



Configuring the CSS as a Client of a RADIUS Server

The Remote Authentication Dial-In User Service (RADIUS) protocol is a distributed client/server protocol that protects networks against unauthorized access. RADIUS uses the User Datagram Protocol (UDP) to exchange authentication and configuration information between the CSS authentication client and the active authentication server that contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software.

When a user remotely logs in to a CSS operating as a RADIUS client, the CSS sends an authentication request (including username, encrypted password, client IP address, and port ID) to the central RADIUS server. The RADIUS server is responsible for receiving user connection requests, authenticating users, and returning all configuration information necessary for the client to deliver services to the users. Transactions between the RADIUS client and the RADIUS server are authenticated through the use of a shared secret.

Once the RADIUS server receives the authentication request, it validates the sending client and consults a database of users to match the login request. If no response is returned by the RADIUS server within a period of time, the authentication request is retransmitted a predefined number of times. The RADIUS client can forward requests to an alternate secondary RADIUS server in the event that the primary server is down or is unreachable.

In a configuration where both a primary RADIUS server and a secondary RADIUS server are specified, and one or both of the RADIUS servers become unreachable, the CSS automatically transmits a keepalive authentication request to query the server(s). The CSS transmits the username “query” and the password “areyouup” to the RADIUS server (encrypted with the RADIUS server’s key) to determine the server’s state. The CSS continues to send this keepalive authentication request until the RADIUS server indicates it is available.

Use the **radius-server** command and its options to specify the RADIUS server host (primary RADIUS server, and, optionally, a secondary RADIUS server), communication time interval settings, and a shared secret text string. This command is available in global configuration mode.

This chapter contains the following major sections:

- [RADIUS Configuration Quick Start](#)
- [Configuring a RADIUS Server for Use with the CSS](#)
- [Specifying a Primary RADIUS Server](#)
- [Specifying a Secondary RADIUS Server](#)
- [Configuring the RADIUS Server Timeouts](#)
- [Configuring the RADIUS Server Retransmits](#)
- [Configuring the RADIUS Server Dead-Time](#)
- [Showing RADIUS Server Configuration Information](#)

After configuring the RADIUS server, enable RADIUS authentication for console and virtual logins (if the username and password pair is not in the local user database) through the **virtual authentication** and **console authentication** commands. Refer to [Chapter 1, Controlling CSS Access](#) for details on the two commands.

RADIUS Configuration Quick Start

[Table 3-1](#) provides a quick overview of the steps required to configure the RADIUS feature on a CSS. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI command, refer to the sections following the table.

Table 3-1 RADIUS Configuration Quick Start

Task and Command Example

1. Configure the authentication settings on the Cisco Secure ACS in the Network Configuration section of the Cisco Secure ACS HTML interface, the Add AAA Client page, and complete the following fields:
 - AAA Client Hostname
 - AAA Client IP Address
 - Key
 - Authenticate Using

See the [“Configuring Authentication Settings”](#) section.

2. To determine the privilege level of users accessing the CSS, configure the user accounts on the RADIUS server. See the [“Configuring Authorization Settings”](#) section.
3. Use the **radius-server primary** command to specify a primary RADIUS server used to authenticate user information from the CSS RADIUS client (console or virtual authentication). See the [“Specifying a Primary RADIUS Server”](#) section.

```
(config)# radius-server primary 172.27.56.76 secret Hello
```

4. Use the **radius-server secondary** command to specify a secondary RADIUS server to authenticate user information from the CSS RADIUS client (console or virtual authentication). See the [“Specifying a Secondary RADIUS Server”](#) section.

```
(config)# radius-server secondary 172.27.56.79 secret Hello
```

Table 3-1 RADIUS Configuration Quick Start (continued)

Task and Command Example
<p>5. Use the virtual authentication command to configure the primary, secondary, and tertiary virtual authentication method. See Chapter 1, Controlling CSS Access.</p> <pre>#(config) virtual authentication primary radius</pre>
<p>6. (Recommended) Use the show radius command and its options to display information and statistics about the RADIUS server configuration. See the “Showing RADIUS Server Configuration Information” section.</p> <pre>(config)# show radius config all (config)# show radius statistics all</pre>

The following running-configuration example shows the results of entering the commands in [Table 3-1](#).

```
!***** GLOBAL *****
radius-server primary 172.27.56.76 secret Hello auth-port 1645
radius-server secondary 172.27.56.79 secret Hello auth-port 1645
virtual authentication primary radius
```

Configuring a RADIUS Server for Use with the CSS

This section provides background information on the setup of a RADIUS server. It is intended as a guide to help ensure proper communication with a RADIUS server and a CSS operating as a RADIUS client.

The following sections summarize the recommended settings for the Cisco Secure Access Control Server (ACS) when used as a centralized RADIUS server with the CSS.

