



Managing Users

- [aaa](#), on page 3
- [auth-secret-key](#), on page 4
- [default domain-name](#), on page 5
- [domain](#), on page 6
- [login-access-list](#), on page 7
- [muser local](#), on page 8
- [muser radius](#), on page 9
- [muser tacacs+](#), on page 10
- [radius host](#), on page 11
- [radius host binding](#), on page 12
- [service password-encryption](#), on page 13
- [show domain](#), on page 14
- [show login-access-list](#), on page 15
- [show muser](#), on page 16
- [show running-config oam](#), on page 17
- [show tacacs+](#), on page 18
- [show username](#), on page 19
- [show username privilege-auth](#), on page 20
- [show username silent](#), on page 21
- [show users](#), on page 22
- [state active](#), on page 23
- [state block](#), on page 24
- [stop](#), on page 25
- [tacacs+](#), on page 26
- [tacacs+ authentication-type](#), on page 27
- [tacacs+ encrypt-key](#), on page 28
- [tacacs+ preemption-time](#), on page 29
- [timeout](#), on page 30
- [username](#), on page 31
- [username change-password](#), on page 33
- [username change-privilege-pwd](#), on page 34
- [username failmax](#), on page 35
- [username online-max](#), on page 36

- [username privilege-auth-remote-user](#), on page 37
- [username privilege-auth](#), on page 38
- [username silent-time](#), on page 39

aaa

To enter Authentication Authorization and Accounting (AAA) configuration mode, use the **aaa** command in global configuration mode.

aaa

Command Modes

Global configuration (config)

Examples

This example shows how to enter AAA configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)#
```

Related Commands

| Command | Description |
|----------------------------------|--|
| auth-secret-key | Configures a RADIUS authentication key |
| default domain-name | Enables or disables the default domain |
| domain <i>domain_name</i> | Specifies a RADIUS domain name |

auth-secret-key

To configure a RADIUS authentication key, use the **auth-secret-key** command in AAA configuration mode. To delete the configured RADIUS authentication key, use the **no** form of the command.

auth-secret-key *key*
no auth-secret-key

| Syntax Description | <i>key</i> | The secret key. |
|--------------------|------------|-----------------|
|--------------------|------------|-----------------|

Command Modes AAA configuration (config-aaa)

Usage Guidelines Use this command in the AAA configuration mode.

Examples This example shows how to configure a RADIUS authentication key

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# auth-secret-key key1
```

| Related Commands | Command | Description |
|------------------|---------|-------------------------------|
| | aaa | Enters AAA configuration mode |

default domain-name

To enable or disable the default domain, use the **default domain-name** command in AAA configuration mode.

default domain-name {**enable** *domain-name* | **disable**}

Syntax Description

| | |
|--------------------|--|
| enable | Enables the default domain. |
| <i>domain-name</i> | The default domain name The format is string. |
| disable | Disables the default domain. |

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure the default domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# radius host binding cisco
Device(config-aaa-domain-default1)# state active
Device(config-aaa-domain-default1)# exit
Device(config-aaa)# default domain-name enable domain1
Succeed in setting default domain.
```

Related Commands

| Command | Description |
|------------|-------------------------------|
| aaa | Enters AAA configuration mode |

domain

To specify a RADIUS domain name, use the **domain** *domain_name* command in AAA configuration mode.

domain *domain_name*

Syntax Description

domain_name

The name of the domain.

The format is string.

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to specify the RADIUS domain name

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain domain1
Device(config-aaa-domain-domain1)#
```

Related Commands

| Command | Description |
|---------|-------------------------------|
| aaa | Enters AAA configuration mode |

login-access-list

To allow access for specific IP addresses, use the **login-access-list** {snmp | ssh | telnet} command in global configuration mode. To block all IP addresses, use the **no login-access-list** command.

login-access-list {snmp *ip_address mask* | ssh *ip_address mask* | telnet *ip_address mask* | telnet-limit *max_user_number*}

no login-access-list {snmp {all | *ip_address mask*} | ssh {all | *ip_address mask*} | telnet {all | *ip_address mask*} | telnet-limit *max_user_number*}

| Syntax Description | | |
|--|--|--|
| snmp | | The SNMP client. |
| ssh | | The SSH client. |
| telnet | | The Telnet client. |
| all | | Deletes all IP address. |
| <i>ip_address</i> | | The IP address. |
| <i>mask</i> | | The IP address mask. |
| telnet-limit <i>max_user_number</i> | | Limit the number of Telnet user logins. The range is from 0 to 5. |

Command Modes Global configuration (config)

Usage Guidelines 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.

