# 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 that a server group be used for accounting. |
| | *group-list* | Space-delimited list that specifies one or more configured RADIUS server groups. |
| | **local** | Specifies that the local database be used for accounting. |

**Command Default**     The local database is the default.

**Command Modes**     Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**     The **group** *group-list* method refers to a set of previously defined RADIUS or TACACS+ 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.

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

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

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

**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. |
| **tacacs-server host** | Configures TACACS+ servers. |

# aaa authentication login console

To configure authentication, authorization, and accounting (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. |
| | *group-list* | Space-separated list of RADIUS or TACACS+ server groups. The list can include the following: |
| | | • **radius** for all configured RADIUS servers. |
| | | • **tacacs+** for all configured TACACS+ servers. |
| | | • Any configured RADIUS or TACACS+ server group name. |
| | **none** | (Optional) Specifies to use the username for authentication. |
| | **local** | (Optional) Specifies to use the local database for authentication. |

**Command Default**    The local database

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(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.

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.

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

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

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

```
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. |
| | **tacacs-server host** | Configures TACACS+ servers. |

# aaa authentication login default

To configure the default authentication, authorization, and accounting (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 that a server group be used for authentication. |
| | *group-list* | Space-separated list of RADIUS or TACACS+ server groups that can include the following: <br>• **radius** for all configured RADIUS servers. <br>• **tacacs+** for all configured TACACS+ servers. <br>• Any configured RADIUS or TACACS+ server group name. |
| | **none** | (Optional) Specifies that the username be used for authentication. |
| | **local** | (Optional) Specifies that the local database be used for authentication. |

**Command Default**    The local database

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(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.

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.

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

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

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

```
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. |
| | **tacacs-server host** | Configures TACACS+ servers. |

# aaa authentication login error-enable

To configure that the authentication, authorization, and accounting (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.

**Command Default**   Disabled

**Command Modes**   Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(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 this situation, the following message is displayed if you have enabled the displaying of login failure messages:

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

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

```
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)# no aaa authentication login error-enable
```

**Related Commands**

| Command | Description |
|---|---|
| **show aaa authentication** | Displays the status of the AAA authentication failure message display. |

# aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) 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.

**Command Default**     Disabled

**Command Modes**     Global configuration mode

**Command History**

| Release | Modification |
|---------|--------------|
| 5.2(1)N1(1) | This command was introduced. |

**Examples**     This example shows how to enable MS-CHAP authentication:

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

This example shows how to disable MS-CHAP authentication:

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

**Related Commands**

| Command | Description |
|---------|-------------|
| **show aaa authentication** | Displays the status of MS-CHAP authentication. |

# aaa authorization commands default

To configure default authentication, authorization, and accounting (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** | **none**]

> **no aaa authorization commands default** [**group** *group-list*] [**local** | **none**]

**Syntax Description**

| group | (Optional) Specifies to use a server group for authorization. |
|---|---|
| *group-list* | List of server groups. |
| | The list can include the following: |
| | • **tacacs+** for all configured TACACS+ servers. |
| | • Any configured TACACS+ server group name. |
| | The name can be a space-separated list of server groups, and a maximum of 127 characters. |
| local | (Optional) Specifies to use the local role-based database for authorization. |
| none | (Optional) Specifies to use no database for authorization. |

**Command Default**    None

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    To use this command, you must enable the TACACS+ feature by 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 or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

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

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

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

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

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

| Related Commands | Command | Description |
|---|---|---|
| | **aaa authorization config-commands default** | Configures default AAA authorization methods for configuration commands. |
| | **aaa server group** | Configures AAA server groups. |
| | **feature tacacs+** | Enables the TACACS+ feature. |
| | **show aaa authorization** | Displays the AAA authorization configuration. |
| | **tacacs-server host** | Configures a TACACS+ server. |

# aaa authorization config-commands default

To configure the default authentication, authorization, and accounting (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** | **none**]

