Managing User Configuration, Cisco Catalyst PON Series Switches

First Published: 2020-11-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

User Management

Overview of User Management

User management allows you to manage users, user levels, user permissions, and other user-related tasks. There are three user levels:

- Normal user: Normal users have the lowest privilege level. They can only enter execution configuration mode and view system configuration information. However, normal users cannot make any configuration changes, including modifying their own password.
- Administrator: Administrators have all the rights of normal users, including configuring a device and modifying their own password. However, administrators cannot add new users or modifying the passwords of other users.

  Note Unless otherwise specified, all the configuration logging in references indicate an admin logging in.

- Super user: A super user is the default user created in a device. A device can have only one super user who cannot be deleted. A super user has all the permissions, including performing all switch configurations, adding new users, modifying users' passwords as well as their own, and deleting users. The default login password for a super user is 123456.

Note

- A user can log in through the serial port, SSH, Telnet, or web terminal.
- Although you can create up to 15 users, only five users can be online at the same time.

About Silence Mechanism

The Silence Mechanism feature allows you to configure the consecutive login failure limit for each user. If the number of consecutive login failures exceed the limit, the corresponding user will be locked out and not allowed to log in for a certain period, which is known as silent time. This feature is disabled by default.

Configure User-Management Tasks

The following section provides information on how to configure user-management tasks.

Configure User Management

To configure user management, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**username** *username* **privilege** *pri-value* **password** {**0** | **7**} *password* **Example:** `Device(config)# username test privilege 0 password 0 123`	Adds a new user. • **username** *username*: Specifies the username of the user • **privilege** *pri-value*: Specifies the privilege level. • A privilege value of 0 or 1 refers to a normal user. • A privilege value between 2 and 15 refers to administrator user. • Super user (admin) requires no configurations. If you do not enter a permission value when you create a user, the system will automatically assign it with normal permissions. • **password** {**0** | **7**}: Specifies the password encryption type. • A value of 0 means the password is in plain text. • A value of 7 means the password is in cipher text.

	Command or Action	Purpose
		Configure the password encryption type as 0 for a new user. When you configure the **service password-encryption** command, a password configured in plain text (0) is decrypted in decompilation and the decrypted password type changes to 7. - *password*: Specifies the password. The password must be numeric.
Step 4	**service password-encryption** **Example:** `Device(config)# service password-encryption`	Saves the password in cipher text
Step 5	**username change-password** **Example:** `Device(config)# username change-password`	(Optional) Modifies the user password.
Step 6	[**no**] **username** *username* **privilege** *new-pri* **password** {**0**|**7**} *password* **Example:** `Device(config)# username test privilege 2 password 0 123`	(Optional) Modifies the user privilege level. Use the **no username** *username* command to delete a user.

Step 7	**username** *username* **terminal** {**all** | **console** | **ssh** | **telnet** | **web** | **none** }
	Example:
	`Device(config)# username test terminal all`
		(Optional) Configures the login mode.

Step 8	**username online-max** *username value* **Example:** `Device(config)# username online-max test 4`	(Optional) Configures the maximum number of online users.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Step 10	**stop** {*username* | **vty** [**all** | **user-id**] }
	Example:
	`Device(config)# stop test`
		(Optional) Forces user or users to go offline.

Step 11	[**no**] **timeout** *value* **Example:** `Device(config)# timeout 15`	(Optional) Configures the timeout value.

Configure Silence Mechanism

To configure the silence mechanism, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	[**no**] **username failmax** {*fail-value* | *username fail-value*}
	Example:
	`Device(config)# username failmax test 4`
		Configures the number of times consecutive login failures occurred.
		Use the **no username failmax** {*fail-value* | *username fail-value*} to disable the number of times consecutive login failure have occurred.

Step 4	**username silent-time** *value* **Example:** `Device(config)# username silent-time 5`	(Optional) Configures the silent time.

Monitor User Management

Use the following commands to monitor user management.

Table 1: Commands to Monitor User Management

Command	Purpose
show username [*username*]	Displays user information.
show users	Displays online users.
show username silent	Displays the silence configurations.

