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.
group-list	Space-separated list of server groups that can include the following: • **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

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 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 groups** 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 that one server group, the Cisco 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# configure terminal
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 groups	Displays AAA server group information.
tacacs-server host	Configures TACACS+ servers.

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.
group-list	Space-separated list of RADIUS server groups that can include the following: • **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

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 groups** 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 that one server group, the Cisco 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 authentication, authorization, and accounting (AAA) methods for accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group group-list
```

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 groups	Displays AAA server group information.

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

group-list	Space-separated list of RADIUS server groups that can include the following: • **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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** 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 groups** command to display the RADIUS server groups on the device.

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

This command requires the Advanced Services license.

Examples

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

```
switch# configure terminal
swtich(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 groups	Displays the AAA server groups.

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

group-list	Space-separated list of RADIUS server groups that can include the following: • **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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

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 groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco 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 802.1X authentication:

```
switch# configure terminal
switch(config)# aaa authentication do1x default group Dot1xGroup
```

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

```
switch# configure terminal
switch(config)# no aaa authentication do1x 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 groups	Displays the AAA server groups.

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

group-list	Space-separated list of RADIUS server groups that can include the following: • **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

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 groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco 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# configure terminal
switch(config)# aaa authentication eou default group EoUGroup
```

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

```
switch# configure terminal
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 groups	Displays the AAA server groups.

aaa authentication login ascii-authentication

To enable ASCII authentication for passwords on a TACACS+ server, use the **aaa authentication login ascii-authentication** command. To revert to the default, use the **no** form of this command.

aaa authentication login ascii-authentication

no aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Only the TACACS+ protocol supports this feature.

This command does not require a license.

Examples

This example shows how to enable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# aaa authentication login ascii-authentication
```

This example shows how to disable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# no aaa authentication login ascii-authentication
```

Related Commands

Command	Description
show aaa authentication login ascii-authentication	Displays the status of the ASCII authentication for passwords.

aaa authentication login chap enable

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

aaa authentication login chap enable

no aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You cannot enable both CHAP and MSCHAP or MSCHAP V2 on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable CHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login chap enable
```

This example shows how to disable CHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login chap enable
```

Related Commands

Command	Description
show aaa authentication login chap	Displays the status of CHAP authentication.

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 {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login console {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

Syntax Description

fallback error local	Enables fallback to local authentication for the console login if remote authentication is configured and all AAA servers are unreachable. Fallback to local authentication is enabled by default. **Note** Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend disabling fallback to local authentication for only the default login or the console login, not both.
group	Specifies to use a server group for authentication.
group-list	Space-separated list of server groups. The list can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured RADIUS, TACACS+, or LDAP server group name.
none	(Optional) Specifies that no authentication is to be used.
local	Specifies to use the local database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	Support for LDAP server groups was added.
5.0(2)	The **fallback error local** keyword was added**.**
4.0(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, **group ldap,** and **group** *group-list* methods refer to a set of previously defined RADIUS, TACACS+, or LDAP servers. Use the **radius-server host, tacacs-server host, or ldap-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 groups** command to display the server groups on the device.

If you specify more that one server group, the Cisco 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, the authentication can fail. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

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

This command does not require a license.

Examples

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

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

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

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

Related Commands

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

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 {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login default {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

Syntax Description

fallback error local	Enables fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable. Fallback to local authentication is enabled by default. **Note** Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend disabling fallback to local authentication for only the default login or the console login, not both.
group	Specifies a server group list to be used for authentication.
group-list	Space-separated list of server groups that can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured RADIUS, TACACS+, or LDAP server group name.
none	(Optional) Specifies that no authentication is to be used.
local	Specifies to use the local database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	Support for LDAP server groups was added.
5.0(2)	The **fallback error local** keyword was added**.**
4.0(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, **group ldap**, and **group** *group-list* methods refer to a set of previously defined RADIUS, TACACS+, or LDAP servers. Use the **radius-server host, tacacs-server host**, or **ldap-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 groups** command to display the server groups on the device.

If you specify more that one server group, the Cisco 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, the authentication fails. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

This command does not require a license.

Examples

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

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

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

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

Related Commands

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

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

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

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

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

Related Commands

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

aaa authentication login invalid-username-log

To include the username in authentication failed messages for all failure reasons, use the **aaa authentication login invalid-username-log** command. To revert to the default, use the **no** form of this command. This applies to both local and remote authentication.

aaa authentication login invalid-username-log

show aaa authentication login invalid-username-log

no aaa authentication login invalid-username-log

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

It is a Configuration Mode Command

Command History

Release	Modification
7.1	This Command was introduced.

Usage Guidelines

The above command will cause the username to be included in authentication failed messages for all failure reasons. This is irrespective of whether the username is valid or not since under some conditions the switch cannot determine a username's validity. This applies to both local and remote authentication.

This command does not require a license.

Examples

This example shows how to include the username in authentication failed messages for all failure reasons:

