



A Commands

This chapter describes the Cisco NX-OS security commands that begin with A.

aaa accounting default

To configure authentication, authorization, and accounting (AAA) methods for accounting, use the **aaa accounting default** command. To revert to the default, use the **no** form of this command.

```
aaa accounting default {group group-list | local}
```

```
no aaa accounting default {group group-list | local}
```

Syntax Description		
group		Specifies to use a server group for accounting.
<i>group-list</i>		Space-separated list of server groups that can include the following: <ul style="list-style-type: none">• radius for all configured RADIUS servers.• Any configured RADIUS or TACACS+ server group name. The maximum number of names in the list is eight.
local		Specifies to use the local database for accounting.

Defaults	local
-----------------	--------------

Command Modes	Global configuration
----------------------	----------------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The **group** *group-list* methods refer to a set of previously defined servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify the **group** method, the **local** method, or both, and they fail, then the accounting authentication fails.

If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch# config t
switch(config)# aaa accounting default group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
show aaa group	Display AAA server group information.
tacacs-server host	Configures TACACS+ servers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa accounting dot1x

To configure authentication, authorization, and accounting (AAA) methods for accounting for 802.1X authentication, use the **aaa accounting dot1x** command. To revert to the default, use the **no** form of this command.

```
aaa accounting dot1x {group group-list | local}
```

```
no aaa accounting dot1x {group group-list | local}
```

Syntax Description

group	Specifies to use a server group for accounting.
<i>group-list</i>	Space-separated list of RADIUS server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
local	Specifies to use the local database for accounting.

Defaults

local

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **group group-list** methods refer to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify the **group** method, the **local** method, or both, and they fail, then the accounting authentication fails.

If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch# config t  
switch(config)# aaa accounting default group radius
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
show aaa group	Display AAA server group information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authentication cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authentication, use the **aaa authentication cts default group** command. To remove a server group from the default AAA authentication server group list, use the **no** form of this command.

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

Syntax Description	<i>group-list</i>	Space-separated list of RADIUS server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
---------------------------	-------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	<p>To use this command, you must enable the Cisco TrustSec feature using the feature cts command.</p> <p>The <i>group-list</i> refers to a set of previously defined RADIUS servers. Use the radius-server host command to configure the host servers. Use the aaa group server command to create a named group of servers.</p> <p>Use the show aaa group command to display the RADIUS server groups on the device.</p> <p>If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.</p> <p>This command requires the Advanced Services license.</p>
-------------------------	--

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure the default AAA authentication RADIUS server group for Cisco TrustSec:

```
switch# config t
switch(config)# aaa authentication cts default group RadGroup
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature cts	Enables the Cisco TrustSec feature.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa group	Displays the AAA server groups.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authentication dot1x default group

To configure AAA authentication methods for 802.1X, use the **aaa authentication dot1x default group** command. To revert to the default, use the **no** form of this command.

```
aaa authentication dot1x default group group-list
```

```
no aaa authentication dot1x default group group-list
```

Syntax Description	<i>group-list</i>	Space-separated list of RADIUS server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
---------------------------	-------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	<p>You must use the feature dot1x command before you configure 802.1X.</p> <p>The <i>group-list</i> refers to a set of previously defined RADIUS servers. Use the radius-server host command to configure the host servers. Use the aaa group server command to create a named group of servers.</p> <p>Use the show aaa group command to display the RADIUS server groups on the device.</p> <p>If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.</p> <p>This command does not require a license.</p>
-------------------------	---

Examples	<p>This example shows how to configure methods for 802.1X authentication:</p> <pre>switch# config t switch(config)# aaa authentication dot1x default group Dot1xGroup</pre>
-----------------	---

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to revert to the default methods for 802.1X authentication:

```
switch# config t  
switch(config)# no aaa authentication dot1x default group Dot1xGroup
```

Related Commands

Command	Description
feature dot1x	Enables 802.1X.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa group	Displays the AAA server groups.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authentication eou default group

To configure AAA authentication methods for EAP over UDP (EoU), use the **aaa authentication eou default group** command. To revert to the default, use the **no** form of this command.

