

AAA Administration

- Setting up RADIUS for Management Users, on page 1
- Setting up TACACS+, on page 40
- Maximum Local Database Entries, on page 48

Setting up RADIUS for Management Users

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 controller 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 32 RADIUS authentication and accounting servers.
- 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 Cisco 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.

Note **Functionality change introduced in Release 8.5.140.0**:

When RADIUS aggressive failover for controller is disabled: Packet is retried for six times unless there is a termination from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after three timeout events (18 consecutive retries) from multiple clients (previously, from exactly three clients).

When RADIUS aggressive failover for controller is enabled: Packet is retried for six times unless there is a termination from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after one timeout event (6 consecutive retries) from multiple clients (previously, from exactly one client).

It means 18 consecutive retries per RADIUS server (both AUTH and ACCT) can be from multiple clients. Therefore, it is not always guaranteed that each packet will be retried for six times.

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.

This section contains the following subsections:

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.
- A network address translation (NAT) scenario when IPSec is enabled on traffic between the controller and RADIUS server is not supported.

Configuring RADIUS Authentication (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Authentication**.

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 2 From the **Auth Called Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message for network users. 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 3 From the **MAC Delimiter** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message for network users. The following options are available:

- Colon
- Hyphen
- Single-hyphen
- None

Step 4 Click **Apply**. Perform one of the following:

- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Authentication Servers > Edit** page appears.
- To add a RADIUS server, click **New**. The **RADIUS Authentication Servers > New** page appears.

Step 5 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 6 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 7 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 8 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 9 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 10 (Optional) Check the **Apply Cisco ISE Default settings** check box.

Enabling Cisco ISE Default settings changes the following parameters:

- CoA is enabled by default.
- The Authentication server details (IP and shared-secret) are also applied to the Accounting server.
- The Layer 2 security of the WLAN is set to WPA+WPA2
- 802.1X is the default AKM.
- MAC filtering is enabled if the Layer 2 security is set to None.

The Layer 2 security is either WPA+WPA2 with 802.1X or None with MAC filtering. You can change these default settings if required.

Step 11 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.

Step 12 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 13 If you are configuring a new RADIUS authentication server, from the **Support for CoA** 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 CoA 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 14 In the **Server Timeout** 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 15 Check the **Network User** check box to enable network user authentication, or uncheck it to disable this feature. The default value is unchecked. 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.

Step 16 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 17 Enter the **Management Retransmit Timeout** value, which denotes the network login retransmission timeout for the server.

Step 18 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 19 Check the **PAC Provisioning** check box to enable PAC for RADIUS authentication, or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, the entry is considered by the RADIUS authentication server to provision PAC for users.

Note
You must not enable PAC Provisioning for RADIUS authentication server, if the **Tunnel Proxy** check box is enabled for an AAA server.

Step 20 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
From Release 8.3 onwards, IPSec is supported over IPv6 interfaces as well.

Step 21 If you enabled IPsec, 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 22 Click **Apply**.

Step 23 Click **Save Configuration**.

Step 24 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Configuring RADIUS Accounting Servers (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Accounting**.

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 2 From the **Acct Called 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 3 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 4 Click **Apply**. Perform one of the following:

- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Accounting Servers > Edit** page is displayed.
- To add a RADIUS server, click **New**. The **RADIUS Accounting Servers > New** page is displayed.

Step 5 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 6 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 7 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 8 In the **Shared Secret** and **Confirm Shared Secret** text boxes, enter the shared secret key to be used for accounting between the controller and the server.

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

Step 9 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 1813 for accounting.

Step 10 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 11 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.

Step 12 Check the **Network User** check box to enable network user accounting, or uncheck it to disable this feature. The default value is unchecked. 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.

Step 13 Check the **Management** check box to enable management accounting, 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 accounting server for management users, and accounting requests go to the RADIUS server.

Step 14 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 15 Check the **PAC Provisioning** check box to enable PAC for RADIUS accounting, or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, the entry is considered by the RADIUS accounting server to provision PAC for users.

Note
You must not enable PAC Provisioning for RADIUS accounting server, if the **Tunnel Proxy** check box is enabled for an AAA server.

Step 16 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
From Release 8.3 onwards, IPSec is supported over IPv6 interfaces as well.

Step 17 If you enabled IPsec, choose the **IPSec Profile Name** from the drop-down list.

a) From the IPSec drop-down list, choose one of the following options as the accounting 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.

Step 18 Click **Apply**.

Step 19 Click **Save Configuration**.

Step 20 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Configuring RADIUS (CLI)

Procedure

- 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-mac-ssid-ap-group** | **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 Called 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 be used for IPSEC sessions.
- **config radius auth ipsec ike auth-mode pre-shared-key** *index hex/asciisecret*—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** {**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 Called 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-mac-ssid-ap-group**—Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>.
- **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 ignores all inactive servers for all active RADIUS requests. If probing is enabled, the RADIUS server will be probed at every probing time interval irrespective of the probe response having been received or not. For more information, see CSCvc01761.Active management RADIUS servers are probed only if management-kick-out feature is enabled.