Examples This example shows how to delete all IP addresses from the SNMP client.

```
Device> enable
Device# configure terminal
Device(config)# no login-access-list snmp all
Delete access ip address successfully.
```

| Related Commands | Command | Description |
|------------------|-------------------------------|--|
| | show login-access-list | Displays the list of allowed IP addresses. |

muser local

To enable local authentication mode, use the **muser local** command in global configuration mode.

muser local

Command Modes Global configuration (config)

Examples

This example shows how to enable local authentication mode

```
Device> enable
Device# configure terminal
Device(config)# muser local
Config manager user authentication successfully.
```

Related Commands

| Command | Description |
|-------------------|---|
| show muser | Displays the authentication configuration |

muser radius

To enable RADIUS remote authentication, use the **muser radius** *radius_name* command in global configuration mode.

muser radius *radius_name* {**pap** | **chap**} {**account** | **local**}

Syntax Description

| | |
|--------------------|---|
| <i>radius_name</i> | The RADIUS host name. The format is string. The range is from 1 to 32. |
| pap | The password authentication protocol (PAP) |
| chap | The challenge handshake authentication protocol (CHAP) |
| account | Manages login accounting through the RADIUS server. |
| local | Allows local authentication when the remote authentication fails. |

Command Modes

Global configuration (config)

Examples

This example shows how to enable RADIUS remote authentication.

```
Device> enable
Device# configure terminal
Device(config)# muser radius cisco pap local
```

Related Commands

| Command | Description |
|-------------------|---|
| show muser | Displays the authentication configuration |

muser tacacs+

To enable TACACS+ remote authentication mode, use the **muser tacacs+** command in global configuration mode.

muser tacacs+ {**author** | **account** | **command-account** | **local**}

Syntax Description

| | |
|------------------------|--|
| 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 the remote authentication fails. |

Command Modes

Global configuration (config)

Examples

This example shows how to enable TACACS+ remote authentication.

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

Related Commands

| Command | Description |
|-------------------|---|
| show muser | Displays the authentication configuration |

radius host

To configure a RADIUS server name, use the **radius host** command in AAA configuration mode.

radius host *radius_name*

| | | |
|---------------------------|--------------------|------------------------------|
| Syntax Description | <i>radius_name</i> | The name of the RADIUS serve |
|---------------------------|--------------------|------------------------------|

Command Modes AAA configuration (config-aaa)

Usage Guidelines Use this command in the AAA configuration mode.

Examples

This example shows how to configure a RADIUS server name

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
```

Related Commands

| Command | Description |
|-------------------------|--|
| aaa | Enters AAA configuration mode |
| show radius host | Displays the RADIUS host configuration |

radius host binding

To bind a domain to the RADIUS server name, use the **radius host binding** command in AAA configuration mode.

radius host binding *radius-name*

Syntax Description

| | |
|--------------------|--|
| <i>radius-name</i> | The RADIUS name server. The format is string. |
|--------------------|--|

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to bind the RADIUS host to the domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain radius1
Device(config-aaa-domain-radius1)# radius host binding cisco
```

Related Commands

| Command | Description |
|-------------------------|--|
| aaa | Enters AAA configuration mode |
| show radius host | Displays the RADIUS host configuration |

service password-encryption

To save a password in cipher text, use the **service password-encryption** command in global configuration mode.

service password-encryption

Command Modes

Global configuration (config)

Examples

This example shows how to save a password in cipher text

```
Device> enable
Device# configure terminal
Device(config)# service password-encryption
```

show domain

To display the domain configuration, use the **show domain** command in privileged EXEC or global configuration mode.

show domain [*domain_name*]

| Syntax | Description |
|--------------------|--|
| <i>domain_name</i> | The name of the domain. The format is string. |

| Command Modes | Description |
|-------------------------------|-------------|
| Privileged EXEC (#) | |
| Global configuration (config) | |

Examples

This example shows how to display the domain configuration.

```
Device> enable
Device# configure terminal
Device(config)# show domain domain1
Default domain name : domain1
DomainName          : domain1
RADIUSServerName    : cisco
Access-limit        : disabled
AccessedNum         : 0
Scheme               : radius
State                : Block
```

Total [1] item(s).

show login-access-list

To display the list of allowed IP addresses, use the **show login-access-list** command in privileged EXEC or global configuration mode.

show login-access-list

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the list of allowed IP addresses.

```
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 telnet
2    0.0.0.0    255.255.255.255 ssh
```

