Extreme AirDefense Base

XCA Configurations for AirDefense Base Container

9036648-00 Rev AA

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

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

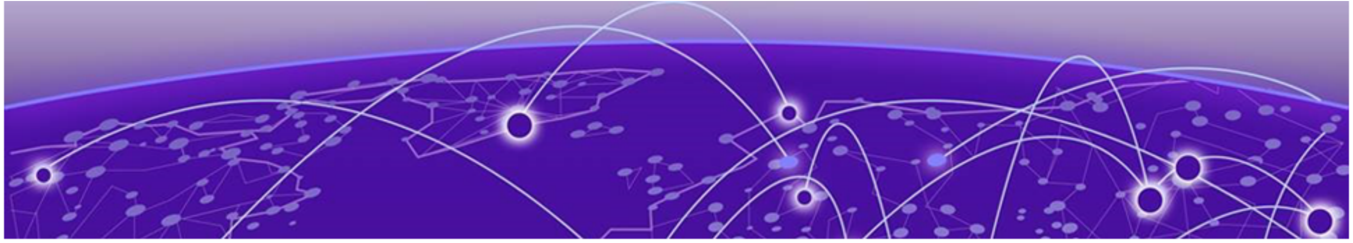
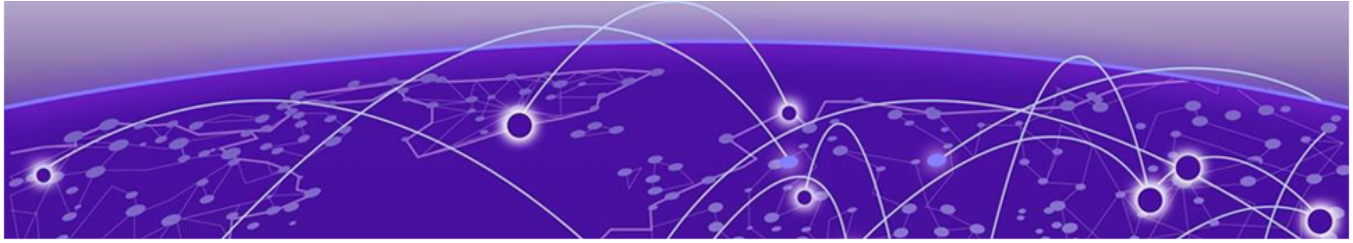


Table of Contents



Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

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.

Table 1: Notes and warnings (continued)

Icon	Notice type	Alerts you to...
⚠	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 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 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/software compatibility matrices for Campus and Edge products

Supported transceivers and cables for Data Center products

Other resources, like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

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 2826. 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 Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).

3. Select the products for which you would like to receive notifications.

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

4. Select **Submit**.

Providing Feedback

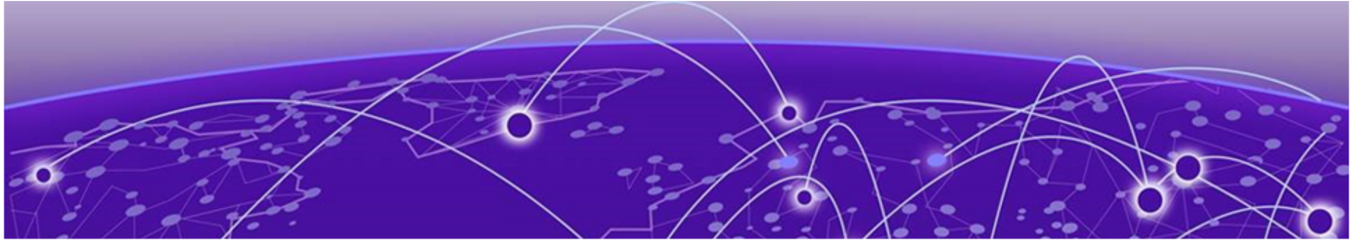
The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



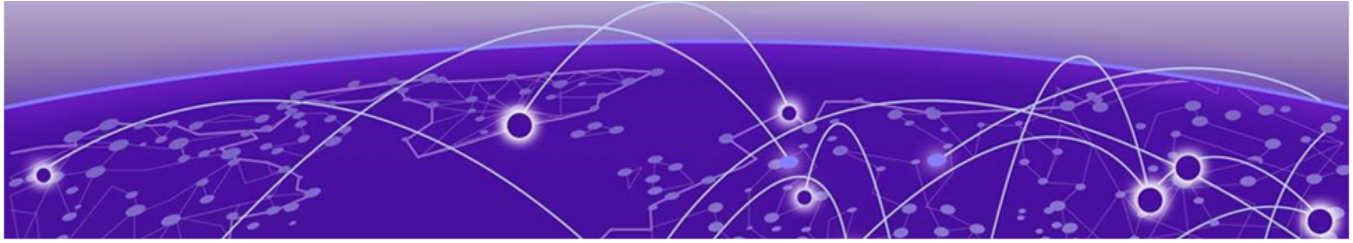
Introduction

Use this document to learn about the steps required before you can use the AirDefense Base application container on the ExtremeCloud Appliance (XCA) server for evaluating the AirDefense Base application.

