CHAPTER 4

Configuring AAA

This chapter describes how to configure Authentication, Authorization, and Accounting (AAA) on Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About AAA

This section includes the following topics:

AAA Security Services

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing the Cisco CG-OS router. The Cisco CG-OS router supports Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, the Cisco CG-OS router performs local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A pre-shared secret key provides security for communication between the Cisco CG-OS router and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

AAA security provides the following services:

- Authentication—Identifies users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption.

  Authentication is the process of verifying the identity of the person or device accessing the Cisco CG-OS router, which is based on the user ID and password combination provided by the entity trying to access the Cisco CG-OS router. The Cisco CG-OS routers allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

- Authorization—Provides access control.

  AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in Cisco CG-OS is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

- Accounting—Provides the method for collecting information, logging the information locally on the Cisco CG-OS router, and sending the information to the AAA server for billing, auditing, and reporting.

  The accounting feature tracks and maintains a log of every management session used to access the Cisco CG-OS router. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally on the Cisco CG-OS router or send them to remote AAA servers.

Note Cisco CG-OS software supports authentication, authorization, and accounting independently. For example, you can configure authentication and authorization without configuring accounting.

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+ security
- Multiple backup devices

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over local AAA services on the Cisco CG-OS router:

- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.

- It is more efficient to define and manage user attributes for Cisco CG-OS routers within centralized AAA servers, which can be a shared resource for multiple routers rather than configuring local AAA services on each Cisco CG-OS router independently. Additionally, AAA Server Groups can provide additional redundancy.

AAA Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting by using server groups. A server group is a set of remote AAA servers that implement the same AAA protocol. The purpose of a server group is to provide for failover servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, then the next remote server in the group is queried until one of the servers sends a response. If all the AAA servers in the server group fail to respond, then that server group option is considered a failure. When required, you can specify multiple server groups. If the Cisco CG-OS router encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

AAA configuration in the Cisco CG-OS router is service-based, which means that you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell version 2 (SSHv2) login authentication
- Console login authentication
- User management session accounting

Table 4-1 provides the relevant CLI command for each AAA service configuration option.

Table 4-1 AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login	**aaa authentication login default**
Console login	**aaa authentication login console**
User session accounting	**aaa accounting default**

You can specify the following authentication methods for the AAA services:

- RADIUS server groups—Uses the global pool of RADIUS servers for authentication
- Specified server groups—Uses specified RADIUS or TACACS+ server groups for authentication
- Local—Uses the local username or password database for authentication
- None—Uses only the username

Note If the chosen authentication method employs all RADIUS servers, rather than a specific server group, the Cisco CG-OS router chooses the RADIUS server from the global pool of configured RADIUS servers, in the order of configuration. Servers from this global pool can also be configured within a RADIUS server group on the Cisco CG-OS router.

Table 4-2 shows the AAA authentication methods that you can configure for the AAA services.

Table 4-2 AAA Authentication Methods for AAA Services

AAA Service	AAA Methods
Console login authentication	Server groups, local, and none
User login authentication	Server groups, local, and none
User management session accounting	Server groups and local

