

Lokale Webauthentifizierung mit lokaler Authentifizierung konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Parameterzuordnung](#)

[Datenbank für die Authentifizierung](#)

[Konfigurieren](#)

[Lokale Webauthentifizierung mit lokaler Authentifizierung in der CLI](#)

[MethodenlistenFürLokaleAuthentifizierung](#)

[Parameterzuordnungen](#)

[WLAN-Sicherheitsparameter](#)

[Richtlinienprofil erstellen](#)

[Policy-Tag erstellen](#)

[Zuweisen eines Richtlinien-Tags zu einem AP](#)

[Gastbenutzername erstellen](#)

[Lokale Webauthentifizierung mit lokaler Authentifizierung über die WebUI](#)

[Überprüfung](#)

[Lokale Web-Authentifizierung auf lokalem FlexConnect-Switching](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die lokale Webauthentifizierung mit der lokalen Authentifizierung auf einem Wireless LAN Controller (WLC) der Serie 9800 konfigurieren.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse des Konfigurationsmodells des 9800 WLC verfügen.

Anforderungen

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

- Cisco WLC der Serie 9800
- Umfassende Kenntnisse der Web-Authentifizierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800-CL WLC Cisco IOS® XE Version 17.12.5
- Cisco Access Point C9117AXI:

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.

Hintergrundinformationen

Local Web Authentication (LWA) ist eine Authentifizierungsmethode für das Wireless Local Area Network (WLAN), die auf dem WLC konfiguriert werden kann. Wenn ein Benutzer das WLAN aus der Liste der verfügbaren Netzwerke auswählt, wird er zu einem Webportal weitergeleitet. In diesem Portal kann der Benutzer je nach Konfiguration aufgefordert werden, einen Benutzernamen und ein Kennwort einzugeben, eine Richtlinie für die akzeptable Nutzung (Acceptable Use Policy, AUP) zu akzeptieren oder eine Kombination aus beiden Aktionen durchzuführen, um die Verbindung abzuschließen.

Informationen zu den vier Arten von Web-Authentifizierungsseiten, die während des Anmeldevorgangs angezeigt werden, finden Sie im Leitfaden [Konfigurieren der lokalen Web-Authentifizierung](#), und überprüfen Sie die verfügbaren Optionen für den Web-Authentifizierungstyp. Weitere Informationen finden Sie im Abschnitt [Authentifizierungstypen im Handbuch Lokale Webauthentifizierung mit externer Authentifizierung konfigurieren](#).

Parameterzuordnung

Die Parameterzuordnung ist ein wichtiges Konfigurationselement auf einem WLC, das die Webauthentifizierung aktiviert. Es besteht aus einer Reihe von Einstellungen, die verschiedene Aspekte des Web-Authentifizierungsprozesses steuern, darunter den Authentifizierungstyp, Umleitungs-URLs, angehängte Parameter, Timeouts und benutzerdefinierte Webseiten. Um die webbasierte Authentifizierung für eine bestimmte SSID zu aktivieren und zu verwalten, muss diese Zuordnung mit dem WLAN-Profil verknüpft werden.

Der Wireless LAN Controller verfügt über eine globale Standardparameterzuordnung, Administratoren können jedoch benutzerdefinierte Parameterzuordnungen erstellen, um das Web-Authentifizierungsverhalten an spezifische Anforderungen anzupassen.

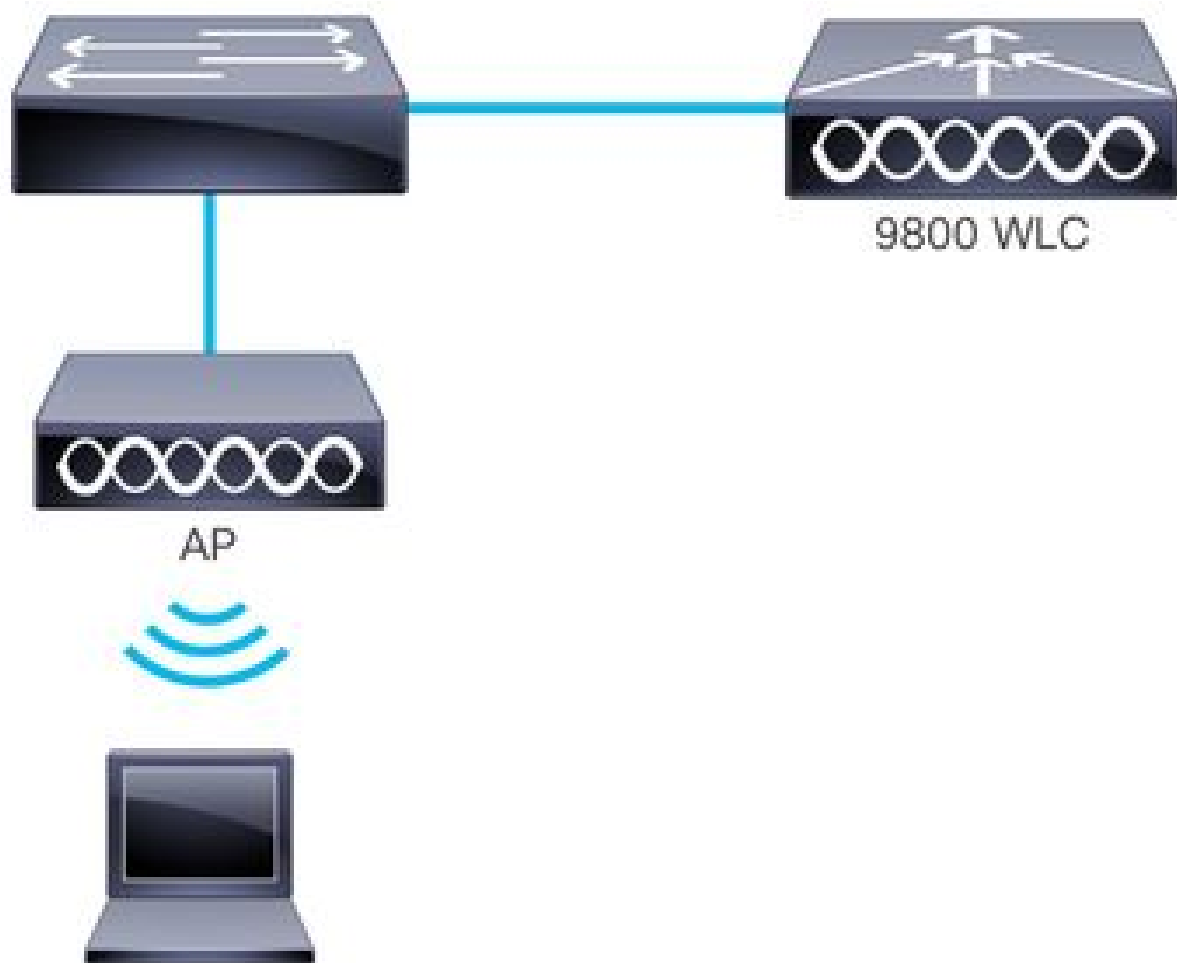
Datenbank für die Authentifizierung

Wenn die Parameterzuordnung für die Verwendung eines Benutzernamens und Kennworts konfiguriert ist, müssen Sie die Authentifizierungsdaten definieren, die lokal im WLC gespeichert werden. Wenn Sie ein Gastbenutzerkonto über die GUI erstellen, können Sie die maximale Anzahl

