# Konfigurieren der Access Point-Autorisierung in einem Unified Wireless Network

### Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Lightweight AP-Autorisierung Konfigurieren Konfiguration mithilfe der internen Autorisierungsliste des WLC Überprüfung AP-Autorisierung für einen AAA-Server Konfigurieren der Cisco ISE zur Autorisierung von APs Konfigurieren eines neuen Geräteprofils, für das MAB kein NAS-Port-Type-Attribut erfordert Konfigurieren des WLC als AAA-Client auf der Cisco ISE Hinzufügen der AP-MAC-Adresse zur Endpunktdatenbank auf der Cisco ISE Fügen Sie die AP-MAC-Adresse der Benutzerdatenbank auf der Cisco ISE hinzu (optional) **Definieren eines Policy Sets** Überprüfung Fehlerbehebung

# Einleitung

In diesem Dokument wird die Konfiguration des WLC zur Autorisierung des Access Points (AP) anhand der MAC-Adresse der APs beschrieben.

### Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Konfiguration einer Cisco Identity Services Engine (ISE)
- Kenntnisse der Konfiguration von Cisco APs und Cisco WLCs
- Kenntnisse der Cisco Unified Wireless Security-Lösungen

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:  WLCs mit AireOS 8.8.111.0-SoftwareWave1-APs: 1700/2700/3700 und 3500 (1600/2600/3600 werden weiterhin unterstützt, AireOS-Unterstützung endet jedoch mit Version 8.5.x)Wave2-APs: 1800/2800/3800/4800, 1540 und 1560 ISE-Version 2.3.0.298

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Lightweight AP-Autorisierung

Während des AP-Registrierungsprozesses authentifizieren sich die APs und WLCs gegenseitig mithilfe von X.509-Zertifikaten. Die X.509-Zertifikate werden werkseitig von Cisco im geschützten Flash-Speicher sowohl des AP als auch des WLC gebrannt.

Werkseitig installierte Zertifikate werden auf dem AP als MIC (Manufacturing-Installed Certificates) bezeichnet. Alle nach dem 18. Juli 2005 hergestellten Cisco APs verfügen über MICs.

Zusätzlich zu dieser gegenseitigen Authentifizierung, die während des Registrierungsvorgangs stattfindet, können die WLCs die APs, die sich bei ihnen registrieren, anhand der MAC-Adresse des AP einschränken.

Das Fehlen eines sicheren Kennworts bei Verwendung der MAC-Adresse des Access Points ist kein Problem, da der Controller den Access Point mithilfe des MIC authentifiziert, bevor er den Access Point über den RADIUS-Server autorisiert. Die Verwendung des MIC bietet eine starke Authentifizierung.

Die AP-Autorisierung kann auf zwei Arten erfolgen:

- Verwenden der internen Autorisierungsliste des WLC
- Verwenden der MAC-Adressdatenbank auf einem AAA-Server

Das Verhalten der APs unterscheidet sich je nach verwendetem Zertifikat:

- APs mit SSCs Der WLC verwendet nur die Liste interner Autorisierungen und leitet für diese APs keine Anforderung an einen RADIUS-Server weiter.
- APs mit MICs WLC kann entweder die auf dem WLC konfigurierte Liste interner Autorisierungen verwenden oder einen RADIUS-Server zur Autorisierung der APs verwenden.

In diesem Dokument wird die AP-Autorisierung unter Verwendung der internen Autorisierungsliste und des AAA-Servers beschrieben.

# Konfigurieren

### Konfiguration mithilfe der internen Autorisierungsliste des WLC

Verwenden Sie auf dem WLC die AP-Autorisierungsliste, um die APs anhand ihrer MAC-Adresse einzuschränken. Die AP-Autorisierungsliste finden Sie unter Security > AP Policies in der WLC-

Benutzeroberfläche ein.

Dieses Beispiel zeigt, wie der Access Point mit einer MAC-Adresse hinzugefügt wird. 4c:77:6d:9e:61:62.

- 1. Klicken Sie in der Benutzeroberfläche des WLC-Controllers auf Security > AP Policies und die Seite "AP Policies" (AP-Richtlinien) wird angezeigt.
- 2. Klicken Sie auf Add -Taste auf der rechten Seite des Bildschirms.

| սիսիս   |                  |                          |             |          |              |                   |      | Save Configuration | Ping  | Logout   <u>R</u> efresh |
|---|------------------|--------------------------|-------------|----------|--------------|-------------------|------|--------------------|-------|--------------------------|
| cisco   | MONITOR WL       | ANS <u>C</u> ONTROLLER   | WIRELESS    | SECURITY | MANAGEMENT   | C <u>O</u> MMANDS | HELP | <u>F</u> EEDBACK   |       | 🔒 <u>H</u> ome           |
| Security  | AP Policies      |                          |             |          |              |                   |      |                    | Apply | Add                      |
| ▼ AAA<br>General<br>▼ RADIUS                                      | Policy Configu   | ration                   |             |          |              |                   |      | -                  |       |                          |
| Authentication<br>Accounting<br>Auth Cached Users                 | Accept Self Sign | ned Certificate (SSC)    |             |          |              |                   |      |                    |       |                          |
| Fallback  | Accept Manufac   | tured Installed Certific | ate (MIC)   |          |              |                   |      |                    |       |                          |
| DNS<br>Downloaded AVP   | Accept Local Si  | nificant Certificate (LS | C)          |          |              |                   |      |                    |       |                          |
| ▶ TACACS+   | Authorize MIC A  | APs against auth-list or | AAA         |          |              |                   |      |                    |       |                          |
| LOGI Net Users<br>MAC Filtering                                   | Authorize LSC 4  | APs against auth-list    |             |          |              |                   |      |                    |       |                          |
| <ul> <li>Disabled Clients</li> <li>User Login Policies</li> </ul> | AP Authorizatio  | on List                  |             |          | Ent          | ries 1 - 5 of 5   | -    |                    |       |                          |
| Password Policies   | Search by MAC    |                          | Searc       | h        |              |                   |      |                    |       |                          |
| Local EAP     Advanced EAP  | MAC address /    | Serial Number            | Certificate | Type SI  | HA1 Key Hash |                   |      |                    |       |                          |