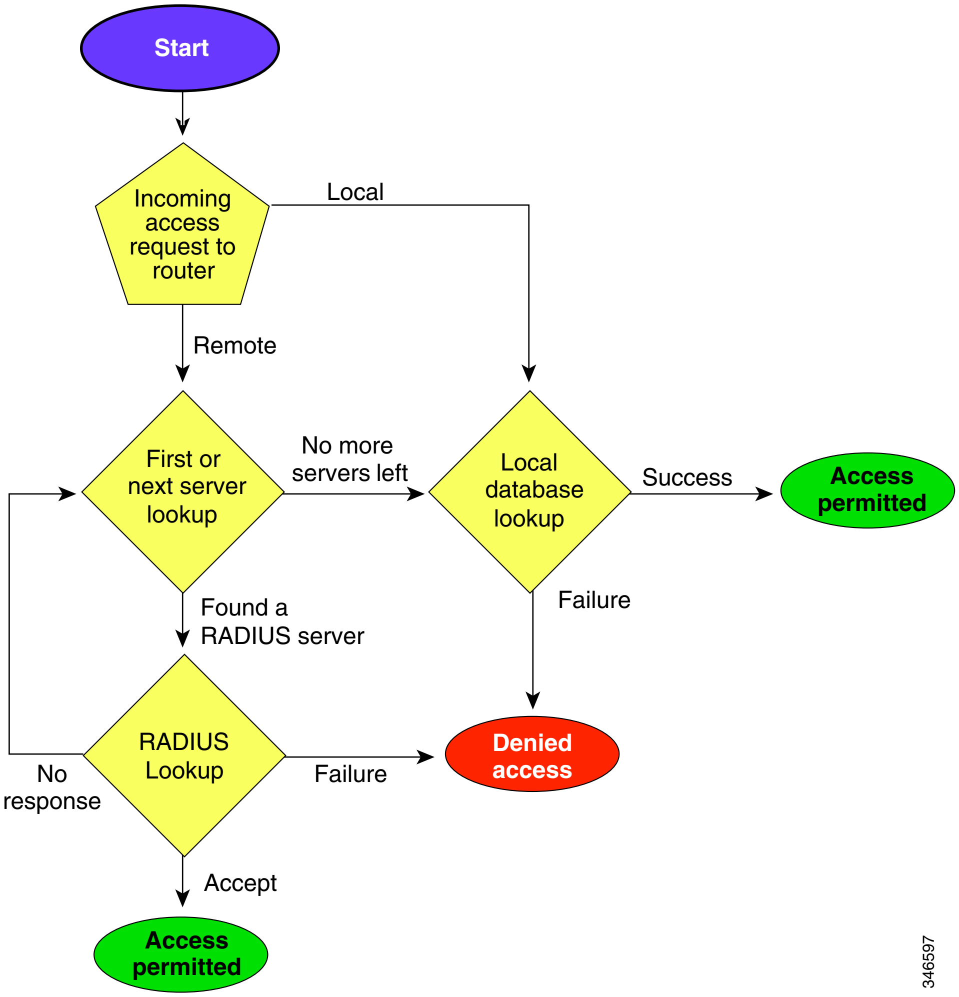
Note For console login authentication and user login authentication, and user management session accounting, the Cisco CG-OS router queries each option in the order specified. The local option is the default method when other configured options fail.

Authentication and Authorization Process for User Login

Figure 4-1 shows a flow chart of the authentication and authorization process for user login. The following list explains the process:

1. When you log in to one of the required Cisco CG-OS routers, you can use the Telnet, SSHv2, or console login options. Cisco recommends employing SSHv2 for increased security.
2. When you configure the AAA server groups using the server group authentication method, the Cisco CG-OS router sends an authentication request to the first AAA server in the group as follows:
   - If the AAA server fails to respond, then the Cisco CG-OS router queries the next AAA server and so on until a remote AAA server responds to the authentication request.
   - If all AAA servers in the server group fail to respond, then the Cisco CG-OS router contacts servers in the next server group.
   - If all configured methods fail, then the local database on the Cisco CG-OS router is used for authentication.
3. When the Cisco CG-OS router successfully authenticates through a remote AAA server, the following possibilities apply:
   - If the AAA server protocol is RADIUS, then the server downloads an authentication response to the Cisco CG-OS router that includes user roles, which are part of the cisco-av-pair attribute.
   - If the AAA server protocol is TACACS+, then the Cisco CG-OS router sends another request to the same server to get the user roles specified as custom attributes for the shell.
   - If the user roles are not successfully retrieved from the remote AAA server by the Cisco CG-OS router, then the Cisco CG-OS router assigns the user the *vdc-operator* role. For more information on user roles, refer to Chapter 7, “Configuring User Accounts and RBAC.”
4. When the Cisco CG-OS router successfully authenticates your username and password, the Cisco CG-OS router logs you in and assigns you the roles configured in the local database.

Figure 4-1 Authorization and Authentication Flow for User Login



Note "No more servers left" means that there is no response from any server within available server groups.

Prerequisites for AAA

Ensure that at least one RADIUS or TACACS+ server is IP reachable. (See the Configuring RADIUS Servers, page 2-6 and Configuring TACACS+ Server Hosts, page 3-7.)

Ensure that the Cisco CG-OS router is recognized as a client of the AAA servers.

Ensure that you configure the pre-share secret key on the Cisco CG-OS router and the remote AAA servers.

Ensure that the remote server responds to AAA requests from the Cisco CG-OS router. (See Manually Monitoring RADIUS Server or Groups, page 2-16 and the Manually Monitoring TACACS+ Servers or Groups, page 3-16.)

Guidelines and Limitations for AAA

The Cisco CG-OS software does not support all-numeric usernames, whether created with TACACS+ or RADIUS, or created locally, and does not create local users with all-numeric names. When an all-numeric username exists on an AAA server and it is entered during login, the Cisco CG-OS router does not log in the user.