gleichzeitiger Anmeldungen pro Gastkonto festlegen. Gültige Werte liegen zwischen 0 und 64, wobei 0 bedeutet, dass für diesen Gastbenutzer unbegrenzte gleichzeitige Anmeldungen zulässig sind.

LWA ist in erster Linie für kleine Bereitstellungen vorgesehen. Es unterstützt die Integration mit anderen Authentifizierungsmethoden, können Sie die [unterstützte Kombination von Authentifizierungen für einen Client](#) für weitere Informationen überprüfen.

Das Bild stellt eine generische LWA-Topologie dar:



Generische LWA-Topologie mit lokaler Authentifizierung

Geräte in der Netzwerktopologie von LWA:

- Client/Supplicant: Initiiert eine Verbindungsanforderung an das WLAN, später an die DHCP- und DNS-Server, und antwortet auf Mitteilungen vom WLC.
- Access Point: Ist mit einem Switch verbunden, überträgt er das Gast-WLAN und stellt Wireless-Verbindungen zu Gast-Geräten bereit. Er lässt DHCP- und DNS-Datenverkehr zu, bevor der Gastbenutzer die Authentifizierung abschließt, indem er gültige

Anmeldeinformationen eingibt, eine AUP akzeptiert oder eine Kombination aus beiden Aktionen ausführt.

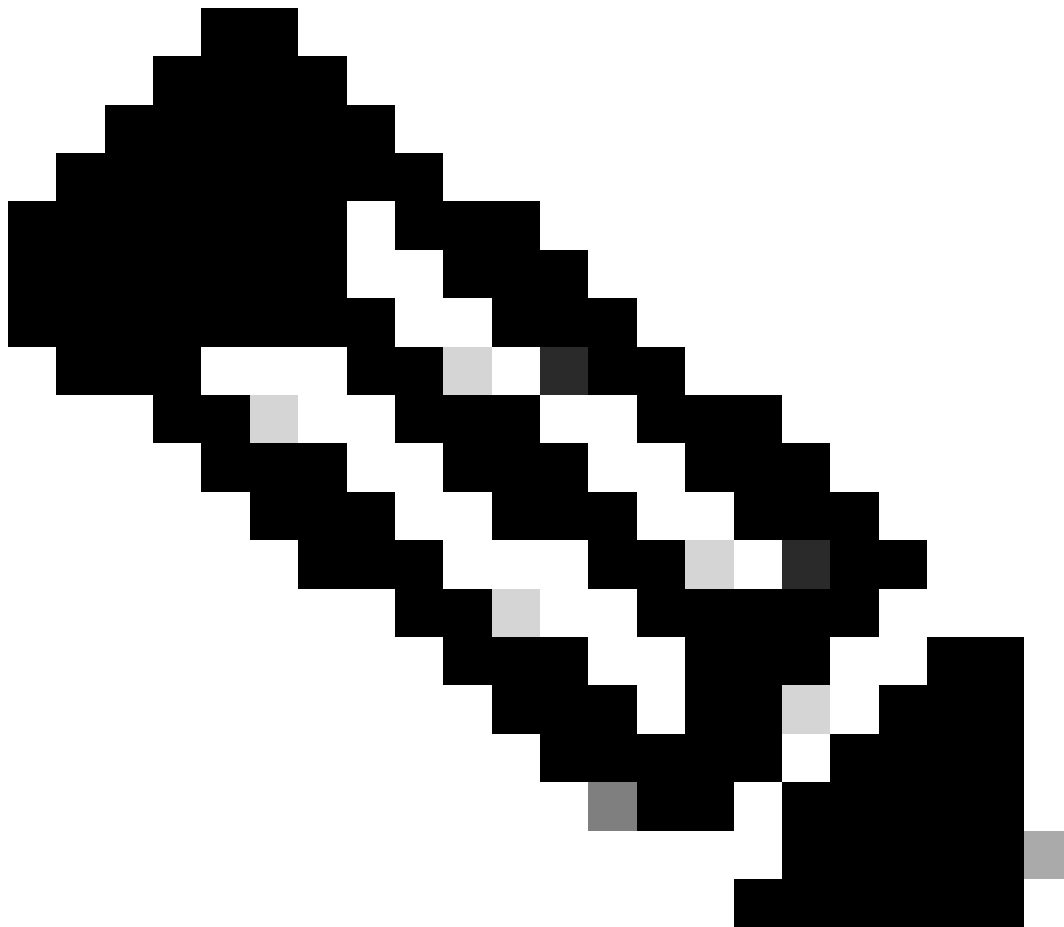
- WLC/Authentifizierer: Verwaltet die APs und Client-Geräte. Der WLC hostet die Umleitungs-URL und erzwingt die Zugriffskontrollliste (Access Control List, ACL), die den Datenverkehr regelt und die beim Konfigurieren der Parameterzuordnung standardmäßig erstellt wird. HTTP-Anfragen von Gastbenutzern werden abgefangen und an ein Webportal (Anmeldeseite) weitergeleitet, in dem sich die Benutzer authentifizieren müssen. Der WLC erfasst Benutzeranmeldeinformationen, authentifiziert Gäste und überprüft die lokale Datenbank auf die Gültigkeit der Anmeldeinformationen.
- Authentifizierungsserver: In diesem Szenario fungiert der WLC als Authentifizierungsserver. Es überprüft die Anmeldeinformationen des Gastbenutzers und gewährt oder verweigert den Netzwerkzugriff entsprechend.

