

AAA Commands

- aaa accounting, on page 1
- aaa authentication attempts login, on page 4
- aaa authentication enable default, on page 4
- aaa authentication login, on page 5
- aaa authentication password-prompt, on page 7
- aaa authentication ppp, on page 7
- aaa authentication username-prompt, on page 8
- aaa authorization, on page 9
- aaa authorization config-commands, on page 10
- aaa authorization console, on page 11
- aaa authorization credential download default, on page 12
- aaa lockout-policy, on page 13
- aaa group server tacacs+, on page 14
- aaa netconf-accounting, on page 14
- ip tacacs source-interface, on page 15
- ip vrf forwarding (server-group), on page 16
- lockout-policy, on page 17
- login block-for, on page 19
- login quiet-mode access-class, on page 20
- login-rate, on page 21
- multi-factor-auth duo, on page 21
- server-private (TACACS+), on page 23
- tacacs server address ipv4, on page 24
- tacacs server key, on page 25
- tacacs server port, on page 25
- tacacs server timeout, on page 26

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use TACACS+, use the **aaa accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting { **system** | **exec** | **network** | **connection** *connection-name* | **commands** *level* } [**default**] { **start-stop** | **stop-only** } **group** *group-name*
no aaa accounting { **system** | **exec** | **connection** *connection-name* | **commands** *level* } [**default**] { **start-stop** | **stop-only** } **group** *group-name*

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
commands **connection** **exec**	Specifies the accounting method list. Enter at least one of the following keywords: • **commands**: Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**: Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**: Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
network	Runs accounting for all network-related service requests.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	Sends a stop accounting record for all cases including authentication failures regardless of whether the **aaa accounting send stop-record authentication failure** command is configured.
group *group-name*	Server groups for aaa accounting with *group-name* as character string or radius or tacacs+ as defined by **aaa group server** command.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **exec**, **commands**, **connection**, **system** keywords and **group** *group-name*, **local** , **none** methods are supported.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional method qualified: **network**
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Support for multi-group configuration is added.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional methods qualified: **group tacacs+**

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

For usage guidelines, see the Cisco IOS XE aaa accounting command.

The table below contains descriptions of keywords for AAA accounting methods.

Table 1: aaa accounting Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.

Examples

The following example shows how to define a default command accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
aaa accounting commands 15 default stop-only group tacacs+

aaa authorization commands 15 default local group tacacs+

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

aaa accounting system default start-stop group tacacs+

aaa accounting network default group tacacs+
```

The following example shows how to configure multiple groups:

```
aaa accounting commands 15 default start-stop group tacacs+ broadcast logger group radius
```

aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login**command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

aaa authentication attempts login *number-of-attempts*
no aaa authentication attempts login

Syntax Description

number-of-attempts	Number of login attempts. Range is from 1 to 25. Default is 3.

Command Default

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine whether a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

aaa authentication enable default *method1* [*method2* . . .]
no aaa authentication enable default *method1* [*method2* . . .]

Syntax Description

method1 [*method2...*]	At least one of the keywords described in the table below.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Command qualified for use in Cisco vManage CLI templates. **group** *group-name* and **enable** keywords are supported.

Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in the table below. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

For usage guidelines, see the Cisco IOS XE aaa authentication enable default command.



Note To prevent being locked out in User EXEC mode when the command **aaa authentication enable default enable** is present in the running or startup configuration, configure an enable password on the device.

Table 2: aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication. **Note** An authentication request fails over to the next authentication method only if no enable password is configured on the router.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.

Examples

```
aaa authentication enable default group tacacs-511 enable
```

aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login { **default** *list-name* } *method1* [*method2* . . .]
no aaa authentication login { **default** *list-name* } *method1* [*method2* . . .]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in. See the “Usage Guidelines” section for more information.

method1 [*method2...*]	The list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below.

Command Default

AAA authentication at login is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **default**, **group** *group-name* keyword-argument pair are supported.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional parameters qualified: , **group tacacs+**, and **local** keywords were added as methods for authentication.

Usage Guidelines

If the **default** keyword is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** keyword is not set.

For usage guidelines, see the Cisco IOS XE aaa authentication login command.

The table below describes the method keywords.

Table 3: aaa authentication login Methods Keywords

Keyword	Description
enable	Uses the enable password for authentication. This keyword cannot be used.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.