When you have a user account configured on a local Cisco CG-OS router that has the same name as a remote user account on an AAA server, Cisco CG-OS applies the user roles for the local user account to the remote user, instead of the user roles configured on the AAA server.

Default Settings

Table 4-3 lists the default settings for AAA parameters.

Table 4-3 Default AAA Parameters

Parameters	Default
Console authentication method	Local
Default authentication method	Local
Login authentication failure messages	Disabled
Default accounting method	Local
Accounting log display length	250 KB

Configuring AAA

This section includes the following topics:

- Process for Configuring AAA, page 4-6
- Configuring Default Login Authentication Methods, page 4-7
- Enabling the Default User Role for Authentication, page 4-8
- Enabling Login Authentication Failure Messages, page 4-8
- Configuring AAA Accounting Default Methods, page 4-9
- Using AAA Server VSAs, page 4-10

Process for Configuring AAA

To configure AAA authentication and accounting, follow these steps:

Step 1 When you want to use remote RADIUS or TACACS+ servers for authentication, and to configure the hosts on your Cisco CG-OS router, refer to Chapter 2, “Configuring RADIUS” and Chapter 3, “Configuring TACACS+”).

Step 2 Enable the Default User Role for Authentication. (See Enabling the Default User Role for Authentication, page 4-8.)

Step 3 Enable the Login Authentication Failure Messages. (See Enabling Login Authentication Failure Messages, page 4-8.)

Step 4 Configure default login authentication methods for user logins. (See Configuring Default Login Authentication Methods, page 4-7.)

Step 5 Configure default AAA accounting default methods. (See Configuring AAA Accounting Default Methods, page 4-9.)

Configuring Default Login Authentication Methods

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco CG-OS router (default)

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa authentication login default** {**group** *group-list* [**none**]| **local**	Configures the default authentication methods. *group-list*—Space-separated list of server groups that can include any configured RADIUS or TACACS+ server group name. **local—**Specifies the local database of the Cisco CG-OS router for authentication. **none**—Uses no authentication. The default login method is **local**, which the Cisco CG-OS router uses when no methods are configured or when all the configured methods fail to respond.
Step 3	**show aaa authentication**	(Optional) Displays the configuration of the default login authentication methods.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure default login authentication methods for the Cisco CG-OS router.

```
router# configure terminal
router(config)# aaa authentication login default group va_reston2
router(config)# copy running-config startup-config
```

Enabling the Default User Role for Authentication

You can enable the default user role that allows remote users who do not have a user role to log in to the Cisco CG-OS router through a RADIUS or TACACS+ server. The default user role on the Cisco CG-OS router is *network-operator*. For more information on user roles, see Chapter 7, "Configuring User Accounts and RBAC."

Note Although references to a default VDC might be seen in CLI displays, the Cisco CG-OS router does not support the configuration of more than one VDC. The Cisco CG-OS router only supports a default VDC.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ servers or server groups.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa user default-role**	Enables the default user role for AAA authentication. The default is enabled. You can disable the default user role feature by using the **no** form of this command.
Step 3	**show aaa user default-role**	(Optional) Displays the AAA default user role configuration as either enabled or disabled on the Cisco CG-OS router.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable the default user role of *network-operator* for remote authentication to the Cisco CG-OS router through a AAA (RADIUS or TACACS+) server.

```
router# configure terminal
router(config)# aaa user default-role
router(config)# copy running-config startup-config
```

Enabling Login Authentication Failure Messages

When you enable login failure messages on the Cisco CG-OS router, the following messages display when access to remote AAA servers fails and the local user database takes precedence:

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

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ servers or server groups.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa authentication login error-enable**	Enables login authentication failure messages. The default is disabled.
Step 3	**show aaa authentication login error-enable**	(Optional) Displays whether the login failure message configuration is enabled or disabled.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable authentication failure messages on the Cisco CG-OS router that will appear on a user (client) terminal when authentication with a RADIUS or TACACS+ server fails.

```
router# configure terminal
router(config)# aaa authentication login error-enable
router(config)# copy running-config startup-config
```

Configuring AAA Accounting Default Methods

The Cisco CG-OS router supports TACACS+ and RADIUS methods for accounting and reports user activity to TACACS+ or RADIUS security servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs, which are stored on the designated AAA server.

When you activate AAA accounting, the Cisco CG-OS router reports these attributes as accounting records, which are then stored in an accounting log on the defined AAA security server.

