

Lokale Webauthentifizierung mit externer Authentifizierung konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Webauthentifizierung](#)

[Authentifizierungstypen](#)

[Datenbank für die Authentifizierung](#)

[Lokale Webauthentifizierung](#)

[Lokale Webauthentifizierung mit externer Authentifizierung](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration der lokalen Webauthentifizierung mit externer Authentifizierung über die CLI](#)

[AAA-Server und -Servergruppe konfigurieren](#)

[Lokale Authentifizierung und Autorisierung konfigurieren](#)

[Parameterzuordnungen konfigurieren](#)

[WLAN-Sicherheitsparameter konfigurieren](#)

[Wireless-Richtlinienprofil erstellen](#)

[Policy-Tag erstellen](#)

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

[Lokale Webauthentifizierung mit externer Authentifizierung auf der WebUI konfigurieren](#)

[AAA-Konfiguration auf dem 9800 WLC](#)

[WebAuth-Konfiguration](#)

[WLAN-Konfiguration](#)

[Richtlinienprofilkonfiguration](#)

[Richtlinien-Tag-Konfiguration](#)

[Richtlinien-Tag-Zuweisung](#)

[ISE-Konfiguration](#)

[Gastclient verbinden](#)

[Überprüfung](#)

[show wlan summary](#)

[Konfiguration der Parameterzuordnung anzeigen](#)

[AAA-Informationen anzeigen](#)

[Fehlerbehebung](#)

[Häufige Probleme](#)

[Bedingtes Debuggen und Radio Active Trace und eingebettete Paketerfassung](#)



Einleitung

In diesem Dokument wird beschrieben, wie Sie die lokale Webauthentifizierung mit externer Authentifizierung auf einem 9800 WLC und der ISE konfigurieren.

Voraussetzungen

Anforderungen

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

- Konfiguration der 9800 Wireless LAN Controller (WLC)
- Lightweight Access Points (LAP)
- Einrichten und Konfigurieren einer externen Webserver-Identity Services Engine (ISE).
- Einrichten und Konfigurieren von DHCP- und DNS-Servern

Verwendete Komponenten

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

- 9800-40 WLC Cisco IOS® XE, Version 17.18.4a mit APSP1 und APSP2
- Identity Services Engine (ISE), Version 3.2.0.542
- Cisco® Wireless Access Point der Serie 9172I, Version 17.18.4.202

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.

Webauthentifizierung

Die Webauthentifizierung ist eine Sicherheitsfunktion auf Layer 3, die Gastbenutzern den Zugriff

auf das Netzwerk ermöglicht.

Diese Funktion bietet einfachen und sicheren Gastzugriff auf offene SSIDs, ohne dass ein Benutzerprofil konfiguriert werden muss. Sie kann auch mit Layer-2-Sicherheitsmethoden verwendet werden.

Der Zweck der Webauthentifizierung besteht darin, nicht vertrauenswürdigen Geräten (Gästen) den Zugriff auf das Netzwerk mit eingeschränkten Netzwerkzugriffsberechtigungen über ein Gast-WLAN zu ermöglichen, das mit Sicherheitsmechanismen konfiguriert werden kann, und die Sicherheit des Netzwerks nicht zu beeinträchtigen. Damit Gastbenutzer auf das Netzwerk zugreifen können, müssen sie sich erfolgreich authentifizieren, d. h., sie müssen die richtigen Anmeldeinformationen angeben oder die Richtlinie für akzeptable Nutzung (AUP) akzeptieren, um Zugriff auf das Netzwerk zu erhalten.

Die Web-Authentifizierung ist ein Vorteil für Unternehmen, da sie die Loyalität der Benutzer fördert, das Unternehmen zur Einhaltung der Vorschriften verpflichtet, einen Haftungsausschluss zu verwenden, den der Gastbenutzer akzeptieren muss, und dem Unternehmen ermöglicht, mit Besuchern in Kontakt zu treten.

Bei der Bereitstellung der Webauthentifizierung muss berücksichtigt werden, wie das Gastportal und die Authentifizierung gehandhabt werden. Es gibt zwei gängige Methoden:

- Lokale Webauthentifizierung (LWA): Eine Methode zur Umleitung von Gastbenutzern zu einem Portal direkt vom WLC. Die Umleitung und die Pre-WebAuth-ACL werden lokal auf dem WLC konfiguriert.
- Zentrale Webauthentifizierung (CWA): Eine Methode zur Umleitung von Gastbenutzern, bei der die Umleitungs-URL und die Umleitungs-ACL zentral auf einem externen Server (z. B. der ISE) konfiguriert und über RADIUS an den WLC übermittelt werden. Bei der zentralen Webauthentifizierung befinden sich die Umleitungs-URL und die Umleitungs-ACL zentral auf einem externen Server (z. B. RADIUS). Der RADIUS-Server ist derjenige, der die Authentifizierung übernimmt. Er sendet Anweisungen an den WLC. In CWA benötigt der WLC kein lokales Web-Authentifizierungszertifikat, sondern nur ein Zertifikat auf dem zentralen Webportal und einen zentralen Authentifizierungsserver wie die ISE. Um CWA genauer zu lesen, navigieren Sie zu [Configure Central Web Authentication \(CWA\) on Catalyst 9800 WLC and ISE](#).

Bei der lokalen Webauthentifizierung kann das Webportal auf dem WLC oder auf einem externen Server vorhanden sein. Im LWA mit External Authentication ist das Webportal auf dem WLC vorhanden. In LWA mit External Web Server befindet sich das Webportal auf einem externen Server (z. B. Cisco DNA Spaces). Ein Beispiel für ein LWA mit einem externen Webserver wird detailliert beschrieben unter: [Konfigurieren von DNA Spaces Captive Portal mithilfe des Catalyst 9800 WLC](#)

Darstellung der verschiedenen Web-Authentifizierungsmethoden:

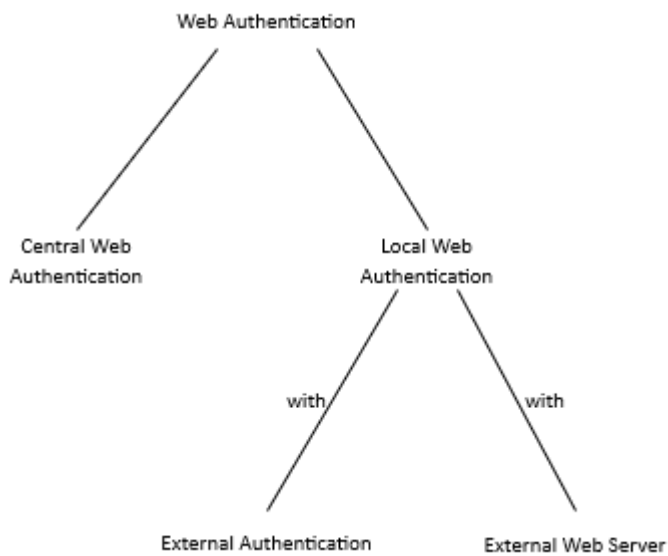


Diagramm der verschiedenen Web-Authentifizierungsmethoden



Anmerkung: Wenn Sie Wi-Fi 7 APs mit Webauthentifizierung auf einem 9800 WLC bereitstellen, stellen Sie sicher, dass Sie eine empfohlene Cisco IOS XE-Version (z. B. 17.18.4a oder höher) verwenden.