Related Commands

| Command | Description |
|--|---|
| login-access-list {snmp ssh telnet} | Allows access for specific IP addresses |

show muser

To display the authentication configuration, use the **show muser** command in privileged EXEC or global configuration mode.

show muser

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the authentication configuration.

```
Device> enable
Device# configure terminal
Device(config)# show muser
Show manager user authentication.
Authentication type : local
Admin-Remote-Auth: Disable
```


show running-config oam

To display the timeout configuration, use the **show running-config oam** command in privileged EXEC or global configuration mode.

show running-config oam

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the timeout configuration.

```
Device> enable
Device# configure terminal
Device(config)# show running-config oam
![OAM]
no login-access-list snmp 0.0.0.0 255.255.255.255
service password-encryption
username text privilege 0 password 7 884863d2
banner
screen-rows per-page 55
hostname 2
telnet limit 3
exit
timeout 100
configure terminal
telnetclient timeout 2
ip icmp mask-reply
```

show tacacs+

To display the TACACS+ configuration, use the **show tacacs+** command in privileged EXEC or global configuration mode.

show tacacs+

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the TACACS+ configuration.

```
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
```

show username

To display the user information, use the **show username** command in privileged EXEC or global configuration mode.

show username *username*

| Syntax Description | <i>username</i> | The user name. |
|--------------------|-----------------|----------------|
|--------------------|-----------------|----------------|

| Command Modes | Privileged EXEC (#) Global configuration (config) |
|---------------|--|
|---------------|--|

Examples

This example shows how to view the user information.

```
Device> enable
Device# configure terminal
Device(config)# show username admin
display user information
Terminal type: C=Console, T=Telnet, S=SSH, W=Web
Global Failmax: n/a
User Name      Role      Terminal  FailMax  Fail    OnLineMax  OnLine
-----
admin          ADMIN    CTSW      n/a      0      n/a        1
```

| Related Commands | Command | Description |
|------------------|---------------------------------|-------------|
| | username <i>username</i> | Adds a user |

show username privilege-auth

To display the privilege password authentication configuration, use the **show username privilege-auth** command in privileged EXEC or global configuration mode.

show username privilege-auth

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the configuration of second-tier password authentication

```
Device> enable
Device# configure terminal
Device(config)# show username privilege-auth
Privilege-password authentication
  switch: OFF
  remote-user name: remote_admin
  password not configured
```

Related Commands

| Command | Description |
|--------------------------------|--|
| username privilege-auth | Enables privilege password authentication for a local user |

show username silent

To display a user silent period information, use the **show username silent** command in privileged EXEC or global configuration mode.

show username silent

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view a user silent period information

```
Device> enable
Device# configure terminal
Device(config)# show username silent
display user silent period information
Silent Time: 2 minutes
User Name          State      Silent End Time
-----
admin              Off       n/a
text               Off       n/a
```

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| username silent-time | Configures the silent time |
| show username | Displays the user information |

show users

To display the online users, use the **show users** command in privileged EXEC or global configuration mode.

show users

Command Modes

Privileged EXEC (#)

Global configuration (config)

Examples

This example shows how to view the online users.

```
Device> enable
Device# configure terminal
Device(config)# show users
Only 5 users logged in by telnet are allowed to be in privileged mode.
Now 1 users logged in by telnet have been in privileged mode.

User "admin" logged in at time 2001/12/09 16:53:44
Time passed after login: 0 days 0 hours 12 minutes 32 seconds
Time no operation: 0 minutes 0 seconds
Terminal: telnet 1
Transport: telnet
User's IP address: 10.65.75.54
Authentication: local
Radius hostname: N/A
```

state active

To activate a domain, use the **state active** command in AAA configuration mode.

state active

Command Modes

AAA configuration (config-aaa)

Examples

This example shows to activate a configured domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# radius host binding cisco
Device(config-aaa-domain-default1)# state active
Device(config-aaa-domain-default1)# exit
```

Related Commands

| Command | Description |
|-------------|----------------------|
| state block | Deactivates a domain |

state block

To deactivate a domain, use the **state block** command in AAA configuration mode.

state block

Command Modes AAA configuration mode

Examples This example shows how to deactivate a domain.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain default1
Device(config-aaa-domain-default1)# state block
```

Related Commands

| Command | Description |
|---------------------|--------------------|
| state active | Activates a domain |

stop

To force user or users to go offline, use the **stop** command in privileged EXEC mode.

```
stop {username | vty {all vty_list} | telnet {all terminal_id}}
```