You require an API key generated on your ExtremeCloud Appliance (XCA) that will be used to import devices, both BSSs and wireless clients, from XCA into AirDefense Base application. The API key is mandatory to import these devices and to authorize them for WIPS processing.

Once you have imported the API key, you must also ensure that your sensors are pointed towards the AirDefense Base server.

This document describes the steps to achieve the above two requirements before you can evaluate the AirDefense Base application deployed on your ExtremeCloud Appliance.



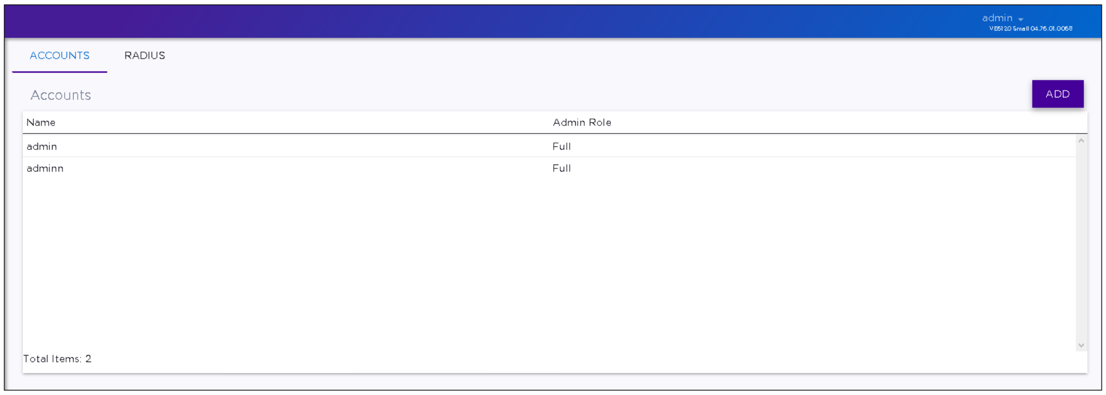
Generating the XCA API Key

You must have the AirDefense Base container application installed on your ExtremeCloud Appliance.

To generate and download the API key to install on your AirDefense Base application:

1. From within the ExtremeCloud Appliance user interface, navigate to the **Accounts** screen using the **Administration** > **Accounts** menu path.

   The **Accounts** screen displays.

   admin
   VE6120 Small 04.76.01.0068

   ACCOUNTS RADIUS

   Accounts

   ADD

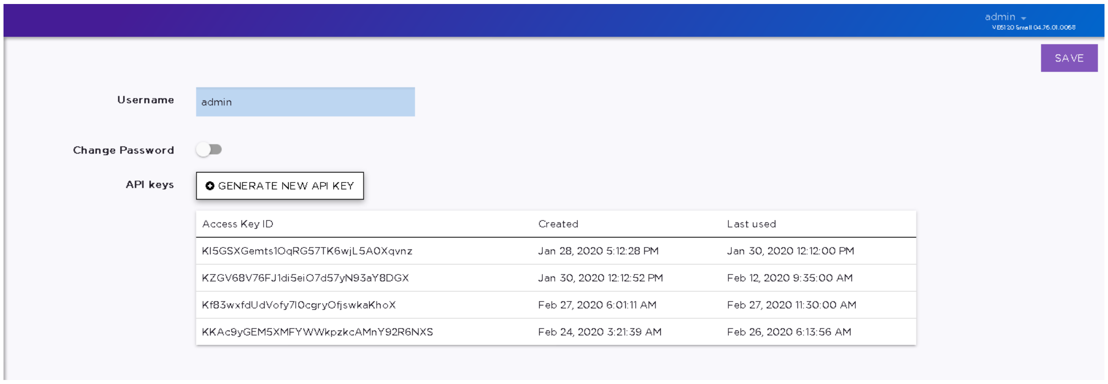
Name	Admin Role
admin	Full
adminn	Full

   Total Items: 2

   Figure 1: Accounts Screen

2. Select an user account that has adequate permission to start, stop, and manage applications on this ExtremeCloud Appliance.