Authentifizierungstypen

Zur Authentifizierung des Gastbenutzers gibt es vier Authentifizierungstypen:

- Webauth: Geben Sie Benutzername und Passwort ein.
- Zustimmung (Web-Passthrough): AUP akzeptieren
- AutomUmgehung: Authentifizierung auf Basis der MAC-Adresse des Gastbenutzergeräts.
- Webbasierte Zustimmung: Eine Mischung aus Benutzername/Kennwort und AUP akzeptieren.

webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 ☒ Accept ☐ Don't Accept OK	banner login ☒ Accept ☐ Don't Accept Username: Password: OK

Vier Authentifizierungstypen zur Authentifizierung des Gastbenutzers

Datenbank für die Authentifizierung

Die Anmeldeinformationen für die Authentifizierung können auf einem LDAP-Server, lokal auf dem WLC oder auf dem RADIUS-Server gespeichert werden.

- Lokale Datenbank: Die Anmeldedaten (Benutzername und Passwort) werden lokal auf dem WLC gespeichert.
- LDAP-Datenbank: Die Anmeldeinformationen werden in der LDAP-Back-End-Datenbank gespeichert. Der WLC fragt den LDAP-Server nach den Anmeldeinformationen eines bestimmten Benutzers in der Datenbank ab.
- RADIUS-Datenbank: Die Anmeldeinformationen werden in der RADIUS-Backend-Datenbank gespeichert. Der WLC fragt den RADIUS-Server nach den Anmeldeinformationen eines bestimmten Benutzers in der Datenbank ab.

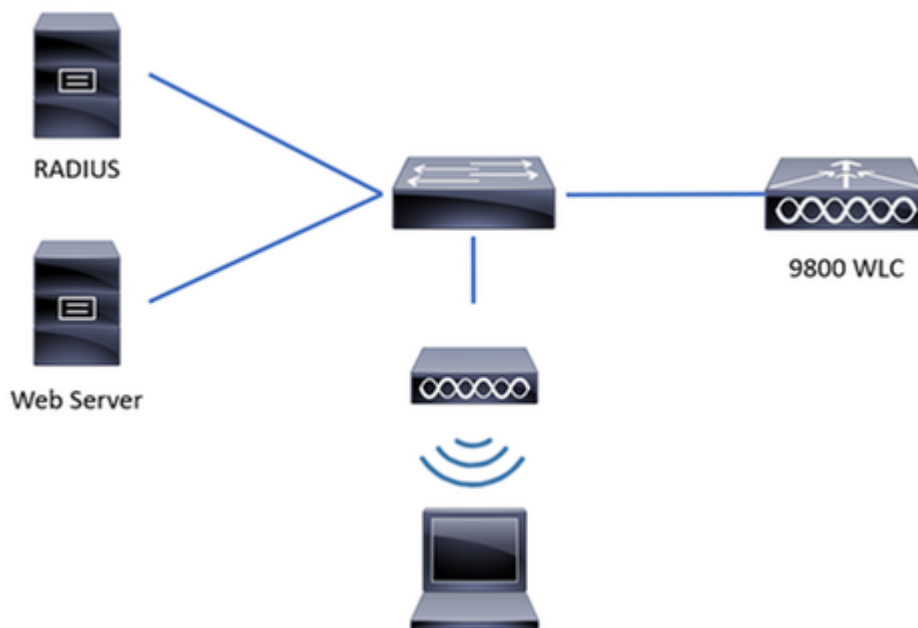
Lokale Webauthentifizierung

Bei der lokalen Web-Authentifizierung wird der Gastbenutzer direkt vom WLC auf ein Web-Portal umgeleitet.

Das Webportal kann sich im WLC oder auf einem anderen Server befinden. Lokal wird die Tatsache, dass sich die Umleitungs-URL und die ACL, die den Datenverkehr abgleicht, auf dem WLC befinden müssen (nicht der Standort des Webportals). Wenn ein Gastbenutzer in LWA eine Verbindung mit dem Gast-WLAN herstellt, fängt der WLC die Verbindung des Gastbenutzers ab

und leitet sie zur Webportal-URL um, über die der Gastbenutzer sich authentifizieren soll. Wenn der Gastbenutzer Anmeldeinformationen (Benutzername und Kennwort) eingibt, erfasst der WLC die Anmeldeinformationen. Der WLC authentifiziert den Gastbenutzer über einen LDAP-Server, einen RADIUS-Server oder eine lokale Datenbank (die Datenbank ist lokal auf dem WLC vorhanden). Im Fall eines RADIUS-Servers (ein externer Server wie die ISE) kann er nicht nur zum Speichern von Anmeldeinformationen verwendet werden, sondern bietet auch Optionen für die Geräteregistrierung und die benutzerseitige Bereitstellung. Bei einem externen Webserver, wie Cisco DNA Spaces, ist dort das Webportal vorhanden. Im LWA befindet sich ein Zertifikat auf dem WLC und ein weiteres im Webportal.

Das Bild stellt die generische LWA-Topologie dar:



Allgemeine Topologie des LWA

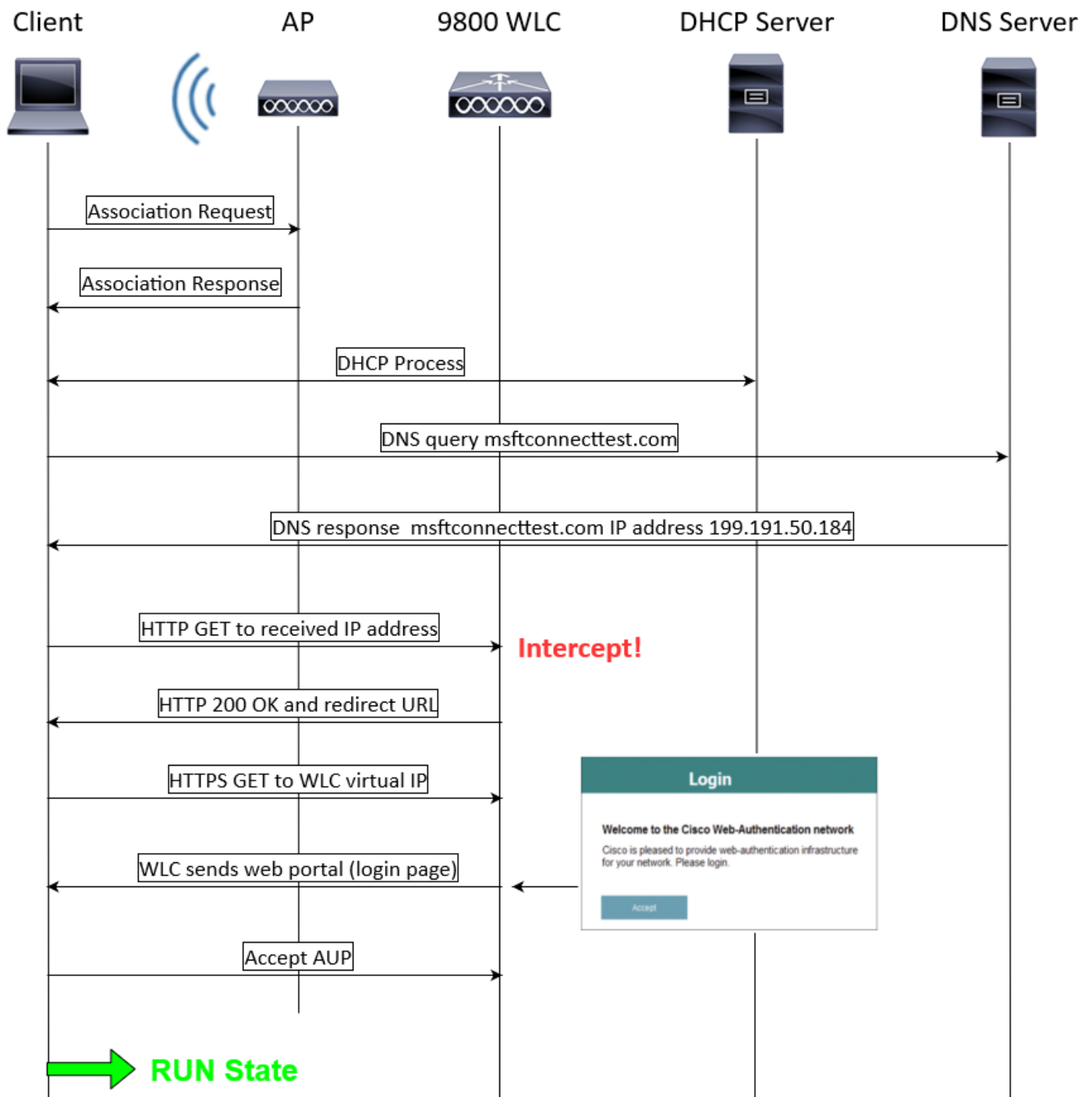
Geräte in der Netzwerktopologie von LWA:

- Kunde: Sendet Anfragen an DHCP- und DNS-Server, fordert Zugriff auf das Gast-WLAN an und antwortet auf Anfragen vom WLC.
- Access Point: Ist mit einem Switch verbunden, überträgt das Gast-WLAN und stellt eine Wireless-Verbindung zu Geräten von Gastbenutzern her. Außerdem werden DHCP- und DNS-Pakete zugelassen, bevor der Gastbenutzer authentifiziert wird (bevor gültige Anmeldeinformationen eingegeben werden).
- WLC: Verwaltet die APs und Clients. Der WLC hostet die Umleitungs-URL und die ACL, die mit dem Datenverkehr übereinstimmt. Abfangen von HTTP-Anfragen von Gastbenutzern, Weiterleitung an ein Webportal (Anmeldeseite), in dem sich Gastbenutzer authentifizieren müssen. Es erfasst die Anmeldeinformationen und authentifiziert die Gastbenutzer und sendet Zugriffsanfragen an einen externen Server, LDAP-Server oder eine lokale Datenbank, um die Gültigkeit der Anmeldeinformationen zu bestätigen.

- Authentifizierungsserver: Antwortet auf Zugriffsanforderungen vom WLC mit Annahme/Ablehnung des Zugriffs. Der Authentifizierungsserver überprüft die Anmeldeinformationen des Gastbenutzers und benachrichtigt den WLC, wenn die Anmeldeinformationen gültig oder ungültig sind. Wenn die Anmeldeinformationen gültig sind, wird der Gastbenutzer für den Zugriff auf das Netzwerk autorisiert (der Authentifizierungsserver bietet Optionen für die Geräteregistrierung und die benutzerseitige Bereitstellung). Wenn die Anmeldeinformationen ungültig sind, wird dem Gastbenutzer der Zugriff auf das Netzwerk verweigert.

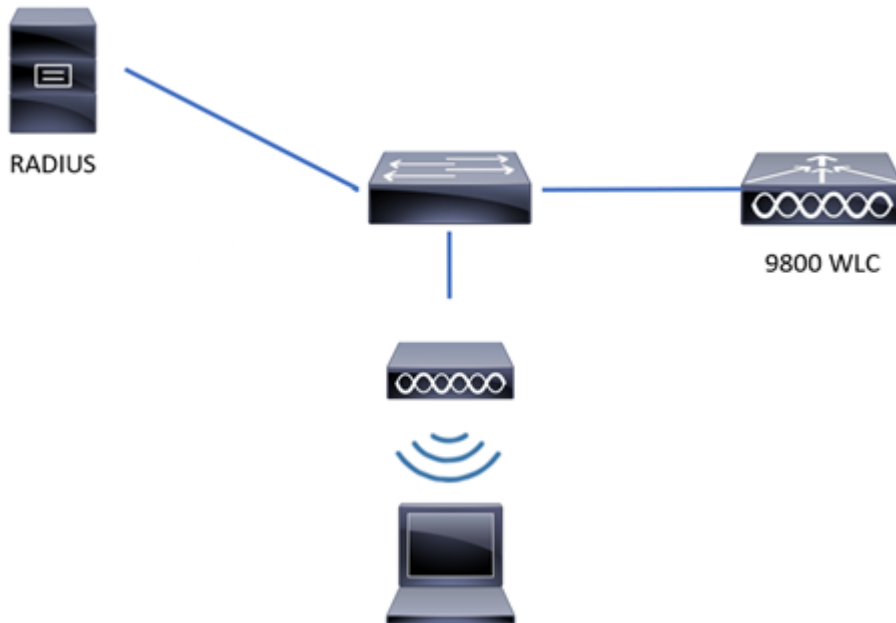
LWA-Fluss:

- Der Gastbenutzer ist einem AP zugeordnet, der das Gast-WLAN überträgt.
- Der Gastbenutzer durchläuft den DHCP-Prozess, um eine IP-Adresse zu erhalten.
- Der Gastbenutzer möchte eine Prüfung der Internetverbindung zum Captive Portal durchführen. Wenn es sich um ein Apple-Gerät handelt, wird das Captive Portal von Apple ausprobiert. Wenn es sich um ein Android-Gerät handelt, versucht es das Android Captive Portal. Wenn es sich um ein Windows-Gerät handelt, versucht es das Windows-Verbindungstestportal.
- Der Gastbenutzer sendet eine DNS-Abfrage, um nach der IP-Adresse des Captive Portals zu fragen. Der DNS-Server antwortet auf die Abfrage mit der entsprechenden IP-Adresse.
- Der Gastbenutzer sendet eine HTTP GET-Nachricht an die IP-Adresse des Captive Portals.
- Der WLC fängt diese Nachricht ab und antwortet dem Gastbenutzer mit HTTP 200 OK und der Umleitungs-URL.
- Der Gastbenutzer sendet eine HTTPS-GET-Nachricht an die virtuelle WLC-IP, und der WLC antwortet mit dem Webportal.
- Der Gastbenutzer wird aufgefordert, die Anmeldeinformationen für die Authentifizierung im Webportal einzugeben.
- Das Webportal leitet den Benutzer mit den bereitgestellten Anmeldeinformationen zurück zum WLC (sofern ein externes Webportal verwendet wird).
- Der WLC authentifiziert den Gastbenutzer über eine lokale Datenbank oder sendet eine Abfrage an den RADIUS- oder LDAP-Server, um zu bestätigen, ob die Anmeldeinformationen korrekt sind (wenn der Authentifizierungstyp "webagree" oder "webauth" ist).
- Wenn die Anmeldeinformationen korrekt sind, authentifiziert der WLC den Gastbenutzer und wechselt in den RUN-Status. Wenn die Anmeldeinformationen falsch sind, löscht der WLC den Gastbenutzer.
- Der WLC leitet den Client zurück auf die ursprüngliche URL, die in den Webbrowser eingegeben wurde.