Note RADIUS server is probed if you enable probing at every probing time interval irrespective of the probe response. For more information, see CSCvc01761.

- 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).

Note While configuring more than seven servers, you must increase the fallback-test interval to 1000 for a default retransmit timeout of 5 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 controller platforms:

  - Cisco 5520 and 8540 controllers 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
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

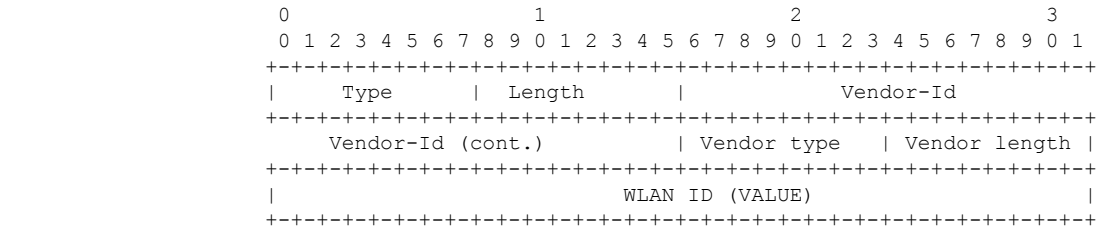
Attribute ID	Description
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name **Note** Guest-Role-Name is honored only on L3 security web authentication with AAA over-ride enabled on the controller.
13	Data-Bandwidth-Average-Contract-US
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 controller.

VAP ID

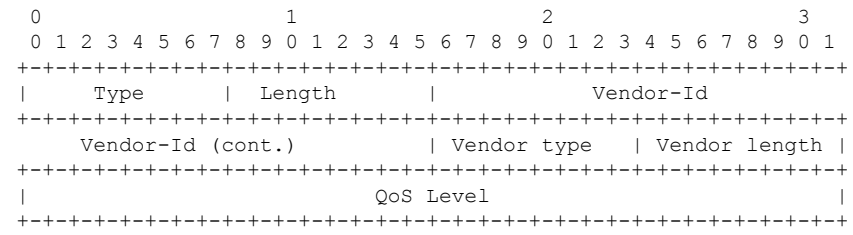
This attribute indicates the WLAN ID of the WLAN to which the client should belong. When the WLAN-ID attribute is present in the RADIUS Access Accept, the system applies the WLAN-ID (SSID) to the client station after it authenticates. The WLAN ID is sent by the controller in all instances of authentication except IPsec. In case of web authentication, if the controller 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.



- 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

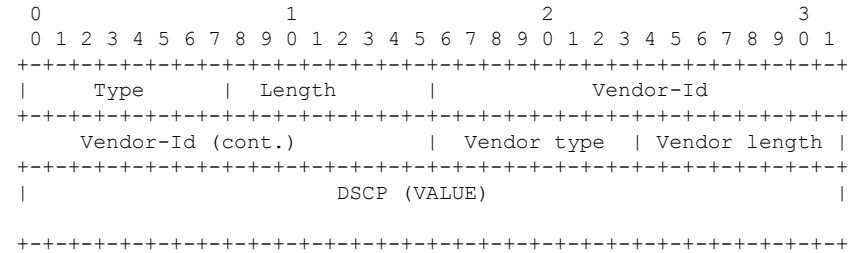
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The fields are transmitted from left to right.



- 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.

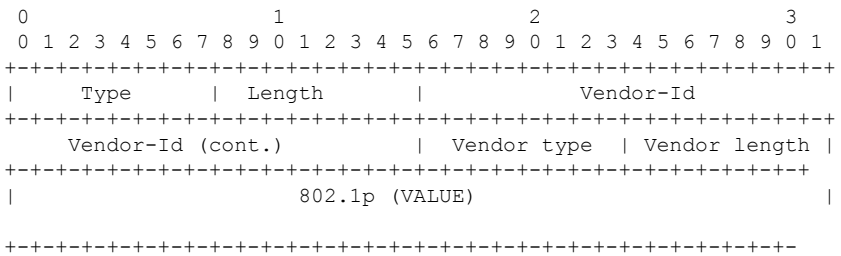


- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179

- Vendor type – 3
- Vendor length – 4
- Value – DSCP value to be applied for the client.

802.1p Tag Type

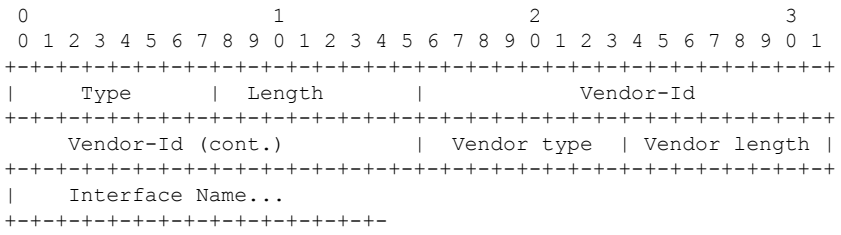
802.1p VLAN tag received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. This attribute defines the 802.1p priority to be applied to the client. When present in a RADIUS Access Accept, the 802.1p value overrides the default specified in the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



- 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.



