



AAA Configuration

With CVDM-VPNSM, you can implement and configure authentication, authorization, and accounting (AAA) on your VPN module. AAA performs the following services:

- *Authentication* identifies users before they are permitted access to the network or network services. Authentication provides the method for identifying users, including username and password, challenge and response, messaging support, and, depending on the security protocol selected, encryption.
- *Authorization* assembles a set of attribute-value pairs that describe privileges for the identified user. These attribute-value pairs are compared to the information contained in a Remote Authentication Dial-In User Service (RADIUS) server database.



Note

For more information on RADIUS, see [Editing Global RADIUS Settings, page 6-5](#).

- *Accounting* logs the services accessed and the network resources consumed by users. Accounting provides the method for collecting and distributing information such as user identities, start and stop times, executed commands, number of packets, and number of bytes.

This chapter contains the following topics:

- [Viewing AAA Settings, page 6-2](#)
- [Configuring AAA Servers, page 6-3](#)
- [Configuring Authentication Lists, page 6-8](#)
- [Configuring Authorization Lists, page 6-13](#)
- [Configuring Accounting Lists, page 6-18](#)

Viewing AAA Settings

From the AAA main page, you can view the AAA settings that are currently configured on the module. To access this page, click **Setup** at the top of the window and then click **AAA Configuration** (see [Figure 6-1](#)).

Figure 6-1 AAA Main Page

The screenshot shows the CiscoView Device Manager for IPSec VPNSM interface. The main window displays the AAA Configuration page. The left sidebar shows the Setup menu with options like Home, Setup, Refresh, Deliver, and Help. The main content area shows the AAA configuration details.

AAA is enabled on the device.

RADIUS Global Settings

Timeout(sec): 5 Key: Source Interface: Edit...

AAA Servers

IP Address	Authentication Port	Accounting Port	Key	Timeout (sec)	Type
3.3.3.3	11	11		1	RADIUS
67.7.7.7	1645	1646	***	5	RADIUS
1.1.1.1	1647	1646		5	RADIUS
3.3.3.3	11	11		5	RADIUS
2.2.2.2	1646	1646		5	RADIUS
56.5.5.5	1645	1646	***	5	RADIUS
5.5.5.5	1645	1646	**	5	RADIUS
2.2.2.2	1645	1646		5	RADIUS
1.1.1.1	1645	1646		5	RADIUS

Add... Edit... Delete

<level1 5> <15> Thu Feb 10 10:59:05 PST 2005

92534

Configuring AAA Servers

To access the AAA overview page, click **Setup** at the top of the window, click **AAA Configuration** from the left-most pane, and then click **AAA** from the [selector](#).

From the AAA Configuration overview page, you can:

- Enable AAA on the device by clicking the Enable AAA link at the top of the page.

**Note**

You can only enable AAA if the enable password for a level 15 user has already been set. Until you have done so, you will not be able to make any configuration changes. However, you will be able to view any AAA-related configuration settings that have already been set on the device.

- View global RADIUS server settings.
- View detail information for the AAA servers configured on the device.
- Add a new AAA server. See [Adding AAA Servers, page 6-6](#) for more information.
- Edit the parameters for an existing AAA server. See [Editing AAA Servers, page 6-7](#) for more information.
- Delete an existing AAA server.

The following table describes the information provided on the AAA Configuration overview page.

GUI Element	Description
RADIUS Global Settings pane	
Timeout (sec) field	Number of seconds that a router should attempt to contact this server before going on to another server.
Key field	Key used when contacting the RADIUS server.
Source Interface field	IP address of the source interface.
Edit button	Click to launch the Edit RADIUS Settings dialog box. See Editing Global RADIUS Settings, page 6-5 for more information.
AAA Servers pane	
IP Address column	IP address of the AAA server.
Authentication Port column	Server port used for authentication requests.
Accounting Port column	Server port used for accounting requests.
Key column	Key used when contacting the AAA server.
Timeout (sec) column	Number of seconds that the router should attempt to contact this server before going on to the next server in the group list. The default is 5 seconds.
Type column	The type of server. Only the RADIUS option is supported.
Add button	Click to launch the Add AAA Server dialog box.
Edit button	With a AAA server selected, click to launch the Edit AAA Server dialog box.
Delete button	With a AAA server selected, click to remove it from the AAA Servers table.

Editing Global RADIUS Settings

RADIUS is an open and scalable client/server security system designed to authenticate remote users. RADIUS-based authentication works by comparing a secret username and password to data stored in a central location, called the RADIUS server. The RADIUS server receives authentication requests and either accepts or rejects them on the basis of information stored in the RADIUS server database. If a submitted username and password are correct, the RADIUS server returns an authentication acknowledgment to the client requesting the services.