Example: Configuring User Management

The following example shows how to configure user management:

```
Device> enable
Device# configure terminal
Device(config)# username test privilege 0 password 0 123
Add user successfully.
```

```
Device(config)# show running-config oam
![OAM]
username test privilege 0 password 0 123
ipaddress 192.168.1.1 255.255.255.0 0.0.0.0
Save the user password in cipher text
Device(config)# service password-encryption
Device(config)# show running-config oam
![OAM]
service password-encryption
username test privilege 0 password 7 884863d2
ipaddress 192.168.1.1 255.255.255.0 0.0.0.0
```

CHAPTER 2

Configuring Second-Tier Authentication

Overview of Second-Tier Password Authentication

A normal user has permission only to enter execution mode to view configuration information. A normal user cannot enter configuration mode to modify the configuration.

A second-tier password allows a normal user to pass second-tier authentication and perform all administrator tasks. The Second-Tier Password Authentication feature is disabled by default.

A second-tier password can be used for both local and remote authentication. If user management is configured with local authentication, the second-tier password is also authenticated with local authentication. If user management is configured with remote authentication, the second-tier password is also authenticated with remote authentication.

With local authentication configured, if a normal user logs in to the privileged mode, the device prompts the user for the password. A normal user needs to enter a second-tier password for successful authentication. With remote authentication configured, if a normal user logs in to the privileged mode, the device automatically uses the configured username and second-tier password for successful authentication.

Configure Second-Tier Password Authentication

To configure second-tier password authentication, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **username privilege-auth** **Example:** `Device(config)# username privilege-auth`	Enables authentication. Use the **no username privilege-auth** to disable authentication.
Step 4	**username change-privilege-pwd** {**0** | **7**} *password* **Example:** `Device(config)# username change-privilege-pwd 4 123`	Configures the password for second-tier password authentication. If the password is selected as 0, it indicates that the password is in plain text. If you select 7, the password is in cipher text. You must use the corresponding plain text for authentication.
Step 5	[**no**] **username privilege-auth-remote-user** *username* **Example:** `Device(config)# username privilege-auth-remote-user test`	Configures the username for second-tier password authentication. Use the **no username privilege-auth-remote-user** *username* to remove the username.

Monitor Second-Tier Authentication

Use the following command to monitor second-tier authentication.

Table 2: Command to Monitor Second-Tier Authentication

Command	Purpose
show username privilege-auth	Displays the second-tier password authentication configuration.

ConfigurationExample:ConfiguringSecond-TierAuthentication

The following example shows how to create a normal user with username and password as **test/test**:

```
Device> enable
Device# configure terminal
Device(config)# username test privilege 0 password 0 test
```

The following example shows how to log in as a normal user if second-tier password authentication is not configured:

```
Device> enable
Device# configure terminal
```

```
Device(config)# quit
Username:test
Password:****
```

The following example shows how to configure a username for second-tier password authentication (it defaults to local authentication, and the authentication is optional):

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth-remote-user test
```

The following example shows how to configure a password for second-tier password authentication. (When a user enters privileged mode, the password is required.)

```
Device> enable
Device# configure terminal
Device(config)# username change-privilege-pwd 0 123456
Please input your login password : ****
Change password successfully.
```

The following example shows the error message when the wrong password is entered:

```
Device> enable
Please input password : ****
Password is error.
Device>
```

CHAPTER 3

Configuring Remote Authentication

Overview of Remote Authentication

The User Management feature manages all the tasks related to user authentication and authorization. The types of authentication and authorization are dependent on the device they are performed. If authentication and authorization are performed by the device itself, it is called local authentication. If authentication and authorization are performed on an authentication server such as a RADIUS server, it is called remote authentication.

Remote authentications work only if the user login credentials are stored on the authentication server and a connection exists between the device and the authentication server.

Local authentication is used by default.

Remote authentication supports RADIUS authentication and TACACS+ authentication. You can configure both remote authentication and local authentication for a device. However, the remote authentication takes precedence. Moreover, local authentication is attempted only when remote authentication fails.

Configure Remote Authentication

The following sections provide remote authentication configuration information.

Configure Local Authentication

To configure local authentication, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**muser local** **Example:** `Device(config)# muser local`	Enables local authentication mode.

Configuring RADIUS Remote Authentication

Configuring RADIUS remote authentication involves the following tasks:

1. Configure the RADIUS remote authentication mode.
2. Configure the RADIUS authentication server.
3. Configure the RADIUS domain configurations.

Configure the RADIUS Remote Authentication Mode

To configure the RADIUS remote authentication mode, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**muser radius** *radius-name* {**pap** | **chap**} [**account** |**local**] **Example:** `Device(config)# muser radius r1 pap`	Enables RADIUS remote authentication.

Configure the RADIUS Authentication Server

To configure the RADIUS authentication server, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa** **Example:** `Device(config)# aaa`	Enters AAA configuration mode.
Step 4	**radius host** *radius-name* **Example:** `Device(config-aaa)# radius host r1`	Configures the RADIUS server name.
Step 5	{**primary-auth-ip** | **second-auth-ip**} *ip-address auth-port* **Example:** `Device(config-aaa-radius-r1)# primary-auth-ip 192.0.2.1 20`	Configures the RADIUS authentication server address and port details.
Step 6	**auth-secret-key** *key-value* **Example:** `Device(config-aaa-radius-r1)# auth-secret-key 10`	Configures the RADIUS authentication key.
Step 7	**preemption-time** *value* **Example:** `Device(config-aaa-radius-r1)# preemption-time 2`	(Optional) Configures the recovery time to change to the primary server. **Note** The default value is 0. Configuring the default value indicates no changeover.

Configure the RADIUS Domain Configurations

To configure the RADIUS domain configurations, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**aaa** **Example:** `Device(config)# aaa`	Enters AAA configuration mode.
Step 4	**domain** *domain-name* **Example:** `Device(config-aaa)# domain r1`	Configures the RADIUS domain name.
Step 5	**radius host binding** *radius-name* **Example:** `Device(config-aaa-domain-r1)# radius host binding r1`	Binds the domain to the RADIUS server.
Step 6	**state active** **Example:** `Device(config-aaa-domain-r1)# state active`	Activates the domain.
Step 7	**state block** **Example:** `Device(config-aaa-domain-r1)# state block`	(Optional) Deactivates the domain.
Step 8	**exit** **Example:** `Device(config-aaa-domain-r1)# exit`	(Optional) Returns to AAA configuration mode.

Step 9	**default domain-name** {**enable** *domain-name* | **disable**}
	Example:
	`Device(config-aaa)# default domain-name enable domain1`
		(Optional) Enables or deletes the default domain.
		Use the **default domain-name enable** *domain-name* command to enable the default domain.
		Use the **default domain-name disable** command to delete the default domain.

Configure TACACS+ Remote Authentication

To configure TACACS+ remote authentication, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**muser tacacs+** [**author** |**account** |**command-account** |**local**] **Example:** `Device(config)# muser tacacs+`	Enables TACACS+ remote authentication mode. • **author**: Allows login authorization through the TACACS+ server • **account**: Manages login accounting through the TACACS+ server. • **command-account**: Forwards all the command lines to the TACACS+ server through the TACACS+ account packet. • **local**: Allows local authentication when remote authentication fails.
Step 4	[**no**] **tacacs+ encrypt-key** **Example:** `Device(config)# tacacs+ encrypt-key`	(Optional) Enables password encryption. The default password encryption is clear text. Use the **no tacacs+ encrypt-key** command to disable password encryption.

Step 5	**tacacs+ authentication-type** {**ascii** | **chap** | **pap**}
	Example:
	`Device(config)# tacacs+ authentication-type ascii`
		(Optional) Configures an authentication type.
		The authentication types available are:
		• ASCII
		• Password Authentication Protocol (PAP)
		• Challenge Handshake Authentication Protocol (CHAP)
		The default is ASCII.

Step 6	**tacacs+** {**primary** | **secondary**} {**server** *ip-address*} [**encrypt-key** *value* | **key** *value* | **port** *port-num* | **timeout** *value*]
	Example:
	`Device(config)# tacacs+ primary server 192.168.1.10`
	` key 123456`
		Configures the TACACS + server.

Step 7	**tacacs+ preemption-time** *value* **Example:** `Device(config)# tacacs+ preemption-time 20`	(Optional) Configures the recovery time to change to the primary server. **Note** The default value is 0. Configuring the default value indicates no changeover.

Monitor Remote Authentication

Use the following commands to monitor remote authentication.

Table 3: Commands to Monitor Remote Authentication

Command	Purpose
show muser	Displays the authentication configuration.
show radius host [**radius-name**]	Displays the RADIUS host configuration.
show domain [*domain-name*]	Displays the domain configuration.
show tacacs+	Displays the TACACS+ configuration.

Configuration Example: Configuring Remote Authentication

The following example shows how to configure the authentication type:

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ authentication-type ascii
Device(config)# end
```