```
aaa authentication login default group tacacs+ local
```

```
aaa authentication login default group tacacs-511
```

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

aaa authentication password-prompt *text-string*
no aaa authentication password-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”).

Command Default

There is no user-defined *text-string*, and the password prompt appears as “Password.”

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication password-prompt command.

Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp *list-name method1*
no aaa authentication ppp *list-name method1*

Syntax Description

list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below.

Command Default

AAA authentication methods on serial interfaces running PPP are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. **local** keyword is supported.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication ppp command.

Table 4: aaa authentication ppp Methods

Keyword	Description
local	Uses the local username database for authentication.

Examples

The following example shows how to create a AAA authentication list called *dialinppp* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp dialinppp local
```

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

aaa authentication username-prompt *text-string*
no aaa authentication username-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”).

Command Default

There is no user-defined *text-string*, and the username prompt appears as “Username.”

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.



Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt "Enter your name here:"
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **commands** *level* | **exec** | **network** } { **default** *list-name* } [*method1* [*method2* . . .]]
no aaa authorization { **commands** *level* | **exec** | **network** } { **default** *list-name* } [*method1* [*method2* . . .]]

Syntax Description

commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility returns user profile information such as the autocommand information.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **config-commands**, **exec**, **command**, **network**, **default** keywords and **group** *group-name*, **local** , **none** methods are supported
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional methods qualified: **group tacacs+**

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization command.

The table below describes the method keywords.

Table 5: aaa authorization Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **aaa group server** *group-name* command.
group tacacs+	Uses the list of all TACACS+ servers for authorization as defined by the **aaa group server tacacs**+ command.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Examples

The following example shows how to define aaa authorization:

```
aaa authorization commands 15 default local group tacacs+
aaa authorization network default local
aaa authorization commands 2 default group tacacs-511 local none
```

aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the **aaa authorization config-commands** command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

aaa authorization config-commands
no aaa authorization config-commands

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage CLI template

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization config-commands command.

Examples

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

aaa authorization console
no aaa authorization console

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization console command.

Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode. To disable the authorization method list from using the local credentials, use the **no** form of this command.

aaa authorization credential download { **default** | **auth_list** } [**cache**] [**group**] [**if-authenticated**] [**local**] [**none**] [**radius**] [**tacacs**]
no aaa authorization credential download { **default** | **auth_list** }

Syntax Description

default	Specifies the authorization methods that follow the default list.
auth_list	Specifies the named authorization method list.
cache	(Optional) Uses a cache server group for authorization.
group	(Optional) Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **aaa group server group-name** command.
if-authenticated	(Optional) Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	(Optional) Uses the local database for authorization.
none	(Optional) Indicates that no authorization is performed.
radius	(Optional) Uses RADIUS for authorization.
tacacs	(Optional) Uses TACACS+ for authorization.

Command Default

Disabled, unless the **aaa authorization** command is configured, in which case all config-commands require authorization.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the **aaa authorization credential-download** command for downloading EAP credentials from the local database or from the RADIUS, or LDAP server as defined by aaa group server command.

Examples

The following example shows how to set an authorization method list to use local credentials:

```
Device(config)# aaa authorization credential-download default local
```

The following example shows how to configure four groups to set an authorization method list:

```
Device(config)# aaa authorization credential-download Ap-Auth group radius-group cache ldap
 local if-authenticated
```

aaa lockout-policy

To configure the authentication, authorization, and accounting (AAA) user lockout policy in system configuration mode for Cisco SD-WAN Manager, use the **aaa lockout-policy** command in system configuration mode.

To disable the system lockout policy, use the **no** form of this command.

aaa lockout-policy **fail-attempts** *attempt-count* **fail-interval** *fail-int* **lockout-interval** *lockout-int*

no aaa lockout-policy

Syntax Description

fail-attempts *attempt-count*	Specifies the number of failed authentication attempts before the user is locked out. Default: 5 Range: 1 - 3600
fail-interval *fail-int*	Specifies the duration in seconds of failed authentication attempts before the user is locked out. Default: 900 Range: 1 - 3600
lockout-interval *lockout-int*	Specifies the lockout duration in seconds. Default: 900 Range: 1 - 3600

Command Modes

system configuration (config-system)

Command History

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.12.1	This command is supported in Cisco SD-WAN.

Usage Guidelines

Use the **aaa lockout-policy** command to configure notifications for unauthorized activity.

Examples

The following example shows how to configure the lockout policy:

```
sdwan-manager(config)# system
sdwan-manager(config-system)# aaa
```

```
sdwan-manager(config-aaa)# lockout-policy lockout-interval 600 fail-interval 60 fail-attempts
 5
```

In the above example, **fail-attempts** is 5, **fail-interval** is 60, and **lockout-interval** is 600. The result is that if there are 5 failed attempts to log in within 60 seconds, then the Cisco SD-WAN Manager does not allow additional attempts for a period of 600 seconds (10 minutes).

