



AAA Administration

- [Setting up RADIUS, page 1](#)
- [Setting up TACACS+, page 27](#)
- [Maximum Local Database Entries, page 37](#)
- [Information About Configuring Maximum Local Database Entries, page 37](#)
- [Configuring Maximum Local Database Entries \(GUI\), page 38](#)
- [Configuring Maximum Local Database Entries \(CLI\), page 38](#)

Setting up RADIUS

Information About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a backend database similar to local and TACACS+ and provides authentication and accounting 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 RADIUS server. If multiple databases are configured, you can specify the sequence in which the backend database must be tried.

**Note**

Clients using Microsoft Windows 10 with default (zero-touch config) supplicant fail to connect to Cisco WLC when there is no CA certificate to validate the server certificate. This is because the supplicant does not pop up a window to accept the server certificate and silently rejects the 802.1X authentication. Therefore, we recommend that you do either of the following:

- Manually install a third-party CA certificate on the AAA server, which the clients using Microsoft Windows 10 can trust.
- Use any other supplicant, such as Cisco AnyConnect, which pops up a window to trust or not trust the server certificate. If you accept the trust certificate, then the client is authenticated.

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

Whenever a user successfully executes an action, the RADIUS 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 RADIUS accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting 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 defined in the protocol and a shared secret key configured on both devices.

You can configure multiple RADIUS accounting and authentication servers. For example, you may want to have one central RADIUS authentication server but several RADIUS accounting 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, then the third one if necessary, and so on.

When a management user is authenticated using a RADIUS server, only the PAP protocol is used. For web authentication users, PAP, MSCHAPv2 and MD5 security mechanisms are supported.

RADIUS Server Support

- You can configure up to 17 RADIUS authentication and accounting servers each.
- If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.
- One Time Passwords (OTPs) are supported on the controller using RADIUS. In this configuration, the controller acts as a transparent passthrough device. The controller forwards all client requests to the RADIUS 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.
- To create a read-only controller user on the RADIUS sever, you must set the service type to NAS prompt instead of Callback NAS prompt. If you set the service type to Callback NAS Prompt, the user authentication fails while setting it to NAS prompt gives the user read-only access to the controller.

Also, the Callback Administrative service type gives the user the lobby ambassador privileges to the controller.

- If RADIUS servers are mapped per WLAN, then controller do not use RADIUS server from the global list on that WLAN.
- To configure the RADIUS server:
 - Using Access Control Server (ACS)—See the latest Cisco Secure Access Control System guide at <https://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>.
 - Using Identity Services Engine (ISE)—See the Configuring External RADIUS Servers section in the Cisco Identity Services Engine Administrator Guide at <https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html>.

Primary and Fallback RADIUS Servers

The primary RADIUS server (the server with the lowest server index) is assumed to be the most preferable server for the controller. If the primary server becomes unresponsive, the controller switches to the next active backup server (the server with the next lowest server index). The controller continues to use this backup server, unless you configure the controller to fall back to the primary RADIUS server when it recovers and becomes responsive or to a more preferable server from the available backup servers.

RADIUS 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 > RADIUS** menu, which you can use to get RADIUS IP information from a DNS. The DNS query is disabled by default.

Restrictions on Configuring RADIUS

- You can configure the session timeout value for RADIUS server up to 65535 seconds. The controller does not support configuring session timeout value for RADIUS server higher than 65535 seconds.
- The session timeout value configured on RADIUS server if set beyond 24 days, then the RADIUS session timeout value does not override the session timeout value configured locally over a WLAN.
- 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.
- A network address translation (NAT) scenario when IPsec is enabled on traffic between Cisco WLC and RADIUS server is not supported.

Configuring RADIUS on the ACS

Step 1 Choose **Network Configuration** on the ACS main page.

Step 2 Choose **Add Entry** under AAA Clients to add your controller to the server. The Add AAA Client page appears.

Figure 1: Add AAA Client Page on CiscoSecure ACS

Step 3 In the **AAA Client Hostname** text box, enter the name of your controller.

Step 4 In the **AAA Client IP Address** text box, enter the IP address of your controller.

Step 5 In the **Shared Secret** text box, enter the shared secret key to be used for authentication between the server and the controller.