   The following screen displays.

   admin
   VE6120 Small 04.76.01.0068

   SAVE

   Username: admin

   Change Password

   API keys: GENERATE NEW API KEY

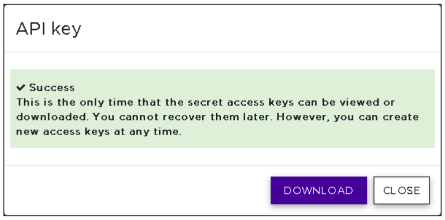
Access Key ID	Created	Last used
KI5GSXGemts1OqRG57TK6wjL5A0Xqvnz	Jan 28, 2020 5:12:28 PM	Jan 30, 2020 12:12:00 PM
KZGV68V76FJ1di5eiO7d57yN93aY8DGX	Jan 30, 2020 12:12:52 PM	Feb 12, 2020 9:35:00 AM
Kf83wxfdUdVofy7l0cgryOfjswkaKhoX	Feb 27, 2020 6:01:11 AM	Feb 27, 2020 11:30:00 AM
KKAc9yGEM5XMFYWWkpzkcAMnY92R6NXS	Feb 24, 2020 3:21:39 AM	Feb 26, 2020 6:13:56 AM

   Figure 2: Account Information Screen

   This screen displays details about the selected ExtremeCloud account. The **API keys** table at the bottom of the screen displays a list of API keys issued to this user account, if any.

3. Select the **GENERATE NEW API KEY** button to generate a new API key for this ExtremeCloud Appliance user account.

   The following message displays.



API key

✔ Success
This is the only time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Figure 3: Key Successfully Created Message

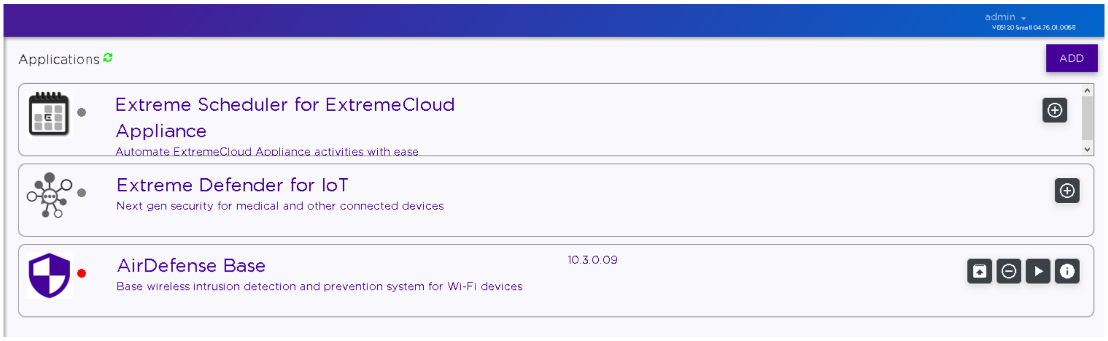
4. Select the **DOWNLOAD** button and save the generated API Key to your local PC.

   The downloaded API key is saved to your PC and is always named as *<your-user-name>_api_key.json*. For example, if the username is *john* then this file will be named as *john_api_key.json*.

   Make a note of the location where this file is saved as it will be required later in the process.

5. Navigate to the **Applications** screen using the **Administration** > **Applications** menu path.

   The **Applications** screen displays.



Extreme Scheduler for ExtremeCloud Appliance
Automate ExtremeCloud Appliance activities with ease