Configuring Authentication Settings

To configure the authentication settings on Cisco Secure ACS, go to the Network Configuration section of the Cisco Secure ACS HTML interface, the Add AAA Client page, and complete the following fields:

- AAA Client Hostname - Enter a name you want assigned to the CSS.
- AAA Client IP Address - Enter the IP address of the CSS Ethernet Management port or of a CSS circuit (depending on how the CSS is configured to communicate with the Cisco Secure ACS).
- Key - Enter the shared secret that the CSS and Cisco Secure ACS use to authenticate transactions. For correct operation, you must specify the identical shared secret on both the Cisco Secure ACS and the CSS. The key is case-sensitive.
- Authenticate Using - Select the **RADIUS (IETF)** network security protocol to use the standard IETF RADIUS attributes with the CSS.

Configuring Authorization Settings

To determine the privilege level of users accessing the CSS, you must configure the user accounts on the RADIUS server.

To configure the group authorization settings:

1. From the Group Setup section of the Cisco Secure ACS HTML interface, Group Setup Select page, select the group for which you want to configure RADIUS settings.
2. From the Group Settings section of the Cisco Secure ACS HTML interface, click the **IETF RADIUS Attributes, [006] Service-Type** checkbox. Then select **Administrative**. Administrative is required to enable RADIUS authentication for privileged user (SuperUser) connection with the CSS.

To add a user to a group, go to the **User Setup** section of the Cisco Secure ACS HTML interface:

- On the User Setup Select page, specify a username.
- On the User Setup Edit page, specify the following:
 - Password Authentication - Select an applicable authentication type from the list.
 - Password - Specify and confirm a password.
 - Group - Select the previously created RADIUS group to which you want to assign the user.

Specifying a Primary RADIUS Server

To specify a primary RADIUS server used to authenticate user information from the CSS RADIUS client (console or virtual authentication), use the **radius-server primary** command. The syntax for this global configuration mode command is:

```
radius-server primary ip_address secret string [auth-port port_number]
```

Options and variables for this command are as follows:

- **primary** *ip_address* - The IP address or host name for the primary RADIUS server. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).
- **secret** *string* - The shared secret text string between the primary RADIUS server and the CSS RADIUS client. The shared secret allows authentication transactions between the client and primary RADIUS server to occur. Enter the shared secret as a case-sensitive string with no spaces (16 characters maximum).
- **auth-port** *port_number* - (Optional) The UDP port on the primary RADIUS server allocated to receive authentication packets from the RADIUS client. Valid entries are 0 to 65535. The default is 1645.

To specify a primary RADIUS server, enter:

```
(config)# radius-server primary 172.27.56.76 secret Hello auth-port
30658
```

To remove a primary RADIUS server, enter:

```
(config)# no radius-server primary
```

Specifying a Secondary RADIUS Server

The CSS directs authentication requests to the secondary RADIUS server when the specified RADIUS primary server is unavailable. To specify a secondary RADIUS server to authenticate user information from the CSS RADIUS client (console or virtual authentication), use the **radius-server secondary** command.



Note

Configuration of a secondary RADIUS server is optional.

The syntax for this global configuration mode command is:

```
radius-server secondary ip_address secret string { auth-port port_number }
```

Options and variables for this command are as follows:

- **secondary** *ip_address* - The IP address or host name for the secondary RADIUS server. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).
- **secret** *string* - The shared secret text string between the secondary RADIUS server and the CSS RADIUS client. The shared secret allows authentication transactions between the client and secondary RADIUS server to occur. Enter the shared secret as a case-sensitive string with no spaces (16 characters maximum).
- **auth-port** *port_number* - (Optional) The UDP port on the primary RADIUS server allocated to receive authentication packets from the RADIUS client. Valid entries are 0 to 65535. The default is 1645.

To specify a secondary RADIUS server, enter:

```
(config) radius-server secondary 172.27.56.79 secret Hello auth-port  
30658
```

To remove a secondary RADIUS server, enter:

```
(config)# no radius-server secondary
```

Configuring the RADIUS Server Timeouts

By default, the CSS waits 10 seconds for the RADIUS server (primary or secondary) to reply to an authentication request before retransmitting requests to the RADIUS server. Use the **radius-server timeout** command to specify the time interval that the CSS waits for the RADIUS server (primary or secondary) to reply to an authentication request before retransmitting requests to the RADIUS server. You configure the number of retransmitted requests to the server through the **radius-server retransmit** command (see the “[Configuring the RADIUS Server Retransmits](#)” section). Valid entries are 1 to 255 seconds.