**no aaa authorization config-commands default** [**group** *group-list*] [**local** | **none**]

| Syntax Description | | |
|---|---|---|
| **group** | (Optional) Specifies to use a server group for authorization. | |
| *group-list* | List of server groups. | |
| | The list can include the following: | |
| | • **tacacs+** for all configured TACACS+ servers. | |
| | • Any configured TACACS+ server group name. | |
| | The name can be a space-separated list of server groups, and a maximum of 127 characters. | |
| **local** | (Optional) Specifies to use the local role-based database for authorization. | |
| **none** | (Optional) Specifies to use no database for authorization. | |

**Command Default**    None

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    To use this command, you must enable the TACACS+ feature by 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 or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

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

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

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **aaa authorization commands default** | Configures default AAA authorization methods for EXEC commands. |
| **aaa server group** | Configures AAA server groups. |
| **feature tacacs+** | Enables the TACACS+ feature. |
| **show aaa authorization** | Displays the AAA authorization configuration. |
| **tacacs-server host** | Configures a TACACS+ server. |

# aaa authorization ssh-certificate

To configure the default authentication, authorization, and accounting (AAA) authorization method for TACACS+ 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:<br><br>• **tacacs+** for all configured TACACS+ servers.<br><br>• Any configured TACACS+ server group name. The server group name can be a maximum of 127 characters. |
| local | Specifies to use the local database for authentication. |

**Command Default**   local

**Command Modes**   Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(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+ and LDAP 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, 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 the local database with certificate authentication as the default AAA authorization method:

```
switch# configure terminal
```

```
switch(config)# aaa authorization ssh-certificate default local
switch(config)#
```

| Related Commands | Command | Description |
|---|---|---|
| | aaa authorization ssh-publickey | Configures local authorization with the SSH public key as the default AAA authorization method. |
| | feature tacacs+ | Enables the TACACS+ feature. |
| | show aaa authorization | Displays the AAA authorization configuration. |

# aaa authorization ssh-publickey

To configure local authorization with the Secure Shell (SSH) public key as the default AAA authorization method for TACACS+ 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 server group name can be a maximum of 127 characters. |
| **local** | Specifies to use the local database for authentication. |

**Command Default**    **local**

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    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 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 local authorization with the SSH public key as the default AAA authorization method:

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default local
switch(config)#
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa authorization ssh-certificate** | Configures local authorization with certificate authentication as the default AAA authorization method. |
| | **show aaa authorization** | Displays the AAA authorization configuration. |

# 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. |
|---|---|---|

**Command Default**  None

**Command Modes**  Global configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Examples**  This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:

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

This example shows how to delete a RADIUS server group:

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

**Related Commands**

| Command | Description |
|---|---|
| **show aaa groups** | Displays server group information. |

# aaa user default-role

To enable the default role assigned by the authentication, authorization, and accounting (AAA) server administrator for remote authentication, use the **aaa user default-role** command. To disable the default role, 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.

**Command Default**    Enabled

**Command Modes**    Global configuration mode

**Command History**

| Release | Modification |
|---------|--------------|
| 5.2(1)N1(1) | This command was introduced. |

**Examples**    This example shows how to enable the default role assigned by the AAA server administrator for remote authentication:

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

This example shows how to disable the default role assigned by the AAA server administrator for remote authentication:

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

**Related Commands**

| Command | Description |
|---------|-------------|
| **show aaa user default-role** | Displays the status of the default user for remote authentication. |
| **show aaa authentication** | Displays AAA authentication information. |

# action

To specify what the switch 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 forward**}

> **no action** {**drop forward**}

**Syntax Description**

| | |
|---|---|
| **drop** | Specifies that the switch drops the packet. |
| **forward** | Specifies that the switch forwards the packet to its destination port. |

**Command Default**    None

**Command Modes**    VLAN access-map configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**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.

**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 switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
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. |