```
switch# configure terminal
switch(config)# aaa authentication login invalid-username-log
```

This example shows how to exclude the username in authentication failed messages for all failure reasons:

```
switch# configure terminal
switch(config)# no aaa authentication login invalid-username-log
```

aaa authentication login mschap enable

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

aaa authentication login mschap enable

no aaa authentication login mschap enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You cannot enable both MSCHAP and CHAP or MSCHAP V2 on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable MSCHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschap enable
```

This example shows how to disable MSCHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschap enable
```

Related Commands

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

aaa authentication login mschapv2 enable

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication at login, use the **aaa authentication login mschapv2 enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschapv2 enable

no aaa authentication login mschapv2 enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You cannot enable both MSCHAP V2 and CHAP or MSCHAP on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable MSCHAP V2 authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschapv2 enable
```

This example shows how to disable MSCHAP V2 authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschapv2 enable
```

Related Commands

Command	Description
show aaa authentication login mschapv2	Displays the status of MSCHAP V2 authentication.

aaa authentication rejected

To configure the login block per user, use the **aaa authentication rejected** command. To remove the login block per user, use the **no** form of this command.

aaa authentication rejected *attempts* **in** *seconds* **ban** *block-seconds*

no aaa authentication rejected

Syntax Description

attempts	Number of login attempts fail before a user is blocked.
seconds	Time period within which the login attempt fails.
block-seconds	Time period in which the user is blocked after a failed login attempt.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

This feature is applicable only for local users.

Examples

The following example shows how to configure the login parameters to block a user for 300 seconds when 5 login attempts fail within a period of 60 seconds.

```
switch# configure terminal
swtich(config)# aaa authentication rejected 5 in 60 ban 300
```

Related Commands

Command	Description
clear aaa local user blocked	Clears the blocked local user.
show aaa authentication	Displays the AAA authentication configuration.
show aaa local user blocked	Displays the blocked local users.

aaa authorization commands default

To configure default AAA authorization methods for all EXEC commands, use the **aaa authorization commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization commands default [**group** *group-list* [**local**] | **local**]

no aaa authorization commands default [**group** *group-list* [**local**] | **local**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name.
local	(Optional) Specifies to use the local role-based database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	The **none** keyword was deprecated.
4.2(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **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 groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.

Caution Command authorization disables user role based authorization control (RBAC), including the default roles.

Note Command authorization is available only to non-console sessions. If you use a console to login to the server, command authorization is disabled.

Note By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

This command does not require a license.

Examples

This example shows how to configure the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# aaa authorization commands default group TacGroup local
Per command authorization will disable RBAC for all users. Proceed (y/n)?
```

Note If you press **Enter** at the confirmation prompt, the default response is **n**.