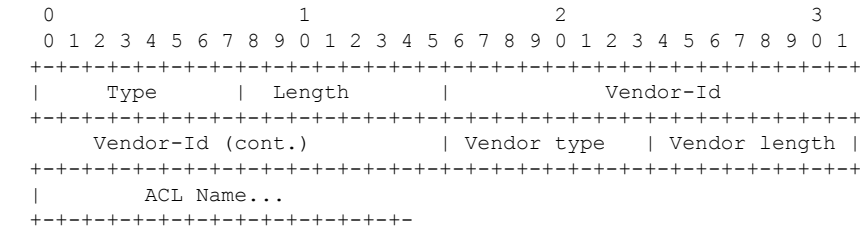
- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5

- 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.



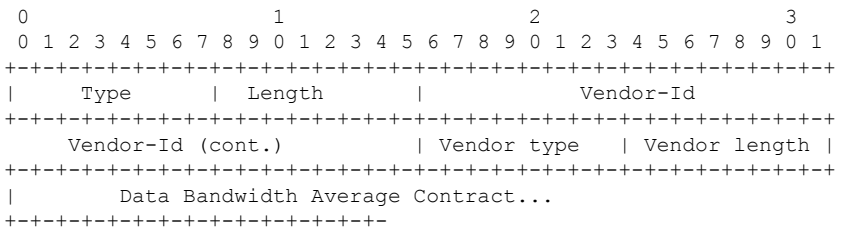
- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled. The client will be de-authenticated if the ACL is not preconfigured on the controller. The actual named AAA attribute for an IPv6 ACL is ***Airespace-IPv6-ACL-Name***, which is similar to the *Airespace-ACL-Name* attribute that is used for provisioning an IPv4-based ACL. The AAA attribute returned contents should be a string equal to the name of the IPv6 ACL as configured on the controller.

Data Bandwidth Average Contract

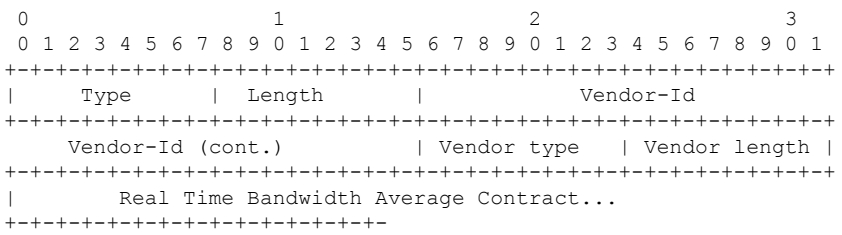
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied for a client for non-realtime traffic such as TCP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Average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



- 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

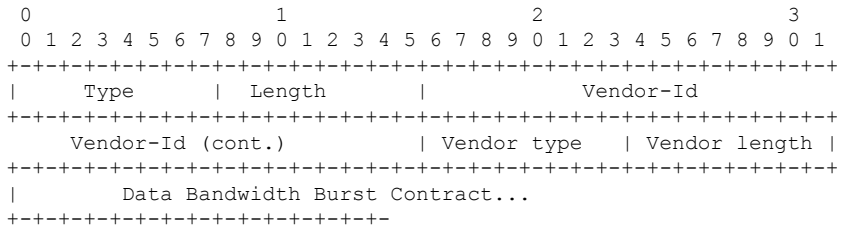
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Real Time Bandwidth Average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



- 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.

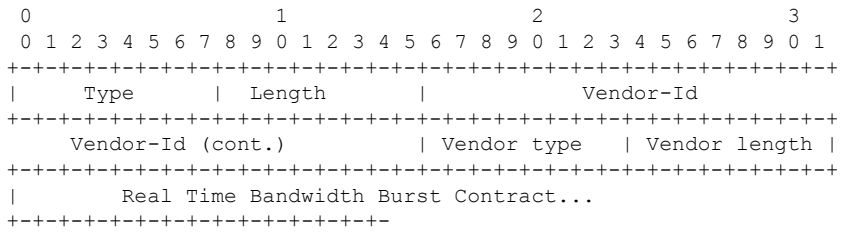


- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 9
- Vendor length – 4
- Value – A value in kbps

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.

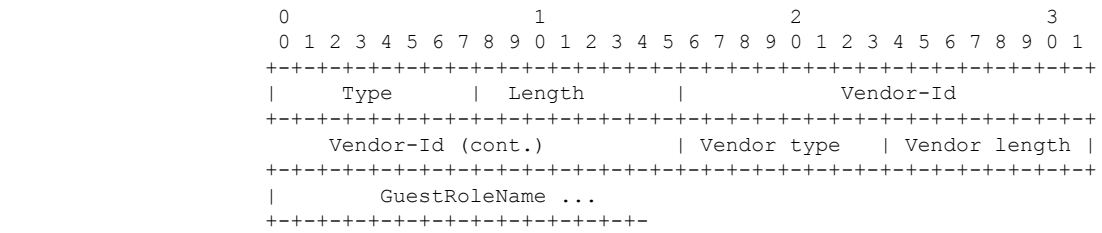
Note If you try to implement Average Data Rate and Burst Data Rate as AAA override parameters to be pushed from a AAA server, both Average Data Rate and Burst Data Rate have to be sent from ISE.