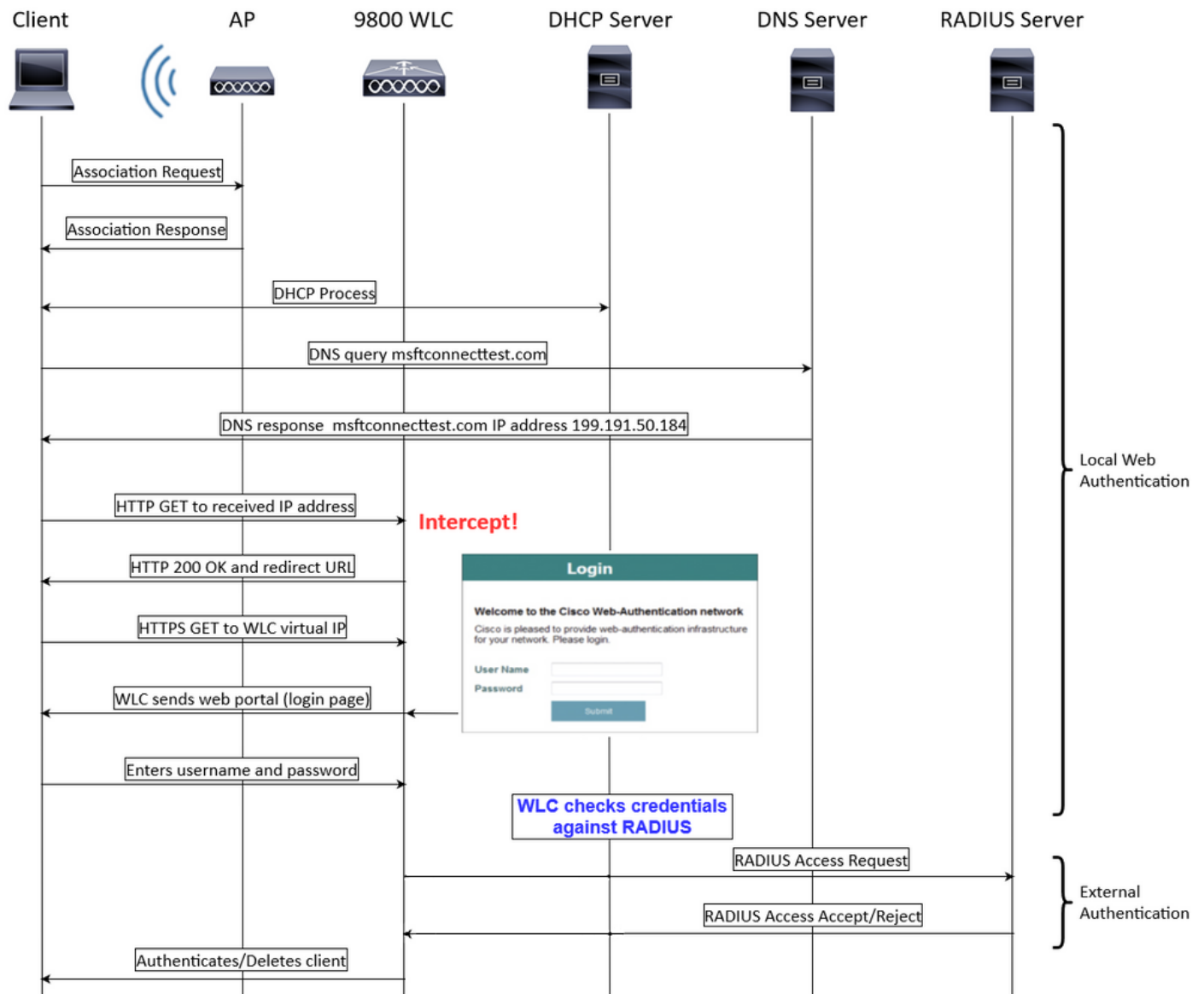
LWA-Fluss

Lokale Webauthifizierung mit externer Authentifizierung



Allgemeine Topologie von LWA-EA

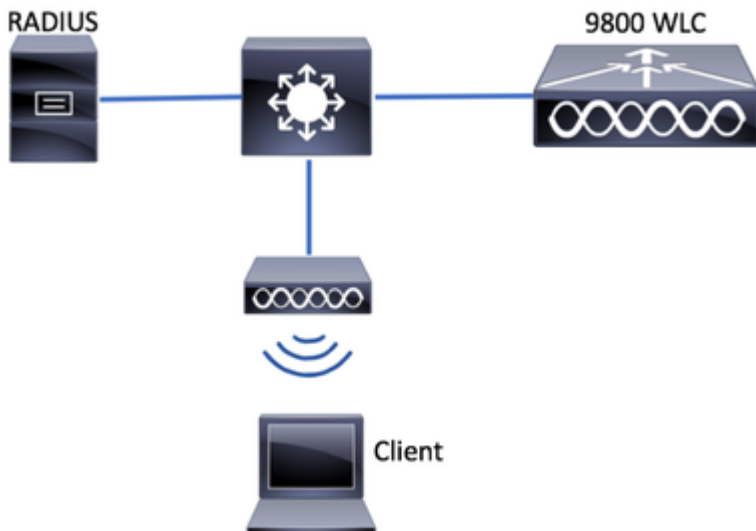
LWA-EA ist eine Methode des LWA, bei der sich das Webportal und die Umleitungs-URL auf dem WLC befinden und die Anmeldeinformationen auf einem externen Server wie der ISE gespeichert werden. Der WLC erfasst die Anmeldeinformationen und authentifiziert den Client über einen externen RADIUS-Server. Wenn ein Gastbenutzer Anmeldeinformationen eingibt, vergleicht der WLC die Anmeldeinformationen mit RADIUS, sendet eine RADIUS-Zugriffsanforderung und erhält vom RADIUS-Server eine RADIUS-Zugriffsgenehmigung bzw. -ablehnung. Wenn die Anmeldeinformationen korrekt sind, wechselt der Gastbenutzer in den Status "RUN". Wenn die Anmeldeinformationen falsch sind, wird der Gastbenutzer vom WLC gelöscht.



LWA-EA-Fluss

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm



Anmerkung: In diesem Konfigurationsbeispiel wird nur das zentrale Switching/die zentrale Authentifizierung behandelt. Die Flex Local Switching-Konfiguration stellt geringfügig andere Anforderungen für die Konfiguration der Webauthentifizierung.

Konfiguration der lokalen Webauthentifizierung mit externer Authentifizierung über die CLI

AAA-Server und -Servergruppe konfigurieren

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Lokale Authentifizierung und Autorisierung konfigurieren

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
```

```
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

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

WLAN-Sicherheitsparameter konfigurieren

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
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
```

Wireless-Richtlinienprofil erstellen

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Policy-Tag erstellen

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

```
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Zuweisen eines Richtlinien-Tags zu einem AP

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

Zum Abschließen der ISE-Konfiguration springen Sie bitte zum Abschnitt ISE-Konfiguration.