3. Unter Add AP to Authorization List, geben Sie AP MAC Adresse (nicht die MAC-Adresse des AP-Funkmoduls). Wählen Sie dann den Zertifikatstyp aus, und klicken Sie auf Add.In diesem Beispiel wird ein Access Point mit einem MIC-Zertifikat hinzugefügt. Anmerkung: Wählen Sie für APs mit SSCs ssc unter Zertifikatstyp.

|   |             |              |                    |                |          |            |                   |      | Save            | Configuration | Ping | Logout Refresh |
|---|-------------|--------------|--------------------|----------------|----------|------------|-------------------|------|-----------------|---------------|------|----------------|
| cisco   | MONITOR     | WLANs        |                    | WIRELESS       | SECURITY | MANAGEMENT | C <u>O</u> MMANDS | HELP | <b>FEEDBACK</b> |               |      | 🔒 <u>H</u> ome |
| Security  | AP Polici   | es           |                    |                |          |            |                   |      |                 |               |      | Apply          |
| <ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> </ul>      | Policy Con  | figuratio    | n                  |                |          |            |                   | _    |                 |               |      |                |
| Authentication<br>Accounting<br>Auth Cached Users                 | Accept Se   | lf Signed C  | ertificate (SSC)   |                |          |            |                   |      |                 |               |      |                |
| Fallback  | Accept Ma   | nufactured   | Installed Certific | ate (MIC)      |          |            |                   |      |                 |               |      |                |
| DNS<br>Downloaded AVP   | Accept Lo   | cal Signific | ant Certificate (L | SC)            |          |            |                   |      |                 |               |      |                |
| TACACS+   | Authorize   | MIC APs a    | gainst auth-list o | AAA            |          |            |                   |      |                 |               |      |                |
| Local Net Users<br>MAC Filtering                                  | Authorize   | LSC APs a    | gainst auth-list   |                |          |            |                   |      |                 |               |      |                |
| <ul> <li>Disabled Clients</li> <li>User Login Policies</li> </ul> | Add AP to   | Authoriz     | ation List         |                |          |            |                   |      |                 |               |      |                |
| AP Policies   | MAC Addr    | ess          |                    | 4c:77:6d:9e:61 | :62      |            |                   |      |                 |               |      |                |
| Local EAP   | Certificate | Туре         |                    | MIC            | •        |            |                   |      |                 |               |      |                |
| Advanced EAP  |             |              | ſ                  | Add            |          |            |                   |      |                 |               |      |                |
| Priority Order  | -           |              |                    |                |          |            |                   |      |                 |               |      |                |
| Certificate   | AP Author   | ization Li   | st                 |                |          | En         | tries 0 - 0 of 0  |      |                 |               |      |                |
| Access Control Lists  | Consch by b |              |                    | Sear           | -h       |            |                   |      |                 |               |      |                |
| Wireless Protection     Policies                                  | MAC addre   | ss / Cer     | tificate           | Jocard         |          |            |                   |      |                 |               |      |                |
| Web Auth  | Serial Num  | iber Typ     | e SHA1             | (ey Hash       |          |            |                   |      |                 |               |      |                |
| TrustSec  |             |              |                    |                |          |            |                   |      |                 |               |      |                |
| Local Policies  |             |              |                    |                |          |            |                   |      |                 |               |      |                |
| ▶ Umbrella  |             |              |                    |                |          |            |                   |      |                 |               |      |                |
| Advanced  |             |              |                    |                |          |            |                   |      |                 |               |      |                |

Der AP wird der AP-Autorisierungsliste hinzugefügt und ist unter AP Authorization List.

4. Aktivieren Sie unter "Policy Configuration" das Kontrollkästchen für Authorize MIC APs against auth-list or AAA.Wenn dieser Parameter ausgewählt ist, überprüft der WLC zuerst die lokale Autorisierungsliste. Wenn die AP-MAC nicht vorhanden ist, wird der RADIUS-Server überprüft.

| cisco  | MONITOR WLANS CONTROLLER                | WIRELESS SECU    | RITY MANAGEMENT | COMMANDS          | HELP | Save Cor<br>FEEDBACK | nfiguration Ping Logout Refres |
|--|---|------------------|-----------------|-------------------|------|----------------------|--------------------------------|
| Security   | AP Policies                             |                  |                 |                   |      |                      | Apply Add                      |
| <ul> <li>AAA</li> <li>General</li> <li>▼ RADIUS</li> </ul> | Policy Configuration                    |                  |                 |                   |      |                      |                                |
| Authentication<br>Accounting<br>Auth Cached Users          | Accept Self Signed Certificate (SSC)    | este (MTC)       |                 |                   |      |                      |                                |
| DNS  | Accept Local Significant Certificate (L | .SC)             |                 |                   |      |                      |                                |
| ► TACACS+  | Authorize MIC APs against auth-list o   | or AAA           |                 |                   |      |                      |                                |
| LDAP<br>Local Net Users<br>MAC Filtering                   | Authorize LSC APs against auth-list     |                  |                 |                   |      |                      |                                |
| An Policies  | AP Authorization List                   |                  | En              | itries 1 - 5 of 5 |      |                      |                                |
| Password Policies  | Search by MAC                           | Search           |                 |                   |      |                      |                                |
| Local EAP  | MAC address / Carlal Number             | Cartificate Ture | Cust Kau Hash   |                   |      |                      |                                |
| Advanced EAP   | Ac:77:6d:9a:61:62                       | MIC              | Shar Key hash   |                   |      |                      |                                |
| Priority Order   | 70:43:79:26:39:68                       | MIC              |                 |                   |      |                      |                                |
| Certificate  | 88:f0:31:7e:e0:38                       | MIC              |                 |                   |      |                      |                                |
| Access Control Lists                                       | f4:db:e6:43:c4:b2                       | MIC              |                 |                   |      |                      |                                |
| Wireless Protection<br>Policies                            | fc:5b:39:e7:2b:30                       | MIC              |                 |                   |      |                      |                                |
| ▶ Web Auth   |   |                  |                 |                   |      |                      |                                |
| TrustSec   |   |                  |                 |                   |      |                      |                                |

