



Extreme AirDefense: WiNG Controller Import via CLI



Copyright © 2019 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

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	4
Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
Documentation and Training.....	6
Chapter 1: Introduction	7
Chapter 2: Import WiNG Controllers Using CLI	8
Chapter 3: Important Notes and Limitations when importing using CLI	11



Preface

This guide provides the instructions and supporting information to import devices into AirDefense server using the WIPAdmin CLI interface.

Conventions

This section discusses the conventions used in this guide.

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.
<i>New!</i>	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.

Terminology

When features, functionality, or operation is specific to a switch family, such as ExtremeSwitching, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the switch.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have 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 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, you can do so in two ways:

- Use our short online feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Please 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.

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: 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

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

Subscribing 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 with your information (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 Click **Submit**.

Documentation and Training

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
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

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

1 Introduction

You can now import devices into your AirDefense server using the WIPAdmin CLI interface. When you import devices, AirDefense fetches a list of access points, BSSs, and wireless clients from the wireless controllers in your AirDefense managed network. These imported devices are then created within your AirDefense server.

When devices are imported into your system, AirDefense can use Action Manager Rules to sanction these devices and enable these devices to generate WIPS alarms.

Additionally, AirDefense creates Security Profiles based on the WLAN profiles on the wireless controllers. This reduces errors that can occur when these security profiles are created manually on the AirDefense server. These auto created Security Profiles are not enabled by default and you can modify them to suit your requirements.

2 Import WiNG Controllers Using CLI

Using the CLI method of importing devices into your AirDefense system is faster than the traditional method of importing devices through SNMP polling.

To import WiNG wireless controllers using the WIPAdmin CLI, do the following:

- 1 Login to your WIPAdmin CLI user interface using the `smxmgr` credentials.
- 2 Select the **(C)onfig** menu item.

The following screen displays.

```
*** ADSPadmin ***

(C) Config

(IDS) AirIDS config
(IP) IP address config
(IPv6) IPv6 address config
(NETPORT) Network port speed/duplex config
(DNS) Define DNS servers
(BONDING) High Availability Ethernet config
(HNAME) Set hostname
(DNAME) Set domain name
(TIME) Time/Date config
(TZ) Set timezone
(NTP) Enable/disable NTP
(PING) Enable/disable ICMP Echo Request (ping) responses
(SNMPPA) Enable/disable reception Snmp agent requests
(SNMPC) Configure Snmp agent community string.
(SNMPT) Enable/disable SNMP trap reception
(HTT) Enable/disable unencrypted sensor connections
(PANIC) Enable/disable reboot on system error
(UIPORT) Display network port for dashboard access

(Q) to quit (return to previous menu) ->
```

- 3 Select the **(I) AirIDS Config** menu item.

The following screen displays.

```
*** ADSPadmin ***

(I) IDS config

(MCORE) Enable/disable Multi-Core
(MCLEAR) Clear all multi-core site assignments
(SSLV3) Enable/disable SSLv3 for Sensor-Server Communication
(FTMODE) Enable/disable Fast Termination on the Server and Sensor
(SPOOF) Enable/disable Spoof Mac Detection on the Server
(IMPORT) Import the controller/switch into the Server

(Q) to quit (return to previous menu) ->
```

- 4 In the prompt, enter `import` to launch the import action.

```
*** ADSPadmin ***

(I) IDS config

(MCORE) Enable/disable Multi-Core
(MCLEAR) Clear all multi-core site assignments
(SSLV3) Enable/disable SSLv3 for Sensor-Server Communication
(FTMODE) Enable/disable Fast Termination on the Server and Sensor
(SPOOF) Enable/disable Spoof Mac Detection on the Server
(IMPORT) Import the controller/switch into the Server

(Q) to quit (return to previous menu) -> import
```


When this option is selected, the screen displays the IP addresses of the last five (5) wireless controllers imported into the AirDefense system.

```

Last 5 known Switch/controller imported entries:
The following switch(s)/controller(s) imported with the credentials:

(1)      10.234.101.104 admin

Enter line number to select the switch/controller
Add a new switch/controller to import

(Q) to quit (return to previous menu)  -> 1

Enter the CLI password
-> xxxxxxxx
    
```

- From the list of wireless controllers that were imported earlier, select the line number for the wireless controller that you want to import again.

You are prompted to enter the login password for the selected wireless controller.

- Enter the correct password for the wireless controller and select the [Enter] key.

AirDefense starts polling the selected wireless controller to fetch the relevant data. This process cannot be interrupted and you must wait for it to complete before you can proceed to the next activity.

- To import data from a wireless controller not listed in the last imported list, enter A in the prompt.

The following screen displays.

```

Last 5 known Switch/controller imported entries:
The following switch(s)/controller(s) imported with the credentials:

(1)      10.234.101.104 admin

Enter line number to select the switch/controller
Add a new switch/controller to import

(Q) to quit (return to previous menu)  -> A

Enter the IP address of the controller/switch to import
format: 172.16.0.102      -> 10.0.0.1

Enter the CLI username
-> xxxxxx

Enter the CLI password
-> xxxxxx
    
```

- Provide the following information for the wireless controller.

Field	Description
IP Address of the wireless controller	In the prompt, enter the IP address of the wireless controller to connect to.
Enter the CLI username	Enter the user name for an account that has administrative access to the wireless controller.
Enter the CLI password	Enter the password for the user account entered above.



AirDefense connects to the wireless controller and starts importing the devices. This process cannot be interrupted and you must wait for it to complete before you can proceed to the next activity.



3 Important Notes and Limitations when importing using CLI

The following is a list of benefits and limitations that you need to keep in mind when importing wireless controllers through the CLI;

- Using the CLI method of importing devices into your AirDefense system is faster than the traditional method of importing devices through SNMP polling.
- When devices are imported into the AirDefense system, they are created under the *Unplaced Devices* category. You must manually move these devices to their appropriate location in your AirDefense hierarchy.
- The Security Profiles that were created at import are not enabled by default. You must enable each security profile manually.