This example shows how to revert to the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# no aaa authorization commands default group TacGroup local
```

Related Commands

Command	Description
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
terminal verify-only	Enables the command authorization verification.
test aaa authorization command-type	Tests the command authorization using the AAA command authorization methods.

aaa authorization config-commands default

To configure default AAA authorization methods for all configuration commands, use the **aaa authorization config-commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization config-commands default [**group** *group-list* [**local**] | **local**]

no aaa authorization config-commands default [**group** *group-list* [**local**] | **local**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name.
local	(Optional) Specifies to use the local role-based database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	The **none** keyword was deprecated.
4.2(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **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 groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.

Caution Command authorization disables user role based authorization control (RBAC), including the default roles.

Note Command authorization is available only to non-console sessions. If you use a console to login to the server, command authorization is disabled.

Note By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

This command does not require a license.

Examples

This example shows how to configure the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# aaa authorization config-commands default group TacGroup local
```

This example shows how to revert to the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# no aaa authorization config-commands default group TacGroup local
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
terminal verify-only	Enables the command authorization verification.
test aaa authorization command-type	Tests the command authorization using the AAA command authorization methods.

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

group-list	Space-separated list of RADIUS server groups that can include the following: • **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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use the **aaa authorization cts default group** command, you must enable the Cisco TrustSec feature using the **feature cts** 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 groups** command to display the RADIUS server groups on the device.

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

This command requires the Advanced Services license.

Examples

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

```
switch# configure terminal
swtich(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 groups	Displays the AAA server groups.

aaa authorization ssh-certificate

To configure the default AAA authorization method for TACACS+ or Lightweight Directory Access Protocol (LDAP) servers, use the **aaa authorization ssh-certificate** command. To disable this configuration, use the **no** form of this command.

aaa authorization ssh-certificate default {**group** *group-list* | **local**}

no aaa authorization ssh-certificate default {**group** *group-list* | **local**}

Syntax Description

group	Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured TACACS+ or LDAP server group name.
local	Specifies to use the local database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command or the LDAP feature using the **feature ldap** command.

The **group tacacs+**, **group ldap**, and **group** *group-list* methods refer to a set of previously defined TACACS+ and LDAP servers. Use the **tacacs-server host** command or **ldap-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 groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the TACACS+ or LDAP server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Examples

This example shows how to configure LDAP authorization with certificate authentication as the default AAA authorization method for LDAP servers:

```
switch# configure terminal
switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
```

Related Commands

Command	Description
aaa authorization ssh-publickey	Configures LDAP or local authorization with the SSH public key as the default AAA authorization method for LDAP servers.
feature ldap	Enables the LDAP feature.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.

aaa authorization ssh-publickey

To configure Lightweight Directory Access Protocol (LDAP) or local authorization with the Secure Shell (SSH) public key as the default AAA authorization method for LDAP servers, use the **aaa authorization ssh-publickey** command. To revert to the default, use the **no** form of this command.

aaa authorization ssh-publickey default {**group** *group-list* | **local**}

no aaa authorization ssh-publickey default {**group** *group-list* | **local**}

Syntax Description

group	Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **ldap** for all configured LDAP servers. • Any configured LDAP server group name.
local	Specifies to use the local database for authentication.

Defaults

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDAP feature using the **feature ldap** command.

The **group ldap** and **group** *group-list* methods refer to a set of previously defined LDAP servers. Use the **ldap-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 groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the LDAP server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Examples

This example shows how to configure LDAP authorization with the SSH public key as the default AAA authorization method for LDAP servers:

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default group LDAPServer1 LDAPServer2
```

Related Commands

Command	Description
aaa authorization ssh-certificate	Configures LDAP or local authorization with certificate authentication as the default AAA authorization method for LDAP servers.
feature ldap	Enables the LDAP feature.
show aaa authorization	Displays the AAA authorization configuration.

aaa group server ldap

To create a Lightweight Directory Access Protocol (LDAP) server group and enter LDAP server group configuration mode, use the **aaa group server ldap** command. To delete an LDAP server group, use the **no** form of this command.

aaa group server ldap *group-name*

no aaa group server ldap *group-name*

Syntax Description

group-name	LDAP server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you configure LDAP.