Syntax Description

| | |
|--------------------|--|
| <i>username</i> | The username |
| all | Stops all. |
| <i>vty_list</i> | The VTY list. |
| <i>terminal_id</i> | The terminal ID The range is from 0 to 5. |

Command Modes

Privileged EXEC (#)

Examples

This example shows how to force a user offline

```
Device> enable  
Device# stop Jerry
```

tacacs+

To configure the TACACS + server, use the **tacacs+** command in global configuration mode.

tacacs+ {**primary** | **secondary**}**server** *ip_address* [{**encrypt-key** *value* | **key** *key* | **port** *port* | **timeout** *value*}]

| Syntax Description | | |
|---------------------------------|--|---|
| primary | | Configures the primary server. |
| secondary | | Configures the secondary server. |
| server <i>ip_address</i> | | The server IP address. |
| encrypt-key <i>value</i> | | The server key encryption. |
| key <i>key</i> | | The server key configuration. |
| port <i>port</i> | | The TCP port. The range is from 1 to 65535. |
| timeout <i>value</i> | | The connection timeout. The range is from 1 to 70. The default is 5. |

Command Modes Global configuration (config)

Examples

This example shows how to configure the TACACS + primary server

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

Related Commands

| Command | Description |
|---------------------|------------------------------------|
| show tacacs+ | Displays the TACACS+ configuration |

tacacs+ authentication-type

To configure an authentication type, use the **tacacs+ authentication-type** command in global configuration mode.

tacacs+ authentication-type {ascii | chap | pap}

| Syntax Description | ascii | Configures the ASCII authentication type. |
|--------------------|-------------|--|
| | chap | Configures the Challenge Handshake Authentication Protocol (CHAP) authentication type. |
| | pap | Configures the Password Authentication Protocol (PAP) authentication type. |

Command Modes Global configuration (config)

Examples

This example shows how to configure an ASCII authentication type

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

Related Commands

| Command | Description |
|---------------------|------------------------------------|
| show tacacs+ | Displays the TACACS+ configuration |

tacacs+ encrypt-key

To enable password encryption, use the **tacacs+ encrypt-key** command in global configuration mode. To disable password encryption, use the **no tacacs+ encrypt-key** command.

tacacs+ encrypt-key

no tacacs+ encrypt-key

Command Modes

Global configuration (config)

Examples

This example shows how to enable password encryption

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ encrypt-key
```

Related Commands

| Command | Description |
|---------------------|------------------------------------|
| show tacacs+ | Displays the TACACS+ configuration |

tacacs+ preemption-time

To configure the recovery time to switch to the TACACS+ primary server, use the **tacacs+ preemption-time** command in global configuration mode.

tacacs+ preemption-time *time*

| Syntax Description | <i>time</i> | The preemption time The unit in minutes. The range is from 0 to 1440. The default value is 0 |
|--------------------|-------------|--|
|--------------------|-------------|--|

Command Modes Global configuration (config)

Examples

This example shows how to configure the recovery time to switch to the TACACS+ primary server.

```
Device> enable
Device# configure terminal
Device(config)# tacacs+ preemption-time 200
```

| Related Commands | Command | Description |
|------------------|---------------------|------------------------------------|
| | show tacacs+ | Displays the TACACS+ configuration |

timeout

To configure the system idle timeout, use the **timeout** command in privileged Exec mode. To disable the system idle timeout, use the **no timeout** command.

timeout *value*

no timeout

Syntax Description

value

The system idle timeout value.

The range is 1-480. The default timeout value is 20m.

Command Modes

Privileged Exec (#)

Examples

This example shows how to configure the system idle timeout

```
Device> enable
Device# timeout 100
The idle time is : 100 minutes!
```

username

To add a user or modify an existing user privilege level, use the **username** *username* command in global configuration mode. To remove a user, use the **no username** *username* command.

username *username* {**password** {**0** | **7**}*password* | **privilege** *privilege_level* **password** {**0** | **7**}*password* | **terminal** {**all** | **console** | **none** | **ssh** | **telnet** | **web**}}

no username *username*

Syntax Description

| | |
|-------------------------------------|---|
| <i>username</i> | The username. |
| password 0 7 | The password encryption time. <ul style="list-style-type: none"> • A value of 0 means the password is in plain text. • A value of 7 means the password is in cipher text. |
| <i>password</i> | The password. |
| <i>privilege_level</i> | The privilege level. <ul style="list-style-type: none"> • 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. |
| terminal | The login mode The options are <ul style="list-style-type: none"> • console • none • SSH • Telnet • Web |

Command Modes

Global configuration (config)

Usage Guidelines

If you do not enter a permission value when you create a user, the system will automatically assign it with normal permissions.

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 de-compilation and the decrypted password type changes to 7

Examples

This example shows how to add a new user.

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

Related Commands

| Command | Description |
|--------------------------------------|---|
| show username | Displays the user information |
| username change-password | Modifies the user password |
| username change-privilege-pwd | Configures the second-tier password authentication |
| username failmax | Configures a limit on the consecutive failed login attempts |
| username online-max | Configures the duration users are online at the same time |
| username silent-time | Configures the silent time |

username change-password

To modify the user password, use the **username change-password** command in global configuration mode.

username change-password

Command Modes

Global configuration (config)

Examples

This example shows how to modify the user password