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

- Step 6** From the Authenticate Using drop-down list, choose **RADIUS (Cisco Airespace)**.
- Step 7** Click **Submit + Apply** to save your changes.
- Step 8** Choose **Interface Configuration** on the ACS main page.
- Step 9** Choose **RADIUS (Cisco Aironet)**. The RADIUS (Cisco Aironet) page appears.
- Step 10** Under User Group, select the **Cisco-Aironet-Session-Timeout** check box.
- Step 11** Click **Submit** to save your changes.
- Step 12** On the ACS main page, from the left navigation pane, choose **System Configuration**.
- Step 13** Choose **Logging**.
- Step 14** When the Logging Configuration page appears, enable all of the events that you want to be logged and save your changes.
- Step 15** On the ACS main page, from the left navigation pane, choose **Group Setup**.
- Step 16** Choose a previously created group from the Group drop-down list.
Note This step assumes that you have already assigned users to groups on the ACS according to the roles to which they will be assigned.
- Step 17** Click **Edit Settings**. The Group Setup page appears.
- Step 18** Under **Cisco Aironet Attributes**, select the **Cisco-Aironet-Session-Timeout** check box and enter a session timeout value in the edit box.
- Step 19** Specify read-only or read-write access to controllers through RADIUS authentication, by setting the Service-Type attribute (006) to **Callback NAS Prompt** for read-only access or to **Administrative** for read-write privileges. If you do not set this attribute, the authentication process completes successfully (without an authorization error on the controller), but you might be prompted to authenticate again.
Note If you set the Service-Type attribute on the ACS, make sure to select the **Management** check box on the RADIUS Authentication Servers page of the controller GUI.
- Step 20** Click **Submit** to save your changes.
-

Configuring RADIUS (GUI)

-
- Step 1** Choose **Security > AAA > RADIUS**.
- Step 2** Perform one of the following:
- If you want to configure a RADIUS server for authentication, choose **Authentication**.
 - If you want to configure a RADIUS server for accounting, choose **Accounting**.
- Note** The pages used to configure authentication and accounting contain mostly 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.
- The RADIUS Authentication (or Accounting) Servers page appears.
- This page lists any RADIUS 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 From the **Acct Call Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

Note The AP Name:SSID, AP Name, AP Group, Flex Group, AP Location, and VLAN ID options are added in the 7.4 release.

The AP Ethernet MAC Address and AP Ethernet MAC Address:SSID are added in the 7.6 release.

Step 4 From the **Auth Call Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address

- AP Ethernet MAC Address:SSID

- Step 5** Enable RADIUS-to-controller key transport using AES key wrap protection by checking the **Use AES Key Wrap** check box. The default value is unchecked. This feature is required for FIPS customers.
- Step 6** From the **MAC Delimiter** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:
- Colon
 - Hyphen
 - Single-hyphen
 - None
- Step 7** Click **Apply**. Perform one of the following:
- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Authentication (or Accounting) Servers > Edit** page appears.
 - To add a RADIUS server, click **New**. The **RADIUS Authentication (or Accounting) Servers > New** page appears.
- Step 8** 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 RADIUS servers providing the same service.
- Step 9** If you are adding a new server, enter the IP address of the RADIUS server in the **Server IP Address** text box.
- Note** Auto IPv6 is not supported on RADIUS server. The RADIUS server must not be configured with Auto IPv6 address. Use fixed IPv6 address instead.
- Step 10** 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 RADIUS server. The default value is ASCII.
- Step 11** 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 12** If you are configuring a new RADIUS authentication server and want to enable AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure, follow these steps:
- Note** AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.
- a) Check the **Key Wrap** check box.
 - b) From the **Key Wrap Format** drop-down list, choose **ASCII** or **HEX** to specify the format of the AES key wrap keys: Key Encryption Key (KEK) and Message Authentication Code Key (MACK).
 - c) In the **Key Encryption Key (KEK)** text box, enter the 16-byte KEK.
 - d) In the **Message Authentication Code Key (MACK)** text box, enter the 20-byte KEK.
- Step 13** If you are adding a new server, enter the RADIUS server's UDP port number for the interface protocols in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.
- Step 14** From the **Server Status** text box, choose **Enabled** to enable this RADIUS server or choose **Disabled** to disable it. The default value is enabled.
- Step 15** If you are configuring a new RADIUS authentication server, from the **Support for RFC 3576** drop-down list, choose **Enabled** to enable change of authorization, which is an extension to the RADIUS protocol that allows dynamic changes to a user session, or choose **Disabled** to disable this feature. By default, this is set to Disabled state. Support for RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports

disconnect and change of authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.

Step 16 In the **Server Timeout** text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Check the **Key Wrap** check box.

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 17 Check the **Network User** check box to enable network user authentication (or accounting), or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, this entry is considered the RADIUS authentication (or accounting) server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.

Step 18 If you are configuring a RADIUS authentication server, check the **Management** check box to enable management authentication, or uncheck the check box to disable this feature. The default value is checked. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.

Step 19 Enter the **Management Retransmit Timeout** value, which denotes the network login retransmission timeout for the server.

Step 20 If you want to use a tunnel gateway as AAA proxy, check the **Tunnel Proxy** check box. The gateway can function as a proxy RADIUS server as well as a tunnel gateway.