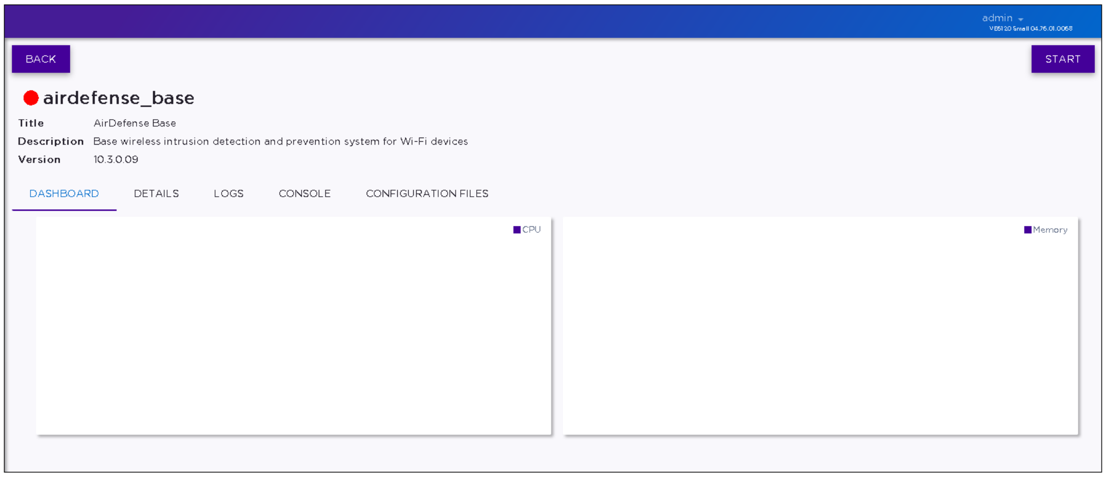
Extreme Defender for IoT
Next gen security for medical and other connected devices

AirDefense Base 10.3.0.09
Base wireless intrusion detection and prevention system for Wi-Fi devices

Figure 4: Applications Screen

6. Select the ⓘ icon for the **AirDefense Base** item in the list of installed applications.

   The AirDefense Base application's configuration screen displays.



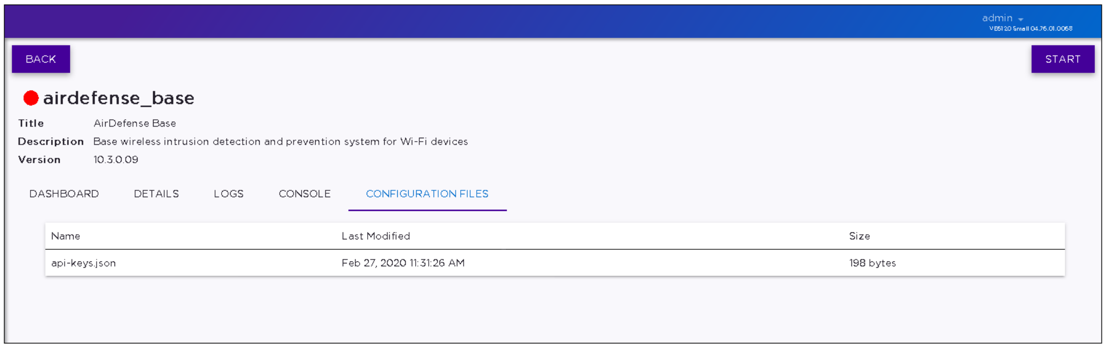
● airdefense_base

Title	AirDefense Base
Description	Base wireless intrusion detection and prevention system for Wi-Fi devices
Version	10.3.0.09

Figure 5: Application Configuration Screen

7. Select the **Configuration Files** tab.

   The screen changes to the following:



● airdefense_base

Title	AirDefense Base
Description	Base wireless intrusion detection and prevention system for Wi-Fi devices
Version	10.3.0.09

Name	Last Modified	Size
api-keys.json	Feb 27, 2020 11:31:26 AM	198 bytes

Figure 6: Configuration Files Tab

If an API key was used previously, this screen displays the date on which the API key was last uploaded to the AirDefense Base application. If this is the first time an API key is being used, then this screen does not display a value in the **Last Modified** field.

8. Select the row with the entry **api-keys.json** in this list.

   If the **Last Modified** field is populated, then the 🗑 ⭱ icon displays. Select the 🗑 icon to delete the existing API key before using the ⭱ icon to upload the new API key.

   If the **Last Modified** field is not populated, then use the ⭱ icon to upload the new API key.

   The **Upload config file** screen displays.