From this dialog box, you can edit the RADIUS server settings for the VPN module.


- Step 1** From the RADIUS Global Settings pane on the AAA Configuration overview page, click **Edit**. The Edit RADIUS Settings dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Source Interface list	Select which interface will serve as the source interface for all AAA servers configured on the VPN module. See Selecting an Interface, page 6-6 for more information.
Timeout (sec) field	Enter the number of seconds that the router should attempt to contact this server before going on to another server. The default is 5 seconds. Valid values range from 1 to 1000 seconds.
Key field	Enter the key used when contacting the RADIUS server.
Confirm Key field	Re-enter the key used when contacting the RADIUS server.

- Step 3 Click **OK**.
- Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).
-

Selecting an Interface

From this dialog box, you can select which interface will serve as the source interface for all AAA servers configured on the VPN module.

- Step 1 In the Edit RADIUS Settings dialog box, click  to launch the Select an Interface dialog box.
- Step 2 Select an interface and click **OK**.
-

Adding AAA Servers

From this dialog box, you can configure the settings for a new AAA server on the module.

- Step 1 From the AAA Servers pane on the AAA Configuration overview page, click **Add**. The Add AAA Server dialog box appears.
- Step 2 Define the following.

GUI Element	Action/Description
IP Address field	Enter the IP address of the server.
Type field	The type of server. This field cannot be edited. Only the RADIUS option is supported.
Key field	Enter the key used when contacting the server.

GUI Element	Action/Description
Confirm Key field	Re-enter the key used when contacting the server.
Accounting Port field	Enter the server port used for accounting requests. The default is 1646.
Authentication Port field	Enter the server port used for authentication requests. The default is 1645.
Timeout (sec) field	Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. The default is 5 seconds. Valid values range from 1 to 1000 seconds.

Step 3 Click **OK**.

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing AAA Servers

From this dialog box, you can edit the settings for an existing AAA server on the module.

Step 1 From the AAA Servers pane on the AAA Configuration overview page, select an AAA server and click **Edit**. The Edit AAA Server dialog box appears.

Step 2 Define the following.

GUI Element	Action/Description
IP Address field	IP address of the selected AAA server. This field cannot be edited.
Type field	Server type of the selected AAA server. This field cannot be edited. Only the RADIUS option is supported.
Key field	Edit the key used when contacting the server.
Confirm Key field	Re-enter the key used when contacting the server.
Accounting Port field	Edit the server port used for accounting requests. The default is 1646.
Authentication Port field	Edit the authentication port used for communicating with the server. The default is 1645.
Timeout (sec) field	Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. The default is 5 seconds. Valid values range from 1 to 1000 seconds.

Step 3 Click **OK**.

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Configuring Authentication Lists

To access the Authentication Lists overview page, click **Setup** at the top of the window, click **AAA Configuration** from the left-most pane, and then click **Authentication Lists** from the [selector](#).

From the Authentication Lists overview page, you can:

- View detail information for the authentication lists configured on the RADIUS server.
- Add a new authentication list. See [Adding Authentication Lists, page 6-10](#) for more information.
- Edit the parameters of an existing authentication list. See [Editing Authentication Lists, page 6-12](#) for more information.
- Delete an existing authentication list.

The following table describes the information provided on the Authentication Lists overview page.

GUI Element	Description
Name field	Name of the authentication list.
Type field	Authorization type used by the authentication list. Only the login option is supported.
Method1 column	Authorization methods used by the authentication list.
Method2 column	There are seven supported values:
Method3 column	<ul style="list-style-type: none"> • None—No authentication occurs
Method4 column	<ul style="list-style-type: none"> • Line—A line user ID and password is used for authentication • Enable—An enable password is used for authentication • Local—The local username database is used for authentication • Local-case—A case-sensitive local username is used for authentication • Group radius—A RADIUS server is used for authentication • Cache radius—A list of all cache RADIUS servers is used for authentication <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>

GUI Element	Description
Add button	Click to launch the Add Authentication List dialog box.
Edit button	With an authentication list selected, click to launch the Edit Authentication List dialog box.
Delete button	With an authentication list selected, click to remove it from the Authentication Lists table.

Adding Authentication Lists

From this dialog box, you can configure the settings for a new authentication list on the module.

- Step 1** From the Authentication Lists overview page, click **Add**. The Add Authentication List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Use name as “default” check box	Select to use the new authentication list as the default authentication list.
Name field	Enter the name of the new authentication list. This field is disabled if the Use name as “default” check box is selected.