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server** tacacs+ command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*
no aaa group server tacacs + *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.2.1r	Command qualified for use in Cisco vManage templates.

Usage Guidelines

For usage guidelines, refer to Cisco IOS XE aaaa group server tacacs+ command.

Examples

The following example shows the configuration of an AAA server group named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
server 10.1.1.1
server 10.2.2.2
server 10.3.3.3
```

aaa netconf-accounting

To enable authentication, authorization, and accounting (AAA) accounting of netconf services for billing or security purposes when you use TACACS+, use the **aaa netconf-accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa netconf-accounting

aaa netconf-accounting { **system** | **exec** | **network** | **connection** *connection-name* }

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
network	Runs accounting for all network-related service requests.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.15.1	Command is introduced.

Usage Guidelines

The **system aaa netconf-accounting** configuration depends on **system aaa accounting**. Only when **system aaa netconf-accounting** is configured, the netconf-accouting also can be configured.

When **system aaa accounting** is deleted, **system aaa netconf-accounting** is also deleted. However, when you delete **system aaa netconf-accounting**, there is no effect on **system aaa accounting**.

Example

The following example shows how to configure netconf accounting:

```
Device (config)# system
Device (config)# aaa netconf-accounting aaalist1
Device (config)#
```

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration mode. To disable use of the specified interface ip address, use the **no** form of this command.

ip tacacs source-interface *interface-name*
no ip tacacs source-interface *interface-name*

Syntax Description

interface-name	Name of the interface that TACACS+ uses for all its outgoing packets.

Command Default

None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **ip tacacs source-interface** command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used if the interface is in the up state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses. You can use the **ip tacacs source-interface** command when the router has many interfaces and ensure that all TACACS+ packets from a particular router have the same IP address. The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a down state, TACACS+ reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

Example

The following example configures TACACS+ to use the IP address of the loopback0 interface for all outgoing TACACS+ packets.

```
Device(config)# ip tacacs source-interface loopback0
```

ip vrf forwarding (server-group)

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the no form of this command.

ip vrf forwarding *vrf-name*
no ip vrf forwarding *vrf-name*

Syntax Description

name	Name assigned to a VRF.

Command Default Server groups use the global routing table.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user using a AAA

```
aaa group server tacacs+ tacacs-511
server-private 172.16.0.1 key 7 110a1016141d
ip vrf forwarding 511
```

lockout-policy

To configure Cisco SD-WAN Manager and other controllers to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period, or who have not logged in for a designated number of days, use the **lockout-policy** command in global configuration mode. To disable the lockout policy, use the **no** form of this command.

lockout-policy {[fail-attempts *attempts* **fail-interval** *fail-interval* [**lockout-interval** *lockout-interval*]] [**num-inactive-days** *days*]}

no lockout-policy {[fail-attempts *attempts* **fail-interval** *fail-interval* [**lockout-interval** *lockout-interval*]] [**num-inactive-days** *days*]}

Syntax Description

fail-attempts *attempts*	Specifies the number of consecutive times a user unsuccessfully attempts to log in to Cisco SD-WAN Manager or other controllers after which the user is locked out. **Note** Attempting to log in through the CLI without providing a password is counted as a failed login attempt. Default: 5 Range: 1 through 3600
fail-interval *fail-interval*	Specifies the period, in seconds, in which consecutive unsuccessful login attempts are counted. For example, if this period is set to 10 seconds and the number of failed login attempts is set to 5, a user is locked out if the user makes 5 consecutive unsuccessful login attempts within 10 seconds. Default: 900 Range: 1 through 3600

lockout-interval *lockout-interval*	Specifies the period, in seconds, after which a user who is locked out because of unsuccessful login attempts can log in. If you do not configure this period, an administrator must manually unlock the account of a locked-out user. Default: 900 Range: 0 through 3600
num-inactive-days *days*	Specifies the number of days since a user last logged in to Cisco SD-WAN Manager or other controllers after which the user is locked out. Range: 2 through 365

Command Default

This command is disabled, and so a lockout policy is not in effect. In this case, by default, Cisco SD-WAN Manager and other controllers allow five consecutive unsuccessful password attempts before an account is locked for 15 minutes or until an administrator unlocks it.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.12.1a	This command was introduced.

Usage Guidelines

When you configure a lockout policy, users who violate the policy cannot log in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager and other controllers.

Examples

The following example shows how to configure a lockout policy of three failed login attempts over a period of 300 seconds, and a reset period of 100 seconds:

```
device(config-system)# aaa
device (config-aaa)# lockout-policy
device (config-lockout-policy)# fail-attempts 3 fail-interval 300 lockout-interval 100
```

The following example shows how to configure an inactivity lockout period of 30 days for user logins:

```
device(config-system)# aaa
device (config-aaa)# lockout-policy
device (config-lockout-policy)# num-inactive-days 30
```

Related Commands

Command	Description
aaa authentication attempts login	Sets the maximum number of login attempts that are permitted before a session is dropped.

Command	Description
multi-factor-auth duo	Configures controllers to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for**command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*
no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Command Default

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE login block-for command.

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Device(config)# login block-for 100 attempts 15 within 100
Device(config)# exit
Device# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged.
All failed login is logged.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login
No login delay has been applied.

     No Quiet-Mode access list has been configured.

     All successful login is logged.


     Router NOT enabled to watch for login Attacks
```

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class**command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-nameacl-number*}
no login quiet-mode access-class {*acl-nameacl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Command Default

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE login quiet-mode access-class command.

Quiet-mode does not support **vrf-also** command. When the router is on quiet mode, the ACL restricts the access to the device. This feature works only when you try to access the device through transport or a non-vrf interface.

Examples

The following example shows how to configure your router to accept hosts only from the ACL “myacl” during the next quiet period:

```
Device(config)# login quiet-mode access-class myacl
```

login-rate

To configure a threshold for detecting frequent logins, use the **login-rate** command in alarms configuration mode.

Use the **no** form of the command to clear the configuration.

Cisco SD-WAN Manager

login-rate { **interval** *seconds* | **num-logins** *count* }

no login-rate

Syntax Description

interval *seconds*	Specify the interval in seconds.
num-logins *count*	Specify the number of logins to be reached before generating an alarm.

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.12.1	This command was introduced.

Examples

The following example shows how to configure the login-rate alarm parameters:

```
sdwan-manager(config)# system
sdwan-manager(config-system)# alarms
sdwan-manager(config-alarms)# login-rate interval 60 num-logins 3
```

Related Commands

Command	Description
alarms	Configures CPU-usage watermarks and polling interval.
show alarms	Displays alarm history and watermarks for CPU, memory, and disk usage, and the disk read and write speeds.

multi-factor-auth duo

To configure Cisco SD-WAN Manager and other controllers to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in, use the multi-factor-auth duo command in global configuration mode. To disable Duo MFA authentication for controllers, use the no form of this command.

multi-factor-auth duo api-hostname *name* **integration-key** *i-key* **secret-key** *s-key*
proxy *proxy-url*

no multi-factor-auth duo api-hostname *name* **integration-key** *i-key* **secret-key** *s-key*

proxy *proxy-url*

Syntax Description

api-hostname *name*	Specifies the API hostname (api-hostname) of your Duo account.
integration-key *i-key*	Specifies the integration key (Ikey) of your Duo account.
secret-key *s-key*	Specifies the secret key (Skey) of your Duo account.
proxy *proxy-url*	Specifies the URL of the proxy that is used to access the Duo server if Cisco SD-WAN Manager is behind a firewall. If an HTTP proxy is configured for Cisco SD-WAN Manager, this proxy is the default value.

Command Default

This command is disabled. So, Cisco SD-WAN Manager and other controllers do not require Duo MFA to verify the identity of users before they log in.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.12.1a	This command was introduced.

Usage Guidelines

- You must have a Duo account with local users created on that account.
- When you configure this command, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password to log in to Cisco SD-WAN Manager or other controllers.
- Duo MFA does not apply to the admin user by default. If you want to enable Duo MFA for the admin user, configure multi-factor-auth duo, then enter the admin-auth-order command.
- If Cisco SD-WAN Manager or another controller does not have internet access, use the following commands to configure proxy information for the device on which Duo MFA is enabled. Enter these commands either from the command line of the device or its device template. This configuration provides access to the Duo MFA feature. The device can be a Cisco SD-WAN Manager server, a Cisco Catalyst SD-WAN Validator, or a Cisco Catalyst SD-WAN Controller.

```
vm # config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key s-key
vm(config-duo)# integration-key i-key
vm(config-duo)# proxy proxy-url
vm(config-duo)# commit
```

Examples

The following example shows how to configure Cisco SD-WAN Manager and other controllers to require Duo MFA to verify the identity of users before they can log in:

```
device(config-system)# aaa
device (config-aaa)# multi-factor-auth duo
device (config-duo)# api-hostname api-xxxxxxxx.duosecurity.com
device (config-duo)# integration-key DIMVTNxxxxxxxxxx
device (config-duo)# secret-key Mxxxxxxxxxxxxx
```