Step 21 Check the **IPSec** check box to enable the IP security mechanism, or uncheck the check box to disable this feature. The default value is unchecked.

Note IPSec is not supported for IPv6. Use this only if you have used IPv4 for Server IP Address.

Step 22 If you enabled IPsec in *Step 17*, follow these steps to configure additional IPsec parameters:

a) From the IPsec drop-down list, choose one of the following options as the authentication protocol to be used for IP security: **HMAC MD5** or **HMAC SHA1**. The default value is HMAC SHA1.

A message authentication code (MAC) is used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is based on cryptographic hash functions. It can be used in combination with any iterated cryptographic hash function. HMAC MD5 and HMAC SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

b) From the IPsec Encryption drop-down list, choose one of the following options to specify the IP security encryption mechanism:

- **DES**—Data Encryption Standard that is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
- **3DES**—Data Encryption Standard that applies three keys in succession. This is the default value.
- **AES CBC**—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt data blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Block Chaining (CBC) mode.
- **256-AES**—Advanced Encryption Standard that uses keys with a length of 256 bits.

c) From the IKE Phase 1 drop-down list, choose one of the following options to specify the Internet Key Exchange (IKE) protocol: **Aggressive** or **Main**. The default value is Aggressive.

IKE Phase 1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets with the benefit of slightly faster connection establishment at the cost of transmitting the identities of the security gateways in the clear.

- d) In the Lifetime text box, enter a value (in seconds) to specify the timeout interval for the session. The valid range is 1800 to 57600 seconds, and the default value is 1800 seconds.
- e) From the IKE Diffie Hellman Group drop-down list, choose one of the following options to specify the IKE Diffie Hellman group: **Group 1 (768 bits)**, **Group 2 (1024 bits)**, or **Group 5 (1536 bits)**. The default value is Group 1 (768 bits).

Diffie-Hellman techniques are used by two devices to generate a symmetric key through which they can publicly exchange values and generate the same symmetric key. Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

Note If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, WLANCC should be enabled to use the IPSec shared secret, default value is used otherwise. You can view the status for the WLANCC and UCAPL prerequisite modes in **Controller > Inventory**.

Step 23 Click **Apply**.

Step 24 Click **Save Configuration**.

Step 25 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Step 26 Specify the RADIUS server fallback behavior, as follows:

- a) Choose **Security > AAA > RADIUS > Fallback to open the RADIUS > Fallback Parameters** to open the fallback parameters page.
- b) From the **Fallback Mode** drop-down list, choose one of the following options:
- **Off**—Disables RADIUS server fallback. This is the default value.
 - **Passive**—Causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
 - **Active**—Causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.
- c) If you enabled Active fallback mode in *Step b*, enter the name to be sent in the inactive server probes in the **Username** text box. You can enter up to 16 alphanumeric characters. The default value is "cisco-probe."
- d) If you enabled Active fallback mode in *Step b*, enter the probe interval value (in seconds) in the Interval in **Sec** text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 27 Specify the RADIUS DNS parameters as follows:

Note IPv6 is not supported for RADIUS DNS.

- a) Choose **Security > AAA > RADIUS > DNS**. The **RADIUS DNS Parameters** page appears.
- b) Check or uncheck the **DNS Query** check box.
- c) In the **Port Number** 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 RADIUS server.
- h) In the **Server IP Address** text box, enter the IP address of the DNS server.
- i) Click **Apply**.

Step 28 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 29 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 30 Click **Apply**.

Step 31 Click **Save Configuration**.

Configuring RADIUS (CLI)

- Specify whether the IP address, system MAC address, AP MAC address, AP Ethernet MAC address of the originator will be sent to the RADIUS server in the Access-Request message by entering this command:

```
config radius callStationIdType {ipaddr | macaddr | ap-macaddr-only | ap-macaddr-ssid |
ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid |
ap-location | ap-name | ap-name-ssid | flex-group-name | vlan-id}
```

This command supports both IPv4 and IPv6 address formats.



Note

The default is System MAC Address.



Caution

Do not use Call Station ID Type for IPv6-only clients.

- Specify the delimiter to be used in the MAC addresses that are sent to the RADIUS authentication or accounting server in Access-Request messages by entering this command:

```
config radius {auth | acct} mac-delimiter {colon | hyphen | single-hyphen | none}
```

where

- **colon** sets the delimiter to a colon (the format is xx:xx:xx:xx:xx:xx).
 - **hyphen** sets the delimiter to a hyphen (the format is xx-xx-xx-xx-xx-xx). This is the default value.
 - **single-hyphen** sets the delimiter to a single hyphen (the format is xxxxxx-xxxxxx).
 - **none** disables delimiters (the format is xxxxxxxxxxxx).
- Configure a RADIUS authentication server by entering these commands:
 - **config radius auth add** *index server_ip_address port_number {ascii | hex} shared_secret*—Adds a RADIUS authentication server.