Lokale Webauthentifizierung mit externer Authentifizierung auf der WebUI konfigurieren

AAA-Konfiguration auf dem 9800 WLC

Schritt 1: Fügen Sie den ISE-Server der 9800 WLC-Konfiguration hinzu.

Navigieren Sie zu Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add (Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server > + Hinzufügen), und geben Sie die RADIUS-Serverinformationen wie im Bild dargestellt ein:

Create AAA Radius Server



General

RadSec

[Show Me How >](#)

Name*	RADIUS	Support for CoA ⓘ	☒ ENABLED
Server Address*	192.0.2.30	CoA Server Key Type	Clear Text
PAC Key	☐	CoA Server Key ⓘ	
Key Type	Clear Text	Confirm CoA Server Key	
Key* ⓘ		VRF	
Confirm Key*		Automate Tester	☐
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

AAA-Konfiguration auf dem 9800 WLC

Schritt 2: Hinzufügen der RADIUS-Servergruppe

Navigieren Sie zu Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add, und geben Sie die Informationen zur RADIUS-Servergruppe ein:

Create AAA Radius Server Group

Name*

RADIUSGROUP

Group Type

RADIUS

Show Me How >

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

☐ DISABLED

IPv4 Source Interface

Search or Select

i

IPv4 VRF

Search or Select

IPv6 Source Interface

Search or Select

i

IPv6 VRF

Search or Select

Available Servers

Assigned Servers

>

<

>>

<<

RADIUS

Cancel

Apply to Device

RADIUS-Servergruppe hinzufügen

Schritt 3: Erstellen Sie eine Liste der Authentifizierungsmethoden.

Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication > + Add:

Quick Setup: AAA Authentication

Method List Name*

LWA_AUTHENTICATION

Type*

login

Group Type

group

Fallback to local

☐

Available Server Groups

radius
ldap
tacacs+

>
<
>>
<<

Assigned Server Groups

RADIUSGROUP

^
^
v
v

Cancel

Apply to Device

Liste der Authentifizierungsmethoden erstellen

Schritt 4: Erstellen Sie eine Liste der Autorisierungsmethoden.

Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authorization > + Add:

Quick Setup: AAA Authorization

Method List Name*

LWA_AUTHORIZATION

Type*

network

Group Type

group

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

Erstellen Sie eine Liste mit Autorisierungsmethoden

WebAuth-Konfiguration

Erstellen oder bearbeiten Sie eine Parameterzuordnung. Wählen Sie den Typ als Webauthentifizierung aus, die virtuelle IPv4-Adresse muss eine Adresse sein, die im Netzwerk nicht verwendet wird, um IP-Adresskonflikte zu vermeiden, und fügen Sie einen Vertrauenspunkt hinzu.

Navigieren Sie zu Configuration > Security > Web Auth > + Add, oder wählen Sie eine Parameterzuordnung aus:

Configuration > Security > Web Auth

+ Add - Delete

Parameter Map Name

global

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name: global

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ File Name

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-94747...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::XX

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☐

Disable HTTP secure server for Web Auth: ☐

Cancel Update & Apply

WebAuth-Konfiguration

WLAN-Konfiguration

Schritt 1: Erstellen Sie das WLAN.

Navigieren Sie zu Configuration > Tags & Profiles > WLANs > + Add (Konfiguration > Tags und Profile > WLANs > +Hinzufügen) und konfigurieren Sie das Netzwerk nach Bedarf.

Add WLAN

General Security Advanced

Profile Name*: LWA_EA

SSID*: LWA_EA

WLAN ID*: 1

Status: ENABLED

Broadcast SSID: ENABLED

Wi-Fi 6E Compatibility: 1/2 requirements met

Wi-Fi 7 Compatibility: 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz Status: ENABLED ⓘ

5 GHz Status: ENABLED

2.4 GHz Status: ENABLED

802.11b/g Policy: 802.11b/g

WLAN erstellen

Schritt 2: Navigieren Sie zu Security > Layer2, und wählen Sie im Layer 2 Security Mode die Option None aus.

The screenshot shows the 'Add WLAN' configuration window. The 'Security' tab is selected, and within it, the 'Layer2' mode is chosen. The security mode is set to 'None', which is highlighted with a red box. Below the security mode options, there are three checkboxes: 'MAC Filtering', 'OWE Transition Mode', and 'Lobby Admin Access', all of which are currently unchecked.

General	Security	Advanced
Layer2	Layer3	AAA
☐ WPA + WPA2		
☐ WPA2 + WPA3		
☐ WPA3		
☐ Static WEP		
☒ None		
MAC Filtering ☐		
OWE Transition Mode ☐		
Lobby Admin Access ☐		

Erstellen der WLAN-Sicherheit

Schritt 3. Navigieren Sie zu Sicherheit > Schicht 3 und Web Policy aktivieren Sie das Kontrollkästchen, Web Auth Parameter Map wählen Sie den Parameternamen und auf Authentifizierungsliste wählen Sie die Authentifizierungsliste zuvor erstellt.

Add WLAN

General
Security
Advanced

Layer2
Layer3
AAA

Web Policy
☒

Web Auth Parameter Map
global

Authentication List
LWA_AUTHENTIC...

Show Advanced Settings >>>

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

Cancel
Apply to Device

Erstellen der Liste für die WLAN-Authentifizierung

Das WLAN wird in der WLAN-Liste angezeigt:

Configuration > Tags & Profiles > WLANs

+ Add
Delete
Clone
Enable WLAN
Disable WLAN
WLAN Wizard

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
☐		LWA_EA	1	LWA_EA	[open],[Web Auth]	

1
10
1 - 1 of 1 items

Erstelltes WLAN

Richtlinienprofilkonfiguration

In einem Richtlinienprofil können Sie neben anderen Einstellungen das VLAN auswählen, dem die Clients zugewiesen sind.

Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues erstellen.

Schritt 1: Erstellen Sie ein neues Richtlinienprofil.

Navigieren Sie zu Configuration > Tags & Profiles > Policy, und konfigurieren Sie Ihr Standard-Richtlinienprofil, oder erstellen Sie ein neues.

Stellen Sie sicher, dass das Profil aktiviert ist.

Add 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*

POLICY_PROFILE

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Neues Richtlinienprofil erstellen

Schritt 2: Wählen Sie das VLAN aus.

Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien) und wählen Sie den VLAN-Namen aus der Dropdown-Liste aus, oder geben Sie die VLAN-ID manuell ein.

Add 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
Disabled ⓘ

Local Subscriber Policy Name
Search or Select

VLAN

VLAN/VLAN Group
VLAN1432

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

Cancel
Apply to Device

Wählen Sie das VLAN aus

Richtlinien-Tag-Konfiguration

Sie verbinden Ihre SSID innerhalb des Richtlinien-Tags mit Ihrem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

Navigieren Sie zu Configuration > Tags & Profiles > Tags > Policy (Konfiguration > Tags und Profile > Tags > Richtlinie) und fügen Sie bei Bedarf eine neue Richtlinie hinzu, wie in der Abbildung dargestellt.