Konfigurieren

Lokale Webauthentifizierung mit lokaler Authentifizierung in der CLI

Methodenlisten für die lokale Authentifizierung

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



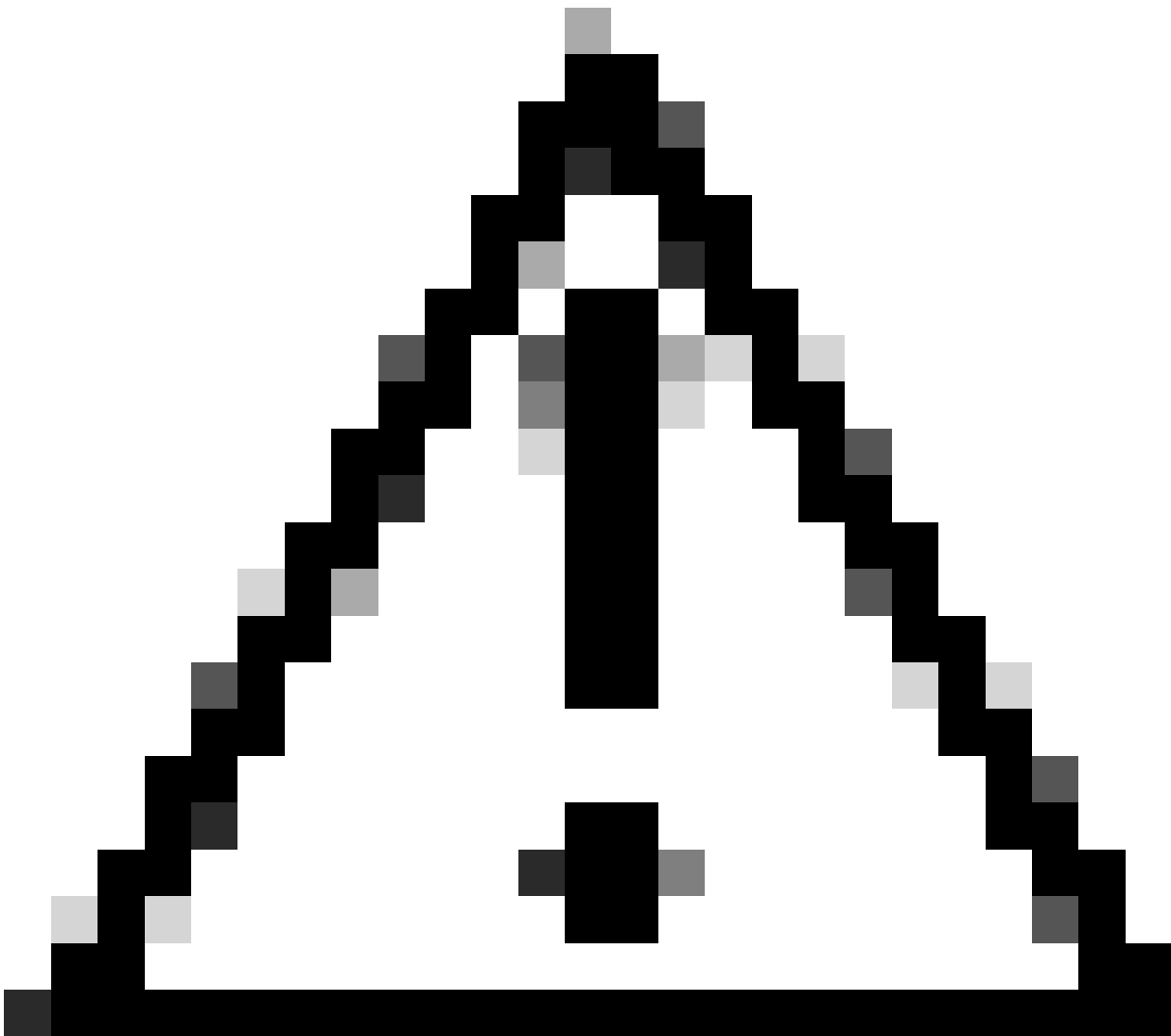
Anmerkung: Damit die Liste der lokalen Anmeldemethoden funktioniert, stellen Sie sicher, dass auf dem WLC die Konfiguration `aaaauthentication network default local` vorhanden ist. Dies ist erforderlich, da der WLC den Benutzer zum Netzwerk autorisiert.

Parameterzuordnungen

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



Vorsicht: Bei der virtuellen IP muss es sich um eine auf RFC 5737 vorgeschlagene, nicht routbare Adresse handeln. Standardmäßig ist IP 192.0.2.1 festgelegt. Weitere Informationen zu virtuellen IP-Adressen finden Sie in den [Best Practices für die Konfiguration der Cisco Catalyst Serie 9800](#). Auf AireOs wurde die meiste Zeit 1.1.1.1 verwendet. Dies wird nicht mehr empfohlen, da es sich um eine öffentliche IP handelt.

Die Möglichkeit, mehrere Parameterzuordnungen zu erstellen, ermöglicht maßgeschneiderte Abläufe: benutzerdefinierte Webseiten und spezifische Präsentationsparameter für jedes WLAN. Die globale Parameterzuordnung bestimmt den Trustpoint und damit das Zertifikat, das der WLC dem Client im Umleitungsportal vorlegt. Darüber hinaus steuert es die Typen des abgefangenen

Client-Datenverkehrs, z. B. HTTP/HTTPS für das Umleitungsportal, die Auflösung von Domänen- oder Hostnamen für die virtuelle IP-Adresse. Durch diese Trennung kann die globale Zuordnung übergeordnete Einstellungen wie Zertifikatsdarstellung und Überwachung des Datenverkehrs verarbeiten, während benutzerdefinierte Parameterzuordnungen ein umfassendes Anwendererlebnis pro WLAN ermöglichen.

WLAN-Sicherheitsparameter

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Richtlinienprofil erstellen

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

Policy-Tag erstellen

```
9800WLC>enable
```

```
9800WLC#configure terminal
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

```
9800WLC(config-policy-tag)# end
```

Zuweisen eines Richtlinien-Tags zu einem AP

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap
```

```
>
```

```
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
```