This command supports both IPv4 and IPv6 address formats.
 - **config radius auth keywrap** {**enable** | **disable**}—Enables AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.
 - **config radius auth keywrap add** {**ascii** | **hex**} *kek mack index*—Configures the AES key wrap attributes
where
 - *kek* specifies the 16-byte Key Encryption Key (KEK).
 - *mack* specifies the 20-byte Message Authentication Code Key (MACK).
 - *index* specifies the index of the RADIUS authentication server on which to configure the AES key wrap.
 - **config radius auth rfc3576** {**enable** | **disable**} *index*—Enables or disables RFC 3576, which is an extension to the RADIUS protocol that allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change-of-authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.
 - **config radius auth retransmit-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS authentication server.
 - **config radius auth mgmt-retransmit-timeout** *index timeout*—Configures the default management login retransmission timeout for a RADIUS authentication server.
 - **config radius auth network** *index* {**enable** | **disable**}—Enables or disables network user authentication. If you enable this feature, this entry is considered the RADIUS authentication server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
 - **config radius auth management** *index* {**enable** | **disable**}—Enables or disables management authentication. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.
 - **config radius auth ipsec** {**enable** | **disable**} *index*—Enables or disables the IP security mechanism.
 - **config radius auth ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.

- **config radius auth ipsec encryption** {256-aes | 3des | aes | des | none} *index*—Configures the IP security encryption mechanism.
- **config radius auth ipsec ike dh-group** {group-1 | group-2 | group-5 | 2048bit-group-14} *index*—Configures the IKE Diffie-Hellman group.
- **config radius auth ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
- **config radius auth ipsec ike phase1** {aggressive | main} *index*—Configures the Internet Key Exchange (IKE) protocol.
- **config radius auth ipsec ike auth-method** {PSK | certificate} *index*—Configures the IKE authentication methods. By default PSK is used for IPSEC sessions.
- **config radius auth ipsec ike auth-mode pre-shared-key** *index hex/ascii-secret*—Configures the IPSEC pre-shared key.
- **config radius auth ipsec ike auth-mode** {pre-shared-key *index hex-ascii-index shared-secret* | certificate *index*} —Configures the IKE authentication method. By default, preshared key is used for IPSEC sessions.
- **config radius auth** {enable | disable} *index*—Enables or disables a RADIUS authentication server.
- **config radius auth delete** *index*—Deletes a previously added RADIUS authentication server.
- Configure a RADIUS accounting server by entering these commands:
 - **config radius acct add** *index server_ip_address port#* {ascii | hex} *shared_secret*—Adds a RADIUS accounting server.
This command supports both IPv4 and IPv6 address formats.
 - **config radius acct server-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS accounting server.
 - **config radius acct network** *index* {enable | disable}—Enables or disables network user accounting. If you enable this feature, this entry is considered the RADIUS accounting server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
 - **config radius acct ipsec** {enable | disable} *index*—Enables or disables the IP security mechanism.
 - **config radius acct ipsec authentication** {hmac-md5 | hmac-sha1} *index*—Configures the authentication protocol to be used for IP security.
 - **config radius acct ipsec encryption** {256-aes | 3des | aes | des | none} *index*—Configures the IP security encryption mechanism.
 - **config radius acct ipsec ike dh-group** {2048bit-group-14 | group-1 | group-2 | group-5} *index*—Configures the IKE Diffie Hellman group.
 - **config radius acct ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
 - **config radius acct ipsec ike auth-mode** {pre-shared-key *index hex-ascii-index shared-secret* | certificate *index*} —Configures the IKE authentication method. By default, preshared key is used for IPSEC sessions.

- **config radius acct ipsec ike phase1 {aggressive | main} index**—Configures the Internet Key Exchange (IKE) protocol.
- **config radius acct {enable | disable} index**—Enables or disables a RADIUS accounting server.
- **config radius acct delete index**—Deletes a previously added RADIUS accounting server.
- **config radius acct region {group | none | provincial}**—Configures the RADIUS region.
- **config radius acct realm {add | delete} radius-index realm-string**—Configures the realm of the RADIUS accounting server.
- **config radius auth callStationIdType {ap-ethmac-only | ap-ethmac-ssid}**—Sets the Called Station ID type to be AP's radio MAC address or AP's radio MAC address with SSID.
- **config radius auth callStationIdType ap-label-address**—Sets the Called Station ID Type to the AP MAC address that is printed on the AP label, for the authentication messages.
config radius auth callStationIdType ap-label-address-ssid—Sets the Call Station ID Type to the <AP label MAC address>:<SSID> format, for the authentication messages.
- **config radius auth callStationIdType ap-group-name**—Sets the Called Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
- **config radius auth callStationIdType ap-location**—Sets the Called Station ID to the AP Location.
- **config radius auth callStationIdType {ap-macaddr-only | ap-macaddr-ssid}**—Sets the Called Station ID type to be AP's radio MAC address or AP's radio MAC address with SSID in the <AP radio MAC address>:<SSID> format.
- **config radius auth callStationIdType {ap-name | ap-name-ssid}**—Sets the Called Station ID type to be AP name or AP name with SSID in the <AP name>:<SSID> format.



Note When the Called Station ID type is set to AP name, the conversion of uppercase letters to lowercase letters for the AP name is not considered. For example, while creating an AP, if the AP name is provided with uppercase letters, then the AP name for the call station ID type gets displayed with upper case letters only.

- **config radius auth callStationIdType flex-group-name**—Sets the Called Station ID type to the FlexConnect group name.
 - **config radius auth callStationIdType {ipaddr | macaddr}**—Sets the Called Station ID type to use the IP address (only Layer 3) or system's MAC address.
 - **config radius auth callStationIdType vlan-id**—Sets the Called Station ID type to the system's VLAN ID.
- Configure the RADIUS server fallback behavior by entering this command:
config radius fallback-test mode {off | passive | active}
 where
- **off** disables RADIUS server fallback.

- **passive** causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
- **active** causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller simply ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.
- If you enabled Active mode in *Step 5*, enter these commands to configure additional fallback parameters:
 - **config radius fallback-test username** *username*—Specifies the name to be sent in the inactive server probes. You can enter up to 16 alphanumeric characters for the *username parameter*.
 - **config radius fallback-test interval** *interval*—Specifies the probe interval value (in seconds).
- Configure RADIUS DNS parameters by entering these commands:
 - **config radius dns global** *port-num {ascii | hex} secret*—Adds global port number and secret information for the RADIUS DNS.
 - **config radius dns query** *url timeout-in-days*—Configures the FQDN of the RADIUS server and timeout after which a refresh is performed to get the latest update from the DNS server.
 - **config radius dns serverip** *ip-addr*—Configures the IP address of the DNS server.
 - **config radius dns {enable | disable}**—Enables or disables the DNS query.
- Configure RADIUS extended source ports support by entering this command:
config radius ext-source-ports {enable | disable}
 Enabling multiple source ports allows the number of outstanding RADIUS requests to be increased. With single source port, the number of outstanding requests was limited to 255 for each authentication and accounting request.
 The number of RADIUS queues supported on various WLC platforms:
 - Cisco 5508 WLC and Cisco WiSM2 support 8 RADIUS queues
 - Cisco 5520, Flex 7510, and 8510, and 8540 WLCs support 16 RADIUS queues
- Save your changes by entering this command:
save config
- Configure the order of authentication when multiple databases are configured by entering this command:
config aaa auth mgmt *AAA_server_type AAA_server_type*
 where *AAA_server_type* is local, RADIUS, or TACACS+.
 To see the current management authentication server order, enter the **show aaa auth** command.
- See RADIUS statistics by entering these commands:
 - **show radius summary**—Shows a summary of RADIUS servers and statistics with AP Ethernet MAC configurations.
 - **show radius auth statistics**—Shows the RADIUS authentication server statistics.

- **show radius acct statistics**—Shows the RADIUS accounting server statistics.
- **show radius rfc3576 statistics**—Shows a summary of the RADIUS RFC-3576 server.
- See active security associations by entering these commands:
 - **show ike {brief | detailed} ip_or_mac_addr**—Shows a brief or detailed summary of active IKE security associations.
 - **show ipsec {brief | detailed} ip_or_mac_addr**—Shows a brief or detailed summary of active IPsec security associations.
- Clear the statistics for one or more RADIUS servers by entering this command:
clear stats radius {auth | acct} {index | all}
- Make sure that the controller can reach the RADIUS server by entering this command:
ping server_ip_address

RADIUS Authentication Attributes Sent by the Controller

The following tables identify the RADIUS authentication attributes sent between the controller and the RADIUS server in access-request and access-accept packets.

Table 1: Authentication Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type ¹
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message

- ¹ To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to **Callback NAS Prompt** for read-only access or to **Administrative** for read-write privileges.

Table 2: Authentication Attributes Honored in Access-Accept Packets (Cisco)

Attribute ID	Description
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL



Note

These Cisco-specific attributes are not supported: Auth-Algo-Type and SSID.

Table 3: Authentication Attributes Honored in Access-Accept Packets (Standard)

Attribute ID	Description
6	Service-Type. To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to Callback NAS Prompt for read-only access or to Administrative for read-write privileges.
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID



Note

Message authentication is not supported.

Table 4: Authentication Attributes Honored in Access-Accept Packets (Microsoft)

Attribute ID	Description
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

Table 5: Authentication Attributes Honored in Access-Accept Packets (Airespace)

Attribute ID	Description
1	VAP-ID
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name Note Guest-Role-Name is honored only on L3 security web authentication with AAA over-ride enabled on the Cisco WLC.
13	Data-Bandwidth-Average-Contract-US
14	Real-Time-Bandwidth-Average-Contract-US
15	Data-Bandwidth-Burst-Contract-US
16	Real-Time-Bandwidth-Burst-Contract-US

Authentication Attributes Honored in Access-Accept Packets (Airespace)

This section lists the RADIUS authentication Airespace attributes currently supported on the Cisco WLC.

VAP ID

This attribute indicates the WLAN ID of the WLAN to which the client should belong. When the WLAN-ID attribute is present in the RADIUS Access Accept, the system applies the WLAN-ID (SSID) to the client station after it authenticates. The WLAN ID is sent by the Cisco WLC in all instances of authentication except IPsec. In case of web authentication, if the Cisco WLC receives a WLAN-ID attribute in the authentication response from the AAA server, and it does not match the ID of the WLAN, authentication is rejected. The 802.1X/MAC filtering is also rejected. The rejection, based on the response from the AAA server, is because of the SSID Cisco AVPair support. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Vendor-Id (cont.)   | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               WLAN ID (VALUE) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 1
- Vendor length – 4
- Value – ID of the WLAN to which the client should belong.

QoS-Level

This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Vendor-Id (cont.)   | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               QoS Level |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
 - 3 – Bronze (Background)
 - 0 – Silver (Best Effort)

- 1 – Gold (Video)
- 2 – Platinum (Voice)

Differentiated Services Code Point (DSCP)

DSCP is a packet header code that can be used to provide differentiated services based on the QoS levels. This attribute defines the DSCP value to be applied to a client. When present in a RADIUS Access Accept, the DSCP value overrides the DSCP value specified in the WLAN profile. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |   Length   |   Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     DSCP (VALUE)                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 3
- Vendor length – 4
- Value – DSCP value to be applied for the client.

802.1p Tag Type

802.1p VLAN tag received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. This attribute defines the 802.1p priority to be applied to the client. When present in a RADIUS Access Accept, the 802.1p value overrides the default specified in the WLAN profile. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |   Length   |   Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     802.1p (VALUE)                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 4

- Vendor length – 3
- Value – 802.1p priority to be applied to a client.

VLAN Interface Name

This attribute indicates the VLAN interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Interface Name... |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – A string that includes the name of the interface the client is to be assigned to.



Note

This attribute only works when MAC filtering is enabled or if 802.1X or WPA is used as the security policy.

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| ACL Name... |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0

- Value – A string that includes the name of the ACL to use for the client

Data Bandwidth Average Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied for a client for non-realtime traffic such as TCP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Average Contract value overrides the Average Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Data Bandwidth Average Contract...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 7
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Average Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Real Time Bandwidth Average Contract value overrides the Average Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Real Time Bandwidth Average Contract...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 8
- Vendor length – 4
- Value – A value in kbps

Data Bandwidth Burst Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Burst Contract value overrides the Burst Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Data Bandwidth Burst Contract...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 9
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Burst Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Real Time Bandwidth Burst Contract value overrides the Burst Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.



Note

If you try to implement Average Data Rate and Burst Data Rate as AAA override parameters to be pushed from a AAA server, both Average Data Rate and Burst Data Rate have to be sent from ISE.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |                               Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Real Time Bandwidth Burst Contract...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 10
- Vendor length – 4
- Value – A value in kbps

Guest Role Name

This attribute provides the bandwidth contract values to be applied for an authenticating user. When present in a RADIUS Access Accept, the bandwidth contract values defined for the Guest Role overrides the bandwidth contract values (based on QoS value) specified for the WLAN. The fields are transmitted from left to right.

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Type      | Length      |      Vendor-Id      |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Vendor-Id (cont.)      | Vendor type  | Vendor length |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      GuestRoleName ...      |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 11
- Vendor length – Variable based on the Guest Role Name length
- Value – A string of alphanumeric characters

Data Bandwidth Average Contract Upstream

This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Data Bandwidth Average Contract value overrides the Average Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Type      | Length      |      Vendor-Id      |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Vendor-Id (cont.)      | Vendor type  | Vendor length |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Data Bandwidth Average Contract Upstream...      |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 13
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Average Contract Upstream

This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Real Time Bandwidth Average Contract value overrides the

Average Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |   Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Real Time Bandwidth Average Contract Upstream...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 14
- Vendor length – 4
- Value – A value in kbps

Data Bandwidth Burst Contract Upstream

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Data Bandwidth Burst Contract value overrides the Burst Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |   Vendor-Id   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Data Bandwidth Burst Contract Upstream...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 15
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Burst Contract Upstream

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to upstream direction from wireless to wired.