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

Guest Role Name

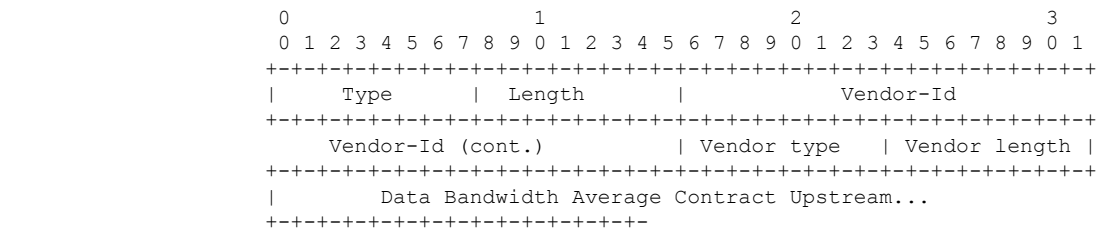
This attribute provides the bandwidth contract values to be applied for an authenticating user. When present in a RADIUS Access Accept, the bandwidth contract values defined for the Guest Role overrides the bandwidth contract values (based on QOS value) specified for the WLAN. The fields are transmitted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



- 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

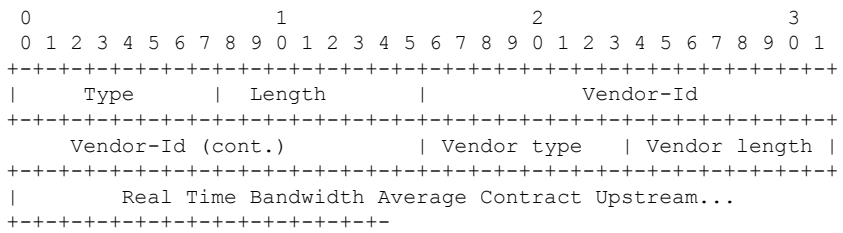
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Data Bandwidth Average Contract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



- 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

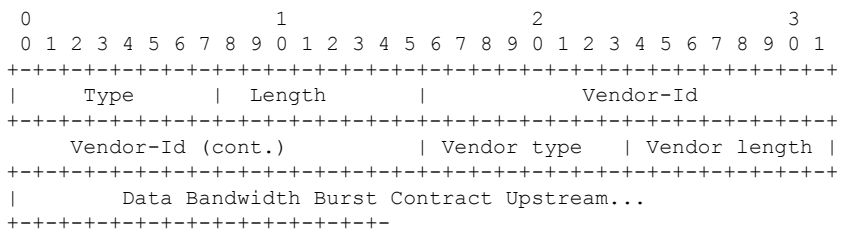
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Real Time Bandwidth Average Contract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



- 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.



- 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)

Attribute ID	Description
43	Accounting-Output-Octets (Stop and interim messages only)
44	Accounting-Session-ID
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. Interim updates can also be triggered by events such as mobility events, every time clients receive IPv4 addresses, PEM state changes, and so on.
7	Accounting-On
8	Accounting-Off
9-14	Reserved for Tunneling Accounting
15	Reserved for Failed

RADIUS VSA

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using vendor specific attributes (VSA). VSA allow vendors to support their own extended attributes otherwise not suitable for general use. VSA are predefined in an XML file. You need to add the vendor specific attributes to the XML file and this XML file is downloaded to the controller. There is no configuration required on the controller to enable the support. The file contains the RADIUS attributes in a specific format as explained by the XML schema to specify the XML tags.

The XML file with the vendor specific attributes defined can be downloaded from a FTP server. The downloaded file is stored in the flash memory and retained across several reboot processes. The file is parsed upon successful download and each time when the controller boots up. The XML file can be uploaded to RADIUS server for authentication and accounting. Once controller parses these values, it stores the file in a separate data structures meant for vendor specific attributes storage. The controller uses these attributes value in authentication or accounting packets, or both based on specified usage format. If there are any errors in the file, the controller parsing fails, and the attributes are not applied. You should address the errors in the file or download the file from the FTP server again to the controller.

This section contains the following subsections:

Sample RADIUS AVP List XML File

You can use the sample RADIUS AVP list XML file for reference. The sample XML file contains only two attributes, one for authentication and the other for accounting. You can add more number of RADIUS attributes and value pairs but those attributes and value pairs should be appended in the format specified.



