6AOSCG0056-29C
September 2014

ADTRAN

Configuration Guide

Configuring Privilege Levels in AOS

This configuration guide outlines the steps necessary to configure privilege levels to specific ADTRAN Operating System (AOS) command line interface (CLI) commands. The guide includes an overview of the default privilege levels, provides the steps necessary to assign commands to privilege levels, and examples to further assist in understanding the concepts presented.

This guide consists of the following sections:

Privilege Levels Overview

The CLI is a text-based method used to communicate with your AOS unit. The CLI prompts you to input commands line by line when you interface with the AOS unit. Each prompt from within AOS has a specific set of available commands and is referred to as a command mode. All of the commands within the command mode are already assigned to a default privilege level, either level 1 or level 7. Each command, or all commands in the command mode, can be reassigned to a different privilege level to prohibit or allow users access to the commands.

There are seven privilege levels used in AOS, 1 through 7. By default, only 1 and 7 are used. With this feature, a command can be set to any privilege level from 1 to 7.

NOTE *The following commands cannot have their privilege levels changed: **disable**, **do**, **enable**, **exit**, and **logout**.*

Users are assigned a privilege level which allows them access to commands configured with the corresponding privilege level or lower. If a user has level 5 privileges, they can execute any of the commands at level 5 or lower. Likewise, if a user has level 7 privileges, they can execute any command in AOS. By default, users are assigned privilege level 1 if no other privilege level is specified for them.

Understanding Command Modes

In order to navigate AOS and understand the hierarchy of commands, you should understand configuration modes, command modes, and how they correspond to command strings.

The three main configuration modes are User, Enable, and Global. The User mode provides the beginning interaction with an AOS unit and is very limited. It displays system information, allows traceroute, ping functions, and opening a Telnet session. The Enable mode is a mid-level tier allowing more functionality. From the Enable mode, you can manage startup and running configurations, manage debug functions, view show output, and enter any of the other configuration modes in AOS. The Global Configuration mode is a higher level tier allowing system-wide configuration settings, setting the system's Enable-level password(s), and access to any of the other configuration modes in AOS.

Beyond the Global Configuration mode, there are more than 100 additional configuration modes which include Interface (physical and virtual), Carrier Ethernet, Routing Protocols, Security and Services, Voice, and Virtual Private Network functions. Each of these are explained in depth in the *ADTRAN Operating System (AOS) Command Reference Guide* available at https://suppportforums.adtran.com. Each of these configuration modes corresponds to a command mode which allows the user access to a set of commands used to make changes to the AOS unit's configuration. Each command mode is identified by a unique command prompt.

There are multiple command modes in AOS and some require access to a lower tiered command mode before reaching the higher tiered command mode. Many of the command modes require entering the Global Configuration mode before you can access the actual configuration command mode. Because of this, it is recommended that you have a good understanding of AOS and the hierarchy present for command modes before attempting to create custom privilege levels.

Hardware and Software Requirements and Limitations

Introduced in AOS R10.11.0 for all AOS devices, this feature can be used on any product. However, due to its complexity, ADTRAN recommends only using it when deemed necessary for your particular network environment. Utilizing this feature requires prior knowledge of ADTRAN products and an in-depth understanding of the AOS CLI. It is not advised to change the privilege levels of commands or users without prior consideration of the recommendations outlined in the section *Preliminary Recommendations* below.

Privilege levels can only be configured using the CLI and do not apply to the web-based graphical user interface (GUI).

This feature was enhanced with AOS R11.3.0 to allow configuring privilege levels for all commands within a command mode using a single command. This functionality is explained in *Define Privilege Levels for Specific Commands on page 8*.

Security Recommendations

Before using this feature, there are some security issues to consider. Privilege levels can only be assigned using the CLI. When a user logs into the AOS GUI, the user has the ability to modify any configuration items available via the GUI, regardless of that user’s assigned privilege level. The CLI privilege level configuration will still be active when logged into the CLI, but it will not restrict configuration access in the GUI. To avoid this potential security breach, the GUI must be secured.