The following example shows how to configure the address and key of the primary authentication server:

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ primary server 192.168.1.10 key 123456
Device(config)# end
```

The following example shows how to configure the address and key of the secondary authentication server (No configuration is required when there is no secondary server.)

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ secondary server 192.168.1.11 key 123456
Device(config)# end
```

The following example shows how to display the TACACS+ configurations:

```
Device> enable
Device# configure terminal
Device(config)# show tacacs+
Primary Server Configurations:
IP address:         : 192.168.1.10
Connection port:    : 49
Connection timeout: : 5
Key:                : 123456
```

```
Secondary Server Configurations:
IP address:         : 192.168.1.11
Connection port:    : 49
Connection timeout: : 5
Key:                : 123456
Device(config)# end
```

The following example shows how to configure TACACS+ to perform remote authentication:

```
Device> enable
Device# configure terminal
Device(config)# muser tacacs+
Device(config)# end
```

CHAPTER 4

Configuring IP Limit

Overview of IP Limit

By default, there is no restriction on the user IP addresses that can access a device as long as a user enters the correct username and password. The IP Limit feature restricts user-based IP addresses that can log in to a device. To configure the IP Limit feature, a device must be configured first to reject access from all IP addresses and then configured with the allowed IP addresses.

The configurations of Telnet user access can also be applied to users who are logged in through SSH.

The IP Limit feature improves system security.

Configure IP Limit

To configure IP limit, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **login-access-list** {**snmp**| **ssh**| **telnet**} {*ip_address*} {*mask*}	(Optional) Allows specified IP access. • *ip_address*: IP address of the server.

	Command or Action	Purpose
	Example: `Device(config)# login-access-list telnet 192.168.1.0 0.0.0.255`	• *mask*: The subnet mask. Use the **no login-access-list** {**snmp** | **ssh** | **telnet**} **all** command to block all IP access. Use the **login-access-list** {**snmp** | **ssh** | **telnet**} **0.0.0.0** [**0.0.0.0** | **255.255.255.255**] command to allow all IP access.
Step 4	**login-access-list telnet-limit** *user-number* **Example:** `Device(config)# login-access-limit telnet-limit user-number`	(Optional) Limits the number of user logins through Telnet and enters privileged mode at the same time. *user-number*: The number of users. The range is 0 to 5.The default is 5.

Monitor IP Limit

Use the following command to monitor IP limit.

Table 4: Command to Monitor IP Limit

Command	Purpose
show login-access-list	Displays the access list configurations.

Configuration Example: Configuring IP Limit

The following example shows how to view the default access list:

```
Device> enable
Device# configure terminal
Device(config)# show login-access-list
sno  ipAddress  wildcard bits    terminal
1    0.0.0.0    255.255.255.255  snmp
2    0.0.0.0    255.255.255.255  web
3    0.0.0.0    255.255.255.255  telnet
Total [3] entry.
```

The following example shows how to block all IP access:

```
Device> enable
Device# configure terminal
Device(config)# no login-access-list telnet all
```

The following example shows how to allow the IP address 192.168.1.0/24 to access a device through telnet:

```
Device> enable
Device# configure terminal
```

```
Device(config)# login-access-list telnet 192.168.1.0 0.0.0.255
Device(config)# show login-access-list
sno  ipAddress    wildcard bits    terminal
1    0.0.0.0      255.255.255.255  snmp
2    0.0.0.0      255.255.255.255  web
3    192.168.1.0  0.0.0.255        telnet
Total [3] entry.
```

CHAPTER 5

Configuring Timeout

Overview of Timeout Period

A timeout period allows a logged-in user to be automatically disconnected after a certain period of inactivity. An inactive user is not only a security threat, but also accounts for high CPU process.

A timeout period can be configured on user connections made through Telnet, SSH, or console terminal. Timeout configurations for web terminal needs to be configured on the web.

Configure Timeout

To configure timeout, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	[**no**] **timeout** *min* **Example:** `Device# timeout 5`	(Optional) Enables and configures the timeout value. The range is 1 to 480 minutes. The default timeout value is 20 m The timeout value is enabled by default.

Monitor Timeout

Use the following command to monitor timeout.

Table 5: Command to Monitor Timeout

Command	Purpose
show running-config oam	Displays the timeout configurations.