Note The maximum number of WLANs that is supported in an AVP download is 32.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file edited by User1-->

<radiusFile>
<avpList SSID_PROF="test" incAuth="true" incAcct="false">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
<avpList SSID_PROF="test" incAcct="true">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
```

```
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
</radiusFile>
```

Downloading RADIUS AVP List (GUI)

Procedure

Step 1 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 2 From the File Type drop-down list, choose **RADIUS AVP List**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the IP Address text box, enter the IPv4 or IPv6 address of the server.

Step 5 In the File Path text box, enter the directory path of the RADIUS AVP list.

Step 6 In the File Name text box, enter the name of the RADIUS AVP list.

Step 7 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.

b) In the Server Login Password text box, enter the password to log into the FTP server.

c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Download** to download the RADIUS AVP list to the controller. A message appears indicating the status of the download.

Step 9 Choose **Security** > **AAA** > **RADIUS** > **Downloaded AVP** to open the Download RADIUS AVP List page.

Step 10 From the WLAN SSID Profile name drop-down list, choose the WLAN SSID profile name.

Step 11 Click the **Auth AVP** tab to view the RADIUS authentication attributes mapped to the AVP list.

Step 12 Click the **Acct AVP** tab to view the RADIUS accounting attributes mapped to the AVP list.

Uploading RADIUS AVP List (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **RADIUS AVP List**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the IP Address text box, enter the IPv4 or IPv6 address of the server.

Step 5 In the File Path text box, enter the directory path of the RADIUS AVP list.

Step 6 In the File Name text box, enter the name of the RADIUS AVP list.

Step 7 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the RADIUS AVP list from the controller. A message appears indicating the status of the upload.

Uploading and Downloading RADIUS AVP List (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Download the RADIUS AVPs in the XML file format from the FTP server to the controller by entering this command:

transfer download datatype radius-avplist

Step 3 Upload the XML file from the controller to the RADIUS server using the command:

transfer upload datatype radius-avplist

Step 4 Display VSA AVPs using the command:

show radius avp-list *ssid-profile-name*

Per-WLAN RADIUS Source Support

The controller sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the controller Dynamic interfaces. If a RADIUS server is reachable via a controller Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the controller will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the controller to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

To filter WLANs, use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

This section contains the following subsections:

Prerequisites for Per-WLAN RADIUS Source Support

- You must implement appropriate rule filtering on the new identity for the authentication server (RADIUS) because the controller sources traffic only from the selected interface.

Configuring Per-WLAN RADIUS Source Support (GUI)

Before you begin

Ensure that the WLAN is in disabled state. You can enable the WLAN after the configuration is done.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID.

Step 3 Click the **Security** tab, and then click the **AAA Servers** tab.

Step 4 Check the **RADIUS Server Overwrite interface** check box to enable the per-WLAN RADIUS source support.

Note
When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

Step 5 From the **Interface Priority** drop-down list, select either **AP Group** or **WLAN** as the interface for RADIUS packet routing.

Step 6 Ensure that the **Interim Interval** for RADIUS Server Accounting is within the valid range.

Step 7 Save the configuration.

Configuring Per-WLAN RADIUS Source Support (CLI)

Procedure

Step 1 Enter the **config wlan disable** *wlan-id* command to disable the WLAN.

Step 2 Enter the following command to enable or disable the per-WLAN RADIUS source support:

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan-id*

Note
When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

Step 3 Enable either an AP group's interface or a WLAN's interface for RADIUS packet routing by entering these commands:

- AP group's interface—**config wlan radius_server overwrite-interface apgroup** *wlan-id*
- WLAN's interface—**config wlan radius_server overwrite-interface wlan** *wlan-id*

Note
Valid WLAN ID range is between 1 and 16.

Step 4 Enter the **config wlan enable** *wlan-id* command to enable the WLAN.

Note
You can filter requests on the RADIUS server side using CiscoSecure ACS. You can filter (accept or reject) a request depending on the NAS-IP-Address attribute through a Network Access Restrictions rule. The filtering to be used is the CLI/DNIS filtering.

Monitoring the Status of Per-WLAN RADIUS Source Support (CLI)

To see if the feature is enabled or disabled, enter the following command:

show wlan *wlan-id*

Example

The following example shows that the per-WLAN RADIUS source support is enabled on WLAN 1.

show wlan *1*

Information similar to the following is displayed:

```
WLAN Identifier.................................. 4
Profile Name..................................... example
Network Name (SSID).............................. example
Status........................................... Enabled
MAC Filtering.................................... Disabled
```

