Configuring TACACS+ Servers for AAA

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

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 35-1 lists supported TACACS+ authorization response attributes for cut-through-proxy connections. Table 35-2 lists supported TACACS+ accounting attributes.

Table 35-1 Supported TACACS+ Authorization Response Attributes

Attribute	Description
acl	Identifies a locally configured ACL to be applied to the connection.
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 35-2 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
All 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 the "Fallback Support" section on page 33-2 and the "How Fallback Works with Multiple Servers in a Group" section on page 33-2.
- To prevent lockout from the ASA when using TACACS+ authentication or authorization, see the "Recovering from a Lockout" section on page 45-31.

Configuring TACACS+ Servers

This section includes the following topics:

Task Flow for Configuring TACACS+ Servers

Step 1 Add a TACACS+ server group. See the "Configuring TACACS+ Server Groups" section on page 35-4.

Step 2 For a server group, add a server to the group. See the "Adding a TACACS+ Server to a Group" section on page 35-4.

Step 3 (Optional) Specify text to display to the user during the AAA authentication challenge process. See the "Adding an Authentication Prompt" section on page 35-5.

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

Step 1 Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**.

Step 2 In the AAA Server Groups area, click **Add**.

The Add AAA Server Group dialog box appears.

Step 3 In the Server Group field, enter a name for the group.

Step 4 From the Protocol drop-down list, choose the TACACS+ server type:

Step 5 In the Accounting Mode field, click **Simultaneous** or **Single**.

In Single mode, the ASA sends accounting data to only one server.

In Simultaneous mode, the ASA sends accounting data to all servers in the group.

Step 6 In the Reactivation Mode field, click **Depletion** or **Timed**.

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.

In Timed mode, failed servers are reactivated after 30 seconds of down time.

Step 7 If you chose the Depletion reactivation mode, enter a time interval in the Dead Time field.

The Dead Time is the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent re-enabling of all servers.

Step 8 In the Max Failed Attempts field, add the number of failed attempts allowed.

This option sets the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive.

Step 9 Click **OK**.

The Add AAA Server Group dialog box closes, and the new server group is added to the AAA Server Groups table.

Step 10 In the AAA Server Groups dialog box, click **Apply** to save the changes to the running configuration.

Adding a TACACS+ Server to a Group

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

Detailed Steps

Step 1 Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**, and in the AAA Server Groups area, click the server group to which you want to add a server.

The row is highlighted in the table.

Step 2 In the Servers in the Selected Group area (lower pane), click **Add**.

The Add AAA Server Group dialog box appears for the server group.

Step 3 From the Interface Name drop-down list, choose the interface name on which the authentication server resides.

Step 4 In the Server Name or IP Address field, add either a server name or IP address for the server that you are adding to the group.

Step 5 In the Timeout field, either add a timeout value or keep the default. The timeout is the duration of time, in seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.

Step 6 Specify the server port. The server port is either port number 139, or the TCP port number used by the ASA to communicate with the TACACS+ server.

Step 7 Specify the server secret key. The shared secret key used to authenticate the TACACS+ server to the ASA. The server secret that you configure here should match the one that is configured on the TACACS+ server. If you do not know the server secret, ask the TACACS+ server administrator. The maximum field length is 64 characters.

Step 8 Click **OK**.

The Add AAA Server Group dialog box closes, and the AAA server is added to the AAA server group.

Step 9 In the AAA Server Groups pane, click **Apply** to save the changes to the running configuration.

Adding an Authentication Prompt

You can specify text to display to the user during the AAA authentication challenge process. You can specify the AAA challenge text for HTTP, FTP, and Telnet access through the ASA when requiring user authentication from TACACS+ servers. This text is primarily for cosmetic purposes and appears above the username and password prompts that users see when they log in.

If you do not specify an authentication prompt, users see the following when authenticating with a TACACS+ server:

Connection Type	Default Prompt
FTP	FTP authentication
HTTP	HTTP authentication
Telnet	None

To add an authentication prompt, perform the following steps:

Step 1 Choose **Configuration > Device Management > Users/AAA > Authentication Prompt.**

Step 2 Enter text in the Prompt field to add as a message to appear above the username and password prompts that users see when they log in.

The following table shows the allowed character limits for authentication prompts:

Application	Character Limit for Authentication Prompt
Microsoft Internet Explorer	37
Telnet	235
FTP	235

Step 3 In the Messages area, add messages in the User accepted message and User rejected message fields.

If the user authentication occurs from Telnet, you can use the User accepted message and User rejected message options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the ASA displays the User accepted message text, if specified, to the user; otherwise, the ASA displays the User rejected message text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The User accepted message and User rejected message text are not displayed.

Step 4 Click **Apply** to save the changes to the running configuration.

Testing TACACS+ Server Authentication and Authorization

To determine whether the ASA can contact a TACACS+ server and authenticate or authorize a user, perform the following steps:

Step 1 From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups table, click the server group in which the server resides.

The row is highlighted in the table.

Step 2 From the Servers in the Selected Group table, click the server that you want to test.

The row is highlighted in the table.

Step 3 Click **Test**.

The Test AAA Server dialog box appears for the selected server.

Step 4 Click the type of test that you want to perform—**Authentication** or **Authorization**.

Step 5 In the Username field, enter a username.

Step 6 If you are testing authentication, in the Password field, enter the password for the username.

Step 7 Click **OK**.

The ASA sends an authentication or authorization test message to the server. If the test fails, ASDM displays an error message.

Monitoring TACACS+ Servers

To monitor TACACS+ servers, see the following panes:

Path	Purpose
Monitoring > Properties > AAA Servers	Shows the configured TACACS+ server statistics.
Monitoring > Properties > AAA Servers	Shows the TACACS+ server running configuration.

Feature History for TACACS+ Servers

Table 35-3 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 35-3 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 screens: Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt.