Configuring TACACS+

Setting up TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is a client/server protocol that provides centralized security for users attempting to gain management access to a controller. It serves as a backend database similar to local and RADIUS. However, local and RADIUS provide only authentication support and limited authorization support while TACACS+ provides three services:

- **Authentication**—The process of verifying users when they attempt to log into the controller.

  Users must enter a valid username and password in order for the controller to authenticate users to the TACACS+ server. The authentication and authorization services are tied to one another. For example, if authentication is performed using the local or RADIUS database, then authorization would use the permissions that are associated with the user in the local or RADIUS database (which are read-only, read-write, and lobby-admin) and not use TACACS+. Similarly, when authentication is performed using TACACS+, authorization is tied to TACACS+.

  Note When multiple databases are configured, you can use the controller GUI or CLI to specify the sequence in which the backend databases should be tried.

- **Authorization**—The process of determining the actions that users are allowed to take on the controller based on their level of access.

  For TACACS+, authorization is based on privilege (or role) rather than specific actions. The available roles correspond to the seven menu options on the controller GUI: MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. An additional role, LOBBY, is available for users who require only lobby ambassador privileges. The roles to which users are assigned are configured on the TACACS+ server. Users can be authorized for one or more roles.

- The minimum authorization is MONITOR only, and the maximum is ALL, which authorizes the user to execute the functionality associated with all seven menu options. For example, a user who is assigned the role of SECURITY can make changes to any items appearing on the Security menu (or designated as security commands in the case of the CLI). If users are not authorized for a particular role (such as WLAN), they can still access that menu option in read-only mode (or the associated CLI **show** commands). If the TACACS+ authorization server becomes unreachable or unable to authorize, users are unable to log into the controller.

Note If users attempt to make changes on a controller GUI page that are not permitted for their assigned role, a message appears indicating that they do not have sufficient privilege. If users enter a controller CLI command that is not permitted for their assigned role, a message may appear indicating that the command was successfully executed although it was not. In this case, the following additional message appears to inform users that they lack sufficient privileges to successfully execute the command: "Insufficient Privilege! Cannot execute command!"

- **Accounting**—The process of recording user actions and changes.

  Whenever a user successfully executes an action, the TACACS+ accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the TACACS+ accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

  Note The logs under TACACS+ records the configurations as user readable statements.

TACACS+ uses Transmission Control Protocol (TCP) for its transport, unlike RADIUS which uses User Datagram Protocol (UDP). It maintains a database and listens on TCP port 49 for incoming requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm that is defined in the protocol and a shared secret key that is configured on both devices.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

The following are some guidelines about TACACS+:

- You must configure TACACS+ on both your CiscoSecure Access Control Server (ACS) and your controller. You can configure the controller through either the GUI or the CLI.
- TACACS+ is supported on CiscoSecure ACS version 3.2 and later releases. See the CiscoSecure ACS documentation for the version that you are running.

- One Time Passwords (OTPs) are supported on the controller using TACACS. In this configuration, the controller acts as a transparent passthrough device. The controller forwards all client requests to the TACACS server without inspecting the client behavior. When using OTP, the client must establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.
- We recommend that you increase the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and you can increase the retransmit timeout value to a maximum of 30 seconds.
- If you want to migrate your configuration from a Cisco 5508 WLC to a Cisco 5520 WLC, the RADIUS or TACACS+ configuration present in Cisco 5508 WLC does not work in Cisco 5520 WLC. We recommend that you configure the RADIUS or TACACS+ configuration again after migration.
- To configure the TACACS+ server:
  - Using Access Control Server (ACS)—See the latest Cisco Secure Access Control System guide at http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html.
  - Using Identity Services Engine (ISE)—See the *ISE TACACS+ Configuration Guide for Wireless LAN Controllers* at http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-TACACS_for_WLC.pdf.

TACACS+ DNS

You can use a fully qualified domain name (FQDN) that enables you to change the IP address when needed, for example, for load-balancing updates. A submenu, DNS, is added to the **Security > AAA > TACACS+** menu, which you can use to get TACACS+ IP information from a DNS. The DNS query is disabled by default.

Note IPv6 is not supported for TACAS+ DNS.

It is not possible to use both the static list and the DNS list at the same time. The addresses that are returned by the DNS override the static entries.

DNS AAA is valid for FlexConnect AP clients that use central authentication.

DNS AAA is not supported to define a RADIUS for FlexConnect AP groups. For FlexConnect clients with local switching, you have to manually define AAA.

Rogue, 802.1X, web authentication, MAC filtering, mesh, and other features that use the global list also use the DNS-defined servers.

This section contains the following subsections:

TACACS+ VSA

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF 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.

Configuring TACACS+ (GUI)

Step 1 Choose **Security** > **AAA** > **TACACS+**.

Step 2 Perform one of the following:

- If you want to configure a TACACS+ server for authentication, choose **Authentication**.
- If you want to configure a TACACS+ server for authorization, choose **Authorization**.
- If you want to configure a TACACS+ server for accounting, choose **Accounting**.

Note The pages used to configure authentication, authorization, and accounting all contain the same text boxes. Therefore, these instructions walk through the configuration only once, using the Authentication pages as examples. You would follow the same steps to configure multiple services and/or multiple servers.

For basic management authentication via TACACS+ to succeed, it is required to configure authentication and authorization servers on the WLC. Accounting configuration is optional.

The TACACS+ (Authentication, Authorization, or Accounting) Servers page appears. This page lists any TACACS+ servers that have already been configured.

- If you want to delete an existing server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 3 Perform one of the following:

- To edit an existing TACACS+ server, click the server index number for that server. The **TACACS+ (Authentication, Authorization, or Accounting) Servers > Edit** page appears.
- To add a TACACS+ server, click **New**. The **TACACS+ (Authentication, Authorization, or Accounting) Servers > New** page appears.

Step 4 If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured TACACS+ servers providing the same service. You can configure up to three servers. If the controller cannot reach the first server, it tries the second one in the list and then the third if necessary.

Step 5 If you are adding a new server, enter the IP address of the TACACS+ server in the **Server IP Address** text box.

Step 6 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret key to be used between the controller and the TACACS+ server. The default value is ASCII.

Step 7 In the **Shared Secret** and **Confirm Shared Secret** text boxes, enter the shared secret key to be used for authentication between the controller and the server.

Note The shared secret key must be the same on both the server and the controller.

Step 8 If you are adding a new server, enter the TACACS+ server's TCP port number for the interface protocols in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 49.

Step 9 In the **Server Status** text box, choose **Enabled** to enable this TACACS+ server or choose **Disabled** to disable it. The default value is Enabled.

Step 10 In the **Server Timeout** text box, enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Note We recommend that you increase the timeout value if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable.

Step 11 Click **Apply**.

Step 12 Specify the TACACS+ DNS parameters as follows:

a) Choose **Security** > **AAA** > **TACACS+** > **DNS**. The **TACACS DNS Parameters** page appears.
b) Select or unselect the **DNS Query** check box.
c) In the **Interval in sec** text box, enter the authentication port number. The valid range is 1 to 65535.

   The accounting port number is an increment of 1 of the authentication port number. For example, if you define the authentication port number as 1812, the accounting port number is 1813. The accounting port number is always derived from the authentication port number.

d) From the **Secret Format** drop-down list, choose the format in which you want to configure the secret. Valid options are ASCII and Hex.
e) Depending on the format selected, enter and confirm the secret.

   Note All servers are expected to use the same authentication port and the same secret.

f) In the **DNS Timeout** text box, enter the number of days after which the DNS query is refreshed to get the latest update from the DNS server.
g) In the **URL** text box, enter the fully qualified domain name or the absolute domain name of the TACACS+ server.
h) In the **Server IP Address** text box, enter the IPv4 address of the DNS server.

   Note IPv6 is not supported for TACACS+ DNS.

i) Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 Repeat the previous steps if you want to configure any additional services on the same server or any additional TACACS+ servers.

Step 15 Specify the order of authentication when multiple databases are configured by choosing **Security** > **Priority Order** > **Management User**. The Priority Order > Management User page appears.

Step 16 In the **Order Used for Authentication** text box, specify which servers have priority when the controller attempts to authenticate management users.

Use the **>** and **<** buttons to move servers between the **Not Used** and **Order Used for Authentication** text boxes. After the desired servers appear in the Order Used for Authentication text box, use the **Up** and **Down** buttons to move the priority server to the top of the list. By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 17 Click **Apply**.

Step 18 Click **Save Configuration**.

Related Topics

Configuring RADIUS (GUI)

Configuring TACACS+ (CLI)

Procedure

- Configure a TACACS+ authentication server by entering these commands:
  - **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ authentication server.
  - **config tacacs auth delete** *index*—Deletes a previously added TACACS+ authentication server.
  - **config tacacs auth** (**enable** | **disable**} *index*—Enables or disables a TACACS+ authentication server.
  - **config tacacs auth server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ authentication server.
- Configure a TACACS+ authorization server by entering these commands:
  - **config tacacs athr add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ authorization server.
  - **config tacacs athr delete** *index*—Deletes a previously added TACACS+ authorization server.
  - **config tacacs athr** (**enable** | **disable**} *index*—Enables or disables a TACACS+ authorization server.
  - **config tacacs athr server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ authorization server.
- Configure a TACACS+ accounting server by entering these commands:
  - **config tacacs acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ accounting server.
  - **config tacacs acct delete** *index*—Deletes a previously added TACACS+ accounting server.
  - **config tacacs acct** (**enable** | **disable**} *index*—Enables or disables a TACACS+ accounting server.
  - **config tacacs acct server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ accounting server.
- See TACACS+ statistics by entering these commands:
  - **show tacacs summary**—Shows a summary of TACACS+ servers and statistics.
  - **show tacacs auth stats**—Shows the TACACS+ authentication server statistics.
  - **show tacacs athr stats**—Shows the TACACS+ authorization server statistics.

  - **show tacacs acct stats**—Shows the TACACS+ accounting server statistics.

- Clear the statistics for one or more TACACS+ servers by entering this command:

  clear stats tacacs [**auth** | **athr** | **acct**] {*index* | *all*}

- Configure the order of authentication when multiple databases are configured by entering this command. The default setting is local and then radius.

  config aaa auth mgmt [**radius** | **tacacs**]

  See the current management authentication server order by entering the **show aaa auth** command.

- Make sure the controller can reach the TACACS+ server by entering this command:

  ping *server_ip_address*

- Configure TACACS+ DNS parameters by entering these commands:

  - **config tacacs dns global** *port-num* {*ascii* | *hex*} *secret*—Adds global port number and secret information for the TACACS+ DNS.
  - **config tacacs dns query** *url timeout-in-days*—Configures the FQDN of the TACACS+ server and timeout after which a refresh is performed to get the latest update from the DNS server.
  - **config tacacs dns serverip** *ip-addr*—Configures the IP address of the DNS server.
  - **config tacacs dns** {**enable** | **disable**}—Enables or disables the DNS query.

- Enable or disable TACACS+ debugging by entering this command:

  debug aaa tacacs {**enable** | **disable**}

- Save your changes by entering this command:

  save config

Related Topics

Configuring RADIUS (CLI)

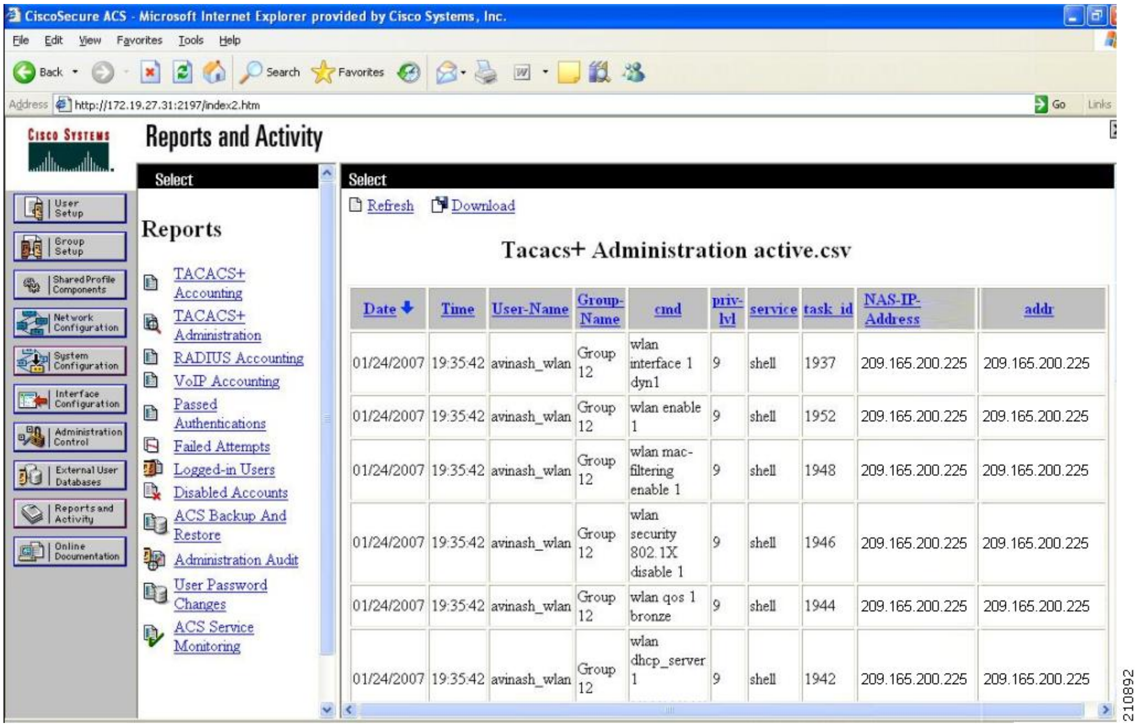
Viewing the TACACS+ Administration Server Logs

Step 1 On the ACS main page, in the left navigation pane, choose **Reports and Activity**.

Step 2 Under Reports, choose **TACACS+ Administration**.

