Debugging on Cisco Wireless Controllers

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                        0x0000000d (13)
  Nas-Ip-Address                  172.20.227.39
  NAS-Identifier                  WLC5520
  Airespace / WLAN-Identifier     0x00000007 (7)
  User-Password                   Cisco123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (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 09:48:12.931: 00:11:22:33:44:55 Sending Accounting request (2) for station
00:11:22:33:44:55
*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 quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 09:48:12.932: Request
Authenticator 3c:b3:09:34:95:be:ab:16:07:4a:7f:86:3b:58:77:26
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Sending the packet
to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 13) to 172.20.227.52:1812 from server queue 5,
proxy state 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 09:48:12.941: 00:11:22:33:44:55 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:
*radiusTransportThread: Oct 06 09:48:12.941: AVP[01] User-Name..................user1 (5
bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[02]
Class..........CACS:rs-acs5-6-0-22/230677882/20696 (35 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[03] Session-Timeout........0x0000001e (30)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[04] Termination-Action....0x00000000 (0)
(4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[05] Tunnel-Type......0x0100000d (16777229)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[06] Tunnel-Medium-Type...0x01000006
(16777222) (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[07] Tunnel-Group-Id.......DATA (3 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: Received radius callback for
test aaa radius request result 0 numAVPs 7.
```

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

*emWeb: Oct 06 10:42:30.638: 00:11:22:33:44:55 Sending Accounting request
(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:  proxyState..................00:11:22:33:44:55-00:00
*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
34:73:58:fd:8f:11:ba:6c:88:96:8c:e5:e0:84:e4:a5
*aaaQueueReader: Oct 06 10:42:30.639: 00:11:22:33:44:55
Sending the packet to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 10:42:30.639: 00:11:22:33:44:55
Successful transmission of Authentication Packet (id 14) to 172.20.227.52:1812 from server
 queue 5,
proxy state 00:11:22:33:44:55-00:00
 . . .
*radiusTransportThread: Oct 06 10:42:30.647: 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
*radiusTransportThread: Oct 06 10:42:30.647: 00:11:22:33:44:55 Returning AAA Error
'Authentication Failed' (-4) for mobile 00:11:22:33:44:55
*radiusTransportThread: Oct 06 10:42:30.647: AuthorizationResponse: 0x3eefd664
*radiusTransportThread: Oct 06 10:42:30.647:  structureSize...............................92
*radiusTransportThread: Oct 06 10:42:30.647:  resultCode.................................-4
*radiusTransportThread: Oct 06 10:42:30.647:
protocolUsed................................0xffffffff
*radiusTransportThread: Oct 06 10:42:30.647:
proxyState.....................00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 10:42:30.647:  Packet contains 0 AVPs:
*radiusTransportThread: Oct 06 10:42:30.647: Received radius callback for
test aaa radius request result -4 numAVPs 0.
```

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        ac14e327000000ca56140f7e
  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

*emWeb: Oct 06 11:42:20.674: 00:11:22:33:44:55 Sending Accounting request
(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:

ac14e327000000cc5614160c
*aaaQueueReader: Oct 06 11:42:20.675: User user1 password lengths don't match
*aaaQueueReader: Oct 06 11:42:20.675: ReProcessAuthentication previous proto 8, next proto
```

```
 40000001
*aaaQueueReader: Oct 06 11:42:20.675: AuthenticationRequest: 0x2b6d2414
*aaaQueueReader: Oct 06 11:42:20.675:  Callback..................................0x101cd740
*aaaQueueReader: Oct 06 11:42:20.675:  protocolType..............................0x40000001
*aaaQueueReader: 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
*aaaQueueReader: Oct 06 11:42:20.675: Request
Authenticator 03:95:a5:d5:16:cd:fb:60:ef:31:5d:d1:52:10:8e:7e
*aaaQueueReader: Oct 06 11:42:20.675: 00:11:22:33:44:55 Sending the packet
 to v4 host 172.20.227.72:1812
*aaaQueueReader: Oct 06 11:42:20.675: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 3) to
172.20.227.72:1812 from server queue 5, proxy state 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 11:42:22.789: 00:11:22:33:44:55 Retransmit the
'Access-Request' (id 3) to 172.20.227.72 (port 1812, qid 5) reached for mobile
00:11:22:33:44:55. message retransmit cnt 1, server retries 15
*radiusTransportThread: Oct 06 11:42:22.790: 00:11:22:33:44:55 Sending the packet to v4
host
172.20.227.72:1812
*radiusTransportThread: Oct 06 11:42:22.790: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 3) to 172.20.227.72:1812 from server queue 5, proxy state
 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 11:42:33.991: 00:11:22:33:44:55 Max retransmit
of Access-Request (id 3) to 172.20.227.72 (port 1812, qid 5) reached for mobile
00:11:22:33:44:55. message retransmit cnt 6, server retransmit cnt 20
*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: 00:11:22:33:44:55 Max servers (tried 1)
retransmission of Access-Request (id 3) to 172.20.227.72 (port 1812, qid 5) reached for
 mobile 00:11:22:33:44:55. message retransmit cnt 6, server r
*radiusTransportThread: Oct 06 11:42:33.991: 00:11:22:33:44:55 Returning AAA Error
'Timeout' (-5) for mobile 00:11:22:33:44:55
*radiusTransportThread: Oct 06 11:42:33.991: AuthorizationResponse: 0x3eefe934
*radiusTransportThread: Oct 06 11:42:33.991:  structureSize...............................92
*radiusTransportThread: Oct 06 11:42:33.991:  resultCode..................................-5
*radiusTransportThread: Oct 06 11:42:33.991:
protocolUsed..............................0xffffffff
*radiusTransportThread: Oct 06 11:42:33.991:
proxyState....................00:11:22:33:44:55-00:00
*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:c7:32:4f
```

