Troubleshooting AAA RADIUS Interactions for WLAN Authentication

- Test AAA RADIUS interactions for WLAN authentication by entering this command:
  
  ```
  test aaa radius username username password password wlan-id wlan-id [apgroup apgroupname server-index server-index]
  ```

  The command parameters include the following:
  - username and password (both in plain text)
  - WLAN ID
  - AP group name (optional)
  - AAA server index (optional)

  This test command sends to the RADIUS server an access request for client authentication. Access request exchange takes place between Cisco WLC and AAA server, and the registered RADIUS callback handles the response.

  The response includes authentication status, number of retries, and RADIUS attributes.

- View the RADIUS response to test RADIUS request by entering this command:

  ```
  test aaa show radius
  ```

Guidelines

- Both username and password must be plain text, similar to MAC authentication
- If AP group is entered, the WLAN entered must belong to that AP group
- If server index is entered, the request to test RADIUS is sent only to that RADIUS server
• If the RADIUS request does not get a response, the request is not sent to any other RADIUS server

• RADIUS server at the server index must be in enabled state

• This test command can be used to verify configuration and communication related to AAA RADIUS server and should not be used for actual user authentication

• It is assumed that the AAA server credentials are set up as required

Restrictions
• No GUI support
• No TACACS+ support

Example: Access Accepted

(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request

Wlan-id........................................ 7
ApGroup Name................................... default-group

Attributes Values
---------- -----
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x00000000d (13)
Nas-Ip-Address 172.20.227.39
NAS-Identifier WLC5520
Airspace / WLAN-Identifier 0x000000007 (7)
User-Password Cisco123
Service-Type 0x000000008 (8)
Framed-MTU 0x0000000013 (19)
Nas-Port-Type 0x00000013 (19)
Tunnel-Type 0x00000000d (13)
Tunnel-Medium-Type 0x000000006 (6)
Tunnel-Group-Id 0x000000051 (81)
Cisco / Audit-Session-Id ac14e327000000c456131b33
Acct-Session-Id 56131b33/00:11:22:33:44:55/210

test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) > test aaa show radius

Radius Test Request

Wlan-id........................................ 7
ApGroup Name................................... default-group

Server Index................................... 2

Radius Test Response

Radius Server Retry Status
---------- ----- -----
172.20.227.52 1 Success

Authentication Response:

Result Code: Success

Attributes Values
---------- -----
User-Name user1
Class CACS:rs-acs5-6-0-22/230677882/20313
Session-Timeout 0x0000001e (30)
Termination-Action 0x00000000 (0)
Tunnel-Type 0x0000000d (13)
Tunnel-Medium-Type 0x00000006 (6)
Tunnel-Group-Id 0x00000051 (81)

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 09:48:12.932: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the mobile: ac14e327000000c85613fb4c
*aaaQueueReader: Oct 06 09:48:12.932: User user1 password lengths don't match
*aaaQueueReader: Oct 06 09:48:12.932: ReProcessAuthentication previous proto 8, next proto 40000001
*aaaQueueReader: Oct 06 09:48:12.932: AuthenticationRequest: 0x2b6d5ab8
*aaaQueueReader: Oct 06 09:48:12.932: Callback...........................................0x101cd740
*aaaQueueReader: Oct 06 09:48:12.932: protocolType.................................0x40000001
*aaaQueueReader: Oct 06 09:48:12.932: proxyState............00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 09:48:12.932: Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 09:48:12.932: Putting the auth request in qid 5, srv=index 1


*radiusTransportThread: Oct 06 09:48:12.941: Access-Accept received from RADIUS server 172.20.227.52 for mobile 00:11:22:33:44:55 receiveId = 0
*radiusTransportThread: Oct 06 09:48:12.941: AuthorizationResponse: 0x146c56b8
*radiusTransportThread: Oct 06 09:48:12.941: structureSize................................263
*radiusTransportThread: Oct 06 09:48:12.941: resultCode...................................0
*radiusTransportThread: Oct 06 09:48:12.941: protocolUsed.................................0x00000001
*radiusTransportThread: Oct 06 09:48:12.941: proxyState............00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 09:48:12.941: Packet contains 7 AVPs:

Example: Access Failed

(Cisco Controller) > test aaa radius username user1 password C123 wlan-id 7 apgroup default-group server-index 2
Radius Test Request

Wlan-id........................................ 7
ApGroup Name................................... default-group
Attributes Values
---------- -----
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x0000000d (13)
Nas-Ip-Address 172.20.227.39
NAS-Identifier WLC5520
.
Tunnel-Type 0x0000000d (13)
Tunnel-Medium-Type 0x00000006 (6)
Tunnel-Group-Id 0x00000051 (81)
Cisco / Audit-Session-Id ac14e327000000c956140806
Acct-Session-Id 56140806/00:11:22:33:44:55/217

Test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) > test aaa show radius

Radius Test Request

Wlan-id........................................ 7
ApGroup Name................................... default-group
Server Index................................... 2
Radius Test Response
Radius Server Retry Status
---------- -----
172.20.227.52 1 Success

Authentication Response:
Result Code: Authentication failed
No AVPs in Response

(Cisco Controller) > debug aaa all enable

(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 10:42:30.638: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the
mobile: ac14e327000000c956140806
*aaaQueueReader: Oct 06 10:42:30.639: User user1 password lengths don't match
*aaaQueueReader: Oct 06 10:42:30.639: ReProcessAuthentication previous proto 8, next proto
40000001
*aaaQueueReader: Oct 06 10:42:30.639: AuthenticationRequest: 0x2b6bdc3c
*aaaQueueReader: Oct 06 10:42:30.639: Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 10:42:30.639: protocolType.................................0x40000001
*aaaQueueReader: Oct 06 10:42:30.639: Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 10:42:30.639: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 10:42:30.639: Request Authenticator
queue 5,
proxy state 00:11:22:33:44:55-00:00

*radiusTransportThread: Oct 06 10:42:30.639: 00:11:22:33:44:55 Access-Reject received from
RADIUS
server 172.20.227.52 for mobile 00:11:22:33:44:55 receiveId = 0
Authentication Failed' (-4) for mobile 00:11:22:33:44:55
*radiusTransportThread: Oct 06 10:42:30.647: structureSize.............................92
Example: Unresponsive AAA Server

(Cisco Controller) > test aaa radius username user1
password C123 wlan-id 7 apgroup default-group server-index 3

Radius Test Request
Wlan-id................................. 7
ApGroup Name............................. default-group
Attributes Values
---------- -----
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x0000000d (13)
Nas-Ip-Address 172.20.227.39
NAS-Identifier WLC5520
...-
Tunnel-Group-Id 0x00000051 (81)
Cisco / Audit-Session-Id ac14e3270000000ca56140f7e
Acct-Session-Id 56140f7e/00:11:22:33:44:55/218

test radius auth request successfully sent. Execute 'test aaa show radius' for response
(Cisco Controller) >test aaa show radius

previous test command still not completed, try after some time

(Cisco Controller) > test aaa show radius

Radius Test Request
Wlan-id................................. 7
ApGroup Name............................. default-group
Server Index.............................. 3

Radius Test Response
Radius Server Retry Status
---------- -----
172.20.227.72 6 No response received from server

Authentication Response:
Result Code: No response received from server
No AVPs in Response

(Cisco Controller) > debug aaa all enable

(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 11:42:20.674: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the mobile:
ac14e3270000000ca56140f7e
*aasQueueReader: Oct 06 11:42:20.675: User user1 password lengths don't match
*aasQueueReader: Oct 06 11:42:20.675: ReProcessAuthentication previous proto 8, next proto 40000001
*aasQueueReader: Oct 06 11:42:20.675: AuthenticationRequest: 0x2b6d2414
*aasQueueReader: Oct 06 11:42:20.675: Callback.........................................0x101cd740
*aasQueueReader: Oct 06 11:42:20.675: protocolType.................................0x40000001
*aasQueueReader: Oct 06 11:42:20.675:
proxyState.........................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 11:42:20.675: Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 11:42:20.675: Putting the quth request in qid 5, srv=index 2
.
.
*radiusTransportThread: Oct 06 11:42:33.991: server_index is provided with test aaa radius request. Not doing failover.
*radiusTransportThread: Oct 06 11:42:33.991: AuthorizationResponse: 0x3eefe934
*radiusTransportThread: Oct 06 11:42:33.991: protocolUsed..............................0xffffffff
*radiusTransportThread: Oct 06 11:42:33.991: Packet contains 0 AVPs:
*radiusTransportThread: Oct 06 11:42:33.991: Received radius callback for test aaa radius request result -5 numAVPs 0.