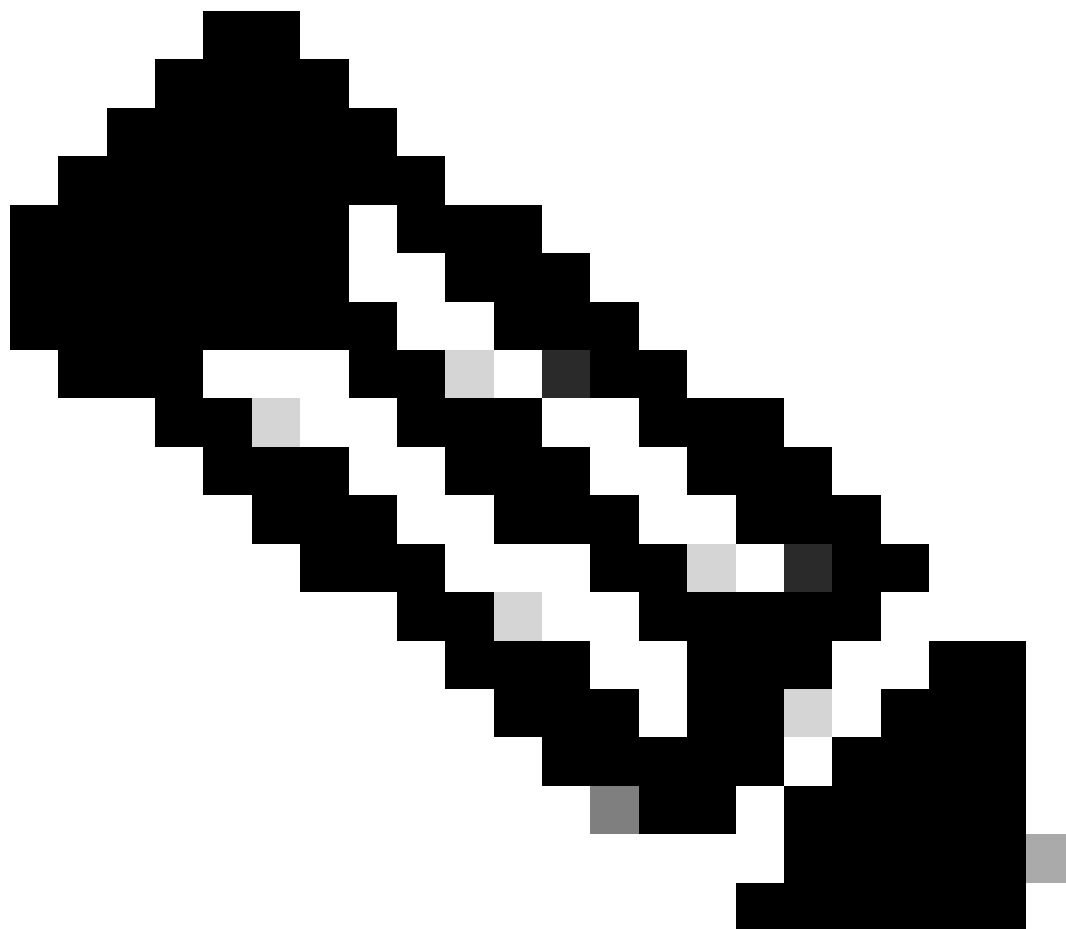
```
9800WLC(config-ap-tag)#end
```

Gastbenutzername erstellen

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description
```

```
guest-user lifetime year 0 month 11 day 30 hour 23
```

```
9800WLC(config-user-name)#end
```

Anmerkung: Wenn Sie die Lebensdauer für den Gastbenutzer auf 1 festlegen, können Sie die nachfolgenden Parameter nicht angeben, d. h. Monate, Tage, Stunden und Minuten, da die maximale Lebensdauer 1 Jahr beträgt.

Lokale Webauthentifizierung mit lokaler Authentifizierung über die WebUI

Methodenlisten für die lokale Authentifizierung

Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication > Add, um die Methodenliste für die spätere Verwendung in der WLAN-Konfiguration zu erstellen.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	login	local	N/A	N/A

Quick Setup: AAA Authentication

Method List Name*

LWA-AUTHENTICATION

Type*

login

Group Type

local

Available Server Groups

radius

ldap

tacacs+

AAA-group

>

<

>>

<<

Assigned Server Groups

^

^

v

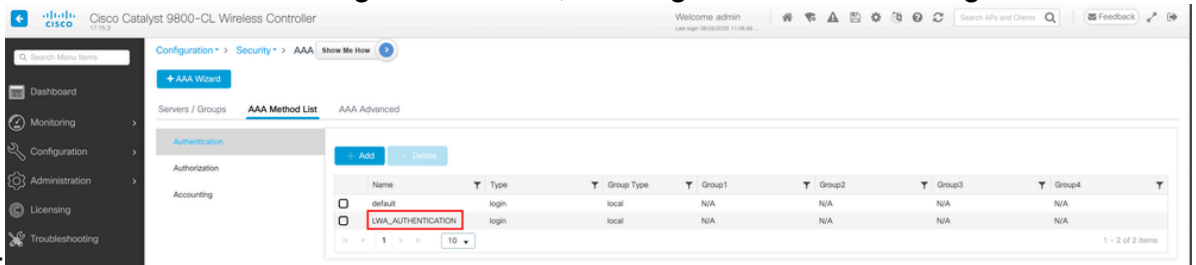
v

Cancel

Apply to Device

Nachdem Sie auf Auf Gerät anwenden geklickt haben, bestätigen Sie die Erstellung der AAA-

Methodenliste:



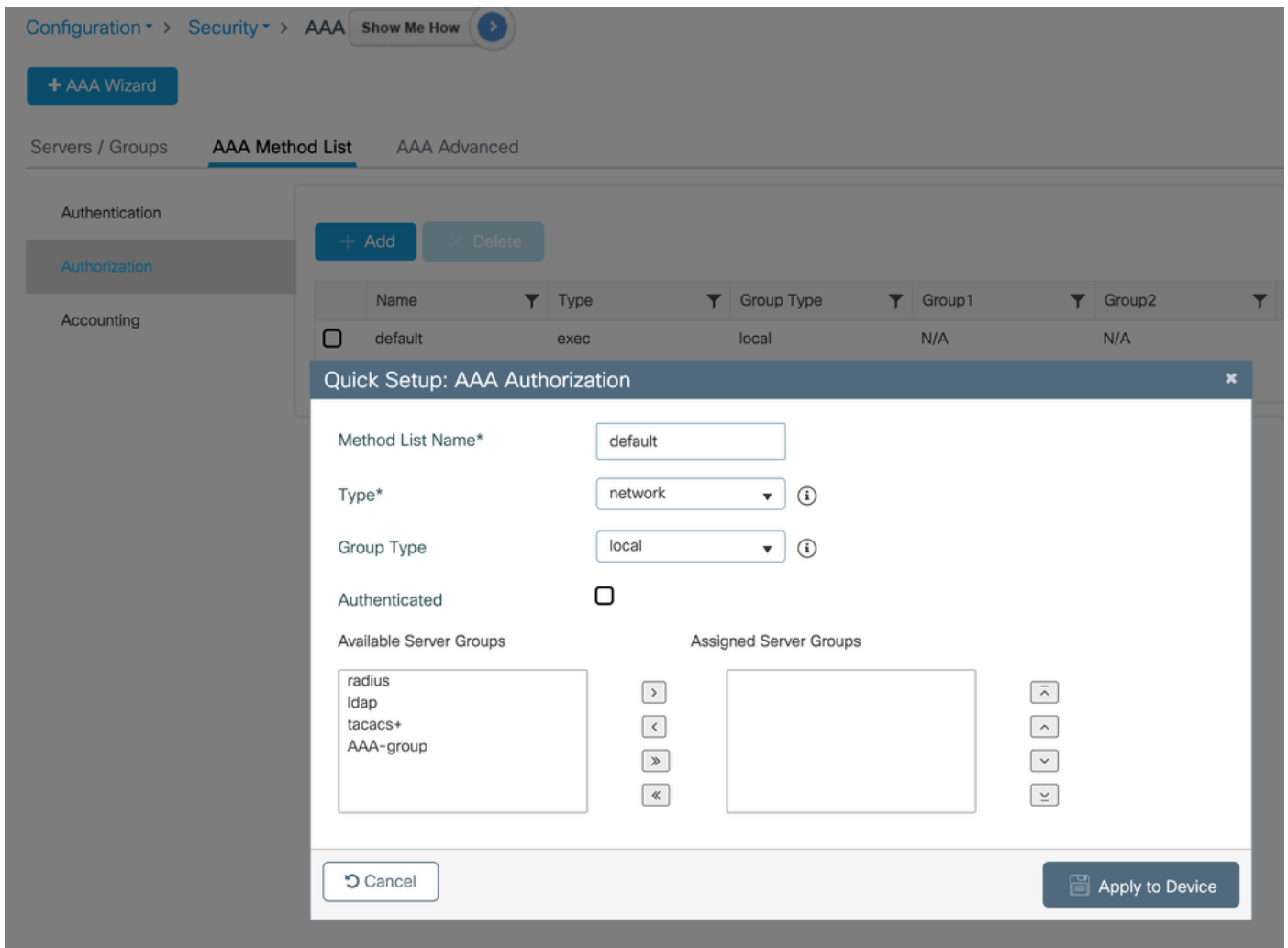
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration page. The left sidebar contains a search bar and a menu with items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the configuration path: Configuration > Security > AAA > AAA Method List. The 'AAA Method List' tab is active, and the 'Authentication' sub-tab is selected. A table lists the configured AAA methods:

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	login	local	N/A	N/A	N/A	N/A
☐ LWA-AUTHENTICATION	login	local	N/A	N/A	N/A	N/A

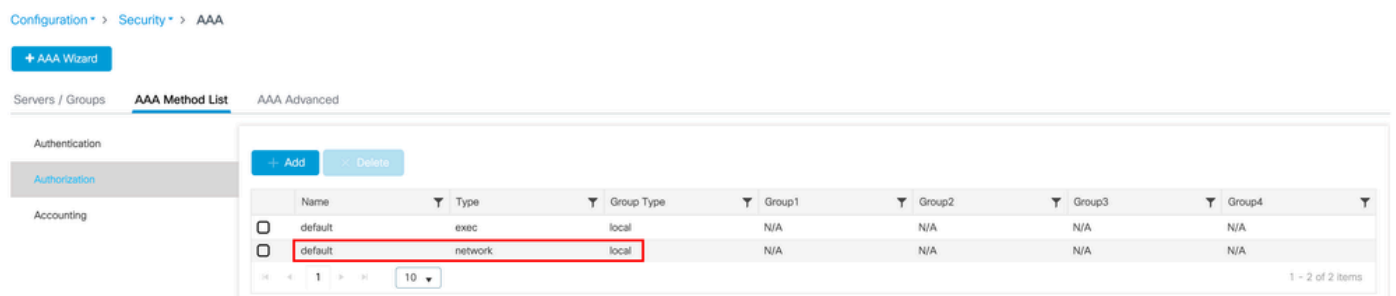
The 'LWA-AUTHENTICATION' entry is highlighted with a red box. The table footer indicates '1 - 2 of 2 items'.

Stellen Sie sicher, dass eine Liste mit lokalen Autorisierungsmethoden vorhanden ist. Dies ist eine Voraussetzung für die Erstellung der Liste mit lokalen Anmeldemethoden.

Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung > Hinzufügen



Nachdem Sie auf Auf Gerät anwenden geklickt haben, bestätigen Sie die Erstellung der AAA-Methodenliste:



Parameterzuordnungen

Globale Parameterzuordnung in Konfiguration bearbeiten > Sicherheit > Webauthentifizierung

Configuration > Security > Web Auth

[Add](#) [Delete](#)

Selected Rows: 0

Parameter Map Name
☐ global

1 10 items per page

General

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Sleeping Client Status: ☐

Sleeping Client Timeout (minutes): 720

Advanced

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☒

Disable HTTP secure server for Web Auth: ☐

Banner Configuration

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ Read From File

Wählen Sie den zu verwendenden Typ der Webauthentifizierung, Virtual IP (Virtuelle IP) und den Vertrauenspunkt aus, den der WLC im Webportal darstellt. In diesem Fall wird das selbstsignierte Zertifikat ausgewählt und wird wahrscheinlich einen Haftungsausschluss von der Art "Ihre Verbindung ist kein privates Netz::ERR_CERT_AUTHORITY_INVALID" verursachen, da es sich um ein LSC (Locally Significant Certificate) handelt und nicht von einer erkennbaren Zertifizierungsstelle im Internet signiert wird. Verwenden Sie ein von einem Drittanbieter unterzeichnetes Zertifikat, um dies zu ändern. Details finden Sie unter [CSR-Zertifikate für Catalyst 9800 WLCs generieren und herunterladen](#). Alternativ gibt es eine Videooption, die das Hochladen und die Erstellung von Trustpoint-[Verlängerungszertifikaten für WebAuth & WebAdmin auf dem Cisco 9800 WLC](#) erläutert. [| Einrichtung des sicheren Wireless LAN-Controllers](#).

Edit Web Auth Parameter



General

Advanced

Parameter-map Name

global

Maximum HTTP connections

100

Init-State Timeout(secs)

120

Type

webauth ▼

Captive Bypass Portal

☐

Disable Success Window

☐

Disable Logout Window

☐

Disable Cisco Logo

☐

Sleeping Client Status

☐

Sleeping Client Timeout
(minutes)

