



Authorization Commands

This chapter describes the commands used to configure authentication, authorization, and accounting (AAA) authorization. AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

For information on how to configure authorization using AAA, refer to the chapter “Configuring Authorization” in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the section “Authorization Configuration Examples” located at the end of the chapter “Configuring Authorization” in the *Cisco IOS Security Configuration Guide*.

aaa authorization

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

```
aaa authorization {network | exec | commands level | reverse-access | configuration} {default |
  list-name} method1 [method2...]
```

```
no aaa authorization {network | exec | commands level | reverse-access | configuration | default
  | list-name}
```

Syntax Description		
network		Runs authorization for all network-related service requests, including SLIP ¹ , PPP ² , PPP NCPs ³ , and ARA ⁴ .
exec		Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.
commands		Runs authorization for all commands at the specified privilege level.
<i>level</i>		Specific command level that should be authorized. Valid entries are 0 through 15.
reverse-access		Runs authorization for reverse access connections, such as reverse Telnet.
configuration		Downloads the configuration from the AAA server.
default		Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
<i>list-name</i>		Character string used to name the list of authorization methods.
<i>method1</i> [<i>method2</i> ...]		One of the keywords listed in Table 7 .
		<ol style="list-style-type: none"> 1. Serial Line Internet Protocol 2. Point-to-Point Protocol 3. Point-to-Point Protocol Network Control Programs 4. AppleTalk Remote Access

Defaults Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(5)T	Group server support was added as a method keyword for this command.

Usage Guidelines Use the **aaa authorization** command to enable authorization and to create named methods lists, defining authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods

will be performed. A method list is simply a named list describing the authorization methods to be used (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

**Note**

The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Use the **aaa authorization** command to create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization method(s) tried in the given sequence.

**Note**

In [Table 7](#), the **group radius**, **group tacacs+**, and **group group-name** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Method keywords are described in [Table 7](#).

Table 7 *aaa authorization Methods*

Keyword	Description
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
krb5-instance	Uses the instance defined by the kerberos instance map command.
local	Uses the local database for authorization.
none	No authorization is performed.

Cisco IOS software supports the following six methods for authorization:

- **RADIUS**—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The network access server does not request authorization information; authorization is not performed over this line/interface.
- **Local**—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- **Kerberos Instance Map**—The network access server uses the instance defined by the **kerberos** instance map command for authorization.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARA connection.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and refuse authorization.

For a list of supported RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.



Note

There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example defines the network authorization method list named “scoobee”, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization will be performed.

```
aaa authorization network scoobee group radius local
```

Related Commands	Command	Description
	aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
	aaa new-model	Enables the AAA access control model.

aaa authorization config-commands

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

aaa authorization config-commands

no aaa authorization config-commands

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(6.02)T	This command was changed from being enabled by default to being disabled by default.

Usage Guidelines If the **aaa authorization commands level method** command is enabled, all commands, including configuration commands, are authorized by authentication, authorization, and accounting (AAA) using the method specified. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command has been entered, AAA authorization of configuration commands is completely disabled. Care should be taken before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands** command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands level method** command.



Note

You will get the same result if you (1) do not configure this command, or (2) configure **no aaa authorization config-commands**.

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

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

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

```
aaa authorization reverse-access {group radius | group tacacs+}
```

```
no aaa authorization reverse-access {group radius | group tacacs+}
```

Syntax Description

group radius	Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session.
group tacacs+	Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session.

Defaults

This command is disabled by default, meaning that authorization for reverse Telnet is not requested.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.

Usage Guidelines

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction—from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to open Telnet sessions to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. This command provides an additional (optional) level of security by requiring authorization in addition to authentication. When this command is enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Examples

The following example causes the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs+** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host** command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example configures a generic TACACS+ server to grant a user, “jim,” reverse Telnet access to port tty2 on the network access server named “site1” and to port tty5 on the network access server named site2:

```
user = jim
  login = cleartext lab
  service = raccess {
    port#1 = site1/tty2
    port#2 = site2/tty5
  }
```

**Note**

In this example, “site1” and “site2” are the configured host names of network access servers, not DNS names or alias.

The following example configures the TACACS+ server (CiscoSecure) to authorize a user named Jim for reverse Telnet:

```
user = jim
  profile_id = 90
  profile_cycle = 1
  member = Tacacs_Users
  service=shell {
    default cmd=permit
  }
  service=raccess {
    allow "c2511e0" "tty1" ".*"
    refuse ".*" ".*" ".*"
    password = clear "goaway"
```

**Note**

CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(x) through version 2.2(1).

An empty “service=raccess { }” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*. For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or later.

The following example causes the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key goaway
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named “jim” reverse Telnet access at port tty2 on network access server site1:

```
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=site1/tty2"
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={nasname}/{tty number}" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*.

aaa authorization template

To enable usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF), use the **aaa authorization template** command in global configuration mode. To disable the new authorization, use the **no** form of this command.

aaa authorization template

no aaa authorization template

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Examples

The following example enables usage of a remote customer template:

```
aaa authorization template
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.
template	Accesses the template configuration mode for configuring a particular customer profile template.

aaa dnis map authorization network group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group (the server group that will be used for AAA authorization), use the **aaa dnis map authorization network group** global configuration command. To unmap this DNIS number from the defined server group, use the **no** form of this command.

```
aaa dnis map dnis-number authorization network group server-group-name
```

```
no aaa dnis map dnis-number authorization network group server-group-name
```

Syntax Description	Parameter	Description
	<i>dnis-number</i>	Number of the DNIS.
	<i>server-group-name</i>	Character string used to name a group of security servers functioning within a server group.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines This command lets you assign a DNIS number to a particular AAA server group so that the server group can process authorization requests for users dialing in to the network using that particular DNIS number. To use this command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Examples The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authorization requests for users dialing in with DNIS 7777:

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authorization network group group1
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA access control model.
	aaa dnis map accounting network group	Maps a DNIS number to a AAA server group used for accounting services.

Command	Description
aaa dnis map authentication ppp group	Maps a DNIS number to a AAA server used for authentication services.
aaa dnis map enable	Enables AAA server selection based on DNIS number.
aaa group server	Groups different server hosts into distinct lists and methods.
radius-server host	Specifies and defines the IP address of the RADIUS server host.

authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the **no** form of this command.

authorization { **arap** | **commands** *level* | **exec** | **reverse-access** } [**default** | *list-name*]

no authorization { **arap** | **commands** *level* | **exec** | **reverse-access** } [**default** | *list-name*]

Syntax Description

arap	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
commands	Enables authorization on the selected lines for all commands at the specified privilege level.
<i>level</i>	Specific command level to be authorized. Valid entries are 0 through 15.
exec	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
reverse-access	Enables authorization to determine if the user is allowed reverse access privileges.
default	(Optional) The name of the default method list, created with the aaa authorization command.
<i>list-name</i>	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the aaa authorization command.

Defaults

Authorization is not enabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
 authorization commands 15 charlie
```

Related Commands	Command	Description
	aaa authorization	Sets parameters that restrict user access to a network.

ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization** command in interface configuration mode. To disable authorization, use the **no** form of this command.

ppp authorization [**default** | *list-name*]

no ppp authorization

Syntax Description

default	(Optional) The name of the method list is created with the aaa authorization command.
<i>list-name</i>	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the aaa authorization command.

Defaults

Authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp authorization charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.