ExtremeWireless™

Extreme AirDefense: Configuring AirDefense for Multiple WIPS (AirIDS) Engines

9036129-00

Published March 2019

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 guide provides the instructions and supporting information required to enable support for multiple WIPS (AirIDS) engines on your AirDefense server.

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.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
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.

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

The AirDefense appliance is a server that processes incoming messages from all the sensors that are a part of the AirDefense managed system. With the exponential increase in the number of sensors and the wireless client devices seen by them, the amount of data being processed by these existing systems have also increased exponentially. Using a server running on a single core to process so much data slows down the ability to use the tremendous amount of generated data to make critical security decisions effectively and immediately.

The underlying hardware devices used by AirDefense have always been multicore. However, the AirDefense server software was designed to run on a single core. With this *Enabling Multiple WIPS (AirIDS) Engine* (Multicore) enhancement included in this release, the AirDefense server software gains the ability to run on multiple cores on the same hardware. With this feature, AirDefense has gained the ability to enhance its scalability in future releases.

With the introduction of multicore support, you can see improvements in overall performance in your existing deployments. You can see these performance improvements in back end processing and in the user interface. This feature does not increase the total number of supported sensors but enhances the ability to process the data that is received from these sensors and those wireless devices seen by these sensors.

2 Enable Multiple WIPS Engines

Important Notes and Limitations when using Multicore

After upgrading your AirDefense instance to version 10.1, it is recommended that you run your system in single core mode for at least 2 to 3 hours. This enables the system to recalibrate its database and make it ready for multicore configuration.

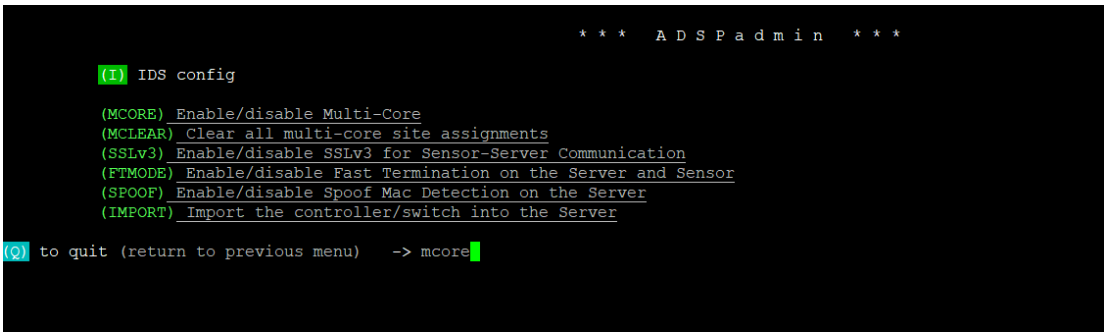
Important
Please ensure that you have a backup of your server's current configuration and copies of the latest forensic files before starting this conversion process.

To enable multiple WIPS engines on your instance of AirDefense:

1 Login to your AirDefense WIPSadmin CLI user interface using the *smxmgr* credentials.

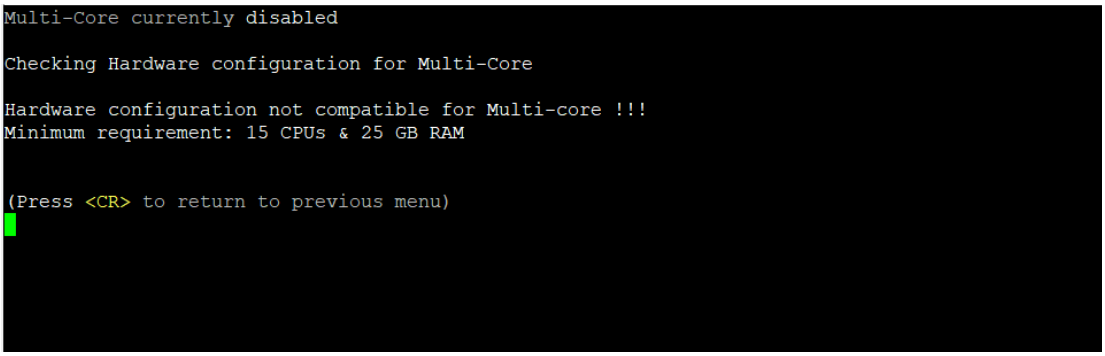
2 Navigate to the **Config** > **IDS Config** screen.