720

Virtual IPv4 Address

192.0.2.1

Trustpoint

TP-self-signed-... ▼

Virtual IPv4 Hostname

Virtual IPv6 Address

XXXXXX::X

Web Auth intercept
HTTPs

☐

Enable HTTP server for
Web Auth

☒

Disable HTTP secure
server for Web Auth

☐

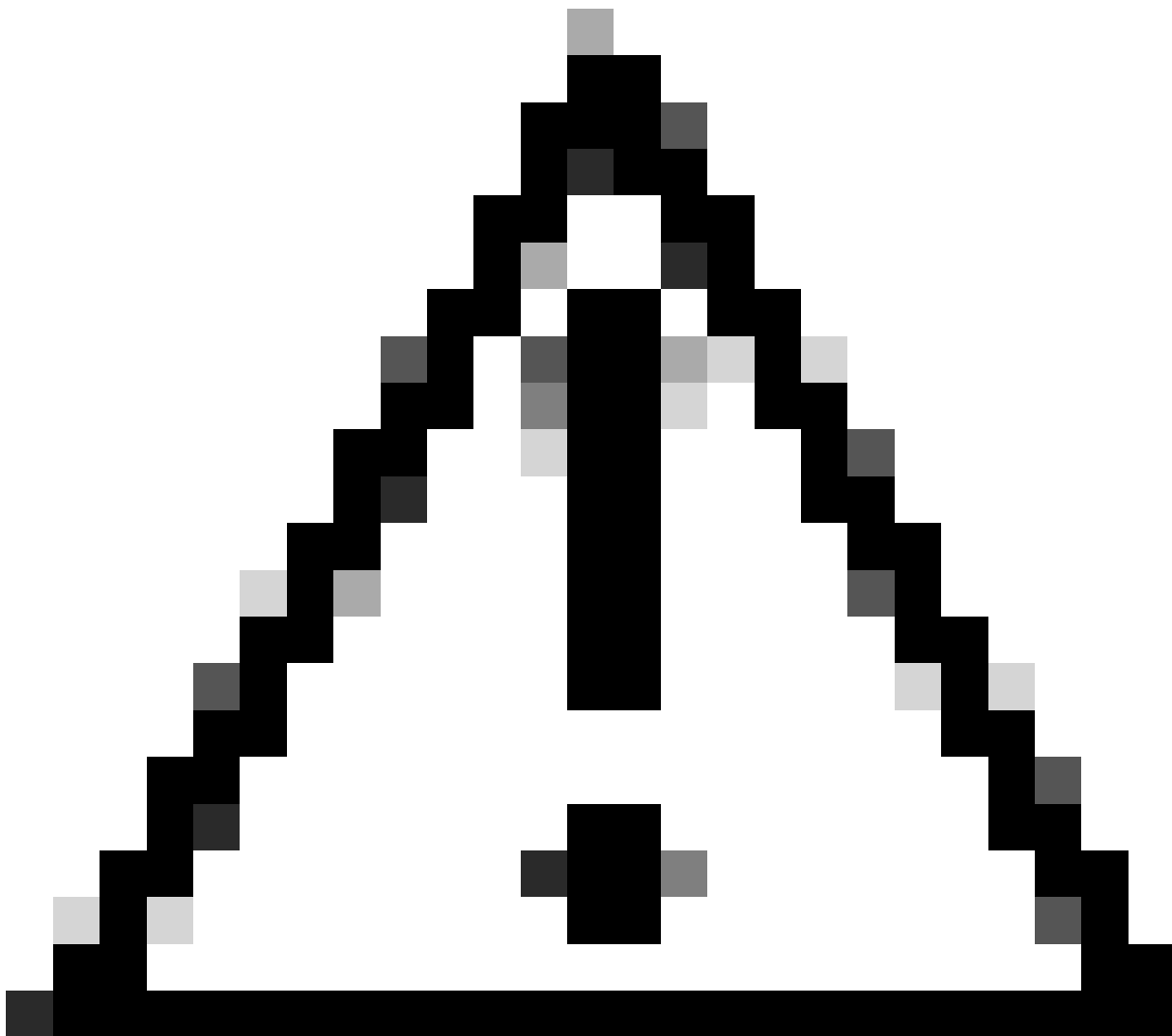
Banner Configuration

Banner Title

Banner Type

☒ None ☐ Banner Text

☐ Read From File



Vorsicht: Wenn HTTP auf dem 9800 global deaktiviert ist, stellen Sie sicher, dass das Kontrollkästchen Enable HTTP server for Web Auth (HTTP-Server für Webauthentifizierung aktivieren) aktiviert ist, da Cisco die Abhängigkeit dieser Prozesse voneinander getrennt hat. Es wird erwartet, dass Clients oder Supplicants einen HTTP-Verbindungsprozess initiieren, und dass diese Sitzung vom Controller abgefangen wird, um das Webportal zu präsentieren. Aus diesem Grund wird nicht empfohlen, Web Auth Intercept HTTPS zu aktivieren, es sei denn, dies ist unbedingt erforderlich, da diese Einstellung für die meisten Bereitstellungen nicht erforderlich ist und die CPU-Auslastung des Controllers erhöhen kann, was sich möglicherweise auf die Leistung auswirken kann.

WLAN-Sicherheitsparameter

Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und klicken Sie auf Add.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Profile Name*

LWA_LA

SSID*

LWA LA

WLAN ID*

1

Status

ENABLED ☒

Broadcast SSID

ENABLED ☒

Radio Policy ⓘ

6 GHz

Status

ENABLED ☒☒ Slot 2/3

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED ☒☒ Slot 0☒ Slot 1☒ Slot 2

2.4 GHz

Status

ENABLED ☒☒ Slot 0802.11b/g
Policy

802.11b/g ▼

Wählen Sie auf der Registerkarte Sicherheit für Layer 2 die Option Keine aus.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering ☐

OWE Transition Mode ☐

Lobby Admin Access ☐

Fast Transition

Status

Adaptive Ena... ▼

Over the DS

☐

Reassociation Timeout *

20

Aktivieren Sie auf der Registerkarte Sicherheit für Layer 3 das Kontrollkästchen Webrichtlinie, und wählen Sie im Dropdown-Menü und in der Authentifizierungsliste die zuvor konfigurierte Parameterzuordnung aus.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy



[<< Hide](#)

Web Auth Parameter Map

global



On MAC Filter Failure



Splash Web Redirect



DISABLED

Authentication List

LWA_AUTHENTI...



Preauthentication ACL

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

IPv4

None



IPv6

None



Richtlinienprofil erstellen

Um das Richtlinienprofil zu erstellen, das mit dem WLAN-Profil verknüpft werden soll, navigieren Sie zu Configuration > Tags & Profiles > Policy.

Edit Policy Profile



⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

LWA_CentralSW

Description

Enter Description

Status

ENABLED ☒

Passive Client

☐ DISABLED

IP MAC Binding

ENABLED ☒

Encrypted Traffic Analytics

☐ DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED ☒

Central Authentication

ENABLED ☒

Central DHCP

ENABLED ☒

Flex NAT/PAT

☐ DISABLED

Wählen Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das VLAN aus, von dem aus Clients/Komponenten eine IP anfordern sollen.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

☐

HTTP TLV Caching

☐

DHCP TLV Caching

☐

WLAN Local Profiling

Global State of Device Classification

Enabled ⓘ

Local Subscriber Policy Name

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

2622 ▼ ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼ ⓘ

IPv6 ACL

Search or Select ▼ ⓘ

URL Filters ⓘ

Pre Auth

Search or Select ▼ ⓘ

Post Auth

Search or Select ▼ ⓘ

Policy-Tag erstellen

Für diesen Konfigurationsleitfaden wurde ein benutzerdefiniertes Richtlinien-Tag mit dem Namen LWA erstellt.

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

LWA

Description

LWA_LA

✓ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
☐ LWA_LA	LWA_CentralSW

1 - 1 of 1 items

Zuordnen des WLAN- und Richtlinienprofils

Um die Switching-Richtlinien aus dem Richtlinienprofil und dem WLAN zu verknüpfen, navigieren Sie zu Configuration > Tags & Profiles > WLANs, wählen Sie das WLAN Profile aus, und klicken Sie auf Add to Policy Tags (Zu Richtlinien-Tags hinzufügen).