GUI Element	Action/Description
Type field	<p>Authorization type used by the new authentication list.</p> <p>This field cannot be edited. Only the login option is supported.</p>
Method1 column	<p>Authorization methods used by the authentication list.</p>
Method2 column	<p>There are seven supported values:</p>
Method3 column	<ul style="list-style-type: none"> • None—No authentication occurs
Method4 column	<ul style="list-style-type: none"> • Line—A line user ID and password is used for authentication
	<ul style="list-style-type: none"> • Enable—An enable password is used for authentication
	<ul style="list-style-type: none"> • Local—The local username database is used for authentication
	<ul style="list-style-type: none"> • Local-case—A case-sensitive local username is used for authentication
	<ul style="list-style-type: none"> • Group radius—A RADIUS server is used for authentication
	<ul style="list-style-type: none"> • Cache radius—A list of all cache RADIUS servers is used for authentication
	<p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>

Step 3 Click **OK**.

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing Authentication Lists

From this dialog box, you can edit the settings for an existing authentication list on the module.

-
- Step 1** From the Authentication Lists overview page, select an authentication list and click **Edit**. The Edit Authentication List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Name field	Name of the selected authentication list. This field cannot be edited.
Type field	Authorization type used by the selected authentication list. This field cannot be edited. Only the login option is supported.
Method1 column	Authorization methods used by the authentication list.
Method2 column	There are seven supported values: <ul style="list-style-type: none"> • None—No authentication occurs • Line—A line user ID and password is used for authentication • Enable—An enable password is used for authentication • Local—The local username database is used for authentication • Local-case—A case-sensitive local username is used for authentication • Group radius—A RADIUS server is used for authentication • Cache radius—A list of all cache RADIUS servers is used for authentication A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.
Method3 column	
Method4 column	

- Step 3 Click **OK**.
- Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).
-

Configuring Authorization Lists

To access the Authorization Lists overview page, click **Setup** at the top of the window, click **AAA Configuration** from the left-most pane, and then click **Authorization Lists** from the [selector](#).

From the Authorization Lists overview page, you can:

- View detail information for the authorization lists configured on the RADIUS server.
- Add a new authorization list. See [Adding Authorization Lists, page 6-15](#) for more information.
- Edit the parameters of an existing authorization list. See [Editing Authorization Lists, page 6-16](#) for more information.
- Delete an existing authorization list.

The following table describes the information provided on the Authorization Lists overview page.

GUI Element	Description
Name column	Name of the authorization list.
Type column	Authorization type used by the authorization list. Only the network option is supported.
Method1 column Method2 column Method3 column Method4 column	<p>Authorization methods used by the authorization list.</p> <p>There are five supported values:</p> <ul style="list-style-type: none"> • None—No authentication occurs • Local—The local username database is used for authentication • If-authenticated—Access to the requested function is granted after the user has been successfully authenticated • Group radius—A RADIUS server is used for authentication • Cache radius—A list of all cache RADIUS servers is used for authentication <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>
Add button	Click to launch the Add Authorization List dialog box.
Edit button	With an authorization list selected, click to launch the Edit Authorization List dialog box.
Delete button	With an authorization list selected, click to remove it from the Authorization Lists table.

Adding Authorization Lists

From this dialog box, you can configure the settings for a new authorization list on the module.

- Step 1** From the Authorization Lists overview page, click **Add**. The Add Authorization List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Use name as “default” check box	Select to use the new authorization list as the default authorization list.
Name field	Enter the name of the new authorization list. This field is disabled if the Use name as “default” check box is selected.
Type field	Authorization type used by the new authorization list. This field cannot be edited. Only the network option is supported.
Method1 list	Select the authorization methods used by the new authorization list.
Method2 list	There are five supported values:
Method3 list	<ul style="list-style-type: none"> • None—No authentication occurs
Method4 list	<ul style="list-style-type: none"> • Local—The local username database is used for authentication • If-authenticated—Access to the requested function is granted after the user has been successfully authenticated • Group radius—A RADIUS server is used for authentication • Cache radius—A list of all cache RADIUS servers is used for authentication
	A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.

- Step 3** Click **OK**.
- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).
-

Editing Authorization Lists

From this dialog box, you can edit the settings for an existing authorization list on the module.