For example, to configure the RADIUS server timeout interval to 1 minute (60 seconds), enter:

```
(config)# radius-server timeout 60
```

To reset the RADIUS server retransmit request to the default of 10 seconds, enter:

```
(config)# no radius-server timeout
```

Configuring the RADIUS Server Retransmits

By default, the CSS retransmits three authentication requests to a timed-out RADIUS server before considering the server dead and stopping transmission. Use the **radius-server retransmit** command to specify the number of times the CSS retransmits an authentication request to a timed-out RADIUS server before considering the server dead and stopping transmission. If a secondary RADIUS server has been identified, the server is selected as the active server. Valid entries are 1 to 30 retries.

If the RADIUS server does not respond to the CSS retransmitted requests, the CSS considers the server as dead, stops transmitting to the server, and starts the dead timer as defined through the **radius-server dead-time** command (see the “[Configuring the RADIUS Server Dead-Time](#)” section). If a secondary server is configured, the CSS transmits the requests to the secondary server. If the secondary server does not respond to the request, the CSS considers the server dead and starts the dead timer. If there is no active server, the CSS stops transmitting requests until the primary RADIUS server becomes alive.

For example, to configure the number of RADIUS server retransmissions to 5, enter:

```
(config)# radius-server retransmit 5
```

To reset the RADIUS server retransmit request to the default of 3 retransmissions, enter:

```
(config)# no radius-server retransmit
```

Configuring the RADIUS Server Dead-Time

During the dead-time interval, the CSS sends probe access-request packets to verify that the RADIUS server (primary or secondary) is available and can receive authentication requests. The dead-time interval starts when the server does not respond to the number of authentication request transmissions configured through the **radius-server retransmit** command. When the server responds to a probe access-request packet, the CSS transmits the authentication request to the server.

Use the **radius-server dead-time** command to set the time interval in which the CSS verifies whether a nonresponsive server is operational. Valid entries are 1 to 255 seconds. The default is 5 seconds.

To configure the RADIUS server dead-time to 15 seconds, with probe access-requests enabled, enter:

```
(config)# radius-server dead-time 15
```

To reset the RADIUS server dead-time request to the default of 5 seconds, enter:

```
(config)# no radius-server dead-time
```

Showing RADIUS Server Configuration Information

Use the **show radius** command to display information and statistics about the RADIUS server configuration. The syntax and options for the command are as follows:

- **show radius config [all|primary|secondary]** - Displays RADIUS configuration information for a specific server or all servers, identified by type
- **show radius statistics [all|primary|secondary]** - Displays RADIUS authentication statistics for a specific server or all servers, identified by type

To view the configuration for a RADIUS primary server, enter:

```
(config)# show radius config primary
```

To view the authentication statistics for a RADIUS secondary server, enter:

```
(config)# show radius statistics secondary
```

Table 3-2 describes the fields in the **show radius config** command output.

Table 3-2 *Field Descriptions for the show radius config Command*

Field	Description
Server IP Address	The IP address or host name for the specified RADIUS server
Secret	The shared secret text string between the specified RADIUS server and the CSS RADIUS client
Port	The UDP port on the specified RADIUS server allocated to receive authentication packets from the CSS RADIUS client; the default port number is 1645
State	The operational stats of the RADIUS server (ALIVE, DOWN, UNKNOWN)
Dead Timer	The time interval (in seconds) that the CSS probes a nonresponsive RADIUS server (primary or secondary) to determine whether it is operational and can receive authentication requests
Timeout	The interval (in seconds) that the CSS RADIUS client waits for the RADIUS server to reply to an authentication request before retransmitting requests to the RADIUS server
Retransmit Limit	The number of times the CSS RADIUS client retransmits an authentication request to a timed out RADIUS server before stopping transmission to that server
Probes	The packets that the CSS RADIUS client automatically transmits as a means to determine whether the RADIUS server is still available and can receive authentication requests

Table 3-3 describes the fields in the **show radius statistics** output.

Table 3-3 *Field Descriptions for the show radius statistics Command*

Field	Description
Server IP address	The IP address or host name of the specified RADIUS server
Accepts	The number of times the RADIUS server accepts an authentication request from the CSS RADIUS client
Requests	The number of times the CSS RADIUS client issues an authentication request to the RADIUS server
Retransmits	The number of times the CSS RADIUS client retransmits an authentication request to the active RADIUS server after a timeout occurred
Rejects	The number of times the CSS RADIUS client receives a reject notification from the RADIUS server while trying to establish an authentication request
Bad Responses	The number of times the CSS RADIUS client receives a bad transmission from the RADIUS server
Bad Authenticators	The number of times the RADIUS server denies an authentication request from the CSS RADIUS client
Pending Requests	The number of pending authentication requests to the RADIUS server
Timeouts	The number of times the CSS RADIUS client reached the specified timeout interval while waiting for the RADIUS server to reply to an authentication request
Discarded Authentication Requests	The number of authentication requests that were discarded while the primary or secondary RADIUS server was down

■ Showing RADIUS Server Configuration Information