#### Überprüfung

Um diese Konfiguration zu überprüfen, müssen Sie den AP mit einer MAC-Adresse verbinden 4c:77:6d:9e:61:62 an das Netzwerk und die Überwachung. Verwenden Sie debug capwap events/errors enable und debug aaa all enable Befehle, um dies auszuführen.

Diese Ausgabe zeigt die Fehlerbehebungen an, wenn die MAC-Adresse des Access Points nicht in der Autorisierungsliste des Access Points vorhanden ist:

**Anmerkung:** Einige Zeilen in der Ausgabe wurden aufgrund von Platzbeschränkungen in die zweite Zeile verschoben.

(Cisco Controller) >debug capwap events enable (Cisco Controller) >debug capwap errors enable (Cisco Controller) >debug aaa all enable \*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256 \*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request \*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 277 \*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved) \*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from temporary database. \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap\_wtp\_event\_response, state Capwap\_no\_state

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed! \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256 \*aaaQueueReader: Feb 27 10:15:25.593: Unable to find requested user entry for 4c776d9e6162 \*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 \*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001 \*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638 \*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00 \*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs: \*aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes) 51-4e-c0 (17 bytes) 9e-61-62 (17 bytes) \*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) \*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes) (28271) (2 bytes) \*aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) \*aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator......DATA (16 bytes) \*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0 \*aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770 \*aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0) \*aaaQueueReader: Feb 27 10:15:25.593: protocolUsed..... \*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:CO-00:00

\*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client. \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432 \*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K \*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0 \*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0 \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79 \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256 \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls Connection. \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0724fd8 for AP (192:168:79:151/5256). Notify(true) \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys: lrad:192.168.79.151(5256) mwar:10.48.71.20(5246) \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted successfully for AP 192.168.79.151 \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (10.48.71.20/5246) client (192.168.79.151/5256) \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256) \*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0 \*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for 192.168.79.151:5256

Diese Ausgabe zeigt die Fehlersuche beim Hinzufügen der LAP-MAC-Adresse zur AP-Autorisierungsliste:

