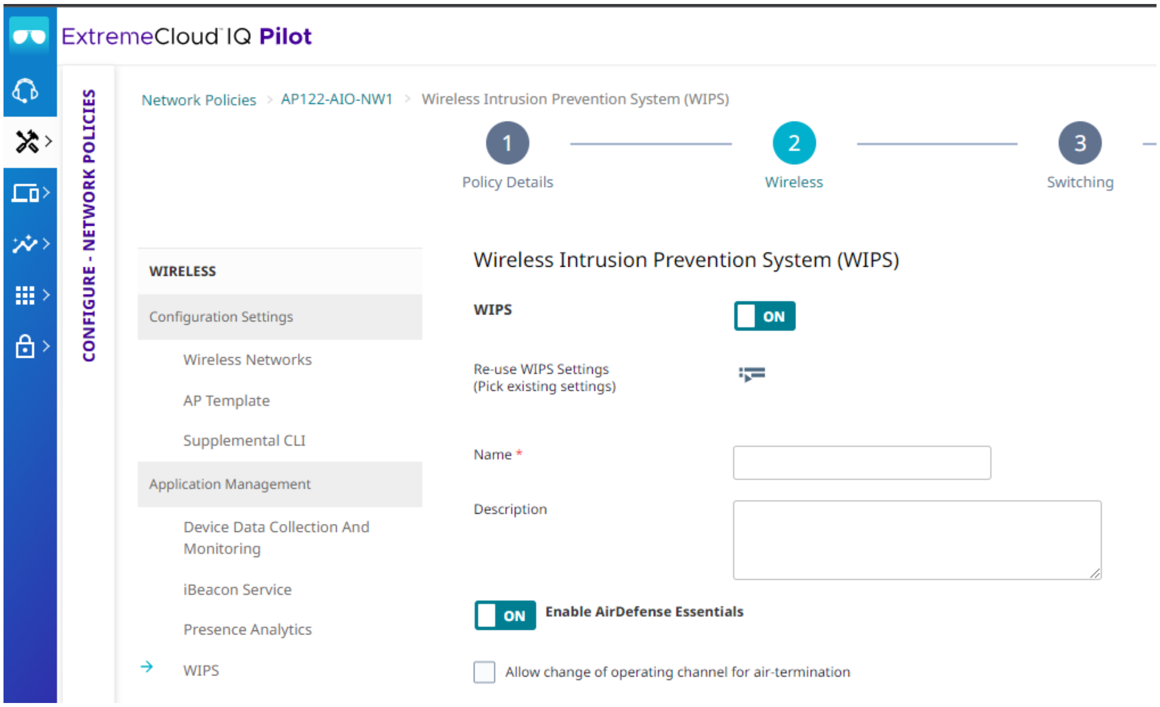
- Log in and Select the Network Policy on page 13

- Configure the AP Template on page 14

Note
The following steps are examples for AP models that only support radio-share sensor mode, each radio interface is currently pre-selected. For any radio-share sensor model AP, the only configuration needed to have the AP operate in radio-share sensor mode is to create and apply a WIPS policy to the Network Policy.

Perform these steps to apply a WIPS policy to the network policy.

1. From the WIRELESS → Configuration Settings → Application Management navigation list, select WIPS.



Wireless Intrusion Prevention System (WIPS)

WIPS ON

Re-use WIPS Settings (Pick existing settings)

Name *

Description

ON Enable AirDefense Essentials

☐ Allow change of operating channel for air-termination

2. Select WIPS and toggle it ON.
3. Select the **Name** field and enter a name for the WIPS policy.
4. Select **Enable AirDefense Essentials** and toggle it ON.
5. Select Save to confirm the changes.

Note
You have created and applied the WIPS policy to the Network Policy. The AP is now ready to be updated with new Network Policy settings.

Continue to the next procedure in the series, Deploy the Policy on page 15.