```
IP Address....................................... 10.10.81.2
. . .
NAS-Identifier................................... v81-nas-id
Active Physical Port............................. LAG (13)
. . .

(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                  v81-nas-id
  Airespace / WLAN-Identifier     0x00000007 (7)
 . . .

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 13:54:52.543: 00:11:22:33:44:55 Sending Accounting request
(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 13:54:52.543: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the
 mobile: ac14e327000000ce5614351c
*aaaQueueReader: Oct 06 13:54:52.544: User user1 password lengths don't match
*aaaQueueReader: Oct 06 13:54:52.544: ReProcessAuthentication previous proto 8, next proto
 40000001
*aaaQueueReader: Oct 06 13:54:52.544: AuthenticationRequest: 0x2b6bf140
*aaaQueueReader: Oct 06 13:54:52.544:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 13:54:52.544:  protocolType.................................0x40000001
*aaaQueueReader: Oct 06 13:54:52.544:  proxyState.....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 13:54:52.544:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 13:54:52.544: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 13:54:52.544: Request
Authenticator bc:e4:8e:cb:56:9b:e8:fe:b7:f9:a9:04:15:25:10:26
*aaaQueueReader: Oct 06 13:54:52.544: 00:11:22:33:44:55 Sending the packet
 to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 13:54:52.544: 00:11:22:33:44:55
Successful transmission of Authentication Packet (id 16) to 172.20.227.52:1812 from server
 queue 5,
proxy state 00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 13:54:52.545: 00000000: 01 10 00 f9 bc e4 8e cb  56 9b e8 fe b7 f9
 a9 04  ........V.......
*aaaQueueReader: Oct 06 13:54:52.545: 00000010: 15 25 10 26 01 07 75 73  65 72 31 1e 22 30
 30 3a  .%.&..user1."00:
*aaaQueueReader: Oct 06 13:54:52.545: 00000020: 30 30 3a 30 30 3a 30 30  3a 30 30 3a 30 30
 3a 45  00:00:00:00:00:E
*aaaQueueReader: Oct 06 13:54:52.545: 00000030: 6e 67 69 6e 65 65 72 69  6e 67 56 38 31 1f
 13 30  ngineeringV81..0
*aaaQueueReader: Oct 06 13:54:52.545: 00000040: 30 3a 31 31 3a 32 32 3a  33 33 3a 34 34 3a
 35 35  0:11:22:33:44:55
*aaaQueueReader: Oct 06 13:54:52.545: 00000050: 05 06 00 00 00 0d 04 06  ac 14 e3 27 20 0c
 76 38  ...........'..v8
*aaaQueueReader: Oct 06 13:54:52.545: 00000060: 31 2d 6e 61 73 2d 69 64  1a 0c 00 00 37 63
 01 06  1-nas-id....7c..
*aaaQueueReader: Oct 06 13:54:52.545: 00000070: 00 00 00 07 02 12 88 65  4b bf 0c 2c 86 6e
 b0 c7  .......eK..,.n..
*aaaQueueReader: Oct 06 13:54:52.545: 00000080: 7a c1 67 fa 09 12 06 06  00 00 00 08 0c 06
 00 00  z.g.............
```