When present in a RADIUS Access Accept, the Real Time Bandwidth Burst Contract value overrides the Burst Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   | Length |           Vendor-Id           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Real Time Bandwidth Burst Contract Upstream...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 16
- Vendor length – 4
- Value – A value in kbps

RADIUS Accounting Attributes

This table identifies the RADIUS accounting attributes for accounting requests sent from a controller to the RADIUS server.

Table 6: Accounting Attributes for Accounting Requests

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
40	Accounting-Status-Type
41	Accounting-Delay-Time (Stop and interim messages only)
42	Accounting-Input-Octets (Stop and interim messages only)
43	Accounting-Output-Octets (Stop and interim messages only)
44	Accounting-Session-ID

Attribute ID	Description
45	Accounting-Authentic
46	Accounting-Session-Time (Stop and interim messages only)
47	Accounting-Input-Packets (Stop and interim messages only)
48	Accounting-Output-Packets (Stop and interim messages only)
49	Accounting-Terminate-Cause (Stop messages only)
52	Accounting-Input-Gigawords
53	Accounting-Output-Gigawords
55	Event-Timestamp
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID
	IPv6-Framed-Prefix
190	IPv6-Framed-Address

This table lists the different values for the Accounting-Status-Type attribute (40).

Table 7: Accounting-Status-Type Attribute Values

Attribute ID	Description
1	Start
2	Stop
3	Interim-Update Note RADIUS Accounting Interim updates are sent upon each client authentication, even if the RADIUS Server Accounting - Interim Update feature is not enabled on the client's WLAN.
7	Accounting-On
8	Accounting-Off
9-14	Reserved for Tunneling Accounting
15	Reserved for Failed

Setting up TACACS+

Information About 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 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.

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 defined in the protocol and a shared secret key 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 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.

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+ on the ACS

Step 1 Choose **Network Configuration** on the ACS main page.

Step 2 Choose **Add Entry** under AAA Clients to add your controller to the server. The Add AAA Client page appears.

Figure 2: Add AAA Client Page on CiscoSecure ACS

Step 3 In the **AAA Client Hostname** text box, enter the name of your controller.

Step 4 In the **AAA Client IP Address** text box, enter the IP address of your controller.

Step 5 In the **Shared Secret** text box, enter the shared secret key to be used for authentication between the server and the controller.

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

- Step 6** From the Authenticate Using drop-down list, choose **TACACS+ (Cisco IOS)**.
- Step 7** Click **Submit + Apply** to save your changes.
- Step 8** On the ACS main page, in the left navigation pane, choose **Interface Configuration**.
- Step 9** Choose **TACACS+ (Cisco IOS)**. The TACACS+ (Cisco) page appears.
- Step 10** Under **TACACS+ Services**, select the **Shell (exec)** check box.
- Step 11** Under **New Services**, select the first check box and enter **ciscowlc** in the Service text box and **common** in the Protocol text box.
- Step 12** Under **Advanced Configuration Options**, select the **Advanced TACACS+ Features** check box.
- Step 13** Click **Submit** to save your changes.
- Step 14** On the ACS main page, in the left navigation pane, choose **System Configuration**.
- Step 15** Choose **Logging**.
- Step 16** When the Logging Configuration page appears, enable all of the events that you want to be logged and save your changes.
- Step 17** On the ACS main page, in the left navigation pane, choose **Group Setup**.
- Step 18** From the Group drop-down list, choose a previously created group.
- Note** This step assumes that you have already assigned users to groups on the ACS according to the roles to which they will be assigned.
- Step 19** Click **Edit Settings**. The Group Setup page appears.
- Step 20** Under **TACACS+ Settings**, select the **ciscowlc common** check box.
- Step 21** Select the **Custom Attributes** check box.
- Step 22** In the text box below Custom Attributes, specify the roles that you want to assign to this group. The available roles are MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, ALL, and LOBBY. The first seven correspond to the menu options on the controller GUI and allow access to those particular controller features. If a user is not entitled for a particular task, the user is still allowed to access that task in read-only mode. You can enter one or multiple roles, depending on the group's needs. Use ALL to specify all seven roles or LOBBY to specify the lobby ambassador role. Enter the roles using this format:
- `role=ROLE`
- For example, to specify the WLAN, CONTROLLER, and SECURITY roles for a particular user group, you would enter the following text:
- ```
role1=WLAN
role2=CONTROLLER
role3=SECURITY?
```
- To give a user group access to all seven roles, you would enter the following text:
- ```
role1=ALL?
```
- Note** Make sure to enter the roles using the format shown above. The roles must be in all uppercase letters, and there can be no spaces within the text.
- Note** You should not combine the MONITOR role or the LOBBY role with any other roles. If you specify one of these two roles in the Custom Attributes text box, users will have MONITOR or LOBBY privileges only, even if additional roles are specified.
- Step 23** Click **Submit** to save your changes.