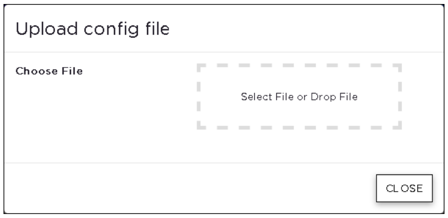
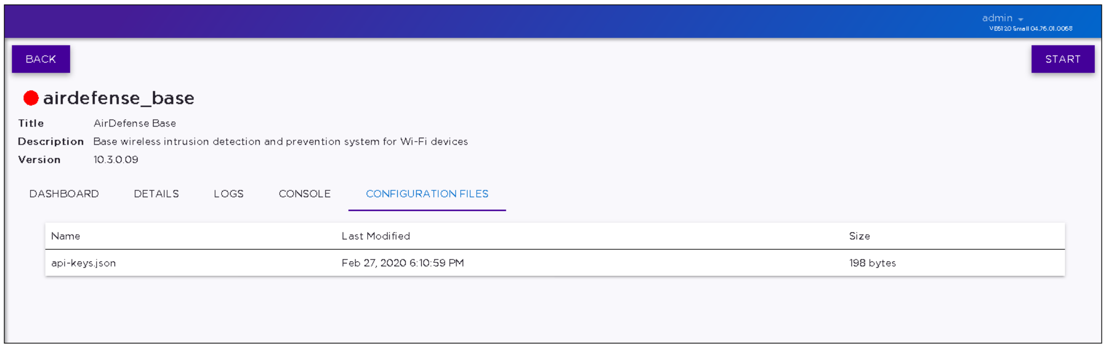


Figure 7: Upload config file Window

9. Use the **Choose File** control to locate and upload the *<your-user-name>_api_key.json* file that you saved earlier.

   The API key is immediately updated.



airdefense_base

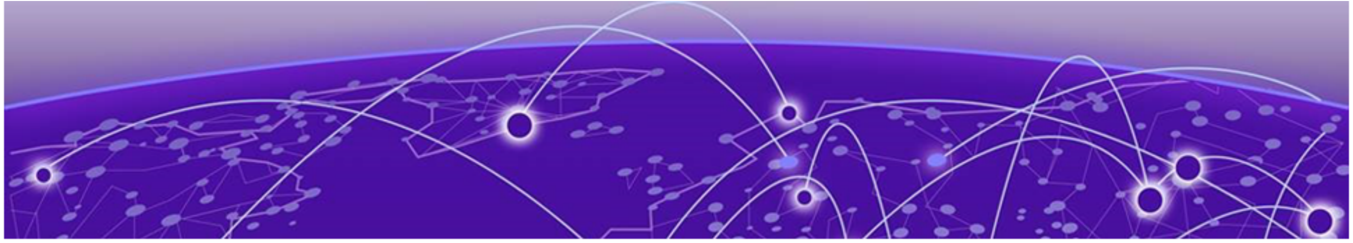
Title AirDefense Base
Description Base wireless intrusion detection and prevention system for Wi-Fi devices
Version 10.3.0.09

Name	Last Modified	Size
api-keys.json	Feb 27, 2020 6:10:59 PM	198 bytes

Figure 8: API Key Updated

> Note
> You can update the API Key anytime. The AirDefense Base application server need not be stopped for this activity. When a new API key is uploaded to the AirDefense Base application server, it will be used from the next polling cycle, which is set at five (5) minutes by default.

The AirDefense Base application is now ready to import BSSs and wireless clients from ExtremeCloud Appliance.



Configuring AirDefense Base Profile in XCA

Important

It is assumed that you have a working ExtremeCloud Appliance with all the required configurations steps completed. It is also assumed that you have downloaded the AirDefense Base application container and have installed and configured it successfully.

Important

Note that this configuration has to be performed for each site that you want the AirDefense Base application to monitor for wireless intrusions. It should also be configured for each device profile that you have created in or added to your site.

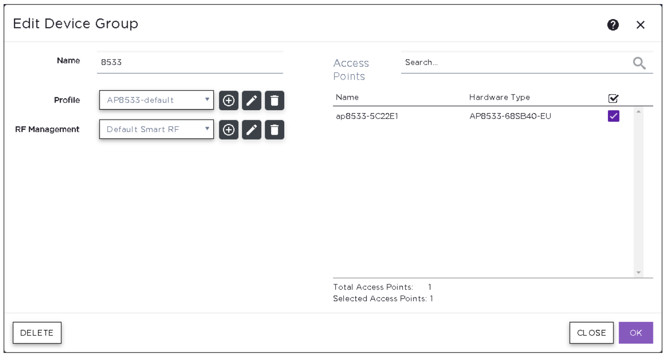
To configure your sensors to start sending data to the onboard AirDefense Base application, you must do the following on each site and for each device profile installed on that site.

1. Select **Configure** > **Sites** in the ExtremeCloud user interface.

   The **Sites** screen displays.
2. From the **Sites** screen, select an existing site for which you want to configure AirDefense Base application settings.

   The **Site Details** screen displays.
3. Select the **Device Groups** tab.
4. Select an existing `Device Group` or create a new one.

   The **Edit Device Group** screen displays.