**Anmerkung:** Einige Zeilen in der Ausgabe wurden aufgrund von Platzbeschränkungen in die zweite Zeile verschoben.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable
```

\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 274

\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
\*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

\*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap\_wtp\_event\_response, state Capwap\_no\_state \*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap\_wtp\_event\_response is not allowed to send in state Capwap\_no\_state for AP 192.168.79.151 \*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 \*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed! \*aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated \*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : 0 \*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile 70:69:5a:51:4e:c0 \*aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408 \*aaaQueueReader: Feb 27 09:50:25.394: resultCode.....0 \*aaaQueueReader: Feb 27 09:50:25.394: proxyState......70:69:5A:51:4E:C0-00:00 \*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs: \*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-Type......0x00000065 (101) (4 bytes) \*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-Identifier.....0x00000000 (0) (4 bytes) \*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB on WLAN ID :0 \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432 \*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K \*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0 \*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0 \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79 \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256 \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap\_ac\_platform.c:2095 - Operation State 0 ===> 4 \*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from capwap\_ac\_platform.c 2136 \*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP

^apikeceiverask: Feb 2/ 09:50:25.394: /0:69:5a:51:4e:C0 Register LWAPP event for AP 70:69:5a:51:4e:c0 slot 0

#### AP-Autorisierung für einen AAA-Server

Sie können WLCs auch so konfigurieren, dass sie RADIUS-Server verwenden, um APs mithilfe

von MICs zu autorisieren. Der WLC verwendet beim Senden der Informationen an einen RADIUS-Server eine MAC-Adresse des AP als Benutzername und Kennwort. Wenn die MAC-Adresse des Access Points beispielsweise 4c:77:6d:9e:61:62sind sowohl der Benutzername als auch das Kennwort, die der Controller für die Autorisierung des AP verwendet, die MAC-Adresse mit dem definierten Begrenzungszeichen.

Dieses Beispiel zeigt, wie die WLCs mithilfe der Cisco ISE für die Autorisierung der APs konfiguriert werden.

- 1. Klicken Sie in der Benutzeroberfläche des WLC-Controllers auf Security > AP Policies. Die Seite "AP-Richtlinien" wird angezeigt.
- Aktivieren Sie unter "Policy Configuration" das Kontrollkästchen f
  ür Authorize MIC APs against auth-list or AAA.Wenn Sie diesen Parameter auswählen, 
  überpr
  üft der WLC zuerst die lokale Autorisierungsliste. Wenn die AP-MAC nicht vorhanden ist, wird der RADIUS-Server 
  überpr
  üft.

| liulu   |  |   |             |          |                 |          |      | Sa <u>v</u> e Co | nfiguration <u>P</u> ing | Logout <u>R</u> efresh |
|---|--|---|-------------|----------|-----------------|----------|------|------------------|--------------------------|------------------------|
| cisco   |  | CONTROLLER                                  | WIRELESS    | SECURITY | MANAGEMENT      | COMMANDS | HELP | <b>FEEDBACK</b>  |                          | n <u>H</u> ome         |
| Security  | AP Policies                              |   |             |          |                 |          |      |                  | Apply                    | Add                    |
| <ul> <li>▼ AAA<br/>General</li> <li>▼ RADIUS</li> </ul>   | Policy Configurati                       | on  |             |          |                 |          |      |                  |                          |                        |
| Authentication<br>Accounting<br>Auth Cached Users<br>Fallback<br>DNS<br>Downloaded AVP<br>TACACS+<br>LDAP<br>Local Net Users<br>MAC Filtering<br>Disabled Clients<br>Disabled Clients | Accept Self Signed<br>Accept Manufactur  | Certificate (SSC)<br>ed Installed Certifica | ate (MIC)   |          |                 |          |      |                  |                          |                        |
|   | Accept Local Signif<br>Authorize MIC APs | against auth-list or                        | C)<br>AAA   |          |                 |          |      |                  |                          |                        |
|   | Authorize LSC APs                        | against auth-list<br>List                   |             | Ent      | ries 1 - 5 of 5 |          |      |                  |                          |                        |
| Password Policies   | Search by MAC                            |   | Searc       | h        |                 |          |      |                  |                          |                        |
| Local EAP     Advanced EAP  | MAC address / Ser                        | ial Number                                  | Certificate | Туре 5   | 6HA1 Key Hash   |          |      |                  |                          |                        |
| h Driority Order  | 4c:77:6d:9e:61:62                        |   | MIC         |          |                 |          |      |                  |                          |                        |
| P Phoney order  | 70:d3:79:26:39:68                        |   | MIC         |          |                 |          |      |                  |                          |                        |
| Certificate   | 88:f0:31:7e:e0:38                        |   | MIC         |          |                 |          |      |                  |                          |                        |
| Access Control Lists  | f4:db:e6:43:c4:b2                        |   | MIC         |          |                 |          |      |                  |                          |                        |
| Wireless Protection     Policies  | fc:5b:39:e7:2b:30                        |   | MIC         |          |                 |          |      |                  |                          |                        |
| Web Auth  |  |   |             |          |                 |          |      |                  |                          |                        |
| ▶ TrustSec  |  |   |             |          |                 |          |      |                  |                          |                        |

3. Navigieren Sie zu Security > RADIUS Authentication von der Controller-GUI aus, um das RADIUS Authentication Servers Seite. Auf dieser Seite können Sie den MAC-Delimiter definieren. Der WLC erhält die MAC-Adresse des AP und sendet sie mithilfe des hier definierten Delimiters an den Radius-Server. Dies ist wichtig, damit der Benutzername mit der Konfiguration im Radius-Server übereinstimmt. In diesem Beispiel No Delimiter wird verwendet, sodass der Benutzername 4c776d9e6162.

| alada   |                  |                          |                  |                                    |                   |                      |                  |            |          | Sa <u>v</u> e Configu | ration <u>P</u> ing Logout | Refresh      |
|---|------------------|--------------------------|------------------|------------------------------------|-------------------|----------------------|------------------|------------|----------|-----------------------|----------------------------|--------------|
| CISCO   | MONITOR          | R <u>W</u> LANS <u>C</u> | ONTROLL          | ER WIRELES                         | S <u>S</u> ECURIT | MANAGEMENT           | COMMANDS         | HELP       | FEEDBACK |                       | 9                          | <u>H</u> ome |
| Security  | RADIU            | S Authenticat            | ion Ser          | vers                               |                   |                      |                  |            |          |                       | Apply Nev                  | v            |