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Advanced **Add To Policy Tags**

+ Add × Delete

☐	Policy Tag	Policy Profile
☐	LWA	LWA_CentralSW

1 10 1 - 1 of 1 items

Zuweisen eines Richtlinien-Tags zu einem AP

Um den AP mit der erstellten Richtlinien-Tag-Nummer zu kennzeichnen, navigieren Sie zu Configuration > Wireless > Access Points, wählen Sie den AP aus, und auf der Registerkarte General (Allgemein) befinden sich rechts die vom AP verwendeten Tags.

Edit AP

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*	9117
Location*	default location
Base Radio MAC	cc0
Ethernet MAC	c00
Admin Status	ENABLED ☒
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled

LED Settings

LED State	ENABLED ☒
Brightness Level	8

Flash Settings

Flash State	☐ DISABLED
-------------	-----------------------------------

 Apply

Time Statistics

Up Time	8 days 15 hrs 26 mins 48 secs
Controller Association Latency	1 sec

Tags

Policy	LWA
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	 

Version

Primary Software Version	17.12.5.41
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.12.5.41
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	172.16.60.40
Static IP (IPv4/IPv6)	☐

 Cancel

 Update & Apply to Device

Gastbenutzernamen erstellen

Wenn Sie den Webauthentifizierungstyp in der Parameterzuordnung ausgewählt haben, wird ein Gastbenutzername benötigt, um diesen zu erstellen. Navigieren Sie dazu zu Konfiguration > Sicherheit > Gastbenutzer.

Die maximale Lebensdauer des Benutzers beträgt 1 Jahr. Mit den verfügbaren Optionen können

Sie etwas Anderes festlegen.

Configuration > Security > Guest User

+ Add

- Delete

Selected Rows: 0

☐ User Name

☐ johndoe

1

10

items per page

Edit Guest User

General

Lifetime

Enter User Name*

johndoe

Years*

1

Password*

Enter Password

Months*

0

☐ Generate password

Days*

0

Confirm Password

Confirm Password

Hours*

0

Description*

Guest-User

Mins*

0

AAA Attribute list

Enter/Select

No. of Simultaneous User Logins*

0

Start Time

15:21:19 UTC Aug 26 2025

Expiry Time

15:21:19 UTC Aug 21 2026

Remaining Time

0 years 11 months 29 days 23 hours 34 mins 24 secs

Überprüfung

Über GUI

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	9ef2.4b16.a507	172.16.74.83	fe80:9c72:4b16:fe16:a507	9117	0	LWA LA	1	WLAN	Run	11ax(2.4)	johndoe	N/A	Local	No

1 ~ 1 of 1 clients

Monitoring > Wireless > Clients

Clients
Sleeping Clients
Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
☐	507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA LA

1
10

Client
360 View
General
QoS Statistics
ATF Statistics
Mobility History
Call Statistics

Client Properties
AP Properties
Security Information
Client Statistics
QoS Properties
EoGRE

MAC Address	507
Client MAC Type	Locally Administered Address
Client DUID	NA
IPv4 Address	172.16.74.83
IPv6 Address	fe80::9cf2:4bff:fe16:a507
User Name	johndoe
Policy Profile	LWA_CentralSW
Flex Profile	N/A
Wireless LAN Id	1
WLAN Profile Name	LWA_LA
Wireless LAN Network Name (SSID)	LWA LA
BSSID	0cd0.f897.acc0
Uptime(sec)	151 seconds
Idle state timeout	N/A
Session Timeout	28800 sec (Remaining time: 28678 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	ON
Current TxRateSet	1.0
Supported Rates	1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
QoS Average Data Rate Upstream	0 (kbps)
QoS Realtime Average Data Rate Upstream	0 (kbps)
QoS Burst Data Rate Upstream	0 (kbps)
QoS Realtime Burst Data Rate Upstream	0 (kbps)
QoS Average Data Rate Downstream	0 (kbps)
QoS Realtime Average Data Rate Downstream	0 (kbps)
QoS Burst Data Rate Downstream	0 (kbps)
QoS Realtime Burst Data Rate Downstream	0 (kbps)
Join Time Of Client	09/10/2025 21:26:11 UTC
Policy Manager State	Run
Last Policy Manager State	Webauth Pending
Transition Disable Bitmap	0x00
User Defined (Private) Network	Disabled
User Defined (Private) Network Drop Unicast	Disabled

OK

Über CLI

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name          Type ID State Protocol Method  Role
-----
9ef2.4b16.a507   xxxxx-9117 WLAN 1 Run  11ax(2.4) Web Auth Local
9800WLC#show wireless client mac-address
```