There are two recommendations that can be implemented to avoid this security issue:

1. Disable the GUI globally whenever the privilege level feature is used.
2. Use a portal list.

To disable the GUI globally, issue the **no http server** command from the Global Configuration mode. It is important to understand this command disables all Hypertext Transfer Protocol (HTTP) access to the AOS device. If this option is not practical, consider using portal lists instead.

A portal list designates specific user names that can access certain services in an AOS unit; such as, SSH, Telnet, or HTTP. If a user name is not part of a portal list granting GUI access, that user name is denied access to the GUI. Create a portal list using the **portal-list** <*name*> <*service*> command, where <*name*> is the portal list name, and <*service*> specifies the service allowed for the user or group of users. Once the portal list has been created, the user names can be associated with the portal list. To assign a particular user name to a portal list, add the **portal-list** <*name*> parameter to the username command as follows:

```
(config)#username <name> portal-list <name> privilege <level> password <password>
```

Refer to *Example 3: Restrict GUI Access Using a Portal List on page 13* for an example configuration. For more information about portal lists, refer to the Portal Lists section of the *Security Best Practices for AOS Products* configuration guide.

Preliminary Recommendations

Careful planning should be performed before applying privilege levels to a network environment. The following recommendations are provided to assist in preparation for creating a privilege level configuration:

1. Determine how many privilege levels will be needed. This has long term implications and will impact the configuration. If the levels are not properly planned beforehand, configuration may have to be changed later to adjust the levels as more levels are added. If creating only one or two levels, ADTRAN recommends skipping levels to leave space between them (for example, use level 3 and 5) so other levels can be added later if necessary.
2. Determine which commands need to be accessible in each level. Start from level 1 and work up to level 7. Each command entered in a lower level will be available to all the levels above it.
3. Test your levels prior to deployment. A simple method to test the configuration is to log in as the configured user, type in a command followed by **?** to display the CLI help text. If the help text for the command is visible, the user has permission to use the command.
4. Consider all commands that could potentially cause service interruption, and make sure they are configured at an appropriate high level to avoid issues (for example, changing an IP address or shutting down an interface).

Configuring the Privilege Levels Using the CLI

The following steps are necessary for configuring privilege levels in the AOS CLI:

1. *Identify Commands Needing Modification on page 5*
2. *Determine the Appropriate Command Mode on page 6*
3. *Define the User's Privilege Level on page 6*
4. *Confirm the User's Privilege Level Assignment on page 7*
5. *Define Privilege Levels for Specific Commands on page 8*

Accessing the CLI

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

1. Boot up 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)#
```

Identify Commands Needing Modification

Prior to making any configuration changes to AOS privilege levels, it is important to plan carefully. Begin by making a list of all commands a specific user will need to complete their job function. It may also be useful to review the output of the configuration necessary to perform the function in question.

For example, the following list of commands are used in Example 1, found later in this document:

show version

show interface

show ip interface brief

show ip route

show ip ospf

show ip ospf neighbor

debug ip ospf

debug ip ospf adjacency

The list above identifies specific **show** and **debug** commands that will need to have the privilege levels altered to allow a specific user access to execute the commands.

The following is an example of reviewing the configuration output to identify which commands need altering:

```
>enable
#configure terminal
(config)#interface ethernet 0/1
(config-eth 0/1)#
(config-eth 0/1)#speed 100
```

The example configuration above identifies several commands that will need the privilege levels altered but are located in different command modes. Access to the Ethernet 0/1 interface requires executing the **interface ethernet 0/1** command from the Global Configuration mode. The Global Configuration mode requires the user to execute the **configure terminal** command. Therefore, the privilege levels will need to be adjusted for all of the following commands:

configure terminal

interface ethernet ***<slot/port>***

speed 100

Determine the Appropriate Command Mode

Once the commands are identified, the next step is to determine from which command mode in AOS each command is executed. To determine this, navigate to the prompt from which the command would be executed, and enter the **show command-mode** or **do show command-mode** command, as appropriate.

> *Since all **show** commands are executed from the Enable mode, this command can be entered omitting the **do** keyword. All other command modes require the inclusion of the **do** keyword to execute a **show** command.*

For example, all **show** and **debug** commands are run from the Enable mode. To determine the name of the command mode at this prompt, enter the **show command-mode** command as follows:

```
>enable
#show command-mode
Command mode is ‘exec’
```

From the output above, it is determined that the **exec** command mode is necessary for changing the privilege level for the **show** and **debug** commands.

When there are multiple command modes to be determined, navigate to each prompt in the AOS CLI where the commands are to be run, and enter the **show command-mode** command or **do show command-mode** command as follows:

```
>enable
#configure terminal
(config)#do show command-mode
Command mode is ‘configterminal’
(config)#interface ethernet 0/1
(config-eth 0/1)#do show command-mode
Command mode is ‘interface-ethernet’
```

From the output above, it is determined that the **exec** command mode is necessary for changing the privilege level for the **show** and **debug** commands. It is also determined that the **configterminal** and **interface-ethernet** command modes are necessary to change the privilege levels for any commands entered at the Ethernet Interface Configuration mode.

Define the User’s Privilege Level

An AOS user must be assigned a privilege level equal to or greater than the privilege level of any command that user needs to be able to execute. Creating a new user and defining the privilege level is one way to accomplish this task. An alternate method is to change the privilege level of an existing user. Both of these methods are accomplished by using the **username** command. By default, if a privilege level is not specified when the user is created, the user is automatically assigned privilege level 1.

From the Global Configuration mode, create a new user and assign a privilege level using the following command:

```
(config)#username <username> privilege <level> password <password>
```

A user can access a higher privilege level than their assigned level during their current session. If provided the Enable password for the higher level, the user can issue the **enable** <*level*> command to access the higher level specified in <*level*>. For example, user **tech** has an assigned privilege level 3 but needs to enter a level 5 command. The user is given the level 5 Enable password to allow them access to the level 5 commands. The user enters the following command:

```
(config)#enable 5
```

The user is then prompted for the password:

```
password:
```

This permits the user to access all level 5 privilege level commands even though the user is logged in using their own login with level 3 privileges. The level 5 Enable password is set using the **enable password level** <*level*> <*password*> command.

Configure a Privilege Level for an SSH Public Key User

A privilege level can also be assigned to the user if secure shell (SSH) public key chain for public key based authentication is being used. The user gains access at the level specified at the time of authentication. The privilege level is assigned when configuring the username after accessing the SSH Server Public Key Configuration mode using the **ssh-server pubkey-chain** command. After accessing the SSH Server Public Key Configuration mode, the following subcommands can be used to assign a privilege level to the username:

```
(config-ssh-pubkey)#username <username> privilege <level> key-hash ssh-hash <input>
(config-ssh-pubkey)#username <username> privilege <level> key-string
```

The **privilege** <*level*> parameter specifies the privilege level for this user at the time of authentication. Valid entries are **1** to **7**. More information on configuring SSH public key chain is available in the *ADTRAN Operating System (AOS) Command Reference Guide* available at https://suppportforums.adtran.com.

Confirm the User's Privilege Level Assignment

The final step is to ensure that the user was correctly assigned a new privilege level. This is accomplished by opening a new session, logging into AOS as the user, and executing the **show privilege** command as follows:

```
Username: <username>
password: <password>
#
#show privilege
Current privilege is 3
```

You can also enter **?** command to view available commands, as follows:

```
#?
```

Define Privilege Levels for Specific Commands

Once you have identified the commands that need to be used along with the corresponding command modes, use the **privilege** command to assign the commands to the appropriate privilege levels. Use the **all** keyword to change the privilege level for all commands in the command mode or commands beyond the specified command string. Use the <*command string*> variable to change the privilege level on the specified command. Using the **all** keyword in conjunction with the <*command string*> variable is useful for changing the privilege level on commands with several parameters, such as **show** and **debug** commands.

> NOTE *As new commands are introduced in future AOS updates, the privilege level of the new commands must be altered for your configuration.*

The command mode name must be entered exactly in order to execute this command. Because the available command modes differ between AOS products, a reliable method for learning the available command mode names is to use the CLI help. Enter the **privilege ?** command to display a list of all available command modes on the AOS device.

From the Global Configuration mode, assign a command privilege level using the following command:

#privilege <*mode*> [**all**] **level** <*level*> [<*command string*>]

Apply to All Commands in Command Mode

For example, the following entry assigns the privilege level 5 to all commands in the Gigabit Ethernet Interface command mode:

#privilege interface-gigabit-ethernet all level 5

Apply to One Specific Command

For example, the following entry assigns the privilege level 4 to the **show version** command:

#privilege exec level 4 show version

Apply to a Group of Commands Within a Command Mode

For example, the following entry assigns the privilege level 3 to all **show ip route** commands:

#privilege exec all level 3 show ip route

The following is a list of commands to which the previous example assigns privilege level 3:

show ip route

show ip route <*ipv4 address*>

show ip route <*ipv4 address*> <*subnet mask*>

show ip route <*ipv4 address*> **longer-prefixes**

show ip route <*ipv4 address*> <*subnet mask*> **longer-prefixes**

show ip route bgp

show ip route bgp verbose

show ip route connected

show ip route ospf

show ip route ospf verbose

show ip route rip

show ip route rip verbose

show ip route static

show ip route static verbose

show ip route summary

show ip route summary realtime

show ip route table

show ip route vrf <*name*>

show ip route vrf <*name*> <*ipv4 address*>

show ip route vrf <*name*> <*ipv4 address*> <*subnet mask*>

show ip route vrf <*name*> <*ipv4 address*> **longer-prefixes**

show ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **longer-prefixes**

show ip route vrf <*name*> **bgp**

show ip route vrf <*name*> **connected**

show ip route vrf <*name*> **ospf**

show ip route vrf <*name*> **rip**

show ip route vrf <*name*> **static**

show ip route vrf <*name*> **summary**

show ip route vrf <*name*> **table**

NOTE *The preceding command list is for illustrative purposes only and displays all possible variations of the **show ip route** command as of the R10.11.0 release. Not all command parameters are applicable to all hardware platforms. Therefore, your particular device may not be capable of executing all parameters listed above.*

Example Configurations

The following examples provide a few scenarios to illustrate and improve your understanding of the privilege level feature. The configuration parameters entered in these examples are sample configurations only. These applications should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. These configurations should not be copied without first making the necessary adjustments to ensure it will function properly in your network.

Example 1: Provide a User Access to Specific Show and Debug Commands

This example illustrates creating a specific user (**tech**) who has access to the AOS device but is only allowed access to certain **show** and **debug** commands to perform specific troubleshooting methods. No other commands are allowed to be executed by the user **tech**. The following is a list of the specific commands that are required for this user:

show version

show interface

show ip interface brief

show ip route

show ip ospf

show ip ospf neighbor

debug ip ospf

debug ip ospf adjacency

Both the user **tech** and the preceding commands must be assigned the same privilege level. By default, most **show** and **debug** commands have a default privilege level of 1. This means that all the basic **show** and **debug** commands would be accessible to the user **tech**. Because the user **tech** only requires access to the specific **show** and **debug** commands listed previously, the rest of the **show** and **debug** commands must be elevated to a level higher than the level selected for the user **tech**.

All **show** and **debug** commands are natively run from Enable mode (command mode **exec**), so you will enter that mode to execute the **show command-mode** command. To discover which command mode to use for the permitted commands listed above, execute the following command from the Enable mode:

```
#show command-mode
Command mode is ‘exec’
```

The output above informs you to use the command mode **exec** to assign privilege levels to these commands.

Next, from the Global Configuration mode, create a new user (**tech)** and assign the privilege level 3, as follows:

```
#configure terminal
(config)#username tech level 3 password “adtran”
```

Once the user is created, elevate all the **show** and **debug** commands to a higher level (level 7 in this example) so that they are not available to privilege level 3 users. (Later, you will specify the individual commands that the user is permitted to execute by changing their privilege levels.) Use the **privilege** <*mode*> **all** command to include all **show** and all **debug** commands as follows:

```
(config)#privilege exec all level 7 show
(config)#privilege exec all level 7 debug
```

Next, specify the individual commands that are permitted for the user **tech** by assigning privilege level 3 as follows:

```
(config)#privilege exec level 3 show version
(config)#privilege exec level 3 show interface
```

```
(config)#privilege exec level 3 show ip interface brief
(config)#privilege exec level 3 show ip route
(config)#privilege exec level 3 show ip ospf
(config)#privilege exec level 3 show ip ospf neighbor
(config)#privilege exec level 3 debug ip ospf
(config)#privilege exec level 3 debug ip ospf adjacency
```

The privilege level configuration should now be finished. Exit the session and log in as the tech user to confirm the configuration.

```
Username: tech
password: adtran
#
```

Ensure the privilege level is correct by issuing the **show privilege** command:

```
#show privilege
Current privilege is 3
```

Use the help **?** command to access the help and view available commands:

```
#?
show            - Show system information
debug           - Debugging functions

#show ?
interfaces      - Interface Table
ip              - IP information
version         - System software and hardware versions

#show ip ?
interface - IP interface status and configuration
ospf            - Display OSPF information
route           - IP routing table

#debug ?
ip              - IP information

#debug ip
ospf            - OSPF information
```

In summary, the following are all the commands required for this example:

```
username tech level 3 password “adtran”
privilege exec level 3 show version
privilege exec level 3 show interface
privilege exec level 3 show ip interface brief
privilege exec level 3 show ip route
privilege exec level 3 show ip ospf
privilege exec level 3 show ip ospf neighbor
privilege exec level 3 debug ip ospf
privilege exec level 3 debug ip ospf adjacency
privilege exec all level 7 show
privilege exec all level 7 debug
```

Example 2: Provide a User Basic Interface Level Configuration Access

This example illustrates creating a specific user (**tech2**) who has access to all native level 1 **show** and **debug** commands. Additionally, the user is given access to the **show running-config** command (the **show running-config** defaults to level 7) and is permitted to change the IP address or shutdown the Ethernet 0/1 interface. This example does not elevate the privilege level of all commands, instead it creates a new user with privilege level 4 and assigns the privilege level 4 to the specific interface commands. By assigning a higher privilege level to the user, access is granted to all lower privilege level commands, such as the **show** and **debug** commands, without altering the command's privilege level.

From the Global Configuration mode, create a new user (**tech2)** and assign the privilege level 4, as follows:

```
#configure terminal
(config)#username tech2 level 4 password "adtran"
```

To discover which command mode to use for the permitted commands, execute the following command from the Enable mode and the specific interface configuration mode:

```
#show command-mode
Command mode is 'exec'
#configure terminal
(config)#do show command-mode
Command mode is 'configterminal'
(config)#interface ethernet 0/1
(config eth-0/1)#do show command-mode
Command mode is 'interface-ethernet'
```

> NOTE *A method does not exist to allow you to specify all interface modes for privilege level configuration. You must set the command privilege level for each interface you wish to permit the user access.*

The output above identifies the command mode **exec** to assign privilege levels for the **show running-config** command and **interface-ethernet** for the Ethernet 0/1 interface commands. Also identified is the command mode **configterminal** which is necessary to access the Ethernet interface. Assign privilege level 4 to each of the permitted commands as follows:

```
(config)#privilege exec level 4 show running-configuration
(config)#privilege exec level 4 configure terminal
(config)#privilege configterminal level 4 interface-ethernet
(config)#privilege interface-ethernet level 4 ip address
(config)#privilege interface-ethernet level 4 shutdown
```

The privilege level configuration is now complete. Exit the session and log in as the user **tech2** to confirm the privilege level configuration.

