6AOSCG0066-29A
September 2014

ADTRAN

Configuration Guide

Configuring Restricted Boot in AOS

This configuration guide outlines the steps necessary to configure the restricted boot feature in ADTRAN Operating System (AOS) devices. The guide includes an overview, provides the steps necessary to configure the feature, and additional resources to further assist in understanding the concepts presented.

This guide consists of the following sections:

Restricted Boot Overview

The ability to restrict AOS functionality upon rebooting a unit into its boot code adds a layer of security preferred in certain deployments. By enabling the restricted boot feature in AOS, a user is prohibited from performing several functions once the device is rebooted into boot code. These functions include bypassing the password, bypassing the startup configuration, erasing individual files, overwriting individual files, and copying files from flash memory.

Specifically, the following commands will no longer be allowed from the boot code when restricted boot is enabled:

bypass [passwords | startup-config]
boot config flash *<primary filename>*
boot config cflash *<primary filename>*
copy *<source file>* **startup-config**
copy cflash *<source file>* **startup-config**
copy flash *<source file>* **cflash**
copy flash *<source file>* **usbdrive0**
copy flash tftp
copy flash xmodem
copy startup-config cflash
copy startup-config usbdrive0
erase *<filename>*
erase startup-config

*The **erase file-system** and **erase *** commands are both allowed for unit recovery when **restricted boot** is enabled.*

Each of these commands are explained in depth in the *ADTRAN Operating System (AOS) Command Reference Guide* available at https://suppportforums.adtran.com.

Hardware and Software Requirements and Limitations

Introduced in AOS R11.4.0, support for restricted boot is available on AOS products as outlined in the *AOS Product Feature Matrix*, located on the ADTRAN Support Forum at https://supportforums.adtran.com.

Restricted boot can only be enabled or disabled using the CLI and is not applicable to the web-based graphical user interface (GUI).

Configuring Restricted Boot Using the CLI

To configure restricted boot in the AOS CLI, use the following steps:

- *Access the CLI on page 3*
- *Enable Restricted Boot on page 3*

Access the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1.

> NOTE *If during the unit's setup process you have changed the default IP address (10.10.10.1), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the prompt as follows:

   >enable

5. If configured, enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

   #configure terminal
   (config)#

Enable Restricted Boot

Enable the restricted boot feature using the **restricted boot** command from the Global Configuration mode as follows:

(config)**#restricted boot**

Additional Resources

There are additional resources available to aid in configuring your AOS unit. The documents listed below are available online at ADTRAN's Support Forum at https://supportforums.adtran.com.

- *AOS Command Reference Guide*
- *Security Best Practices for AOS Products*