Wählen Sie + Hinzufügen:

Add Policy Tag

Name*
POLICY_TAG

Description
Enter Description

WLAN-POLICY Maps : 0

+ Add
X Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Richtlinien-Tag-Konfiguration

Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil:

Add Policy Tag

+ Add
X Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Map WLAN and Policy

WLAN Profile*
LWA_EA
Policy Profile*
POLICY_PRO...

X
✓

> RLAN-POLICY Maps : 0

Cancel
Apply to Device

Richtlinien-Tag-Konfiguration

Richtlinien-Tag-Zuweisung

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu.

Um das Tag einem AP zuzuweisen, navigieren Sie zu Configuration > Wireless > Access Points > AP Name > General Tags, (Konfiguration > Wireless > Access Points > AP-Name > Allgemeine Tags), nehmen Sie die erforderliche Zuweisung vor, und klicken Sie dann auf Update & Apply to Device (Aktualisieren und auf Gerät anwenden).

Configuration > Wireless > Edit AP

General Interfaces High Availability Inventory Geolocation ICap Advanced Support Bundle

General

AP Name* CW9172I-LAB

Location* default location

Base Radio MAC

Ethernet MAC

MLD Base MAC ⓘ

Admin Status ENABLED

AP Mode Local

Operation Status Registered

Fabric Status Disabled

LED Settings

LED State ENABLED

Brightness Level 8

Flash Settings

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy POLICY_TAG

Site default-site-tag

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.18.4.202

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

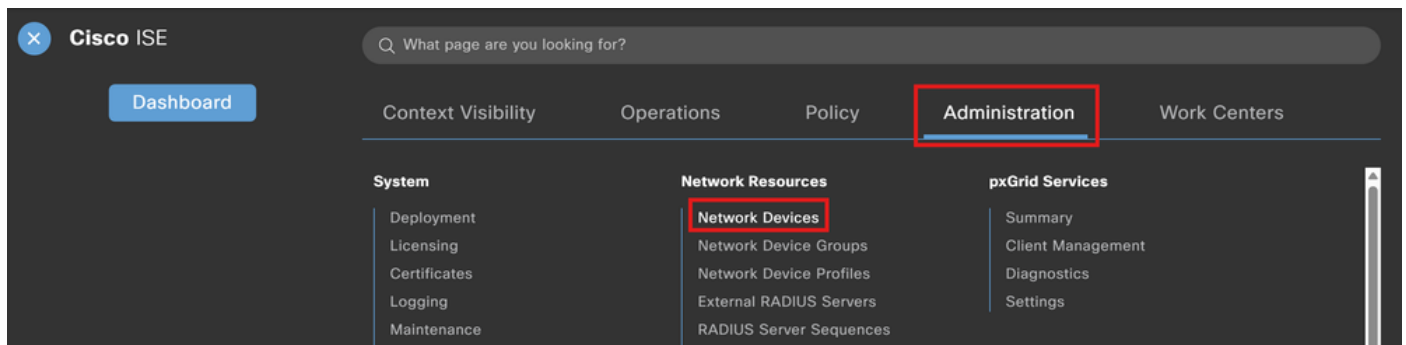
Cancel Update & Apply to Device

Richtlinien-Tag-Zuweisung

ISE-Konfiguration

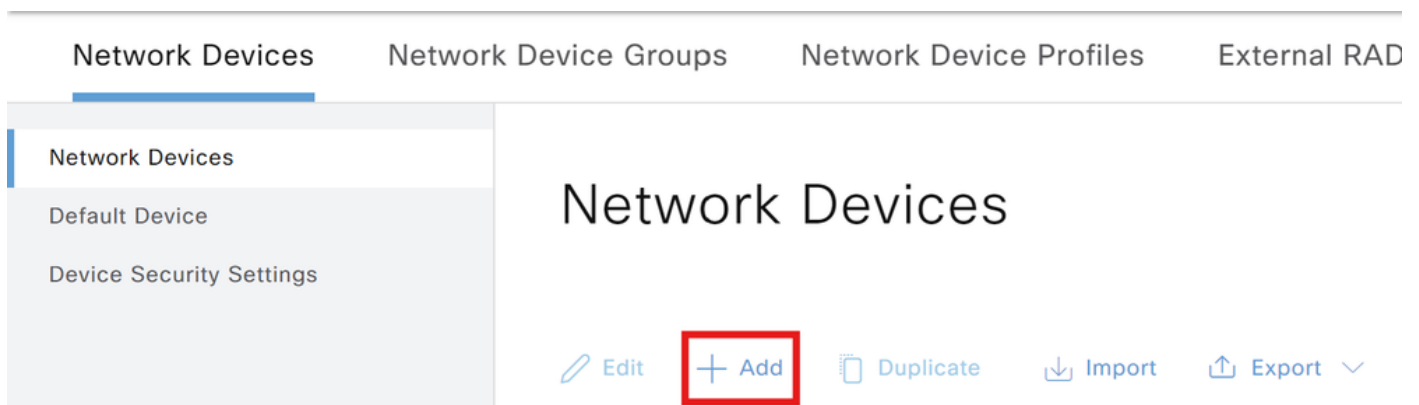
Hinzufügen von 9800 WLC zu ISE

Schritt 1: Navigieren Sie zu Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte), wie im Bild dargestellt.



Hinzufügen von 9800 WLC zu ISE

Schritt 2: Klicken Sie auf +Hinzufügen.



Netzwerkgeräte hinzufügen

Optional können ein angegebener Modellname, eine Softwareversion und eine Beschreibung angegeben und Netzwerkgerätegruppen basierend auf Gerätetypen, Standort oder WLCs zugewiesen werden.

Schritt 3: Geben Sie die 9800 WLC-Einstellungen wie im Bild dargestellt ein. Geben Sie den gleichen RADIUS-Schlüssel ein, der bei der Servererstellung auf der WLC-Seite definiert wurde. Klicken Sie dann auf Senden.

Network Devices

Name

9800-WLC

Description



IP Address



* IP :

192.0.2.20

/

32



Device Profile



Cisco



Model Name



Software Version



Network Device Group

Location

All Locations



[Set To Default](#)

IPSEC

Is IPSEC Device



[Set To Default](#)

Device Type

All Device Types



[Set To Default](#)



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

[Show](#)

Einstellungen des 9800 WLC

Schritt 4: Navigieren Sie zu Administration > Network Resources > Network Devices (Verwaltung

> Netzwerkressourcen > Netzwerkgeräte), um die Liste der Netzwerkgeräte anzuzeigen.