This command does not require a license.

Examples

This example shows how to create an LDAP server group and enter LDAP server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)#
```

This example shows how to delete an LDAP server group:

```
switch# configure terminal
switch(config)# no aaa group server ldap LdapServer
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show aaa groups	Displays server group information.

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

group-name	RADIUS server group name.The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Defaults

None

Command Modes

Global configuration

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 create a RADIUS server group and enter RADIUS server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch# configure terminal
switch(config)# no aaa group server radius RadServer
```

Related Commands

Command	Description
show aaa groups	Displays server group information.

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

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

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

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

Related Commands

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

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

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.

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

sequence-number	(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 *time date*	(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 *time* and *date* arguments, see the "Usage Guidelines" section.
end *time date*	(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 *time* and *date* arguments, see the "Usage Guidelines" section.

Defaults

None

Command Modes

Time-range configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

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# configure terminal
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 or IPv6 ACLs.

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 *start-time* and *end-time* arguments as UTC.
start-time	Time of day and date that the device begins accepting the key. For information about the values for the *start-time* argument, see the "Usage Guidelines" section.
duration *duration-value*	(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.
end-time	(Optional) Time of day and date that the device stops accepting the key. For information about the values for the *time of day* and *date* arguments, see the "Usage Guidelines" section.

Defaults

infinite

Command Modes

Key configuration

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.

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.

access-class

not implemented in 4.1.2

To apply an IPv4 access control list (ACL) to a virtual terminal (VTY) line, use the **access-class** command. To remove an IPv4 ACL from a VTY line, use the **no** form of this command.

access-class *access-list-name* {**in** | **out**}

no access-class *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL.
in	(Optional) Specifies that the device applies the ACL to inbound traffic.
out	(Optional) Specifies that the device applies the ACL to outbound traffic.

Defaults

None

Command Modes

Line configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Because a user can connect to any VTY line, you should set identical restrictions on all virtual terminal lines.

This command does not require a license.

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# config t
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC addresses 0019.D2D0.00AE:

```
switch# config t
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
ip access-list	Provides debugging information for port security.
line	Enables port security globally.
show line	Shows information about port security.

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

no action forward

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.
redirect	Specifies that the device redirects the packet to an interface.
ethernet *slot*/*port*	Specifies the Ethernet interface that the device redirects the packet to.
port-channel *channel-number.subinterface-number*	Specifies the port-channel interface that the device redirects the packet to. **Note** The dot separator is required between the *channel-number* and *subinterface-number* arguments.

Defaults

None

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in an ACL specified by a **match** command in the same access map entry as the **action** command.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01 and add two entries that each have two **match** commands and one **action** command:

```
switch(config-access-map)# 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)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# show vlan access-map

Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
```

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.

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

access-list-name	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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use ARP ACLs to filter ARP traffic when you cannot use DCHP snooping.

No ARP ACLs are defined by default.

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.

Use the **ip arp inspection filter** command to apply the ARP ACL to a VLAN.

This command does not require a license.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01:

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)#
```

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.

authentication (LDAP)

To configure Lightweight Directory Access Protocol (LDAP) authentication to use the bind or compare method, use the **authentication** command. To disable this configuration, use the **no** form of this command.

authentication {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}

no authentication {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}

Syntax Description

bind-first	Sets the LDAP authentication method to bind first.
append-with-base DN *DNstring*	(Optional) Specifies the designated name (DN) string. You can enter up to 63 alphanumeric characters.
compare	Sets the LDAP authentication method to compare.
password-attribute *password*	(Optional) Specifies the user password. You can enter up to 63 alphanumeric characters.

Defaults

Bind method using first search and then bind

Command Modes

LDAP server group configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure LDAP authentication to use the compare method:

```
switch# conf t
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# authentication compare password-attribute TyuL8r
switch(config-ldap)#
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.