Konfigurieren der lokalen EAP-Authentifizierung auf dem Catalyst 9800 WLC

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von lokalem EAP auf Catalyst 9800 WLCs (Wireless LAN-Controllern) beschrieben.

Voraussetzungen

Anforderungen

In diesem Dokument wird die Konfiguration von Local EAP (Extensible Authentication Protocol) auf Catalyst 9800 WLCs beschrieben, d. h. der WLC fungiert als RADIUS-Authentifizierungsserver für die Wireless-Clients.

In diesem Dokument wird davon ausgegangen, dass Sie mit der grundlegenden Konfiguration eines WLAN auf dem 9800 WLC vertraut sind und sich nur auf den WLC konzentrieren, der als lokaler EAP-Server für Wireless-Clients fungiert.

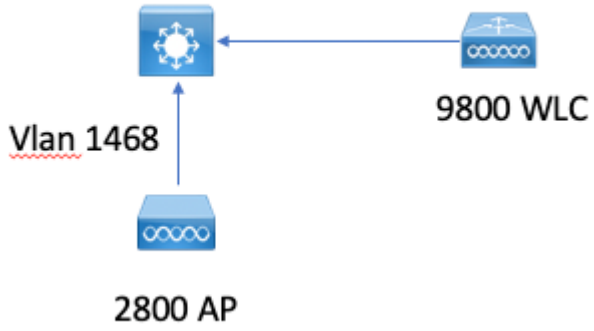
Verwendete Komponenten

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 kennen.

Catalyst 9800 auf Version 16.12.1s

Konfigurieren

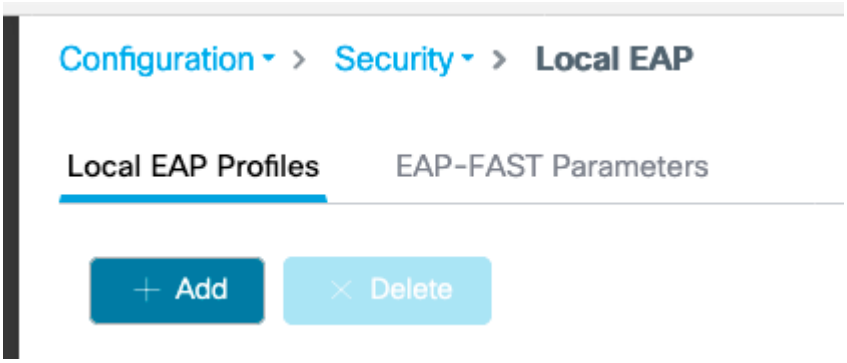
Netzwerkdiagramm



Lokale EAP-Hauptkonfiguration

Schritt 1: Lokales EAP-Profil

Gehen Sie zu **Configuration > Security > Local EAP** in der 9800 Web UI.

