Configuring RADIUS

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 17 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 Access Control Server (ACS): See the latest Cisco Secure Access Control System guide at https://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html.
  - Using Identity Services Engine (ISE): See the Configuring External RADIUS Servers section in the Cisco Identity Services Engine Administrator Guide at https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html.

Primary and Fallback RADIUS Servers

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

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.

This section contains the following subsections:

Configuring RADIUS (GUI)

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

Step 2 Perform one of the following:

- If you want to configure a RADIUS server for authentication, choose **Authentication**.
- If you want to configure a RADIUS server for accounting, choose **Accounting**.

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

The RADIUS Authentication (or Accounting) Servers page appears.

This page lists any RADIUS servers that have already been configured.

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

Step 3 From the **Call Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:

- IP Address
- System MAC Address

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

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

Step 4 Enable RADIUS-to-controller key transport using AES key wrap protection by checking the **Use AES Key Wrap** check box. The default value is unchecked. This feature is required for FIPS customers.

Step 5 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 6 Click **Apply**. Perform one of the following:

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

Step 7 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 8 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 9 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 10 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 11 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 12 If you are adding a new server, enter the RADIUS server's UDP port number for the interface protocols in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 13 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 14 If you are configuring a new RADIUS authentication server, from the **Support for RFC 3576** drop-down list, choose **Enabled** to enable change of authorization, which is an extension to the RADIUS protocol that allows dynamic changes to a user session, or choose **Disabled** to disable this feature. By default, this is set to Disabled state. Support for RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change of authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.

Step 15 In the **Server Timeout** text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Check the **Key Wrap** check box.

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

Step 16 Check the **Network User** check box to enable network user authentication (or accounting), or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, this entry is considered the RADIUS authentication (or accounting) server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.

Step 17 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 18 Enter the **Management Retransmit Timeout** value, which denotes the network login retransmission timeout for the server.

Step 19 Check the **IPSec** check box to enable the IP security mechanism, or uncheck the check box to disable this feature. The default value is unchecked.

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

Step 20 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 21 Click **Apply**.

Step 22 Click **Save Configuration**.

Step 23 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Step 24 Specify the RADIUS server fallback behavior, as follows:

a) Choose **Security** > **AAA** > **RADIUS > Fallback to open the RADIUS > Fallback Parameters** to open the fallback parameters page.

b) From the **Fallback Mode** drop-down list, choose one of the following options:

- **Off**—Disables RADIUS server fallback. This is the default value.
- **Passive**—Causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
- **Active**—Causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

c) If you enabled Active fallback mode in *Step b*, enter the name to be sent in the inactive server probes in the **Username** text box. You can enter up to 16 alphanumeric characters. The default value is “cisco-probe.”

d) If you enabled Active fallback mode in *Step b*, enter the probe interval value (in seconds) in the Interval in **Sec** text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 25 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 26 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 27 Click **Apply**.

Step 28 Click **Save Configuration**.

Related Topics

Configuring TACACS+ (GUI)

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-group-name** | **ap-location** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **vlan-id**}

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.
  - **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** {**3des** | **aes** | **des** | **none**} *index*—Configures the IP security encryption mechanism.
  - **config radius auth ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *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.
- **config radius acct server-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS accounting server.
- **config radius acct network** *index* **{enable** | **disable**}—Enables or disables network user accounting. If you enable this feature, this entry is considered the RADIUS accounting server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
- **config radius acct ipsec** {**enable** | **disable**} *index*—Enables or disables the IP security mechanism.
- **config radius acct ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.
- **config radius acct ipsec encryption** { **3des** | **aes** | **des** | **none**} *index*—Configures the IP security encryption mechanism.
- **config radius acct ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *index*—Configures the IKE Diffie Hellman group.
- **config radius acct ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
- **config radius acct ipsec ike phase1** {**aggressive** | **main**} *index*—Configures the Internet Key Exchange (IKE) protocol.
- **config radius acct** {**enable** | **disable**} index—Enables or disables a RADIUS accounting server.
- **config radius acct delete index**—Deletes a previously added RADIUS accounting server.
- **config radius auth callStationIdType ap-group-name** —Sets the Called Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
- **config radius auth callStationIdType ap-location**—Sets the Called Station ID to the AP Location.

- **config radius auth callStationIdType** {**ap-macaddr-only** | **ap-macaddr-ssid**}—Sets the Called Station ID type to be AP's radio MAC address or AP's radio MAC address with SSID in the <AP radio MAC address>:<SSID> format.
- **config radius auth callStationIdType** {**ap-name** | **ap-name-ssid**}—Sets the Called Station ID type to be AP name or AP name with SSID in the <AP name>:<SSID> format.
- **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. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

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).

- 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*

Related Topics

Configuring TACACS+ (CLI)

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

Attribute ID	Description
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

Attribute ID	Description
81	Tunnel-Group-ID

Note Message authentication is not supported.

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

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

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

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

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

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

QoS-Level

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

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

- Type – 26 for Vendor-Specific

- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
  - 3 – Bronze (Background)
  - 0 – Silver (Best Effort)
  - 1 – Gold (Video)
  - 2 – Platinum (Voice)

Differentiated Services Code Point (DSCP)

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

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

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

802.1p Tag Type

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       802.1p (VALUE)                            |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 4
- Vendor length – 3
- Value – 802.1p priority to be applied to a client.

VLAN Interface Name

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

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

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

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

ACL-Name

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

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

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

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 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.

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

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 7

- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Average Contract

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

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

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

Data Bandwidth Burst Contract

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

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

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 9

- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Burst Contract

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

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

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

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

Guest Role Name

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

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

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

- Vendor-Id – 14179
- Vendor type – 11
- Vendor length – Variable based on the Guest Role Name length
- Value – A string of alphanumeric characters

RADIUS Accounting Attributes

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

Table 6: Accounting Attributes for Accounting Requests

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

Attribute ID	Description
65	Tunnel-Medium-Type
81	Tunnel-Group-ID

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