| AAA     General     RADIUS     Authentication     Accounting  | Auth C<br>Use AE | alled Station ID T       | vpe 🛛 🖾          | P MAC Address:<br>Designed for FIP | SSID •            | nd requires a key wr | p compliant RADI | IUS server | )        |                       |                            |              |
| Auth Cached Users<br>Fallback<br>DNS  | MAC D            | elimiter<br>চালাত        | N                | o Delimiter 🔹                      |                   |                      |                  |            |          |                       |                            |              |
| <ul> <li>TACACS+<br/>LDAP</li> </ul>  | Networl<br>User  | k<br>Management          | Tunne H<br>Proxy | yphen                              | Server Addres     | ss(Ipv4/Ipv6)        |                  |            | Port     | IPSec                 | Admin Status               |              |
| Local Net Users<br>MAC Filtering  |                  |                          |                  | ingle Hypnen                       | 10.48.39.100      |                      |                  |            | 1812     | Disabled              | Enabled                    |              |
| <ul> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul> | ~                | 2                        |                  | lo Delimiter                       | 10.48.39.128      |                      |                  |            | 1812     | Disabled              | Enabled                    |              |
| Local EAP   |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Advanced EAP  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Priority Order  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Certificate   |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Access Control Lists  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Wireless Protection     Policies  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Web Auth  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| TrustSec  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |
| Local Policies  |                  |                          |                  |                                    |                   |                      |                  |            |          |                       |                            |              |

4. Klicken Sie anschließend auf New um einen RADIUS-Server zu definieren.

| a di a di a  |   |  | Saye Configuration Ping Logout Refresh |
|--|---|--|--|
| cisco  | MONITOR WLANS CONTROLLER  | WIRELESS SECURITY MANAGEMENT COMMANDS HELP F | EEDBACK A Home                         |
| Security   | RADIUS Authentication Serve   | rs > New                                     | < Back Apply                           |
| <ul> <li>AAA             General             RADUS             Authentication             Accounting             Auth Cached Users             Fallback             DNS             Downloaded AVP             TACACS+             LDAP             LOAR             MaC Filtering             Disabled Clients             User Login Policies             AP Policies             Paront Policies             Paront Policies             Advanced EAP             Priority Order             Certificate             Access Control Lists             Wrieless Protection             Policies             Web Auth             TrustSec             Local Policies         </li> </ul> | Server Index (Priority)<br>Server IP Address(Ipv4/Ipv6)<br>Shared Secret Format<br>Shared Secret<br>Confirm Shared Secret<br>Apply Cisco ISE Default settings<br>Apply Cisco ACA Default settings<br>Key Wrap<br>Port Number<br>Server Status<br>Support for CoA<br>Server Timeout<br>Network User<br>Management<br>Management Retransmit Timeout<br>Tunnel Proxy<br>PAC Provisioning<br>IPSec<br>Cisco ACA | 3       ▼         10.48.39.128               | 5 server)                              |

5. Definieren Sie die RADIUS-Serverparameter auf dem RADIUS Authentication Servers > New Seite. Zu diesen Parametern gehört der RADIUS Server IP Address, Shared Secret, Port Numberund Server Status. Klicken Sie abschließend auf Apply. In diesem Beispiel wird die Cisco ISE als RADIUS-Server mit der IP-Adresse 10.48.39.128 verwendet.

#### Konfigurieren der Cisco ISE zur Autorisierung von APs

Damit die Cisco ISE APs autorisieren kann, müssen Sie wie folgt vorgehen:

- 1. Konfigurieren des WLC als AAA-Client auf der Cisco ISE
- 2. Fügen Sie der Datenbank der Cisco ISE die AP-MAC-Adressen hinzu.

Sie können die AP-MAC-Adresse jedoch auch als Endpunkte (am besten) oder als Benutzer (deren Kennwörter ebenfalls die MAC-Adresse sind) hinzufügen. Dazu müssen Sie jedoch die Anforderungen für die Kennwortsicherheitsrichtlinien senken.

Da der WLC das NAS-Port-Type-Attribut nicht sendet, das auf der ISE erforderlich ist, um mit dem MAB-Workflow (Mac Address Authentication) übereinzustimmen, müssen Sie dies anpassen.

#### Konfigurieren eines neuen Geräteprofils, für das MAB kein NAS-Port-Type-Attribut erfordert

Navigieren Sie zu Administration > Network device profile und ein neues Geräteprofil erstellen. Aktivieren Sie RADIUS, und legen Sie für den kabelgebundenen MAB-Datenstrom wie im Bild dargestellt fest, dass service-type=Call-check erforderlich ist. Sie können andere Einstellungen aus dem klassischen Cisco Profil kopieren, es soll jedoch kein Attribut "Nas-port-type" für einen kabelgebundenen MAB-Workflow erforderlich sein.

| E Cisco ISE                         |   | Admir                   | istration • Network Resources |
|-------------------------------------|---|-------------------------|-------------------------------|
| Network Devices                     | Network Device Groups                               | Network Device Profiles | External RADIUS Servers       |
| * Name                              | Ciscotemp   |                         |                               |
| Description                         |   |                         | 12                            |
| Icon                                | the Change icon Set T                               | To Default i            |                               |
| Vendor                              | Cisco   |                         |                               |
| Supported Protoc                    | ols   |                         |                               |
| RADIUS                              |   |                         |                               |
| TACACS+                             |   |                         |                               |
| TrustSec                            |   |                         |                               |
| RADIUS Dictionaries                 |   |                         |                               |
| Templates                           |   |                         |                               |
| Expand All / Collapse All           |   |                         |                               |
| $\checkmark$ Authentication         | /Authorization                                      |                         |                               |
| ✓ Flow Type Co<br>✓ Wired MAB deter | onditions<br>cted if the following condition(s) are | met :                   |                               |
| Radius:Se                           | ervice-Type 🗸 =                                     | Call Check              | <u>∼</u>                      |

#### Konfigurieren des WLC als AAA-Client auf der Cisco ISE

- 1. Gehe zu Administration > Network Resources > Network Devices > Add. Die Seite Neues Netzwerkgerät wird angezeigt.
- 2. Definieren Sie auf dieser Seite den WLC Name, Management-

Schnittstelle IP Address und Radius Authentications Settings wie Shared Secret. Wenn Sie die AP-MAC-Adressen als Endpunkte eingeben möchten, verwenden Sie das benutzerdefinierte Geräteprofil, das früher konfiguriert wurde, und nicht das Cisco Standardprofil!

| dentity Services Engine         | Home  Context Visibility  Operations  Policy  Administration  Work Centers  License Warning                                  | e, 0     | ۲ | <b>.</b> 0 |
|---------------------------------|--|----------|---|------------|
