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
```