```
Broadcast SSID.................................. Enabled
AAA Policy Override............................. Disabled
Network Admission Control
...
Radius Servers
   Authentication............................... Global Servers
   Accounting................................... Global Servers
   Overwrite Sending Interface.................. Enabled
Local EAP Authentication........................ Disabled
```

RADIUS Realm

When mobile clients associate to a WLAN, RADIUS realm is received as a part of EAP-AKA identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org*. The realm in the NAI format is represented after the @ symbol, which is specified as *wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org*. If vendor specific attributes are added for MCC as 311 and MNC as 480 to 489, then the NAI format can be represented as: *0311480999999999@wlan.mnc480.mcc311.3gppnetwork.org*.

For a mobile subscriber, the controller sends the authentication request to the AAA server only when the realm in the NAI format received from the device complies as per the given standards. Apart from authentication, accounting requests are also required to be sent to AAA server based on realm filtering.

In order to support realm filtering on the controller, you need to configure realm on the RADIUS. When a user is connected with a particular SSID, the user is authenticated and authorized using the NAI format received against the realm configured on the RADIUS server.

Realm Support on a WLAN

Each WLAN is configured to support NAI realms. Once the realm is enabled on a particular SSID, the lookup is done to match the realms received in the EAP identity response against the configured realms on the RADIUS server.

Realm Support on RADIUS Server

The RADIUS server needs to redirect the authentication and accounting requests based on configured realms. Each RADIUS server support realms to a maximum of 30 each for authentication and accounting.

- **Realm Match for Authentication**—In WPA2 dot1x with EAP methods (similar to EAP AKA), the username is received as part of EAP identity response. The realm is derived from the username and match with the realms configured in the RADIUS authentication server. If there is a match, then the authentication requests are forwarded to the RADIUS server. If there is a mismatch, then the client is deauthenticated.
- **Realm Match for Accounting**—Username is received in access accept messages. When accounting messages are triggered, the realm is derived from the username and compared against the accounting realms configured on the RADIUS accounting server. If succeeded, accounting requests are forwarded to the RADIUS server. If there is a mismatch, the accounting requests are dropped. For example, if realm is configured as **cisco** on the controller, then the username is authenticated as **xyz@cisco** on the RADIUS server.



Note Even if the NAI realm is enabled on a WLAN and if there is no realm in the username, then the behavior is defaulted to no lookup, and the usual selection of the RADIUS server is followed.

Note When the client uses fast re-authentication identity, the realm name is required from the authentication server in order for the controller to forward corresponding requests to the correct server.

When EAP-AKA is used along with realm, fast reauthentication is supported when EAP server responds with AT_NEXT_REAUTH_ID attribute that has both the username portion and realm portion. Purpose of the realm is received controller picks up the right server for the subsequent fast reauthentication requests. For example, host APD server which supports EAP-AKA does not support realm portion. Therefore, the controller supports fast reauthentication only with those EAP servers which have this compatibility.

This section contains the following subsections:

Prerequisites for Configuring RADIUS Realm

RADIUS authentication or accounting server has to be disabled before adding realm and enabled after adding realm on the controller.

Restrictions for Configuring RADIUS Realm

- You can configure a maximum of 17 RADIUS authentication and accounting servers to one controller.
- The total number of realms that you can configure for one RADIUS authentication and accounting server is 30.

Configuring Realm on a WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.
Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.
Step 4 Select the **RADIUS NAI-Realm** check box to enable realm on the WLAN.
Step 5 Click **Apply** to commit your changes.
Step 6 Click **Save Configuration** to save your changes.

Configuring Realm on a WLAN (CLI)

Procedure

Step 1 Enable or disable realm on a WLAN by entering this command:
config wlan *radius_server* **realm** {**enable** | **disable**} *wlan-id*
Step 2 View the realm configuration on a WLAN by entering this command:
show wlan *wlan-id*

Configuring Realm on a RADIUS Authentication Server (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Authentication** to open RADIUS Authentication Servers > Edit page.

Step 2 Click the Realm List link to open the Authentication Server Index page.

Step 3 Enter the realm name in the Realm Name text box.

Step 4 Click **Add**.

Configuring Realm on a RADIUS Authentication Server (CLI)

Procedure

Step 1 Add realm to a RADIUS authentication server by entering this command:
config radius auth realm add *radius_index realm_string*

Step 2 Delete realm from a RADIUS authentication server by entering this command:
config radius auth realm delete *radius_index realm_string*

Step 3 View RADIUS authentication server information by entering this command:
show radius auth detailed *radius_index*

Configuring Realm on a RADIUS Accounting Server (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Accounting** to open RADIUS Accounting Servers > Edit page.

Step 2 Click the Realm List link to open the Accounting Server Index page.

Step 3 Enter the realm name in the Realm Name text box.

Step 4 Click **Add**.

Configuring Realm on a RADIUS Accounting Server (CLI)

Procedure

Step 1 Add realm to a RADIUS accounting server by entering this command:
config radius acct realm add *radius_index realm_string*

Step 2 Delete realm from a RADIUS accounting server by entering this command:

config radius acct realm delete *radius_index realm_string*

Step 3 View RADIUS accounting server information by entering this command:

show radius acct detailed *radius_index*

Disabling Accounting Servers per WLAN (GUI)



Note Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page.

Step 4 Unselect the **Enabled** check box for the Accounting Servers.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

User Login Policies

User Login Policies control the maximum number of concurrent netuser logins under one netuser name. The user name is case sensitive (CSCuu42548). Setting this to 0 means that there is no limit, and 8 is the maximum.