| System      Identity Management | Network Resources     Device Portal Management pxGrid Services     Feed Service     Threat Centric NAC                       |          |   |            |
| Network Devices Network Device  | Sroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services |          |   |            |
| e                               | Network Devices  |          |   |            |
| Network Devices                 | * Name WLC5520   |          |   |            |
| Default Device                  | Description  |          |   |            |
| Device Security Settings        |  |          |   |            |
|                                 | IP Address 🔹 * IP : 10.48.71.20 / 32   | <u>.</u> |   |            |
|                                 |  |          |   |            |
|                                 | O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected                               |          |   |            |
|                                 | * Device Profile data Cisco V +  |          |   |            |
|                                 |  |          |   |            |
|                                 | Model Name   |          |   |            |
|                                 | Software Version   |          |   |            |
|                                 | * Network Device Group   |          |   |            |
|                                 |  |          |   |            |
|                                 | Location LAB Set To Default  |          |   |            |
|                                 | IPSEC No Set To Default  |          |   |            |
|                                 | Device Type WLC-lab Set To Default   |          |   |            |
|                                 |  |          |   |            |
|                                 | ✓ RADIUS Authentication Settings   |          |   |            |
|                                 |  |          |   |            |
|                                 | RADIUS UDP Settings  |          |   |            |
|                                 | Protocol RADIUS  |          |   |            |
|                                 | Shared secret Show   |          |   |            |
|                                 | CoA Port 1700 Set To Default   |          |   |            |
|                                 | RADIUS DTLS Settings ()  |          |   |            |
|                                 | DTLS Required 🔲 (į)  |          |   |            |
|                                 |  |          |   |            |

3. Klicken Sie auf Submit.

#### Hinzufügen der AP-MAC-Adresse zur Endpunktdatenbank auf der Cisco ISE

Navigieren Sie zu Administration > Identity Management > Identities und fügen die MAC-Adressen der Endpunktdatenbank hinzu.

Fügen Sie die AP-MAC-Adresse der Benutzerdatenbank auf der Cisco ISE hinzu (optional)

Wenn Sie das kabelgebundene MAB-Profil nicht ändern und die AP-MAC-Adresse als Benutzer festlegen möchten, müssen Sie die Anforderungen der Kennwortrichtlinie senken.

 Navigieren Sie zu Administration > Identity Management. In diesem Fall müssen wir sicherstellen, dass die Kennwortrichtlinie die Verwendung des Benutzernamens als Kennwort zulässt und die Richtlinie auch die Verwendung von MAC-Adresszeichen zulässt, ohne dass verschiedene Arten von Zeichen erforderlich sind. Navigieren Sie zu Settings > User Authentication Settings > Password Policy:

| cisco Identity Services Engine  | Home  | License Warning 🔺 | ् 🙂 | 0 0 |
|---------------------------------|---|-------------------|-----|-----|
| System      Identity Management | Network Resources     Device Portal Management     pxGrid Service     Feed Service     Threat Centric NAC |                   |     |     |
| Identities Groups External Iden | ntity Sources Identity Source Sequences Settings  |                   |     |     |
| User Custom Attributes          | Password Policy Account Disable Policy  |                   |     |     |
| User Authentication Settings    | Password Policy   |                   |     |     |
| Endpoint Purge                  | Minimum Length: 4 characters (Valid Range 4 to 127)   |                   |     |     |
| Endpoint Custom Attributes      | Password must not contain:  |                   |     |     |
|                                 | User name or its characters in reverse order  |                   |     |     |
|                                 | "cisco" or its characters in reverse order  |                   |     |     |
|                                 | This word or its characters in reverse order:   |                   |     |     |
|                                 | Repeated characters four or more times consecutively  |                   |     |     |
|                                 | Dictionary words, their characters in reverse order or their letters replaced with other characters ()    |                   |     |     |
|                                 | Default Dictionary  |                   |     |     |
|                                 | Custom Dictionary () Choose File No file chosen   |                   |     |     |
|                                 | The newly added custom dictionary file will replace the existing custom dictionary file.                  |                   |     |     |
|                                 | Password must contain at least one character of each of the selected types:                               |                   |     |     |
|                                 | Lowercase alphabetic characters   |                   |     |     |
|                                 | Uppercase alphabetic characters   |                   |     |     |
|                                 | Vumeric characters  |                   |     |     |
|                                 | Non-alphanumeric characters   |                   |     |     |
|                                 | Password History  |                   |     |     |

2. Navigieren Sie anschließend zu Identities > Users und klicke auf Add. Wenn die Seite User Setup (Benutzereinrichtung) angezeigt wird, definieren Sie den Benutzernamen und das Kennwort für diesen Access Point wie dargestellt.

**Tipp:** Verwenden Sie **Description** um das Passwort einzugeben, damit Sie später leicht wissen, was als Passwort definiert wurde.

Beim Kennwort muss es sich auch um die MAC-Adresse des AP handeln. In diesem Beispiel ist es 4c776d9e6162.

| cisco Identity Services Engine     | Home   Context Visibility   Operations   Policy   Administration   Work Centers  License                  | ise Warning 🔺 | Q 🕑 | 0 |
|------------------------------------|---|---------------|-----|---|
| System      Identity Management    | Network Resources      Device Portal Management pxGrid Services      Feed Service      Threat Centric NAC |               |     |   |
| Groups External Identity           | y Sources Identity Source Sequences + Settings  |               |     |   |
|                                    | Network Access Users List > New Network Access User   |               |     |   |
| Latest Manual Network Scan Results | ▼ Network Access User   |               |     |   |
| Latest manual Network Scan Nesuns  | * Name 4c776d9e6162   |               |     |   |
|                                    | Status Enabled -  |               |     |   |
|                                    | Email   |               |     |   |
|                                    | ▼ Passwords   |               |     |   |
|                                    | Password Type: Internal Users 💌   |               |     |   |
|                                    | Password Re-Enter Password  |               |     |   |
|                                    | * Login Password Generate Password (  |               |     |   |
|                                    | Enable Password Generate Password ()  |               |     |   |
|                                    | * User Information  |               |     |   |
|                                    | First Nama  |               |     |   |
|                                    | Fusi Name   |               |     |   |
|                                    |   |               |     |   |