The following screen displays.



3 Select **MCORE** option under the **IDS Config** menu.

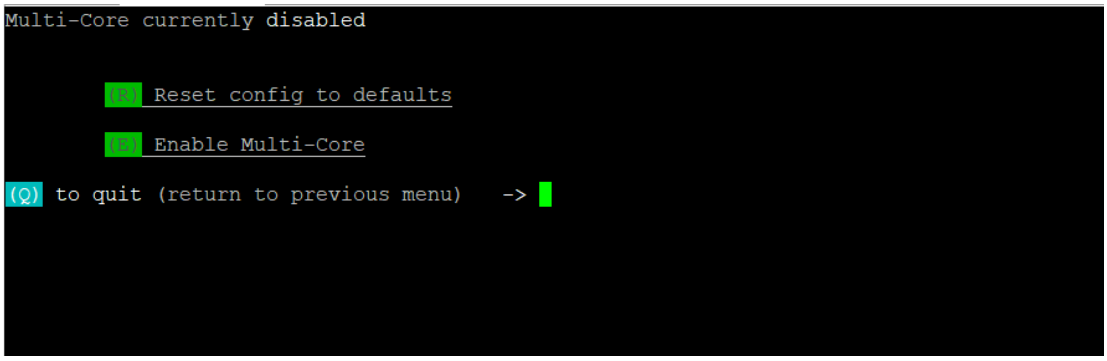
The system displays the current *Multi-Core* status.



Note

Please note that the **(R) Reset config to defaults** and **(E) Enable Multi-core** options will not be available until the underlying AirDefense hardware meets the minimum requirements of having 25 GB RAM and 15 CPU cores.

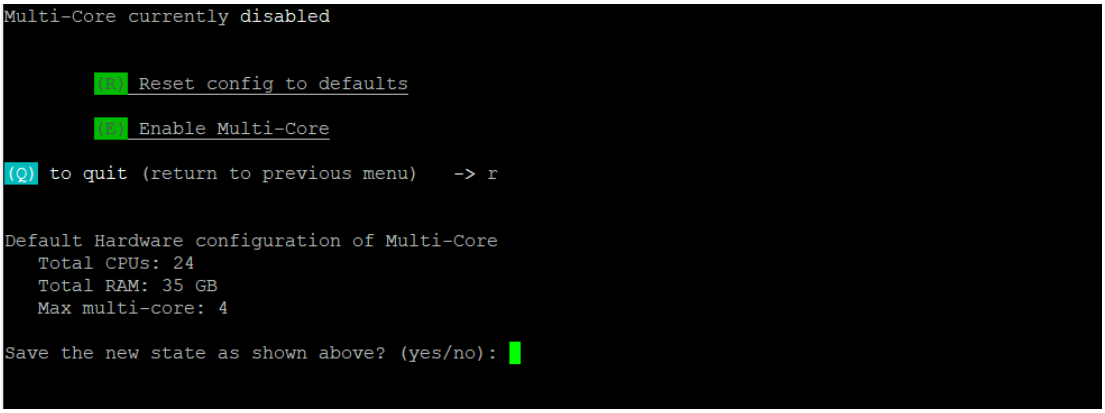
When the underlying AirDefense hardware system meets the above basic requirements, these options will be enabled for use.