Edit Device Group

Name: 8533

Profile: AP8533-default

RF Management: Default Smart RF

Access Points

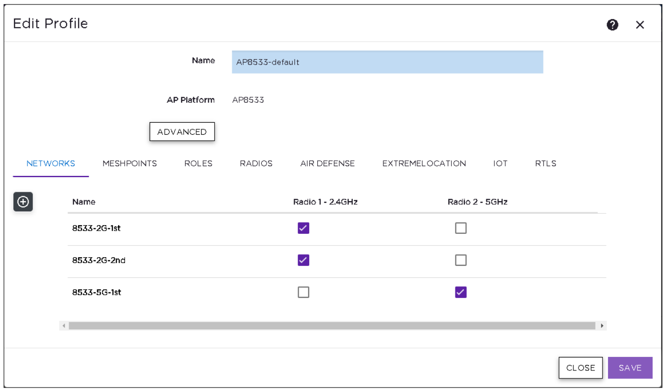
Name	Hardware Type	☑
ap8533-5C22E1	AP8533-68SB40-EU	☑

Total Access Points: 1
Selected Access Points: 1

Figure 9: XCA Device Group Screen

5. Use the **Profiles** drop-down list to select the device profile that you need to configure. Once selected, click the ✎ icon to edit it.

   The **Edit Profile** screen displays.

   Name: AP8533-default

   AP Platform: AP8533

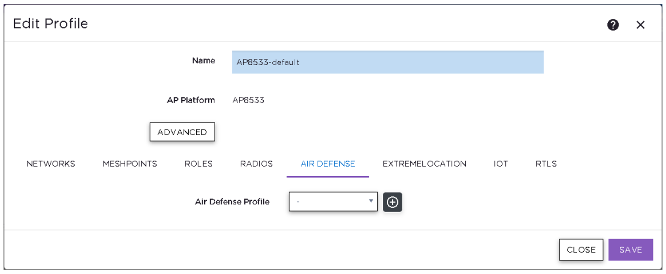
Name	Radio 1 - 2.4GHz	Radio 2 - 5GHz
8533-2G-1st	☑	□
8533-2G-2nd	☑	□
8533-5G-1st	□	☑

   Figure 10: Edit Profile Screen

   To create a new `Device Profile` select the ⊕ icon instead.

6. Select the **AirDefense** tab.

   The **Edit Profile** screen displays.

   Name: AP8533-default

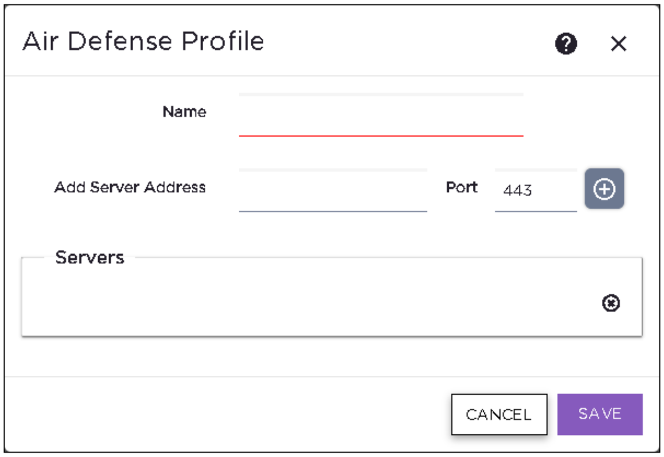
   AP Platform: AP8533

   Air Defense Profile: -

   Figure 11: Edit Profile Screen

7. From the **AirDefense Profile** drop-down list select an existing profile or select the ⊕ icon to create a new profile.

   The **AirDefense Profile** screen displays.



Port 443

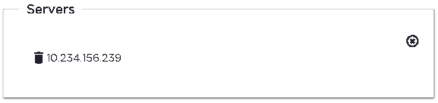
Figure 12: AirDefense Profile Screen

Provide the following information:

Field	Description
Name	Provide a name for this `AirDefense Profile`.
Add Server Address	Enter the IP address of your AirDefense server. Enter the IP address of the ExtremeCloud Appliance here. This is the IP address of the server where the AirDefense Base application is installed.
Port	Enter the value 32032.

Select the ⊕ icon to add this AirDefense Base application's IP address to the list of servers.

The IP address of the XCA server is added to the **Servers** list.



10.234.156.239

Figure 13: Servers List

8. Select the **SAVE** button to save the information in this screen.
9. Close all other popups and dialogs and return to the **Sites** screen.

   The various devices in your site will start sending data to the configured AirDefense Base application server.