|                                    | * Account Options   |               |     |   |
|                                    | Description pass=4c776d9e6162   | /             |     |   |
|                                    | Change password on next login   |               |     |   |
|                                    | w Assound Disoble Deller  |               |     |   |
|                                    |   |               |     |   |
|                                    | Disable account if date exceeds 2019-04-28 (yyyy-mm-dd)   |               |     |   |
|                                    | ▼ User Groups   |               |     |   |
|                                    |   |               |     |   |
|                                    | APS 📀   |               |     |   |
|                                    | Submit Cancel   |               |     |   |

3. Klicken Sie auf submit.

1. Definieren Sie eine Policy Set , um die Authentifizierungsanforderung vom WLC abzugleichen. Zuerst erstellen Sie eine Bedingung, indem Sie zu navigieren Policy > Policy Elements > Conditionsund eine neue Bedingung entsprechend dem

WLC-Standort erstellt, in diesem Beispiel "LAB\_WLC" und Radius:Service-Type Equals Call Check die für die Mac-Authentifizierung verwendet wird. Hier wird die Bedingung 'AP\_Auth' genannt.

| cisco Identity Services Engine  | Home   |        | → Work Centers L    | icense Warning 🔺 🔍 👴 💿 | - 44  |
|---------------------------------|--|--------|---------------------|------------------------|-------|
| Policy Sets Profiling Posture C | Client Provisioning - Policy Elements                                      |        |                     |                        |       |
| Dictionaries Conditions Resu    | ilts   |        |                     |                        |       |
| ( library Candilians            | Library  | Editor |                     |                        |       |
| Smart Conditions                | Search by Name   |        |                     |                        | · · · |
| Time and Date                   |  |        | Radius Service-Type |                        |       |
| Profiling                       |  | 0 b 🕈  | Fouals V Call Check | - m)                   |       |
| Posture                         | AP_Auth  |        | eduna               |                        |       |
| - Network Conditions            | Condition for authe/authz of APs.  | AND V  | LAB_WLC             |                        | 0     |
| Endstation Network Conditions   | BYOD_is_Registered   | 1777   |                     |                        |       |
| Device Network Conditions       | device that has passed the NSP   | 0      | + New AN            | DOR                    |       |
| Device Port Network Conditions  | process  |        |                     |                        | -     |
|                                 | Catalyst_Switch_Local_Web_Authe  | Set    | to 'Is not'         | Duplicate Sav          | e     |
|                                 | Default condition used to match  | D      |                     |                        | _     |
|                                 | aumentication requests for Local Web<br>Authentication from Cisco Catalyst |        |                     |                        |       |
|                                 | Switches   |        |                     |                        |       |

- 2. Klicken Sie auf save.
- 3. Erstellen Sie dann eine neue Allowed Protocols Service für die AP-Authentifizierung. Wählen Sie nur Allow PAP/ASCII:

| cisco Identity Services Engine     | Home  | Operations     Policy | Administration     Work Centers | License Warning 🔺 | 0, 0 | 0 0 |     |
|------------------------------------|---|-----------------------|---------------------------------|-------------------|------|-----|-----|
| Policy Sets Profiling Posture Clie | ent Provisioning    Policy Elements                 | 5                     |                                 |                   |      |     |     |
| Dictionaries Conditions Results    |   |                       |                                 |                   |      |     |     |
| <ul> <li>Authentication</li> </ul> | Allowed Protocols Services List > Allowed Protocols | AP_authentication     |                                 |                   |      |     |     |
| Allowed Protocols                  | Name AP_authenticatio                               | n                     |                                 |                   |      |     | - 1 |
| Authorization                      | Description   |                       |                                 |                   |      |     | - 1 |
| Profiling                          |   |                       |                                 |                   |      |     | - 1 |
| Posture                            |   |                       |                                 |                   |      |     |     |
| Client Provisioning                | Authentication Bypass                               | up (j)                |                                 |                   |      |     |     |
|                                    | Authentication Protoco                              | bis                   |                                 |                   |      |     |     |
|                                    | Allow CHAP  |                       |                                 |                   |      |     | - 1 |
|                                    | Allow MS-CHAPv1                                     |                       |                                 |                   |      |     | - 1 |
|                                    | Allow MS-CHAPv2                                     |                       |                                 |                   |      |     | - 1 |
|                                    | Allow EAP-MD5                                       |                       |                                 |                   |      |     | - 1 |
|                                    | Allow EAP-TLS                                       |                       |                                 |                   |      |     | - 1 |
|                                    | Allow LEAP  |                       |                                 |                   |      |     | - 1 |
|                                    | Allow PEAP  |                       |                                 |                   |      |     |     |

4. Wählen Sie den zuvor erstellten Service im Allowed Protocols/Server Sequence. Erweitern Sie die View und unter Authentication Policy > Use > Internal Users sodass die ISE die interne DB nach dem Benutzernamen/Kennwort des AP durchsucht.

| cy sets Profiling Posture Client Prov  | isloning   Policy Elements   |   |                                      |                    |               |                |
|--|------------------------------|---|--------------------------------------|--------------------|---------------|----------------|
| cy Sets  |                              |   |                                      | F                  | leset         | Save           |
| Status Policy Set Name   | Description                  | Conditions                                | Allowed Protocols / Server Sequences | uence Hits         | Actions       | Vie            |
| arch   |                              | $\frown$                                  |                                      | _                  |               |                |
| Policy4APsAuth   |                              | AP_Auth                                   | AP_authentication * *                | • + 19             | ٥             | 0              |
| O Default  | Default policy set           |   | Default Network Access *             | • + 591            | ٥             | >              |
|  |                              |   |                                      | 3                  | Reset         | Save           |
| ' Identity Services Engine Home  | Context Visibility      O    | perations -Policy + Administration + Work | c Centers License Wa                 | iming 🔺 🔍          | 9 (           | 0              |