4 Select **(E) Enable Multi-core** option to enable the feature.

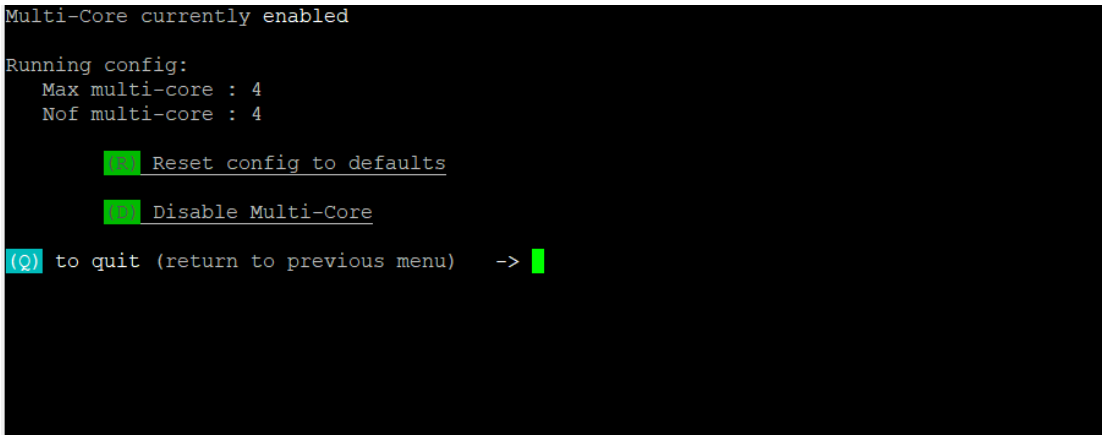
The AirDefense server calculates the number of CPUs and amount of RAM to assign to support the multicore feature. These values are calculated based on the available CPUs and RAM on the server's physical hardware.

The following screen displays.



Once the above calculations are done, they are applied to the AirDefense server and these values are stored internally on the server.

5 Enter `Yes` into the prompt to save the configuration.



Once the configuration is saved and you exit the menu, AirDefense system will automatically restart all existing AirDefense processes and will restart in the multicore mode.

6 Use the **(R) Reset config to defaults** option to reset the number of assigned CPUs and assigned RAM and re-calculate these values.

Once the multicore values are recalculated, you must manually re-enable multicore.

Note

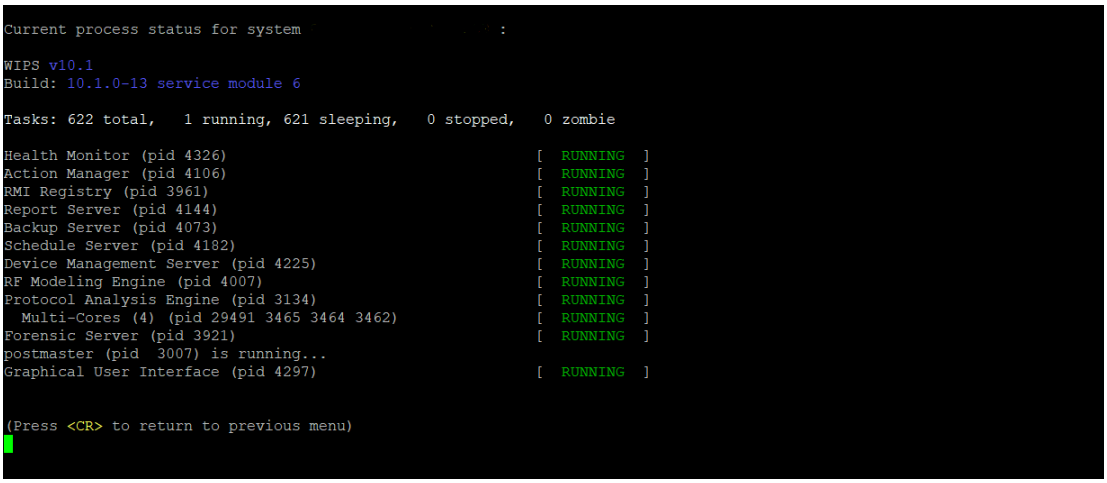
Please note that you cannot reduce the number of cores using the **(R) Reset config to defaults** option.

You can use the **(R) Reset config to defaults** option to re-calculate CPU and RAM on a virtual machine. The virtual machine will not be automatically rebooted when the **(R) Reset config to defaults** option is run on it.

You can also use the **(R) Reset config to defaults** option to restore multicore to defaults when the server configuration is changed as a part of troubleshooting other issues on your AirDefense instance.