- Step 1** From the Authorization Lists overview page, select an authorization list and click **Edit**. The Edit Authorization List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Name field	Name of the selected authorization list. This field cannot be edited.
Type field	Authorization type used by the authorization list. This field cannot be edited. Only the network option is supported.
Method1 list Method2 list Method3 list Method4 list	<p>Edit the authorization methods used by the authorization list.</p> <p>There are five supported values:</p> <ul style="list-style-type: none"> • None—No authentication occurs • Local—The local username database is used for authentication • If-authenticated—Access to the requested function is granted after the user has been successfully authenticated • Group radius—A RADIUS server is used for authentication • Cache radius—A list of all cache RADIUS servers is used for authentication <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>

- Step 3 Click **OK**.
- Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).
-

Configuring Accounting Lists

To access the Accounting Lists overview page, click **Setup** at the top of the window, click **AAA Configuration** from the left-most pane, and then click **Accounting Lists** from the [selector](#).

From the Accounting Lists overview page, you can:

- View detail information for the accounting lists configured on the RADIUS server.
- Add a new accounting list. See [Adding Accounting Lists, page 6-20](#) for more information.
- Edit the parameters of an existing accounting list. See [Editing Accounting Lists, page 6-22](#) for more information.
- Delete an existing accounting list.

The following table describes the information provided on the Accounting Lists overview page.

GUI Element	Description
Name column	Name of the accounting list.
Type column	Authorization type used by the accounting list. Only the network option is supported.
Method1 column Method2 column Method3 column Method4 column	<p>Authorization methods used by the accounting list.</p> <p>There are two supported values:</p> <ul style="list-style-type: none"> • None—no authentication occurs • Radius—a RADIUS server is used for authentication <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>
Notice column	<p>Indicates which accounting notice type is currently set:</p> <ul style="list-style-type: none"> • Start-stop—Records both start and stop actions. • Stop—Records a stop action when service is terminated. • None—Indicates that no accounting notice type is set.
Broadcast column	Indicates whether the broadcast of accounting notices to the configured authorization methods is enabled.
Add button	Click to launch the Add Accounting List dialog box.
Edit button	With an accounting list selected, click to launch the Edit Accounting List dialog box.
Delete button	With an accounting list selected, click to remove it from the Accounting Lists table.

Adding Accounting Lists

From this dialog box, you can configure the settings for a new accounting list on the module.

- Step 1** From the Accounting Lists overview page, click **Add**. The Add Accounting List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Use name as “default” check box	Select to use the new accounting list as the default accounting list.
Name field	Enter the name of the new accounting list. This field is disabled if the Use name as “default” check box is selected.
Type field	Indicates the authorization type used by the new accounting list. This field cannot be edited. Only the network option is supported.
Broadcast check box	Check to enable the broadcast of accounting notices to the configured authorization methods. Note You cannot select this check box if the Accounting Notice type is set to <i>None</i> .
Accounting Notice list	Set the notice type used by the accounting list. Select one of the following radio buttons: <ul style="list-style-type: none"> Start and Stop—Records both start and stop actions. Stop Only—Records a stop action when service is terminated. None—No accounting notice type is set.

GUI Element	Action/Description
Method1 list Method2 list Method3 list Method4 list	<p>Select the authorization methods used by the new accounting list.</p> <p>There are two supported values:</p> <ul style="list-style-type: none"> • None—no authentication occurs • Radius—a RADIUS server is used for authentication <p>Note You cannot edit these values if the Accounting Notice type is set to <i>None</i>.</p> <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>

Step 3 Click **OK**.

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing Accounting Lists

From this dialog box, you can edit the settings for an existing accounting list on the module.

- Step 1** From the Accounting Lists overview page, select an accounting list and click **Edit**. The Edit Accounting List dialog box appears.
- Step 2** Define the following.

GUI Element	Action/Description
Name field	Name of the selected accounting list. This field cannot be edited.
Type field	Authorization type used by the accounting list. This field cannot be edited. Only the network option is supported.
Broadcast check box	Check to enable the broadcast of accounting notices to the configured authorization methods. Note You cannot select this check box if the Accounting Notice type is set to <i>None</i> .

GUI Element	Action/Description
Accounting Notice list	<p>Edit the notice type used by the accounting list.</p> <p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> • Start and Stop—Records both start and stop actions. • Stop Only—Records a stop action when service is terminated. • None—No accounting notice type is set.
Method1 list Method2 list Method3 list Method4 list	<p>Edit the authorization methods used by the accounting list.</p> <p>There are two supported values:</p> <ul style="list-style-type: none"> • None—No authentication occurs • Radius—A RADIUS server is used for authentication <p>Note You cannot edit these values if the Accounting Notice type is set to <i>None</i>.</p> <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>

Step 3 Click **OK**.

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