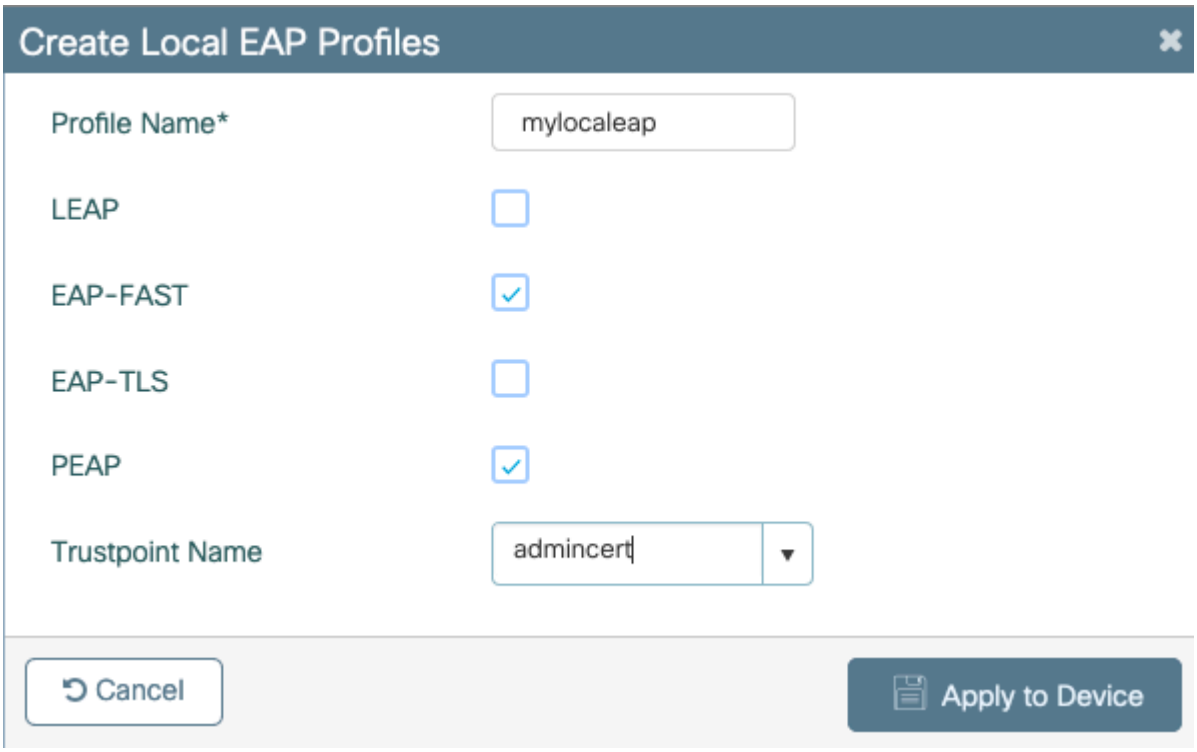


Hinzufügen auswählen

Geben Sie einen Profilnamen ein.

Es wird nicht geraten, LEAP aufgrund seiner schwachen Sicherheit zu verwenden. Bei allen anderen drei EAP-Methoden müssen Sie einen Vertrauenspunkt konfigurieren. Der Grund hierfür ist, dass der 9800, der als Authentifizierer fungiert, ein Zertifikat senden muss, damit der Client ihm vertrauen kann.

Clients vertrauen dem WLC-Standardzertifikat nicht. Daher müssen Sie die Überprüfung des Serverzertifikats auf der Clientseite deaktivieren (nicht empfohlen) oder einen Zertifikatvertrauenspunkt auf dem 9800 WLC installieren, dem der Client vertraut (oder ihn manuell in den Client-Vertrauensspeicher importieren).



CLI:

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Schritt 2: AAA-Authentifizierungsmethode

Sie müssen eine AAA dot1x-Methode konfigurieren, die auch lokal zeigt, um die lokale Benutzerdatenbank zu verwenden (Sie können jedoch z. B. eine externe LDAP-Suche verwenden).

Gehen Sie zu **Konfiguration > Sicherheit > AAA**, und gehen Sie zur Registerkarte **AAA-Methodenliste** für die **Authentifizierung**. Wählen Sie **Hinzufügen aus.**

Wählen Sie den Typ "dot1x" und den lokalen Gruppentyp aus.

Schritt 3: Konfigurieren einer AAA-Autorisierungsmethode

Wechseln Sie zur Unterregisterkarte **Autorisierung**, und erstellen Sie eine neue Methode zum **Herunterladen von Anmeldeinformationen,** und zeigen Sie sie auf lokal.

Gleiches für den Autorisierungstyp **des Netzwerks** tun

CLI:

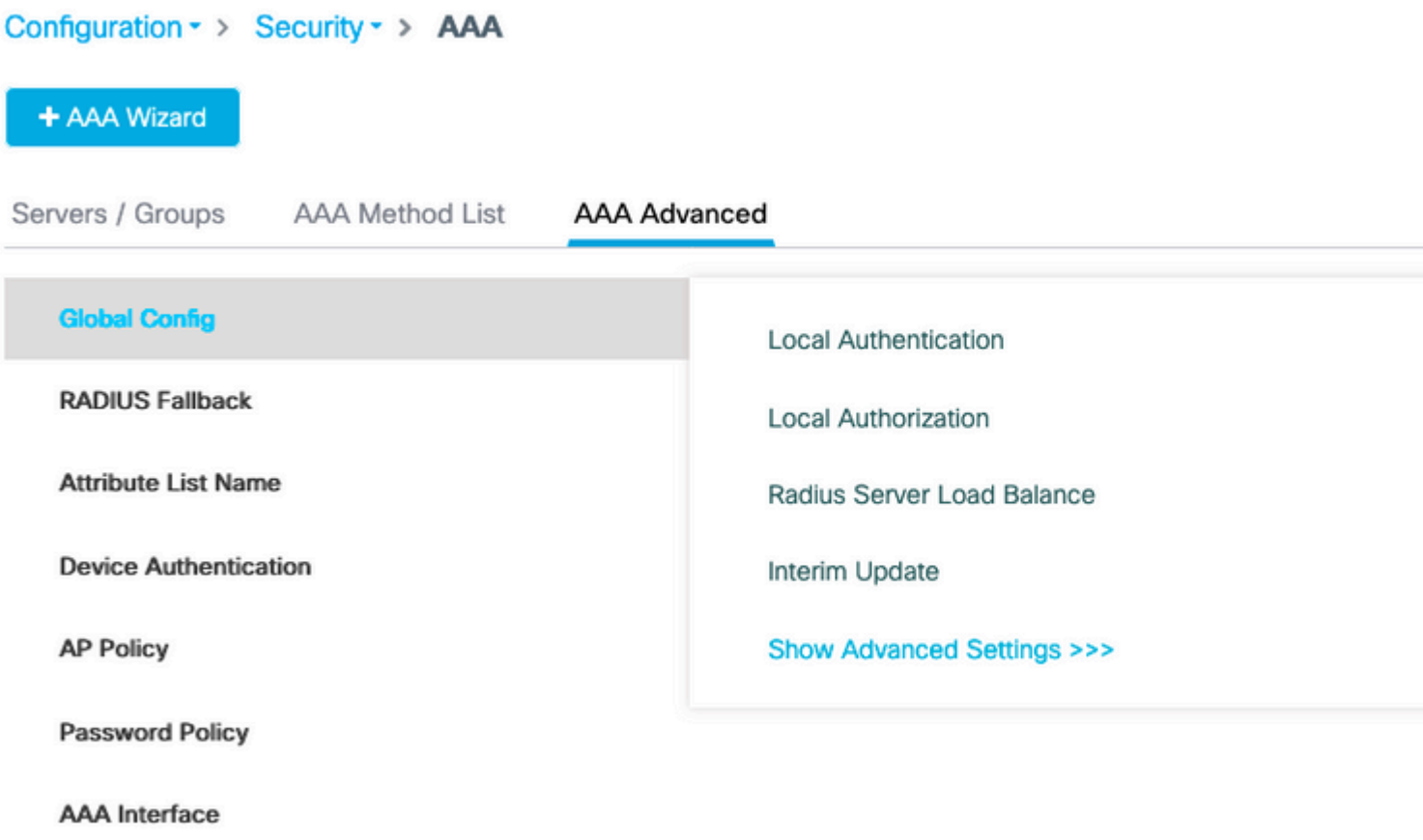
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Schritt 4: Lokale erweiterte Methoden konfigurieren

Wechseln Sie zur Registerkarte **"AAA Advanced**".

Definieren Sie die lokale Authentifizierungs- und Autorisierungsmethode. Da in diesem Beispiel die Methoden "default" credential-download und "Default" dot1x verwendet wurden, müssen Sie hier die Standardeinstellungen für die lokalen Authentifizierungs- und Autorisierungs-Dropdown-Felder festlegen.

Wenn Sie benannte Methoden definiert haben, wählen Sie im Dropdown-Menü "Methodenliste" aus, und in einem anderen Feld können Sie den Methodennamen eingeben.