7 Select **Status** > **Process** menu to view the current process numbers used for the multicore feature.

The following screen displays a list of various processes created by AirDefense.



Important Notes and Limitations when using Multicore

The following is a list of limitations that you need to keep in mind when enabling multicore;

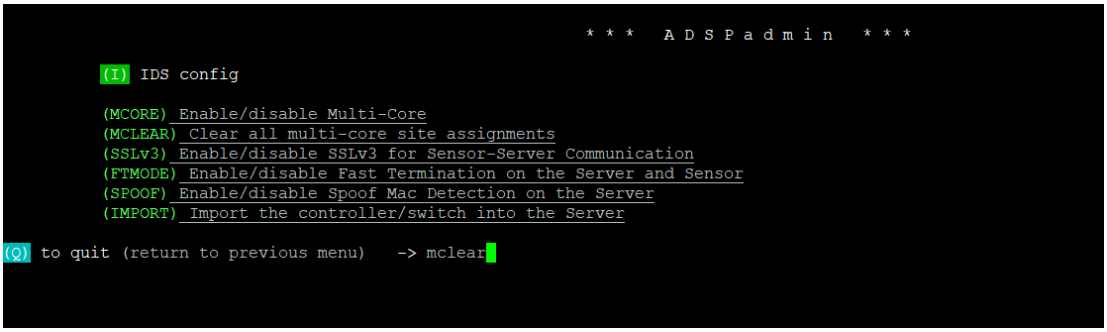
- If, due to system limitations, the new *Max Cores* value is reduced, then the sites that were assigned to the removed cores are re-assigned to the available cores. Devices for these moved sites will be re-loaded from their respective forensic files.
- If the number of available cores increases, sites are not re-assigned to the new cores. When a new site is added to your AirDefense system, it is assigned to one of the new cores.
- For multicore to work, it is required that **Auto Placement Rules** are configured properly. If these rules are not properly set, then these devices will not be allowed to report to AirDefense and their events will not be processed. Sensors still report to AirDefense without Auto Placement Rules being configured properly.
- After upgrading your AirDefense instance to version 10.1, it is recommended that you run your AirDefense server instance for a minimum of 2 to 3 hours in single core mode. This is a needed step

as the system needs to recalibrate its database with old data and make it ready for multicore configuration.

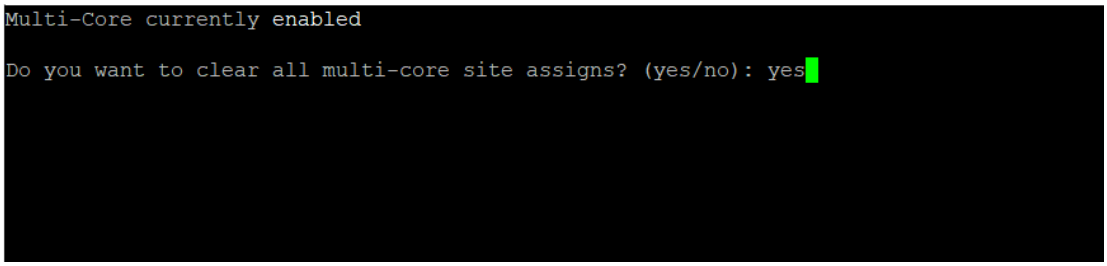
3 Clearing Existing Multicore Site Assignments

In an existing multicore deployment of an AirDefense server, data received from sites are assigned a particular CPU core from the available cores. Sometimes it becomes necessary to reset this configuration to increase your deployment's efficiency. Use the **(MCLEAR) Clear all multi-core site assignments** option to reset the site assignments and to force their re-assignments.

1 Navigate to the **IDS Configuration** screen and type `mclear` in the prompt on the screen.



The following prompt appears.



2 Enter `Yes` to indicate that you want to proceed with clearing all multicore site assignments.

The site to core assignments are reset.

Note

Please note the following:

1 The forensic files for the sites are not modified or lost when the site mapping to cores are reassigned.

2 There will be a delay in viewing the sites on the GUI till these sites are reassigned to their new cores.