Deploy the Policy

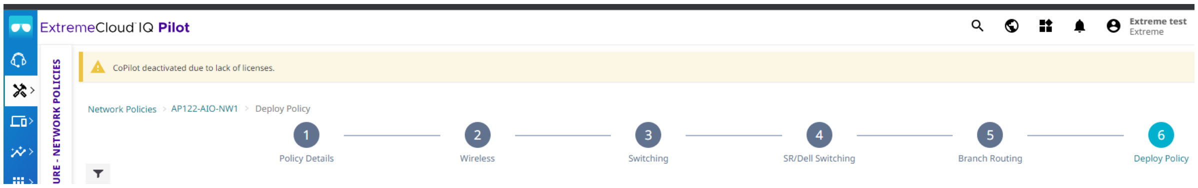
Ensure you have completed the following procedures in sequence:

- Log in and Select the Network Policy on page 13

- Configure the AP Template on page 14
- Apply a WIPS policy to the Network Policy

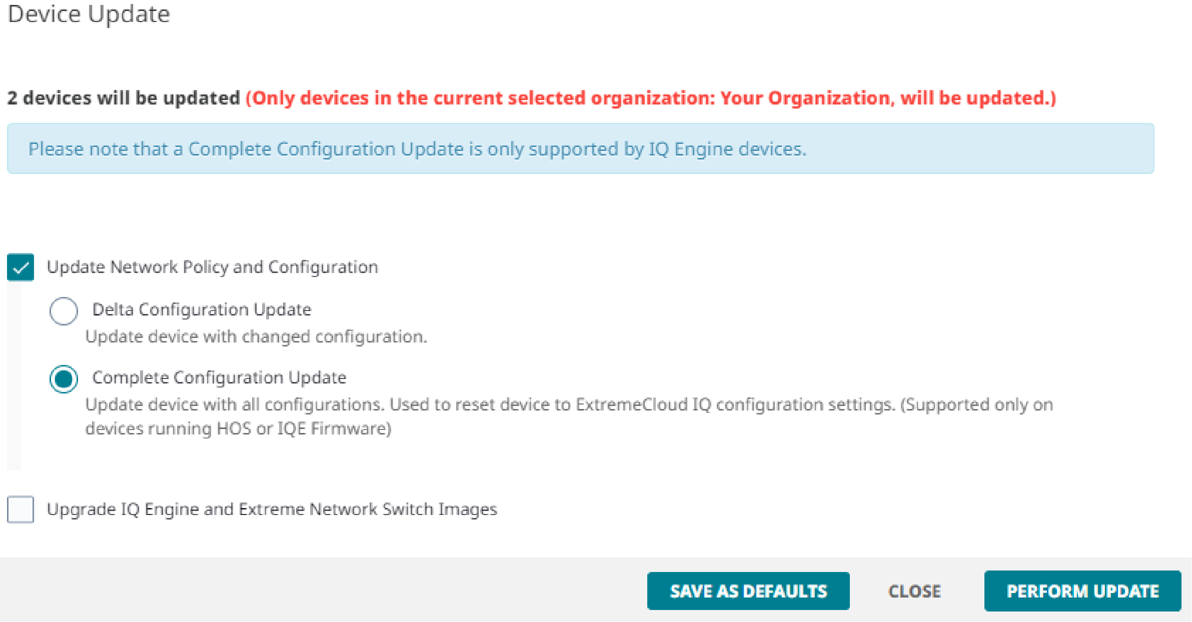
Perform these steps to deploy the updated network policy.

1. Select **6 Deploy Policy**.



CoPilot deactivated due to lack of licenses.

2. Select the check box beside listed APs to apply the network policy to selected devices. ☑ ☑
3. Select UPLOAD
4. In the **Device Update** window, select **Complete Configuration Update**.



Device Update

2 devices will be updated (Only devices in the current selected organization: Your Organization, will be updated.)

Please note that a Complete Configuration Update is only supported by IQ Engine devices.

☑ Update Network Policy and Configuration

○ Delta Configuration Update
Update device with changed configuration.

● Complete Configuration Update
Update device with all configurations. Used to reset device to ExtremeCloud IQ configuration settings. (Supported only on devices running HOS or IQE Firmware)

☐ Upgrade IQ Engine and Extreme Network Switch Images

5. To deploy the configuration, select **Perform Update**.

A green **Audit** icon ✓ indicates a successful AP configuration update.

Note

Updated APs reboot and immediately begin attempting to establish a connection with the Extreme AirDefense Essentials server.