```
*aaaQueueReader: Oct 06 13:54:52.545: 00000090: 05 14 3d 06 00 00 00 13  40 06 00 00 00 0d
 41 06  ..=.....@.....A.
*aaaQueueReader: Oct 06 13:54:52.545: 000000a0: 00 00 00 06 51 04 38 31  1a 31 00 00 00 09
 01 2b  ....Q.81.1.....+
*aaaQueueReader: Oct 06 13:54:52.545: 000000b0: 61 75 64 69 74 2d 73 65  73 73 69 6f 6e 2d
 69 64  audit-session-id
*aaaQueueReader: Oct 06 13:54:52.545: 000000c0: 3d 61 63 31 34 65 33 32  37 30 30 30 30 30
 30 63  =ac14e327000000c
*aaaQueueReader: Oct 06 13:54:52.545: 000000d0: 65 35 36 31 34 33 35 31  63 2c 20 35 36 31
 34 33  e5614351c,.56143
*aaaQueueReader: Oct 06 13:54:52.545: 000000e0: 35 31 63 2f 30 30 3a 31  31 3a 32 32 3a 33
 33 3a  51c/00:11:22:33:
*aaaQueueReader: Oct 06 13:54:52.545: 000000f0: 34 34 3a 35 35 2f 32 32  34
        44:55/224
*radiusTransportThread: Oct 06 13:54:52.560: 5.client sockfd 35 is set. process the msg
*radiusTransportThread: Oct 06 13:54:52.560: ****Enter processIncomingMessages: Received
Radius
response (code=3)
```

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)
  Nas-Ip-Address                  172.20.227.39
  NAS-Identifier                  WLC5520
  . . .
(Cisco Controller) > test aaa show radius

Radius Test Request
  Wlan-id........................................ 7
  ApGroup Name................................... default-group
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
172.20.227.62            6     No response received from server
172.20.227.52            1     Success
Authentication Response:
  Result Code: Success
  Attributes                      Values
  ----------                      ------
  User-Name                       user1
. . .
```

Understanding Debug Client on Wireless Controllers

Use the Wireless Debug Analyzer tool to analyze the debug client output.

Deauthenticating Clients

Using the controller, you can deauthenticate clients based on their user name, IP address, or MAC address. If there are multiple client sessions with the same user name, you can deauthenticate all the client sessions based on the user name. If there are overlapped IP addresses across different interfaces, you can use the MAC address to deauthenticate the clients.

This section contains the following subsections:

Deauthenticating Clients (GUI)

Procedure

Step 1 Choose **Monitor** > **Clients**.

Step 2 On the **Clients** page, click the MAC address of the client.

Step 3 On the **Clients > Detail** page displayed, click **Remove**.

Step 4 Save the configuration.

Deauthenticating Clients (CLI)

Procedure

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}

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.

- The **debug** command enables diagnostic logging of specific events. The log output is directed to the terminal session in which the debug command is entered.
- Only one debug session at a time is active. If one terminal has debugging running, and a **debug** command is entered on another terminal, the debug session on the first terminal is terminated.
- To turn off all debugs, use the **debug disable-all** command.
- To filter the debugs based on client or AP MAC addresses, use the **debug mac addr** *mac-address* command. Up to 10 MAC addresses are supported.
- 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.

Potential Reasons for Controller Reset

This section lists all the potential reasons for a controller reset.

- User initiated reset
- Hard/Unknown reboot
- Reset due to switch-driver crash
- Reset due to DP crash
- Peer-RMI, peer-RP and management default gateway are reachable
- Both controllers are active, same timestamp, rebooting secondary controller
- Mandatory argument is missing for starting redundancy manager transport task
- Failed to create socket to communicate with peer
- Failed to create socket to communicate with peer via secondary link
- Failed bind socket to communicate with peer
- Failed bind socket to communicate with peer via secondary link
- License count was not received from primary controller
- Not reaching Hot Standby
- Standby has not received config files from Active
- Corrupted XMLs transferred from Active to Standby
- Corrupted XMLs in Active controller
- Standby TFTP failure
- New XML downloaded

- Active to Standby request
- Standby IPC failure
- Certificate installed in Standby controller
- Mandatory argument to start redundancy manager ping task is missing
- Self sanity check failed; both controllers are in maintenance state
- Self sanity check failed; in maintenance state because both controllers were active
- Self sanity check failed; current controller became Active before peer reboot
- User has initiated reset
- XML transfer was initiated but role negotiation was not done
- IPC timeout has occurred multiple times
- Role notification timeout has occurred
- Peer sanity check failed
- Active is down, Standby is not ready to take over
- Configuration out of sync
- Configuration download failure
- None of the ports is connected
- None of the local ports is connected
- Peer maintenance mode
- RF keepalive timeout
- Peer notification timeout
- Peer platform sync timeout
- Peer progression failed
- Standby default gateway is not reachable
- Active default gateway is not reachable
- Redundancy management interface and redundancy port are down
- Redundancy port is down
- Redundancy management interface is down
- Standby timeout
- Active timeout
- License count was not received from Primary controller
- XMLs were not transferred from Active to Standby
- Certificate transfer from Active to Standby failed

- Redundant pair assume same role
- Failed to create redundancy manager semaphore
- Failed to create redundancy manager keepalive task
- Failed to create redundancy manager main task
- Failed to create redundancy manager message queue
- Failed to start redundancy manager transport task
- Controller is not in proper state for more than expected time
- Mandatory argument is missing in redundancy manager main task
- Failed to create timer to send sanity messages
- Failed to create timer to send role negotiation message
- Failed to create timer to send the messages to peer
- Failed to create timer for handling max role negotiation time
- Mandatory argument to start keepalive task is missing
- Failed to create the semaphore used for sending keepalive messages
- Reset due to config download
- Watchdog reset
- Unknown reset reason