Related Commands

Command	Description
aaa authentication attempts login	Sets the maximum number of login attempts that are permitted before a session is dropped.
lockout-policy	Configures Cisco SD-WAN Manager and other controllers to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period, or who have not logged in for a designated number of days.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**port** *port-number* | **timeout** *interval* | **key** [**0** | **6** | **7**] *key-string*]

no server-private *ip-address* [**port** *port-number* | **timeout** *interval* | **key** [**0** | **6** | **7**] *key-string*]

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
port *port-number*	(Optional) Specifies the server port number. This option overrides the default, which is port 49. Range: 1 to 65535
timeout *interval*	(Optional) Specifies the server timeout interval. Range: 1 to 1000
key [**0** | **6** | **7**]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global**tacacs-server key** command for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 6 is entered, the string that is entered is considered to be an advanced encryption scheme [AES] encrypted text. If 7 is entered, the string that is entered is considered to be hidden text.
key-string	(Optional) Character string specifying the authentication and encryption key.

Command Default

If server-private parameters are not specified, global configurations are used; if global configurations are not specified, default values are used.

Command Modes TACACS+ server-group configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	**Port** and **Timeout** keywords added in AAA named server implementation.

Usage Guidelines For usage guidelines, see the Cisco IOS XE server-private (TACACS+) command.

Examples

The following example shows how to define the TACACS+ group server and associate private servers with it:

```
Device> enable
Device# config-transaction
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 172.16.0.1 key 7 110a1016141d
```

The following example shows how to configure TACACS+ group server port number and timeout interval:

```
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 172.16.0.1 port 49 timeout 100
```

tacacs server address ipv4

To set the IPv4 address of a specified TACACS+ server, use the **tacacs server address ipv4** command in global configuration mode. To remove the IPv4 address associated with the specified TACACS+ server, use the **no** form of this command.

tacacs server *server-name* **address ipv4** *ipv4-address*
no tacacs server *server-name* **address ipv4** *ipv4-address*

Syntax Description

server-name	Name of TACACS+ server.
ipv4-address	TACACS+ server IPv4 address in the A.B.C.D format.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **tacacs server address ipv4** command to set an IP address for a known TACACS+ server.

Example

The following example configures an IP address of 10.10.10.10 for the TACACS+ server "tacacsserver".

```
Device(config)# tacacs server tacacsserver address ipv4 10.10.10.10
```

tacacs server key

To set an authentication and encryption key of a specified TACACS+ server, use the **tacacs server key** command in global configuration mode. To remove the key associated with the specified TACACS+ server, use the **no** form of this command.

tacacs server *server-name* **key** [*key*]
no tacacs server *server-name* **key** [*key*]

Syntax Description

server-name	Name of TACACS+ server.
key	(optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **tacacs server key** command to set an authentication and encryption key for a known TACACS+ server.

Example

The following example configures an authentication and encryption key "Ys6WhgHS40" for the TACACS+ server "tacacsserver".

```
Device(config)# tacacs server tacacsserver key Ys6WhgHS40
```

tacacs server port

To set the port on which the TACACS server connects with the server host, use the **tacacs server port** command in global configuration mode. To reset port settings, use the **no** form of this command.

tacacs server *server-name* **port** *port-number*
no tacacs server *server-name* **port** *port-number*

Syntax Description

port-number	Specifies the port number. The range is from 1 to 65535. The default value is 49.
server-name	Specifies the name of the private TACACS+ server host.

Command Default

The default port on which the server connects with the server host is 49.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the port integer argument to specify the TCP port number to be used when making connections to the TACACS+ daemon. The default port number is 49.

Examples

The following example shows how to configure the port to 49:

```
Device(config)# tacacs server server1
Device(config-server-tacacs)# timeout 20

Device(config)# tacacs server server1
Device(config-server-tacacs)# port 49
```

tacacs server timeout

To set the interval for which the TACACS server waits for a server host to reply, use the **tacacs server timeout** command in global configuration mode. To restore the default timeout interval, use the **no** form of this command.

tacacs server *name* **timeout** *seconds*
no tacacs server *name* **timeout**

Syntax Description

name	Name of the private TACACS+ server host.
timeout	Configures the time to wait for a reply from the specified TACACS server.
seconds	Timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval for which the server waits for the server host to reply is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE tacacs server timeout command.

Examples

The following example shows how to set the timeout interval to 20 seconds:

```
Device(config)# tacacs server server1 timeout 20
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.
tacacs server address ipv4	Sets the IPv4 address of a specified TACACS+ server.
tacacs server key	Sets an authentication and encryption key of a specified TACACS+ server.