Example: NAS ID

(Cisco Controller) > show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.2.1.82
.
System Nas-Id.................................... WLC5520
WLC MIC Certificate Types........................ SHA1

(Cisco Controller) > show interface detailed engineering_v81

Interface Name................................... engineering_v81
MAC Address..................................... 50:57:a8:37:32:4f
IP Address....................................... 10.10.81.2
.
NAS-Identifier................................... v81-nas-id
Active Physical Port................................ LAG (13)
Radius Test Request
Wlan-id................................. 7
ApGroup Name............................ default-group
Attributes Values
---------- -----
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x000000d (13)
Nas-Ip-Address 172.20.227.39
NAS-Identifier v81-nas-id
Airespace / WLAN-Identifier 0x00000007 (7)

...
Example: Changing MAC Delimiter

(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request
Wlan-id................................. 7
ApGroup Name.......................... default-group
Attributes Values
------- -------
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x0000000d (13)
Nas-Ip-Address 0xac14e327 (-1407917273)
NAS-Identifier WLC5520

... (Cisco Controller) > config radius auth mac-delimiter colon
(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request
Wlan-id................................. 7
ApGroup Name.......................... default-group
Attributes Values
------- -------
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x0000000d (13)

Example: RADIUS Fallback

(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup default-group

Radius Test Request
Wlan-id................................. 7
ApGroup Name.......................... default-group
Attributes Values
------- -------
User-Name user1
Called-Station-Id 00:00:00:00:00:00:EngineeringV81
Calling-Station-Id 00:11:22:33:44:55
Nas-Port 0x0000000d (13)
Understanding Debug Client on Wireless Controllers


Using the CLI to Troubleshoot Problems

If you experience any problems with your controller, you can use the commands in this section to gather information and debug issues.

At the start of a debug session, a message is displayed indicating the following platform details for which the debug session is being started:

- Timestamp
- Cisco controller model
- Cisco release version
- Serial number
- Hostname

Procedure

- **show process cpu**—Shows how various tasks in the system are using the CPU at that instant in time. This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

  The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task that is divided by a range of system priorities.

  The CPU Use field shows the CPU usage of a particular task.
The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in a system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

### Note
If you want to see the total CPU usage as a percentage, enter the `show cpu` command.

- **show process memory**—Shows the allocation and deallocation of memory from various processes in the system at that instant in time.

In the example above, the following fields provide information:

  - The Name field shows the tasks that the CPU is to perform.
  - The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task that is divided by a range of system priorities.
  - The BytesInUse field shows the actual number of bytes used by dynamic memory allocation for a particular task.
  - The BlocksInUse field shows the chunks of memory that are assigned to perform a particular task.
  - The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

- **show tech-support**—Shows an array of information that is related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.

- **show run-config**—Shows the complete configuration of the controller. To exclude access point configuration settings, use the `show run-config no-ap` command.

### Note
If you want to see the passwords in clear text, enter the `config passwd-cleartext enable` command. To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

- **show run-config commands**—Shows the list of configured commands on the controller. This command shows only values that you configured. It does not show system-configured default values.

- **show logging config-history**—This command enhances the `show run-config` command output by displaying the following additional information:

  - List of commands executed arranged in chronological order with the timestamp.
  - User ID
  - The log of executed commands during the current and up to two previous sessions.

The history log records commands that modified the controller configurations. The following commands are recorded in the log:
• config
• save
• transfer
• upload
• download
• reset
• clear

The log file is saved to the `diag_bundle/configlog/configHistory` folder in the controller.

Download the Support Bundle to view the commands that are executed during the current and up to two previous sessions. See the Uploading Configuration Files section under the Management of Cisco WLC chapter.

---

**Note**

The history log file is limited to 10240 entries. The oldest entry is replaced after the entries exceed 10240 entries limit from the time the controller is boot up.