You can create default method lists defining specific accounting methods, which include the following:

- RADIUS server group—Specifies a global pool of RADIUS servers for accounting.
- Specified server group—Uses a specified RADIUS or TACACS+ server group for accounting.
- Local—Uses the local username or password database on the Cisco CG-OS router for accounting.

Note When you configure server groups and the server groups do not respond, by default, the local database on the Cisco CG-OS router is used for authentication.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa accounting default** {**group** *server-group-name* | **local**}	Configures the default accounting method. *server-group-name*– List the server groups on which you want to store accounting logs. **radius**–Uses the global pool of RADIUS servers for accounting. **local**– Uses the local database of the Cisco CG-OS router for accounting. The default method is **local**, which is used when you do not configure any options or when all the configured server groups fail to respond.
Step 3	**show aaa accounting**	(Optional) Displays the configured default AAA accounting method.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to use default accounting methods employed by RADIUS servers.

```
router# configure terminal
router(config)# aaa accounting default group va_reston3
router(config)# copy running-config startup-config
```

Using AAA Server VSAs

You can use Vendor-Specific Attributes (VSAs) to specify user roles on AAA servers.

This section includes the following topics:

- About VSAs, page 4-10
- VSA Format, page 4-11
- Specifying User Roles on AAA Servers, page 4-11

About VSAs

The Internet Engineering Task Force (IETF) draft standard specifies attribute 26 as the method for communicating VSAs between the network access server and the RADIUS server. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and `*` (asterisk) indicates optional attributes.

When you use RADIUS servers for authentication on the Cisco CG-OS router, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

Cisco CG-OS supports the following VSA protocol options:

- Shell—Protocol used in access-accept packets to provide user-profile information.
- Accounting—Protocol used in accounting-request packets. When a value contains any white spaces, put it within double quotation marks.

Cisco CG-OS supports the following attributes:

- roles—Lists all the roles assigned to the user. The value field is a string that stores the list of group names delimited by white space. For example, if you belong to roles network-operator, the value field would be “network-operator.” This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. These examples use the roles attribute:

  ```
  shell:roles=“network-operator vdc-admin”
  shell:roles*“network-operator” vdc-admin
  ```

  The following examples show the roles attribute as supported by FreeRADIUS:

  ```
  Cisco-AVPair = “shell:roles=\“network-operator vdc-admin\””
  Cisco-AVPair = “shell:roles*\“network-operator vdc-admin\””
  ```

Note When you specify a VSA as shell:roles*"network-operator" vdc-admin or "shell:roles*\"network-operator vdc-admin\"", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- accountinginfo—Stores accounting information in addition to the attributes covered by the standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the Cisco CG-OS router, and it can only be used with the accounting protocol-related PDUs.

Specifying User Roles on AAA Servers

You can use the VSA cisco-av-pair on AAA servers to specify user role mapping for the Cisco CG-OS router using this format:

```
shell:roles="roleA roleB …"
```

If you do not specify the role option in the cisco-av-pair attribute, the default user role is network-operator.

For more information on user roles, see Chapter 7, “Configuring User Accounts and RBAC.”

Displaying and Clearing the Local AAA Accounting Log

The Cisco CG-OS router maintains a local log for the AAA accounting activity.

You can display the contents of the log or clear the contents of the log by entering one of the commands below:

Command	Purpose
show accounting log [*size* | **start-time** *year month day hh:mm:ss*]	Displays the contents of the AAA accounting log on the Cisco CG-OS router. *size*–Use to limit command output from the accounting log. The range is from 0 to 250000 bytes. By default, the command output contains up to 250000 bytes of the accounting log. **start-seqnum**–Specifies for the log output.**start-time**–Specifies
clear accounting log	Clears the contents of the AAA accounting log on the Cisco CG-OS router. Enter command at the EXEC level.

Note The AAA accounting log is local to the Cisco CG-OS router.

Verifying Configuration

To display AAA configuration information, enter any or all of the following commands:

Command	Purpose
show aaa accounting	Displays AAA accounting configuration.
show aaa authentication [**login error-enable**]	Indicates if the AAA authentication login error-enable option is enabled or disabled on the Cisco CG-OS router.
show aaa groups	Displays the AAA server group names configured on the Cisco CG-OS router.
show running-config aaa [all]	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

For detailed information about the fields in the output from these commands, see the Command Lookup Tool on Cisco.com.

Configuration Example

The following example shows how to configure AAA:

```
aaa authentication login default group va_reston2
aaa accounting default group va_reston3
```