detail

Client MAC Address : 9ef2.4b16.a507

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

Signal to Noise Ratio : 4 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

Lokale Web-Authentifizierung auf lokalem FlexConnect-Switching

In diesem Szenario wird angenommen, dass sich der Access Point im FlexConnect-Modus befindet. Damit sich ein Access Point im FlexConnect-Modus befindet, benötigen Sie ein Flex-Profil, das mit dem SiteTag verknüpft ist und bei dem das Kontrollkästchen Lokalen Standort aktivieren deaktiviert ist. Dieses Site-Tag verwendet den Standard-ap-join und einen benutzerdefinierten Flex-Profilnamen Flex_LWA:

Configuration > Tags & Profiles > Tags

Policy Site RF AP

Add Delete Clone Reset APs

Site Tag Name

☐ FlexConnect

☐ default-site-tag

1 10

Edit Site Tag

Name* FlexConnect

Description Enter Description

AP Join Profile default-ap-profile

Flex Profile Flex_LWA

Fabric Control Plane Name

Enable Local Site

Load* 0

Zuweisen eines Richtlinien-Tags zu einem AP

Navigieren Sie zu Configuration > Wireless > Access Points, wählen Sie den Access Point aus, und auf der Registerkarte General (Allgemein) rechts sehen Sie die vom Access Point verwendeten Tags.