Network Devices

Selected 0 Total 6  

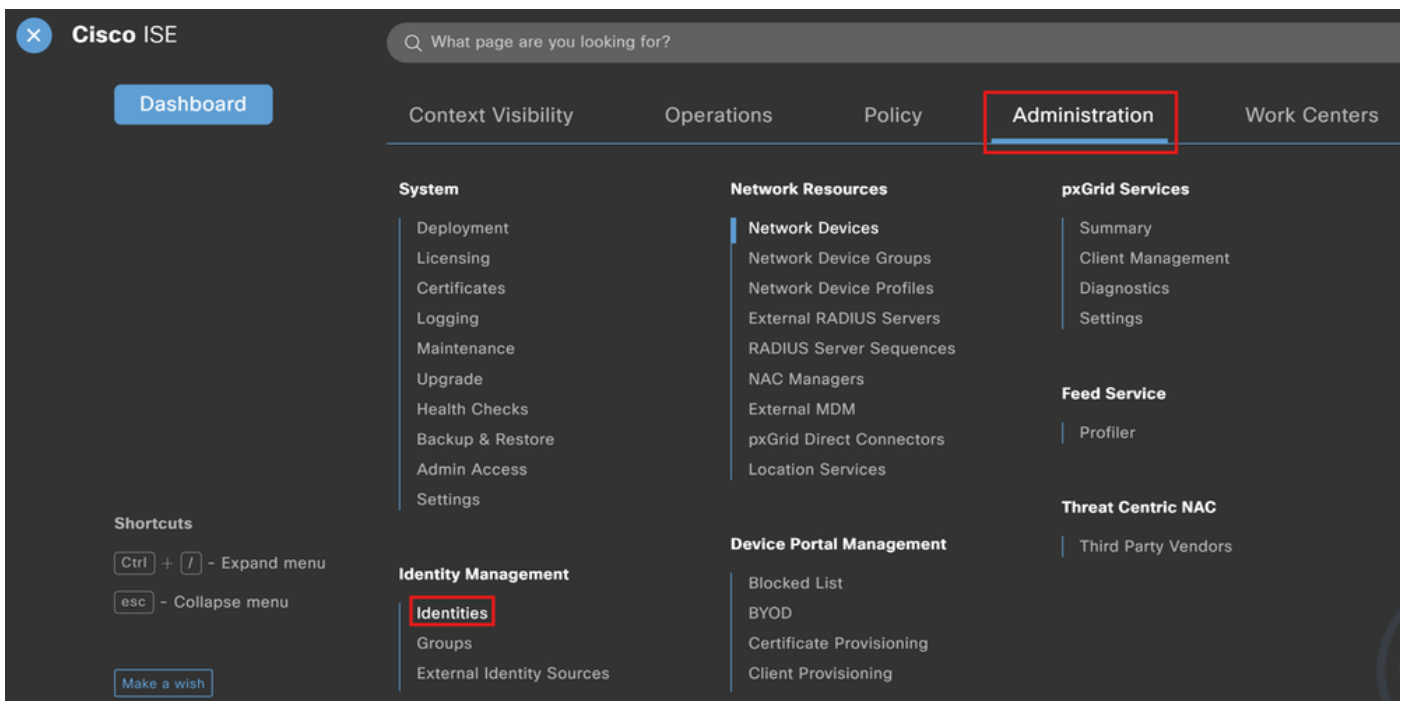
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

☐	Name	IP/Mask	Profile Name	Location	Type
☐	9800		 Cisco 	All Locations	All Device Types
☐	9800-2		 Cisco 	All Locations	All Device Types
☐	9800-40		 Cisco 	All Locations	All Device Types
☐	9800-WLC	192.0.2.20/32	 Cisco 	All Locations	All Device Types

Liste der Netzwerkgeräte

Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie zu Administration > Identity Management > Identities:



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. Below the navigation bar, the 'Administration' section is expanded, showing three main categories: 'System', 'Network Resources', and 'pxGrid Services'. Under 'Network Resources', the 'Network Devices' link is highlighted with a red box. Below 'Network Resources', the 'Identity Management' section is visible, with the 'Identities' link highlighted with a red box. The 'Identities' link is also highlighted with a red box in the 'Identity Management' section. The 'Identities' link is highlighted with a red box. The 'Identities' link is highlighted with a red box.

ISE-Verwaltung - Identitäten

Schritt 2: Navigieren Sie zu Benutzer, und klicken Sie auf +Hinzufügen.

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#)

Status

Username ^

Description

First Name

Last Name

Em:

Benutzer hinzufügen

Schritt 3: Geben Sie den Benutzernamen und das Kennwort für den Gastbenutzer ein, und klicken Sie auf Senden.

[Network Access Users List](#) > [New Network Access User](#)

Network Access User

* Username

guest

Status

☒ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

☒ With Expiration

Password will expire in 60 days

☐ Never Expires

Password

Re-Enter Password

* Login Password

[Generate Password](#)

i

Enable Password

[Generate Password](#)

i

Neuen Benutzer auf ISE erstellen

Schritt 4: Navigieren Sie zu Administration > Identity Management > Identities > Users, um die Benutzerliste anzuzeigen.

Network Access Users

Edit

+ Add

Change Status

Import

Export

Delete

Duplicate

Status

Username

Descripti...