```
aaa authentication eou default group group-list
```

```
no aaa authentication eou default group group-list
```

Syntax Description	<i>group-list</i>	Space-separated list of RADIUS server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
---------------------------	-------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Before configuring EAPoUDP default authentication methods, you must enable EAPoUDP using the **feature eou** command.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure methods for EAPoUDP authentication:

```
switch# config t
switch(config)# aaa authentication eou default group EoUGroup
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to revert to the default methods for EAPoUDP authentication:

```
switch# config t  
switch(config)# no aaa authentication eou default group EoUGroup
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa group	Displays the AAA server groups.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authentication login console

To configure AAA authentication methods for console logins, use the **aaa authentication login console** command. To revert to the default, use the **no** form of this command.

```
aaa authentication login console {group group-list [none] | local | none}
```

```
no aaa authentication login console {group group-list [none] | local | none}
```

Syntax Description

group	Specifies to use a server group for authentication.
<i>group-list</i>	Specifies a space-separated list of server groups. The list can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • tacacs+ for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
none	Specifies to use the username for authentication.
local	Specifies to use the local database for authentication.

Defaults

local

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **group radius**, **group tacacs+**, and **group group-list** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, then the authentication can fail. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

The command operates only in the default VDC (VDC 1).

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure the AAA authentication console login methods:

```
switch# config t  
switch(config)# aaa authentication login console group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
switch# config t  
switch(config)# no aaa authentication login console group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
show aaa group	Displays the AAA server groups.
tacacs-server host	Configures TACACS+ servers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authentication login default

To configure the default AAA authentication methods, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

```
aaa authentication login default {group group-list [none] | local | none}
```

```
no aaa authentication login default {group group-list [none] | local | none}
```

Syntax Description	group	Specifies a server group list to be used for authentication.
	<i>group-list</i>	Space-separated list of server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • tacacs+ for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
	none	Specifies to use the username for authentication.
	local	Specifies to use the local database for authentication.

Defaults local

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

The **group radius**, **group tacacs+**, and **group group-list** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, then the authentication fails. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure the AAA authentication console login method:

```
switch# config t  
switch(config)# aaa authentication login default group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
switch# config t  
switch(config)# no aaa authentication login default group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
show aaa group	Displays the AAA server groups.
tacacs-server host	Configures TACACS+ servers.

Send document comments to nexus7k-docfeedback@cisco.com

aaa authentication login error-enable

To configure that the AAA authentication failure message displays on the console, use the **aaa authentication login error-enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines When you log in, the login is processed by rolling over to the local user database if the remote AAA servers do not respond. In such cases, the following message is displayed on the user's terminal—if you have enabled the displaying of login failure messages:

```
Remote AAA servers unreachable; local authentication done.  
Remote AAA servers unreachable; local authentication failed.
```

This command does not require a license.

Examples This example shows how to enable the display of AAA authentication failure messages to the console:

```
switch# config t  
switch(config)# aaa authentication login error-enable
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
switch# config t  
switch(config)# no aaa authentication login error-enable
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show aaa authentication login error-enable	Displays the status of the AAA authentication failure message display.

Send document comments to nexus7k-docfeedback@cisco.com

aaa authentication login mschap

To enable Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authentication at login, use the **aaa authentication login mschap** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschap

no aaa authentication login mschap

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable MSCHAP authentication:

```
switch# config t
switch(config)# aaa authentication login mschap
```

This example shows how to disable MSCHAP authentication:

```
switch# config t
switch(config)# no aaa authentication login mschap
```

Related Commands

Command	Description
show aaa authentication login mschap	Displays the status of MSCHAP authentication.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa authorization cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authorization, use the **aaa authorization cts default group** command. To remove a server group from the default AAA authorization server group list, use the **no** form of this command.

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

Syntax Description	<i>group-list</i>	Space-separated list of RADIUS server groups that can include the following: <ul style="list-style-type: none"> • radius for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
---------------------------	-------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	<p>To use this command, you must enable the Cisco TrustSec feature using the feature cts command.</p> <p>The <i>group-list</i> refers to a set of previously defined RADIUS servers. Use the radius-server host command to configure the host servers. Use the aaa group server command to create a named group of servers.</p> <p>Use the show aaa group command to display the RADIUS server groups on the device.</p> <p>If you specify more than one server group, the NX-OS software checks each group in the order that you specify in the list.</p> <p>This command requires the Advanced Services license.</p>
-------------------------	--

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure the default AAA authorization RADIUS server group for Cisco TrustSec:

```
switch# config t  
switch(config)# aaa authorization cts default group RadGroup
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show aaa authorization	Displays the AAA authorization configuration.
show aaa group	Displays the AAA server groups.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa group server radius

To create a RADIUS server group and enter RADIUS server group configuration mode, use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this command.