```
username: tech2
password: adtran
#show privilege
Current privilege is 4
#?
#configure terminal
(config)#?
do              - Execute a root command
interface       - Select an interface to configure
exit            - Exit from configure mode
no              - Negate a command or set its defaults

(config)#interface eth 0/1
(config eth-0/1)#?
exit            - Exit from configure mode
ip              - Internet Protocol Version 4
no              - Negate a command or set its defaults
shutdown        - Shutdown Ethernet interface
```

In summary, the following are all the commands required for this example:

```
username tech2 level 4 password “adtran”
!
privilege exec level 4 show running-configuration
privilege interface-ethernet level 4 ip address *
privilege interface-ethernet level 4 shutdown
privilege exec level 4 configure terminal
privilege configterminal level 4 interface ethernet *
```

Example 3: Restrict GUI Access Using a Portal List

The following example illustrates using a portal list to restrict a level 5 user from using the GUI, while retaining all CLI services available to them. In this configuration, a portal list is created named **NotHTTP** allowing access to the FTP, SSH, telnet, and console services only. The user **tech** is assigned this portal list and privilege level 5. The user **tech** will not have access to the GUI interface, but will have access to the CLI at privilege level 5.

```
Portal-list NotHTTP ftp console ssh telnet
!
Username TECH portal-list NotHTTP privilege 5 password ADTRAN
```

Command Summary

The following table summarizes the commands used to configure new privilege levels for the CLI in AOS.

Table 1. Privilege Level Command Summary

Command	Description
(config)#**enable** [**password** <*password*>] [**level** <*level*> [**md5**] <*password*>]	Specifies a privilege level added to the **enable password** command. Valid range for <*level*> is **1** to **7**. The default is level **7**. Enable passwords can be encrypted with md5 (using the optional md5 keyword) or ADTRAN encryption (using the **service password-encryption** command).
(config)#**privilege** <*mode*> [**all**] **level** <*level*> [<*command string*>]	Assigns a privilege level to the commands or the specified command string for the specified command mode. The valid range for <*level*> is **1** to **7**. The <*mode*> variable names the command mode for executing the affected commands. The **all** keyword is optional and changes the privilege level on all commands under the command mode or beyond the specified command string. The <*command string*> is optional and can contain and entire command or partial command string.
(config)#**username** <*user*> **privilege** <*level*> **password** <*password*>	Specifies a privilege level for the user. Valid range for <*level*> is **1** to **7**.
(config)#**ssh-server pubkey-chain** (config-pubkey-chain)#**username** <*username*> **privilege** <*level*> [**key-hash** | **key-string**]	Specifies a privilege level to be associated with an SSH user at the time the user authenticates. Valid range for <*level*> is **1** to **7**.

Troubleshooting

Before and after configuring the privilege levels, there are several commands that can be issued in the CLI to assist in troubleshooting. This section explains these commands and how they can be useful.

Use the **show command-mode** command to identify the command mode to which a command string belongs. Navigate to the area within the CLI from which the command is executed:

```
>enable
#show command-mode
Command mode is ‘exec’
```

Use the **show privilege** command to display the privilege level assigned to the user currently logged into AOS. This command is executed after a user logs into AOS to verify their current privilege level.

```
Username: tech
password: tech
#
#show privilege
Current privilege is 3
```

Additional Resources

There are additional resources available to aid in configuring your AOS unit. Many of the topics discussed in this guide are complex and may require additional information. The documents listed below are available online at ADTRAN's Support Forum at https://supportforums.adtran.com.

- *AOS Command Reference Guide*
- *Configuring SSH Public Key Authentication*