Click the .csv file corresponding to the date of the logs you want to view. The TACACS+ Administration .csv page appears.

Figure 1: TACACS+ Administration .csv Page on CiscoSecure ACS



Tacacs+ Administration active.csv

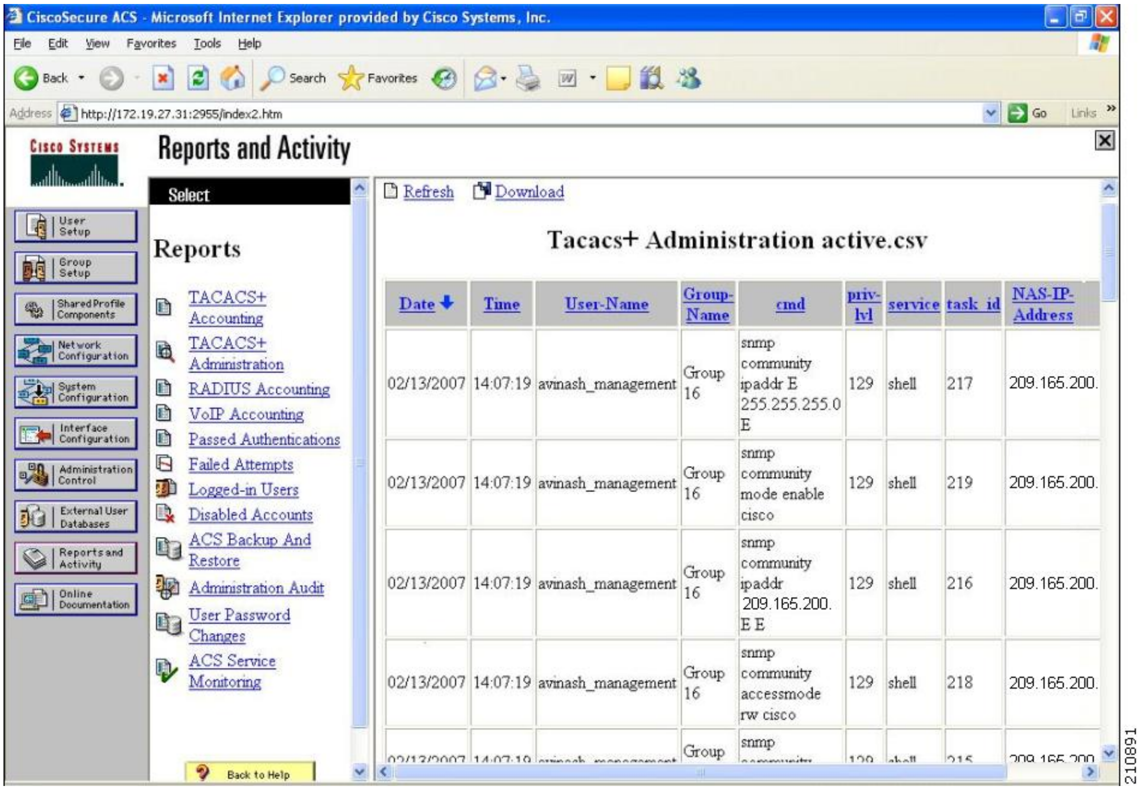
Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	task_id	NAS-IP-Address	addr
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan interface 1 dyn1	9	shell	1937	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan enable 1	9	shell	1952	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan mac-filtering enable 1	9	shell	1948	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan security 802.1X disable 1	9	shell	1946	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan qos 1 bronze	9	shell	1944	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan dhcp_server 1	9	shell	1942	209.165.200.225	209.165.200.225

This page displays the following information:

- Date and time the action was taken
- Name and assigned role of the user who took the action
- Group to which the user belongs
- Specific action that the user took
- Privilege level of the user who executed the action
- IP address of the controller
- IP address of the laptop or workstation from which the action was executed

Sometimes a single action (or command) is logged multiple times, once for each parameter in the command. For example, if you enter the **snmp community ipaddr** *ip_address subnet_mask community_name* command, the IP address may be logged on one line while the subnet mask and community name are logged as "E." On another line, the subnet mask maybe logged while the IP address and community name are logged as "E." See the first and third lines in the example in this figure.

Figure 2: TACACS+ Administration .csv Page on CiscoSecure ACS



Tacacs+ Administration active.csv

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	task_id	NAS-IP-Address
02/13/2007	14:07:19	avinash_management	Group 16	snmp community ipaddr E 255.255.255.0 E	129	shell	217	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community mode enable cisco	129	shell	219	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community ipaddr 209.165.200. E E	129	shell	216	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community accessmode rw cisco	129	shell	218	209.165.200.
02/13/2007	14:07:19	avinash_management	Group	snmp	129	shell	215	209.165.200