```
aaa group server radius group-name
```

```
no aaa group server radius group-name
```

Syntax Description	<i>group-name</i>	RADIUS server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.
Defaults	None	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	<p>This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:</p> <pre>switch# config t switch(config)# aaa group server radius RadServer switch(config-radius)#</pre> <p>This example shows how to delete a RADIUS server group:</p> <pre>switch# config t switch(config)# no aaa group server radius RadServer</pre>	
Related Commands	Command	Description
	show aaa groups	Displays server group information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

aaa group server tacacs+

To create a TACACS+ server group and enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

```
aaa group server tacacs+ group-name
```

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

Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.
--------------------	------------	--

Defaults	None
----------	------

Command Modes	Global configuration
---------------	----------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+. This command does not require a license.
------------------	--

Examples	This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:
----------	--

```
switch# config t
switch(config)# aaa group server tacacs+ TacServer
switch(config-radius)#
```

This example shows how to delete a TACACS+ server group:

```
switch# config t
switch(config)# no aaa group server tacacs+ TacServer
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show aaa groups	Displays server group information.

Send document comments to nexus7k-docfeedback@cisco.com

aaa user default-role

To allow remote users who do not have a user role to log in to the device through RADIUS or TACACS+ using a default user role, use the **aaa user default-role** command. To disable default user roles for remote users, use the **no** form of this command.

aaa user default-role

no aaa user default-role

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines You can enable or disable this feature for the virtual device context (VDC) as needed. For the default VDC, the default role is network-operator. For nondefault VDCs, the default VDC is vdc-operator. When you disable the AAA default user role feature, remote users who do not have a user role cannot log in to the device.

This command does not require a license.

Examples This example shows how to enable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# aaa user default-role
```

This example shows how to disable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# no aaa user default-role
```

Related Commands	Command	Description
	show aaa user default-role	Displays the status of AAA default user role feature.

Send document comments to nexus7k-docfeedback@cisco.com

absolute

To specify a time range that has a specific start date and time, a specific end date and time, or both, use the **absolute** command. To remove an absolute time range, use the **no** form of this command.

```
[sequence-number] absolute [start time date] [end time date]
```

```
no {sequence-number | absolute [start time date] [end time date]}
```

Syntax Description

<i>sequence-number</i>	(Optional) Sequence number of the rule, which causes the device to insert the command in that numbered position in the time range. Sequence numbers maintain the order of rules within a time range. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in a time range has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the time range and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the resequence command to reassign sequence numbers to rules.
start <i>time date</i>	(Optional) Specifies the exact time and date when the device begins enforcing the permit and deny rules associated with the time range. If you do not specify a start time and date, the device enforces the permit or deny rules immediately. For information about value values for the <i>time</i> and <i>date</i> arguments, see the “Usage Guidelines” section.
end <i>time date</i>	(Optional) Specifies the exact time and date when the device stops enforcing the permit and deny commands associated with the time range. If you do not specify an end time and date, the device always enforces the permit or deny rules after the start time and date have passed. For information about the values for the <i>time</i> and <i>date</i> arguments, see the “Usage Guidelines” section.

Defaults

None

Command Modes

Time-range configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The device interprets all time range rules as local time.

If you omit both the **start** and the **end** keywords, the device considers the absolute time range to be always active.

You specify *time* arguments in 24-hour notation, in the form of *hours:minutes* or *hours:minutes:seconds*. For example, in 24-hour notation, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00.

You specify *date* arguments in the *day month year* format. The minimum valid start time and date is 00:00:00 1 January 1970, and the maximum valid start time is 23:59:59 31 December 2037.

This command does not require a license.

Examples

This example shows how to create an absolute time rule that begins at 7:00 a.m. on September 17, 2007, and ends at 11:59:59 p.m. on September 19, 2007:

```
switch# config t
switch(config)# time-range conference-remote-access
switch(config-time-range)# absolute start 07:00 17 September 2007 end 23:59:59 19
September 2007
```

Related Commands

Command	Description
periodic	Configures a periodic time range rule.
time-range	Configures a time range for use in IPv4 ACLs.