Edit AP

General Interfaces High Availability Inventory Geolocation Advanced Support Bundle

General

AP Name* 9117

Location* default location

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode Local

Operation Status Registered

Fabric Status Disabled

LED Settings

LED State DISABLED

Flash Settings

Flash State DISABLED

Apply

Time Statistics

Up Time 8 days 15 hrs 51 mins 4 secs

Controller Association Latency 1 sec

Tags

Policy LWA

Site FlexConnect

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.12.5.41

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 17.12.5.41

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode Not Configured

DHCP IPv4 Address 172.16.60.40

Static IP (IPv4/IPv6)



Warnung: Wenn Sie die Tags ändern, trennt sich der Access Point vom WLC.

Configuration > Wireless > Access Points

▼ All Access Points

Total APs: 1

Misconfigured APs
Tag : 0 Country Code : 0 LSC Fallback : 0 Select an Action ▼

Multiple APs can be configured at once from [Bulk AP Provisioning](#) feature

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Country Code Misconfigured	LSC Fallback Misconfigure
9117	C9117AXI-A	2	✓	8 days 15 hrs 54 mins 53 secs	172.16.60.40	cc0	c00	Flex	No	Registered	Healthy	No	No

Das mit dem WLAN verknüpfte Richtlinienprofil ist "Lokales Switching".

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Advanced **Add To Policy Tags**

+ Add
× Delete

☐	Policy Tag	Policy Profile
☐	LWA	LWA_LocalSW

1
10
1 - 1 of 1 items

Configuration > Tags & Profiles > Policy

+ Add
× Delete
🔄 Clone

Policy Profile Name "is equal to" LWA_LocalSW

Admin Status	Associated Policy Tags	Policy Profile Name
☒		LWA_LocalSW

1
10

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QoS and AVC Mobility Advanced

Name* LWA_LocalSW WLAN Switching Policy

Description Enter Description

Status **ENABLED**

Passive Client **DISABLED**

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics **DISABLED**

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

Central Switching **DISABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT **DISABLED**

Überprüfung

```
9800WLC>enable
```

```
9800WLC#show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type ID	State	Protocol	Method	Role
-------------	---------	---------	-------	----------	--------	------

9ef2.4b16.a507	xxxxx-9117	WLAN 1	Run	11ax(2.4)	Web Auth	Local
----------------	------------	--------	-----	-----------	----------	-------

```
9800WLC#show wireless client mac-address
```

```
detail
```

```
Client MAC Address :
```

```
Client MAC Type : Locally Administered Address
```

```
Client DUID: NA
```

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

The screenshot displays the Cisco WLC interface. On the left, the 'Clients' tab is active, showing a table of client information. The table has columns for Client MAC Address, IPv4 Address, IPv6 Address, AP Name, Slot ID, and SSID. One client is selected, with a 'Delete' button and a refresh icon above the table. Below the table, it says 'Selected 0 out of 1 Clients'. On the right, the 'Client Properties' window is open, showing various client details. The 'General' tab is selected. The 'Policy Profile' and 'Flex Profile' are highlighted with a red box. The 'Policy Profile' is 'LWA_LocalSW' and the 'Flex Profile' is 'Flex_LWA'. Other details include MAC Address (9ef2.4b16.a507), Client MAC Type (Locally Administered Address), Client DUID (NA), IPv4 Address (172.16.74.83), IPv6 Address (fe80::9cf2:4b16:a507), User Name (johndoe), Wireless LAN Id (1), WLAN Profile Name (LWA_LA), Wireless LAN Network Name (SSID) (LWA_LA), BSSID (cc0), Uptime (103 seconds), Idle state timeout (N/A), Session Timeout (28800 sec), Session Warning Time (Timer not running), Client Active State (Active), Power Save mode (OFF), Current TxRateSet (m11 ss2), Supported Rates (1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0), QoS Average Data Rate Upstream (0 kbps), QoS Realtime Average Data Rate Upstream (0 kbps), QoS Burst Data Rate Upstream (0 kbps), QoS Realtime Burst Data Rate Upstream (0 kbps), QoS Average Data Rate Downstream (0 kbps), QoS Realtime Average Data Rate Downstream (0 kbps), QoS Burst Data Rate Downstream (0 kbps), QoS Realtime Burst Data Rate Downstream (0 kbps), Join Time Of Client (09/11/2025 17:38:26 UTC), Policy Manager State (Run), Last Policy Manager State (Webauth Pending), Transition Disable Bitmap (0x00), User Defined (Private) Network (Disabled), and User Defined (Private) Network Drop Unicast (Disabled).

Fehlerbehebung

Der Status "Web Auth Pending" (Webauthentifizierung ausstehend) gibt an, dass der Client mit dem Access Point verknüpft ist, aber den Webauthentifizierungsprozess noch nicht abgeschlossen hat. In diesem Zustand fängt der Controller den HTTP-Datenverkehr des Clients ab und leitet ihn zur Benutzeranmeldung oder zur Annahme von Bedingungen an ein Web-Authentifizierungsportal weiter. Der Client bleibt in diesem Zustand, bis die erfolgreiche Webauthentifizierung abgeschlossen ist. Anschließend wechselt der Client-Richtlinien-Manager-Status zu "Ausführen", und der vollständige Netzwerkzugriff wird gewährt.

Um den Fluss der Client-Verbindung visuell zu sehen, überprüfen Sie den LWA-Fluss aus [Configure Local Web Authentication with External Authentication \(Lokale Web-Authentifizierung mit externer Authentifizierung konfigurieren\)](#).

Die Schritte, die der Client in Bezug auf den Kunden durchläuft, sind im Abschnitt [Fehlerbehebung bei häufigen Problemen mit LWA auf 9800-WLCs](#) dargestellt.

- [Technischer Support und Dokumentation für Cisco Systeme](#)

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.