```
Device> enable
Device# configure terminal
Device(config)# username change-password
```

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |

username change-privilege-pwd

To configure the second-tier password authentication, use the **username change-privilege-pwd** command in global configuration mode.

username change-privilege-pwd {0 | 7}

Syntax Description

{ 0 | 7 }

- A value of 0 means the password is in plain text.
- A value of 7 means the password is in cipher text.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the second-tier password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username change-privilege-pwd 0 123456
```

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |

username failmax

To configure a limit on the consecutive failed login attempts, use the **username failmax** command in global configuration mode. To disable the limit on the consecutive failed login attempts, use the **no username failmax** command.

username failmax *{fail_value | username fail_value}*

no username failmax

Syntax Description

| | |
|-------------------|--|
| <i>fail_value</i> | The fail value. The range is from 1 to 100. |
| <i>username</i> | The username. |

Command Modes

Global configuration (config)

Examples

This example shows how to configure a limit on the consecutive failed login attempts.

```
Device> enable
Device# configure terminal
Device(config)# username failmax 5
```

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |

username online-max

To configure the duration users are online at the same time, use the **username online-max** command in global configuration mode.

username online-max *username value*

Syntax Description

| | |
|-----------------|---|
| <i>username</i> | The username. |
| <i>value</i> | The duration users are online at the same time The range is from 1 to 100. |

Command Modes

Global configuration (config)

Examples

This example shows how to configure the duration users are online at the same time.

```
Device> enable
Device# configure terminal
Device(config)# username online-max mark 100
```

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |

username privilege-auth-remote-user

To enable privilege password authentication for a remote user, use the **username privilege-auth-remote-user** command in global configuration mode. To disable user privilege password authentication, use the **no username privilege-auth** command.

username privilege-auth-remote-user *username*

no username privilege-auth-remote-user

Syntax Description

username The username.

Command Modes

Global configuration (config)

Examples

This example shows how to enable privilege password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth-remote-user mark
Enable Privilege-password authentication OK!
```

Related Commands

| Command | Description |
|----------------------|-------------------------------|
| show username | Displays the user information |

Related Commands

| Command | Description |
|---------------------------------|-------------------------------|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |

username privilege-auth

To enable privilege password authentication for a user, use the **username privilege-auth** command in global configuration mode. To disable user privilege password authentication, use the **no username privilege-auth** command.

username privilege-auth [**always**]

no username privilege-auth

Syntax Description

| | |
|---------------|---|
| always | Configures privilege password authentication for all users. |
|---------------|---|

Command Modes

Global configuration (config)

Examples

This example shows how to enable user privilege password authentication.

```
Device> enable
Device# configure terminal
Device(config)# username privilege-auth
Enable Privilege-password authentication OK!
```

Related Commands

| Command | Description |
|----------------------|-------------------------------|
| show username | Displays the user information |

Related Commands

| Command | Description |
|-------------------------------------|---|
| username <i>username</i> | Adds a user. |
| show username | Displays the user information. |
| show username privilege-auth | Displays the privilege password authentication configuration. |

username silent-time

To configure the silent time, use the **username silent-time** command in global configuration mode.

username silent-time *silent_time*

Syntax Description

silent_time

The silence period time.

The range is from 2 to 1440.

Command Modes

Global configuration (config)

Examples

This example shows how to configure the silent time

```
Device> enable
Device# configure terminal
Device(config)# username silent-time 100
```

Related Commands

| Command | Description |
|----------------------|-------------------------------|
| show username | Displays the user information |

Related Commands

| Command | Description |
|---------------------------------|---|
| username <i>username</i> | Adds a user |
| show username | Displays the user information |
| show username silent | Displays a user silent period information |