Send document comments to nexus7k-docfeedback@cisco.com

accept-lifetime

To specify the time interval within which the device accepts a key during a key exchange with another device, use the **accept-lifetime** command. To remove the time interval, use the **no** form of this command.

accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

no accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

Syntax Description	local	(Optional) Specifies that the device treats the configured times as local times. By default, the device treats the <i>start-time</i> and <i>end-time</i> arguments as UTC.
	<i>start-time</i>	Time of day and date that the device begins accepting the key. For information about the values for the <i>start-time</i> argument, see the “Usage Guidelines” section.
	duration <i>duration-value</i>	(Optional) Specifies the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
	infinite	(Optional) Specifies that the key never expires.
	<i>end-time</i>	(Optional) Time of day and date that the device stops accepting the key. For information about the values for the <i>time of day</i> and <i>date</i> arguments, see the “Usage Guidelines” section.

Defaults infinite

Command Modes Key configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

By default, the device interprets all time range rules as UTC.

By default, the time interval within which the device accepts a key during a key exchange with another device—the accept lifetime—is infinite, which means that the key is always valid.

The *start-time* and *end-time* arguments both require time and date components, in the following format:

hour[:minute[:second]] month day year

You specify the hour in 24-hour notation. For example, in 24-hour notation, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00. The minimum valid *start-time* is 00:00:00 Jan 1 1970, and the maximum valid *start-time* is 23:59:59 Dec 31 2037.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

This example shows how to create an accept lifetime that begins at midnight on June 13, 2008, and ends at 11:59:59 p.m. on August 12, 2008:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008
switch(config-keychain-key)#
```

Related Commands

Command	Description
key	Configures a key.
keychain	Configures a keychain.
key-string	Configures a key string.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

action

To specify what the device does when a packet matches a **permit** command in a VLAN access control list (VACL), use the **action** command. To remove an **action** command, use the **no** form of this command.

action drop [**log**]

no action drop [**log**]

action forward [**capture**]

no action forward [**capture**]

action redirect { **ethernet** *slot/port* | **port-channel** *channel-number.subinterface-number* }

no action redirect { **ethernet** *slot/port* | **port-channel** *channel-number.subinterface-number* }

Syntax	Description
drop	Specifies that the device drops the packet.
log	(Optional) Specifies that the device logs the packets it drops because of the drop keyword.
forward	Specifies that the device forwards the packet to its destination port.
capture	(Optional) Specifies that the device forwards the packet to ports that have the capture function enabled, in addition to the destination port of the packet.
redirect	Specifies that the device redirects the packet to an interface.
ethernet <i>slot/port</i>	Specifies the Ethernet interface that the device redirects the packet to.
port-channel <i>channel-number.subinterface-number</i>	Specifies the port-channel interface that the device redirects the packet to.
	Note The dot separator is required between the <i>channel-number</i> and <i>subinterface-number</i> arguments.

Defaults None

Command Modes VLAN access-map configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in the ACL specified by the **match** command.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the device forwards packets that match the ACL, and enable statistics for traffic that matches the map:

```
switch# config t
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

Related Commands

Command	Description
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics	Enables statistics for an access control list or VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

arp access-list

To create an Address Resolution Protocol (ARP) access control list (ACL) or to enter ARP access list configuration mode for a specific ARP ACL, use the **arp access-list** command. To remove an ARP ACL, use the **no** form of this command.

arp access-list *access-list-name*

no arp access-list *access-list-name*

Syntax Description	<i>access-list-name</i> Name of the ARP ACL. The name can be up to 64 alphanumeric, case-sensitive characters. Names cannot contain a space or quotation mark.				
Defaults	None				
Command Modes	Global configuration				
Supported User Roles	network-admin vdc-admin				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	<p>Use ARP ACLs to filter ARP traffic when you cannot use DHCP snooping.</p> <p>No ARP ACLs are defined by default.</p> <p>When you use the arp access-list command, the device enters ARP access list configuration mode, where you can use the ARP deny and permit commands to configure rules for the ACL. If the ACL specified does not exist, the device creates it when you enter this command.</p> <p>Use the ip arp inspection filter command to apply the ARP ACL to a VLAN.</p> <p>This command does not require a license.</p>				
Examples	<p>This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01:</p> <pre>switch# conf t switch(config)# arp access-list arp-acl-01 switch(config-arp-acl)#</pre>				

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	deny (ARP)	Configures a deny rule in an ARP ACL.
	ip arp inspection filter	Applies an ARP ACL to a VLAN.
	permit (ARP)	Configures a permit rule in an ARP ACL.
	show arp access-lists	Displays all ARP ACLs or a specific ARP ACL.