

TACACS+ Servers for AAA

This chapter describes how to configure TACACS+ servers used in AAA and includes the following sections:

- Information About TACACS+ Servers, page 37-1
- Licensing Requirements for TACACS+ Servers, page 37-2
- Guidelines and Limitations, page 37-3
- Configuring TACACS+ Servers, page 37-3
- Monitoring TACACS+ Servers, page 37-6
- Feature History for TACACS+ Servers, page 37-7

Information About TACACS+ Servers

The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS-CHAPv1.

Using TACACS+ Attributes

The ASA provides support for TACACS+ attributes. TACACS+ attributes separate the functions of authentication, authorization, and accounting. The protocol supports two types of attributes: mandatory and optional. Both the server and client must understand a mandatory attribute, and the mandatory attribute must be applied to the user. An optional attribute may or may not be understood or used.

Note To use TACACS+ attributes, make sure that you have enabled AAA services on the NAS.

Table 37-1 lists supported TACACS+ authorization response attributes for cut-through-proxy connections. Table 37-2 lists supported TACACS+ accounting attributes.

Table 37-1 Supported TACACS+ Authorization Response Attributes

Attribute	Description
acl	Identifies a locally configured ACL to be applied to the connection.

Table 37-1 Supported TACACS+ Authorization Response Attributes (continued)

Attribute	Description
idletime	Indicates the amount of inactivity in minutes that is allowed before the authenticated user session is terminated.
timeout	Specifies the absolute amount of time in minutes that authentication credentials remain active before the authenticated user session is terminated.

Table 37-2 Supported TACACS+ Accounting Attributes

Attribute	Description
bytes_in	Specifies the number of input bytes transferred during this connection (stop records only).
bytes_out	Specifies the number of output bytes transferred during this connection (stop records only).
cmd	Defines the command executed (command accounting only).
disc-cause	Indicates the numeric code that identifies the reason for disconnecting (stop records only).
elapsed_time	Defines the elapsed time in seconds for the connection (stop records only).
foreign_ip	Specifies the IP address of the client for tunnel connections. Defines the address on the lowest security interface for cut-through-proxy connections.
local_ip	Specifies the IP address that the client connected to for tunnel connections. Defines the address on the highest security interface for cut-through-proxy connections.
NAS port	Contains a session ID for the connection.
packs_in	Specifies the number of input packets transferred during this connection.
packs_out	Specifies the number of output packets transferred during this connection.
priv-level	Set to the user privilege level for command accounting requests or to 1 otherwise.
rem_iddr	Indicates the IP address of the client.
service	Specifies the service used. Always set to “shell” for command accounting only.
task_id	Specifies a unique task ID for the accounting transaction.
username	Indicates the name of the user.

Licensing Requirements for TACACS+ Servers

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines

- You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 4 servers in multiple mode.
- If you need to configure fallback support using the local database, see Fallback Support, page 35-2 and the How Fallback Works with Multiple Servers in a Group, page 35-2.
- To prevent lockout from the ASA when using TACACS+ authentication or authorization, see Recovering from a Lockout, page 43-36.

Configuring TACACS+ Servers

This section includes the following topics:

- Task Flow for Configuring TACACS+ Servers, page 37-3
- Configuring TACACS+ Server Groups, page 37-4
- Adding a TACACS+ Server to a Group, page 37-5

Task Flow for Configuring TACACS+ Servers

Step 1 Add a TACACS+ server group. See Configuring TACACS+ Server Groups, page 37-4.

Step 2 For a server group, add a server to the group. See Adding a TACACS+ Server to a Group, page 37-5.

Configuring TACACS+ Server Groups

If you want to use a TACACS+ server for authentication, authorization, or accounting, you must first create at least one TACACS+ server group and add one or more servers to each group. You identify TACACS+ server groups by name.

To add a TACACS+ server group, perform the following steps:

Detailed Steps

	Command	Purpose

Step 1	**aaa-server** *server_tag* **protocol tacacs+**
	
	Example:
	`ciscoasa(config)# aaa-server servergroup1 protocol tacacs+`
	`ciscoasa(config-aaa-server-group)#`
		Identifies the server group name and the protocol.
		
		When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

Step 2	**max-failed-attempts** *number* **Example:** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	Specifies the maximum number of requests sent to a AAA server in the group before trying the next server. The *number* argument can range from 1 and 5. The default is 3. If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the **reactivation-mode** command in the next step. If you do not have a fallback method, the ASA continues to retry the servers in the group.
Step 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **Example:** `ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20`	Specifies the method (reactivation policy) by which failed servers in a group are reactivated. The **depletion** keyword reactivates failed servers only after all of the servers in the group are inactive. The **deadtime** *minutes* keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes. The **timed** keyword reactivates failed servers after 30 seconds of down time.

	Command	Purpose
Step 4	**accounting-mode simultaneous** **Example:** `ciscoasa(config-aaa-server-group)# accounting-mode simultaneous`	Sends accounting messages to all servers in the group. To restore the default of sending messages only to the active server, enter the **accounting-mode single** command.

Examples

The following example shows how to add one TACACS+ group with one primary and one backup server:

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

Adding a TACACS+ Server to a Group

To add a TACACS+ server to a group, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **Example:** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	Identifies the TACACS+ server and the server group to which it belongs. When you enter the **aaa-server host** command, you enter aaa-server host configuration mode.
Step 2	**timeout** *hh:mm:ss* **Example:** `ciscoasa(config-aaa-server-host)# timeout 15`	Specifies the length of time, in seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.

	Command	Purpose
Step 3	**server-port** *port_number* **Example:** `ciscoasa(config-aaa-server-host)# server-port 49`	Specifies the server port as port number 49, or the TCP port number used by the ASA to communicate with the TACACS+ server.
Step 4	**key** **Example:** `ciscoasa(config-aaa-host)# key myexamplekey1`	Specifies the server secret value used to authenticate the NAS to the TACACS+ server. This value is a case-sensitive, alphanumeric keyword of up to 127 characters, which is the same value as the key on the TACACS+ server. Any characters over 127 are ignored. The key is used between the client and the server to encrypt data between them and must be the same on both the client and server systems. The key cannot contain spaces, but other special characters are allowed.

Monitoring TACACS+ Servers

To monitor TACACS+ servers,enter one of the following commands:

Command	Purpose
show aaa-server	Shows the configured TACACS+ server statistics. To clear the TACACS+ server configuration, enter the **clear aaa-server statistics** command.
show running-config aaa-server	Shows the TACACS+ server running configuration. To clear TACACS+ server statistics, enter the **clear configure aaa-server** command.

Feature History for TACACS+ Servers

Table 37-3 lists each feature change and the platform release in which it was implemented.

Table 37-3 Feature History for TACACS+ Servers

Feature Name	Platform Releases	Feature Information
TACACS+ Servers	7.0(1)	Describes how to configure TACACS+ servers for AAA. We introduced the following commands: **aaa-server protocol**, **max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server**, **server-port, key**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **username**, **service-type**, **timeout**.