CLI:

```
aaa local authentication default authorization default
```

Schritt 5: Konfigurieren eines WLAN

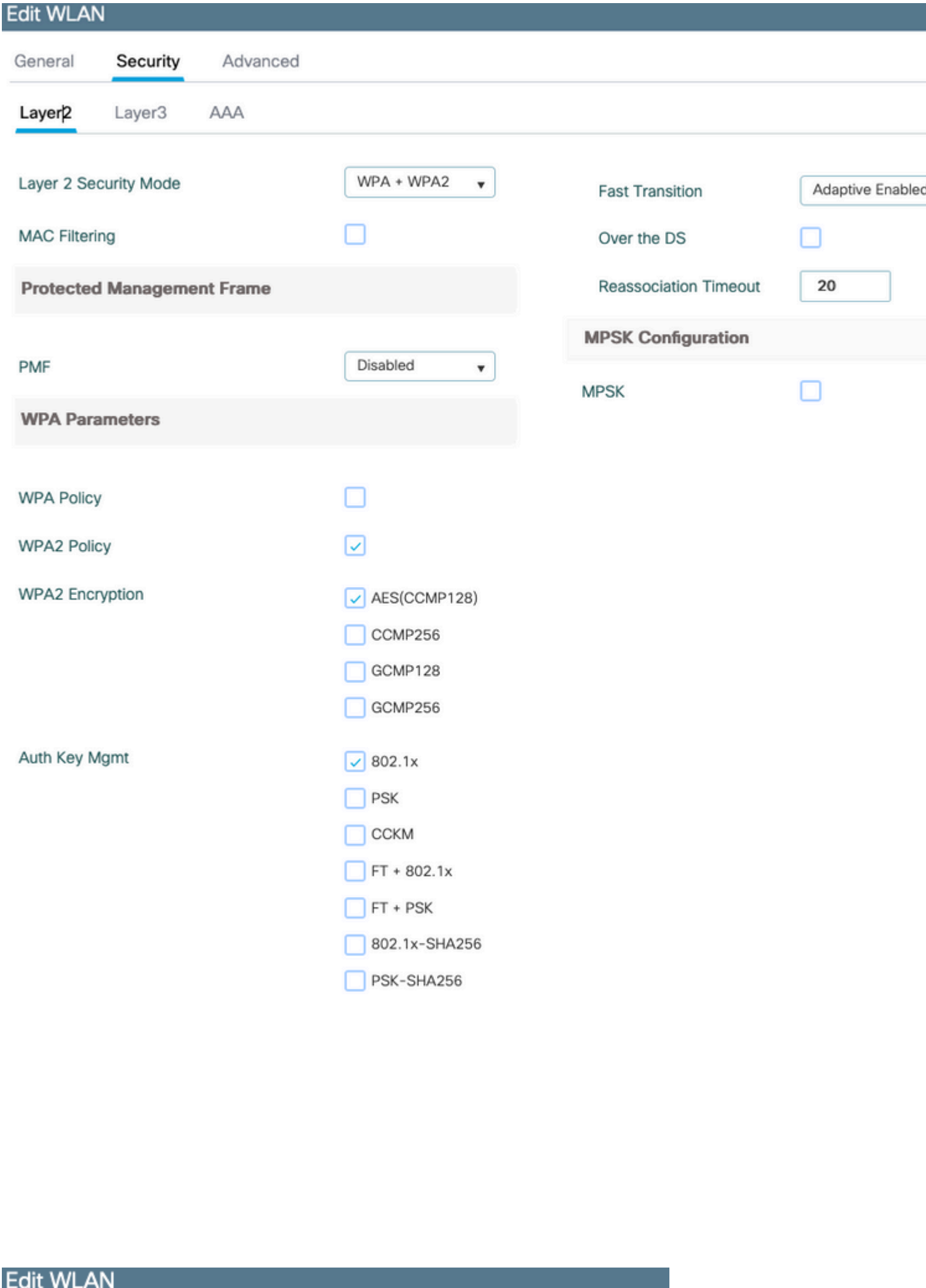
Anschließend können Sie Ihr WLAN für 802.1x-Sicherheit anhand des im vorherigen Schritt definierten lokalen EAP-Profils und der AAA-Authentifizierungsmethode konfigurieren.

Gehen Sie zu Konfiguration > Tags und Profile > WLANs > + Hinzufügen >

Geben Sie die SSID und den Profilnamen an.

Die Option "Punkt1x-Sicherheit" ist standardmäßig unter "Layer 2" ausgewählt.