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.

Note 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:
- Choose **Security > AAA > TACACS+ > DNS**. The **TACACS DNS Parameters** page appears.
 - Select or unselect the **DNS Query** check box.
 - 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.
 - From the **Secret Format** drop-down list, choose the format in which you want to configure the secret. Valid options are ASCII and Hex.
 - 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.
 - 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.
 - In the **URL** text box, enter the fully qualified domain name or the absolute domain name of the TACACS+ server.
 - In the **Server IP Address** text box, enter the IPv4 address of the DNS server.
Note IPv6 is not supported for TACACS+ DNS.
 - 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**.
-

Configuring TACACS+ (CLI)

- 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.
This command supports both IPv4 and IPv6 address formats.
 - **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.
This command supports both IPv4 and IPv6 address formats.
 - **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.
 - **config tacacs athr mgmt-server-timeout** *index timeout*—Configures the default management login server timeout 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.
This command supports both IPv4 and IPv6 address formats.
 - **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.
 - **config tacacs acct mgmt-server-timeout** *index timeout*—Configures the default management login server timeout 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

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 3: TACACS+ Administration .csv Page on CiscoSecure ACS

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows <http://172.19.27.31:2197/index2.htm>. The page title is "Reports and Activity". On the left, there is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity (selected), and Online Documentation. The main content area is titled "Reports" and lists various report categories: TACACS+ Accounting, TACACS+ Administration, RADIUS Accounting, VoIP Accounting, Passed Authentications, Failed Attempts, Logged-in Users, Disabled Accounts, ACS Backup And Restore, Administration Audit, User Password Changes, and ACS Service Monitoring. The "TACACS+ Administration" report is selected, and it displays a table titled "Tacacs+ Administration active.csv". The table has columns: Date, Time, User-Name, Group-Name, cmd, priv-lvl, service, task_id, NAS-IP-Address, and addr. The table contains seven rows of log entries, all dated 01/24/2007 at 19:35:42, performed by user avinash_wlan in Group 12. The actions include commands like "wlan interface 1 dyn1", "wlan enable 1", "wlan mac-filtering enable 1", "wlan security 802.1X disable 1", "wlan qos 1 bronze", and "wlan dhcp_server 1".

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 4: TACACS+ Administration .csv Page on CiscoSecure ACS

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows <http://172.19.27.31:2955/index2.htm>. The page title is "Reports and Activity". On the left is a navigation menu with options like User Setup, Group Setup, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity (selected), and Online Documentation. The main content area is titled "TACACS+ Administration active.csv" and contains a table with columns: Date, Time, User-Name, Group-Name, cmd, priv-lvl, service, task_id, and NAS-IP-Address. The table lists several log entries for the user 'avinash_management' from 'Group 16' on '02/13/2007' at '14:07:19'. The commands include 'snmp community ipaddr E 255.255.255.0 E', 'snmp community mode enable cisco', 'snmp community ipaddr 209.165.200.E E', and 'snmp community accessmode rw cisco'. The task IDs are 217, 219, 216, and 218 respectively, all with a privilege level of 129 and service 'shell'. The NAS IP address for all entries is 209.165.200.

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.

Maximum Local Database Entries

Information About Configuring Maximum Local Database Entries

You can configure the controller to specify the maximum number of local database entries that are used for storing user authentication information. The database entries include local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

Configuring Maximum Local Database Entries (GUI)

-
- Step 1** Choose **Security > AAA > General** to open the General page.
- Step 2** In the Maximum Local Database Entries text box, enter a value for the maximum number of entries that can be added to the local database the next time the controller reboots. The currently configured value appears in parentheses to the right of the text box. The valid range is 512 to 2048, and the default setting is 2048.
The **Number of Entries, Already Used** text box shows the number of entries currently in the database.
- Step 3** Click **Apply** to commit your changes.
- Step 4** Click **Save Configuration** to save your settings.
-

Configuring Maximum Local Database Entries (CLI)

-
- Step 1** Specify the maximum number of entries that can be added to the local database the next time the controller reboots by entering this command:
config database size *max_entries*
- Step 2** Save your changes by entering this command:
save config
- Step 3** View the maximum number of database entries and the current database contents by entering this command:
show database summary
-