User Login Policies also control the logins under Layer 3 authentications and EAP. For EAP logins, the behavior of the maximum number of user logins is affected by the setting of the **Max-Login Ignore Identity Response** option. If you enable this, then the EAP identity response user name values are ignored for the purposes of enforcing a user name login limit.

Configuring User Login Policies (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **User Login Policies**.

Step 2 In the **User Policies** window, enter the maximum number of login sessions for a single user.

The valid range is 0 to 8. The default value is 0. If you set this to 0, unlimited login sessions are permitted for a single user.

Step 3 Save the configuration.

Configuring User Login Policies (CLI)

Procedure

Step 1 Configure the maximum number of login sessions for a single user by entering this command:

config netuser maxUserLogin *count*

The valid range is 0 to 8. The default value is 0. If you set *count* to 0, unlimited login sessions are permitted for a single user.

Step 2 Save the configuration by entering this command:

save config

AAA Override (Identity Networking)

In most wireless LAN systems, each WLAN has a static policy that applies to all clients associated with an SSID. Although powerful, this method has limitations because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco Wireless LAN solution supports identity networking, which allows the network to advertise a single SSID but allows specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking are as follows:

- ACL—When the ACL attribute is present in the RADIUS Access Accept, the system applies the ACL name to the client station after it authenticates, which overrides any ACLs that are assigned to the interface.
- VLAN—When a VLAN Interface-name or VLAN tag is present in a RADIUS Access Accept, the system places the client on a specific interface.

Note The VLAN feature only supports MAC filtering, 802.1X, and WPA. The VLAN feature does not support web authentication or IPsec.

- Tunnel Attributes.

Note When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag), which are described later in this section, are returned, the Tunnel Attributes must also be returned.

The operating system's local MAC filter database has been extended to include the interface name, allowing local MAC filters to specify to which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

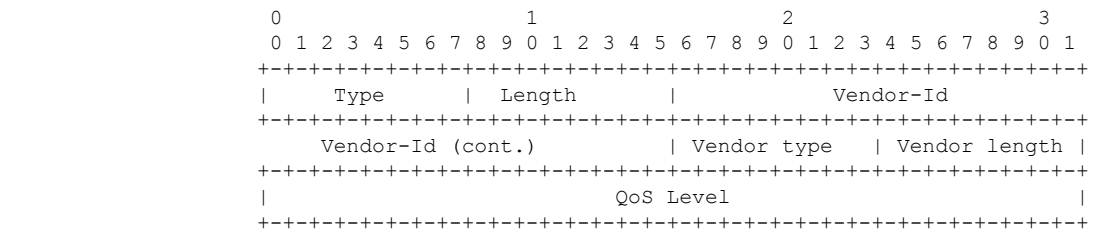
This section contains the following subsection:

RADIUS Attributes Used in Identity Networking

QoS-Level

This section explains the RADIUS attributes used in identity networking.

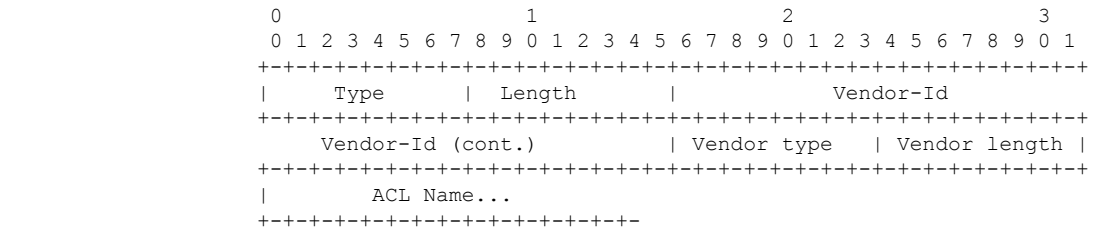
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The text boxes are transmitted from left to right.



- 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)

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 text boxes are transmitted from left to right.

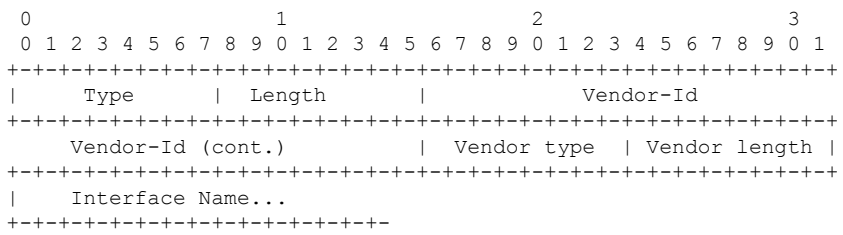


- Type – 26 for Vendor-Specific

- 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

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 text boxes are transmitted from left to right.



- 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.

VLAN Tag

This attribute indicates the group ID for a particular tunneled session and is also known as the Tunnel-Private-Group-ID attribute.

This attribute might be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The text boxes 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     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 81 for Tunnel-Private-Group-ID.
- Length – >= 3
- Tag – The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag text box is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag text box is greater than 0x1F, it should be interpreted as the first byte of the following String text box.
- String – This text box must be present. The group is represented by the String text box. There is no restriction on the format of group IDs.



Note When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag) are returned, the Tunnel Attributes must also be returned.

Tunnel Attributes

RFC 2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC2867 defines tunnel attributes used for accounting. Where the IEEE 802.1X authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular VLAN, defined in IEEE 8021Q, based on the result of the authentication. This configuration can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the AccessRequest.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

The VLAN ID is 12 bits, with a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type String as defined in RFC 2868, for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag text box. As noted in RFC 2868, section 3.1:

- The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet that refer to the same tunnel. Valid values for this text box are 0x01 through 0x1F, inclusive. If the Tag text box is unused, it must be zero (0x00).

- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag text box of greater than 0x1F is interpreted as the first octet of the following text box.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag text box should be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F should be chosen.

Configuring Network Access Identifier (CLI)

You can configure a network access server identifier (NAS-ID) on each WLAN profile, VLAN interface, or AP group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.

If you configure a NAS-ID for an AP group, this NAS-ID overrides the NAS-ID that is configured for a WLAN profile or the VLAN interface. If you configure a NAS-ID for a WLAN profile, this NAS-ID overrides the NAS-ID that is configured for the VLAN interface.

- Configure a NAS-ID for a WLAN profile by entering this command:

  config wlan nasid {*nas-id-string* | **none**} *wlan-id*

- Configure a NAS-ID for a VLAN interface by entering this command:

  config interface nasid {*nas-id-string* | **none**} *interface-name*

- Configure a NAS-ID for an AP group by entering this command:

  config wlan apgroup nasid {*nas-id-string* | **none**} *apgroup-name*

When the controller communicates with the RADIUS server, the NAS-ID attribute is replaced with the configured NAS-ID in an AP group, a WLAN, or a VLAN interface.

The NAS-ID that is configured on the controller for an AP group, a WLAN, or a VLAN interface is used for authentication. The configuration of NAS-ID is not propagated across controllers.

Note If WLAN interface is overridden at AP group then overridden interface NAS ID will be used. Since Interface NASID is given priority over WLAN NAS ID.

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.

Note Both MANAGEMENT and SECURITY roles are needed for creating local management user and IPsec profile.

Note In Release 8.5.135.0, the creation of Authorization server is deprecated. To create an Authorization server, you must create an Authentication server and duplicate it as an Authorization server. Due to this change in functionality, an alarm is generated in Cisco Prime Infrastructure 3.2 as follows:

```
1.Successfully created Authentication server. 2.Failed
to create authorization server:SNMP operation to Device
failed: Set Operation not allowed for TACACS
authorization server.1.Successfully created Accounting
server.
```

The workaround on Cisco PI is to uncheck the Authorization server on the Prime template.

For more information about this change in functionality, see CSCvm01415.

- 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.
- To configure the TACACS+ server, using Cisco 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.

Dynamic Management User Login via AAA Server

The management users, who logged in using local credentials when external AAA servers were not available, are notified to re-authenticate within the set timeframe when external TACACS+ servers are available. Failing to authenticate terminates the user session. TACACS+ uses the TACACS+ fallback-test configuration and the re-authentication configuration is common to RADIUS and TACACS+. This enhancement was introduced in 8.2 release.

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)

Procedure

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 controller. 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 Configure the TACACS+ probe duration mode as follows:

a) Choose **Security** > **AAA** > **TACACS+** > **Fallback**. The **TACACS+ Fallback Parameters** page appears.
b) From the **Fallback Mode** drop-down list, select **Enable**.
c) In the **Interval in sec** text box, enter the time in seconds. The valid range is between 180 and 3600 seconds.
d) Click **Apply**.

Step 14 Configure the re-authentication terminal interval for a user before being logged out as follows:

a) Choose **Security** > **AAA** > **General**. The **AAA General** page appears.

b) In the **Mgmt User Re-auth Interval** text box, enter the time in seconds. The valid range is between 0 and 300.
c) Click **Apply**.

Step 15 Click **Save Configuration**.

Step 16 Repeat the previous steps if you want to configure any additional services on the same server or any additional TACACS+ servers.

Step 17 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 18 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 19 Click **Apply**.

Step 20 Click **Save Configuration**.

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.

    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.

- Configure TACACS+ probe and re-authentication interval by entering these commands:

- **config tacacs fallback-test interval** *seconds*—Enables and sets the probe interval for TACACS+ server. The valid range is `0` to disable and between `180` and `3600` seconds when enabled.
- **config mgmtuser termination-interval** *seconds*—Sets the interval of re-authentication window for the user before being logged out of the system. The valid range is between `0` and `300`. Default value is 0.

- View the user authentication server configuration by entering the following commands:
  - **show aaa auth** —Displays AAA related information for authentication servers.
  - **show tacacs summary** —Displays TACACS+ summary
- Enable or disable TACACS+ debugging by entering this command:

  debug aaa tacacs {**enable** | **disable**}
- Save your changes by entering this command:

  save config

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.

The maximum entries that are supported by each platform are listed in the following table.

Table 8: Maximum Supported Local Database Entries

Platform	Maximum Entries Supported
Cisco 3504 Wireless Controller	12000
Cisco 5520 Wireless Controller	12000
Cisco 8540 Wireless Controller	12000
Cisco Virtual Wireless Controller	2048

Note If you modify the maximum local database entry parameter, you must reboot the controller for the changes to take effect.

This section contains the following subsections:

Related Topics

Restrictions on Managing User Accounts

Configuring Maximum Local Database Entries (GUI)

Procedure

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)

Procedure

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