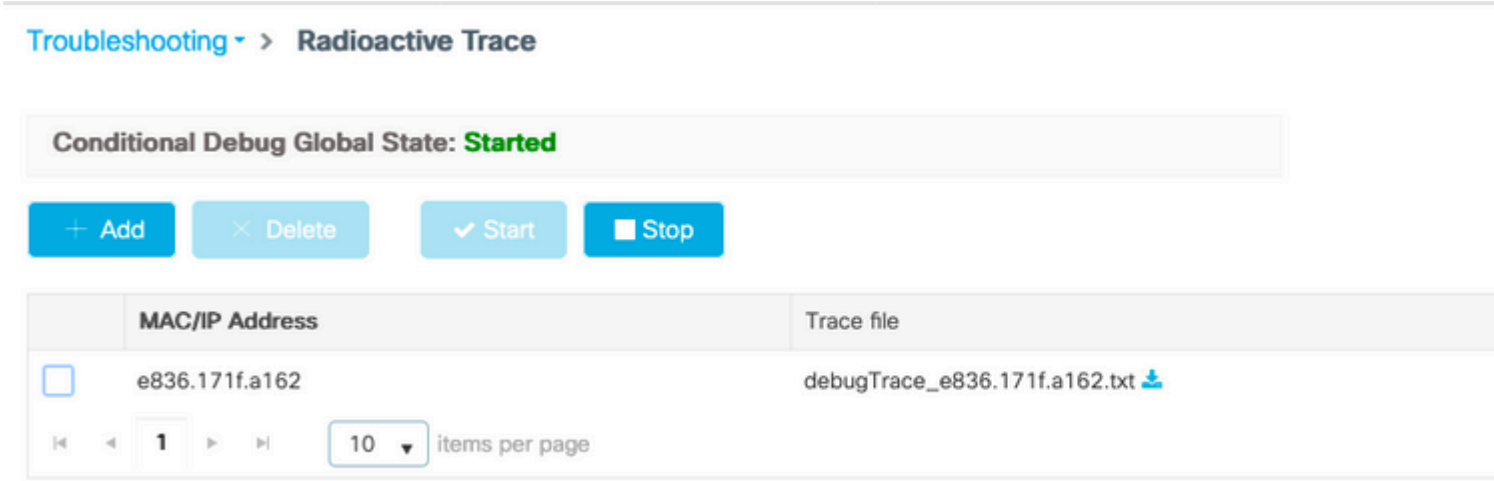
Wählen Sie unter AAA Local EAP Authentication (Lokale EAP-Authentifizierung) aus, und wählen Sie Local EAP profile and AAA Authentication list (Lokales EAP-Profil und AAA-Authentifizierungsliste) aus dem Dropdown-Menü.


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK
Edit WLAN

16.12 und frühere Versionen nur TLS 1.0 für die lokale EAP-Authentifizierung unterstützen. Dies kann zu Problemen führen, wenn Ihr Client nur TLS 1.2 unterstützt, wie es immer üblicher wird. Cisco IOS® XE 17.1 und höher unterstützt TLS 1.2 und TLS 1.0.

Verwenden Sie RadioActive Tracing, um einen bestimmten Client zu behandeln, der Probleme bei der Verbindung hat. Gehen Sie zu **Troubleshooting > RadioActive Trace,** und fügen Sie die Client-MAC-Adresse hinzu.

Wählen Sie **Start** aus, um die Ablaufverfolgung für diesen Client zu aktivieren.



Nachdem das Problem reproduziert wurde, können Sie die Schaltfläche **Generate (Generieren)** auswählen, um eine Datei zu erstellen, die die Debugausgabe enthält.

Beispiel für einen Client, der aufgrund eines falschen Kennworts keine Verbindung herstellen kann

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
```

```
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAPV
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAST
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rais
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication failed
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

Nachverfolgung bei Ausfall

Es ist möglich, die Liste der Fehlerereignisse für eine bestimmte MAC-Adresse mit dem Befehl trace-on-failure zu überprüfen, selbst wenn keine Debugging-Funktionen aktiviert sind.

Im nächsten Beispiel war die AAA-Methode zunächst nicht vorhanden (AAA-Serverausfall), und einige Minuten später verwendete der Client falsche Anmeldeinformationen.

Der Befehl **show logging trace-on-failure summary** in Version 16.12 und früher lautet **show logging profile wireless (filter mac <mac>) trace-on-failure** in Cisco IOS® XE 17.1 und höher. Es gibt keinen technischen Unterschied, außer dass 17.1 und höher Ihnen erlaubt, nach der MAC-Adresse des Clients zu filtern.

```
Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.
Time                          UUID                 Log

--------------------------------------------------------------------------------------------------


2019/10/30 14:51:04.438     0x0      SANET_AUTHC_FAILURE - AAA Server Down username , audit session id 0
2019/10/30 14:58:04.424     0x0      e836.171f.a162 CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN pr
```

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.