| cy Sets Profiling Posture Client Prov  | visioning    Policy Elements |   |                                      |                    |               |                |
| Otatus Delinu Oot Marro  | Description                  | Conditions                                | Allowed Pro                          | ntocols / Server S | equence       | H              |
| Status Policy Set Name   | Dependant                    | Conditione                                | 100000110                            |                    | equence       |                |
| arch   | Description                  | AP_Auth                                   | AP_authent                           | lication           | x + +         | 1              |
| Policy Set Name  | Company                      | AP_Auth                                   | AP_authent                           | lication           | × • +         | ] 1            |
| Policy Set Name  | Coonplant                    | AP_Auth                                   | (AP_authent                          | lication           | x * +         | ] 15           |
| Policy Set Name Policy Set Name Policy 4APsAuth Authentication Policy (1)  + Status Rule Name  | Conditions                   | AP_Auth                                   | (AP_authent<br>Use                   | lication           | × • +<br>Hits | ) 11<br>Action |
| Policy Set Name Policy Set Name Policy 4APsAuth Policy (1)  Status Rule Name earch   | Conditions                   | AP_Auth                                   | (AP_authent<br>Use                   | lication           | × • +<br>Hits | ) 19<br>Action |
| Policy Set Name Policy Set Name Policy 4APsAuth Policy (1)  Status Rule Name Policy Contemport   | Conditions                   | AP_Auth                                   | AP_authent<br>Use                    | lication           | × • +         | ) 1            |
| Policy Set Name Policy Set Name Policy APSAuth Policy (1)  Status Rule Name Rearch Default   | Conditions                   | AP_Auth                                   | Use<br>Internal Users<br>> Options   | ication<br>× •     | Hits          | Action         |
| Status Policy Set Name  arch  Policy4APsAuth  Authentication Policy (1)    Status Rule Name  rearch  Default  Authorization Policy - Local Exceptions  | Conditions                   | AP_Auth                                   | Use<br>Internal Users<br>Options     | x v                | Hits          | 11<br>Action   |
| Status Policy Set Name  arch  Policy4APsAuth  Authentication Policy (1)  + Status Rule Name  earch  Default  Authorization Policy - Local Exceptions  Authorization Policy - Global Exceptions | Conditions                   | AP_Auth                                   | Use<br>Internal Users<br>Options     | ication<br>× •     | Hits          | Action         |

5. Klicken Sie auf Save.

#### Überprüfung

Um diese Konfiguration zu überprüfen, müssen Sie den AP mit der MAC-Adresse 4c:77:6d:9e:61:62 an das Netzwerk und den Monitor anschließen. Verwenden Sie debug capwap events/errors enable und debug aaa all enable Befehle, um dies auszuführen.

Wie aus den Debugs ersichtlich, hat der WLC die AP-MAC-Adresse an den RADIUS-Server 10.48.39.128 übergeben, und der Server hat den AP erfolgreich authentifiziert. Der WAP registriert sich dann beim Controller.

**Anmerkung:** Einige Zeilen in der Ausgabe wurden aufgrund von Platzbeschränkungen in die zweite Zeile verschoben.

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already alloced index 437 \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP

192.168.79.151:5248, already allocated index 437 \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved) \*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from temporary database. \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc. \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap\_wtp\_event\_response, state Capwap\_no\_state \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap\_wtp\_event\_response is not allowed to send in state Capwap\_no\_state for AP 192.168.79.151 \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed! \*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248 \*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248 \*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 \*aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001 \*aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8 \*aaaQueueReader: Feb 27 14:58:07.566: Callback..... \*aaaQueueReader: Feb 27 14:58:07.566: proxyState......70:69:5A:51:4E:C0-00:00 \*aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs: \*aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id......70:69:5a:51:4e:c0 (17 bytes) \*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes) \*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) \*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes) (28271) (2 bytes) \*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) \*aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate:
RADIUS server is ready 10.48.39.128 port 1812 index 1 active 1

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual \*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list \*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into gid:0 of server at index:1 \*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130 \*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812 from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00 \*aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6d .....Zm \*aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61 \*aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51: \*aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d: \*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 01 04 06 9e:61:62.... \*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a\*8 \*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l.... \*aaaQueueReader: Feb 27 14:58:07.566: 0000080: 15 f9 .. \*aaaOueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client. \*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9) \*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 \*\*\* Counted VSA 150994944 AVP of length 28, code 1 atrlen 22) \*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9) \*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22 \*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk \*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown \*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes \*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128 (qid:0) with port:1812, pktId:185 \*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1) \*radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x00000001 \*radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00 \*radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs: \*radiusTransportThread: Feb 27 14:58:07.588: AVP[01] User-Name.....4c776d9e6162 (12 bytes) \*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (65 bytes)

\*radiusTransportThread: Feb 27 14:58:07.588: AVP[03]
Class.....DATA (83 bytes)

```
*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-
Authenticator......DATA (16 bytes)
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

### Fehlerbehebung

Verwenden Sie die folgenden Befehle zur Fehlerbehebung in Ihrer Konfiguration:

- debug capwap events enable—Konfiguriert das Debuggen von LWAPP-Ereignissen
- debug capwap packet enable—Konfiguriert das Debuggen von LWAPP Packet Trace
- debug capwap errors enable—Konfiguriert das Debuggen von LWAPP-Paketfehlern
- debug aaa all enable—Konfiguriert das Debugging aller AAA-Nachrichten

Wenn die ISE im RADIUS-Live-Protokoll den Benutzernamen "UNGÜLTIG" meldet, wenn die APs für die ISE autorisiert werden, bedeutet dies, dass die Authentifizierung anhand der Endpunktdatenbank überprüft wird und Sie das verkabelte MAB-Profil nicht wie in diesem Dokument beschrieben geändert haben. Die ISE betrachtet eine MAC-Adressauthentifizierung als ungültig, wenn sie nicht mit dem Wired/Wireless MAB-Profil übereinstimmt, das standardmäßig das NAS-Port-Attribut erfordert, das nicht vom WLC gesendet wird.

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.