First Name

Last Name

Email Address

User Identity Groups

Admin

Enabled

guest

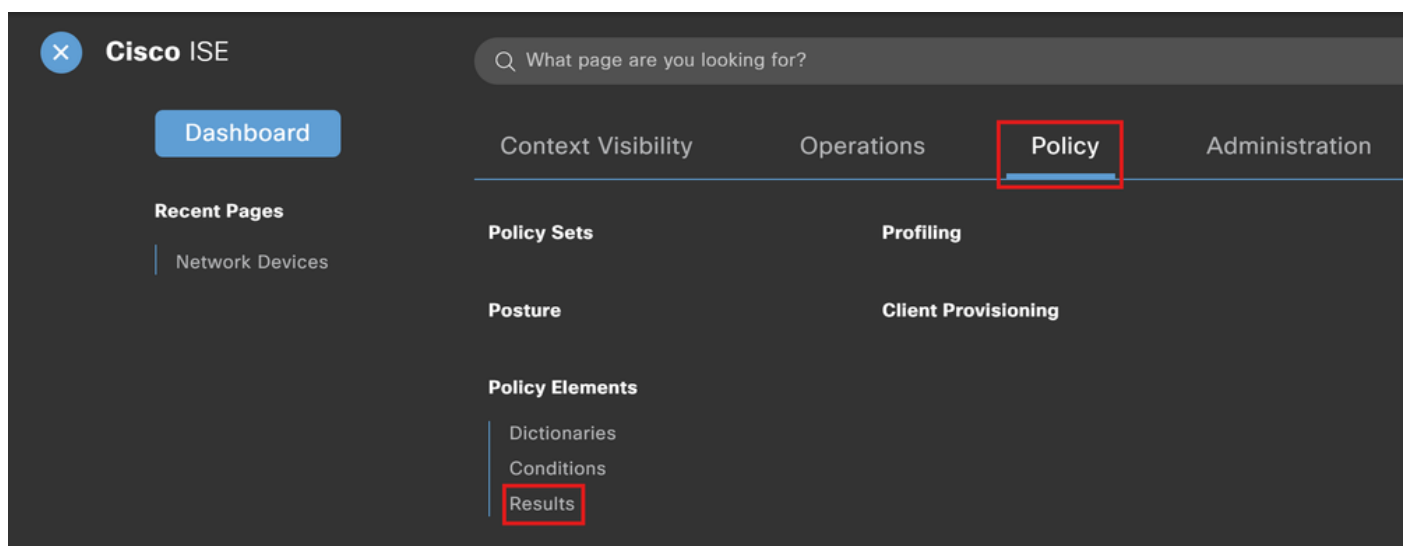
Liste der Netzwerkzugriffsbenutzer

Erstellen des Autorisierungsprofils

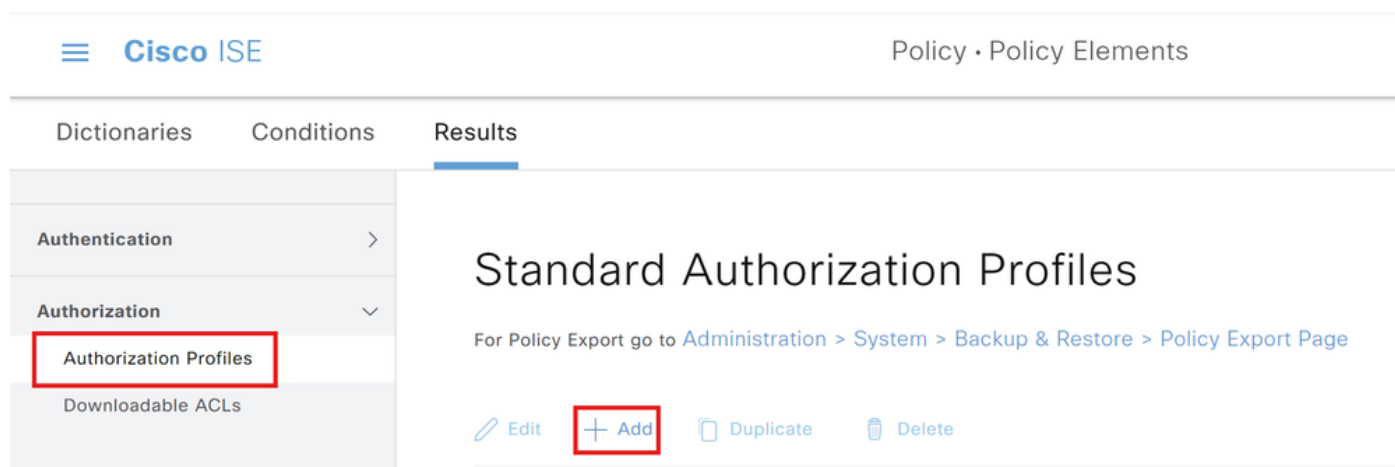
Das Richtlinienprofil ist das Ergebnis, das einem Client basierend auf seinen Parametern (wie MAC-Adresse, Anmeldeinformationen, verwendetes WLAN usw.) zugewiesen wird. Es kann bestimmte Einstellungen wie Virtual Local Area Network (VLAN), Access Control Lists (ACLs), URL-Umleitungen (Uniform Resource Locator) usw. zuweisen.

Diese Schritte zeigen, wie das für die Umleitung des Clients an das Authentifizierungsportal erforderliche Autorisierungsprofil erstellt wird. Beachten Sie, dass in aktuellen Versionen der ISE bereits ein Autorisierungsergebnis von Cisco_Webauth vorhanden ist. Hier können Sie es bearbeiten und den Namen der Umleitungs-ACL so ändern, dass er mit der Konfiguration im WLC übereinstimmt.

Schritt 1: Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse.



Schritt 2: Navigieren Sie zu Autorisierung > Autorisierungsprofile. Klicken Sie auf +Hinzufügen, um ein Autorisierungsprofil zu erstellen.



The screenshot shows the Cisco ISE interface. The top navigation bar includes the Cisco ISE logo and the text 'Policy • Policy Elements'. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Results' tab is active. On the left sidebar, under the 'Authorization' section, 'Authorization Profiles' is highlighted with a red box. In the main content area, the title 'Standard Authorization Profiles' is displayed. Below the title, there is a link: 'For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)'. At the bottom of the main content area, there are four buttons: 'Edit', '+ Add' (highlighted with a red box), 'Duplicate', and 'Delete'.

Autorisierungsprofil hinzufügen

Schritt 3: Erstellen Sie das Autorisierungsprofil LWA_EA_AUTHORIZATION. Bei den Attributdetails muss es sich um Access Type=ACCESS_ACCEPT handeln. Klicken Sie auf Senden.

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name	LWA_EA_AUTHORIZATION
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	☐
Track Movement	☐
Agentless Posture	☐
Passive Identity Tracking	☐

Erstellen des Autorisierungsprofils

Schritt 4: Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile, um die Autorisierungsprofile anzuzeigen.

Dictionaries

Conditions

Results

Authentication >

Authorization ▾

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

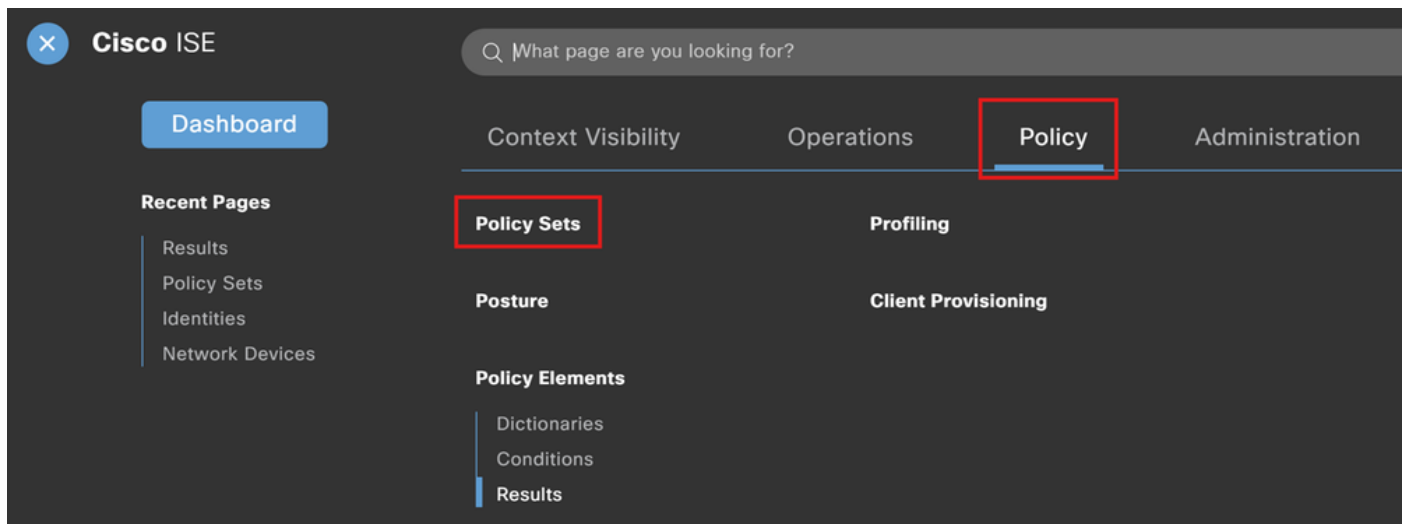
[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

☐	Name	Profile	
☐	9800-admin-priv	 Cisco	i
☐	9800-helpdeskuser-priv	 Cisco	i
☐	AuthZ-Guest	 Cisco	i
☐	AuthZ_Guest-Redirect	 Cisco	i
☐	AuthZ_Mobile	 Cisco	i
☐	Block_Wireless_Access	 Cisco	i
☐	Cisco_IP_Phones	 Cisco	i
☐	Cisco_Temporal_Onboard	 Cisco	i
☐	Cisco_WebAuth	 Cisco	i
☐	LWA_EA_AUTHORIZATION	 Cisco	i

Liste der Autorisierungsprofile

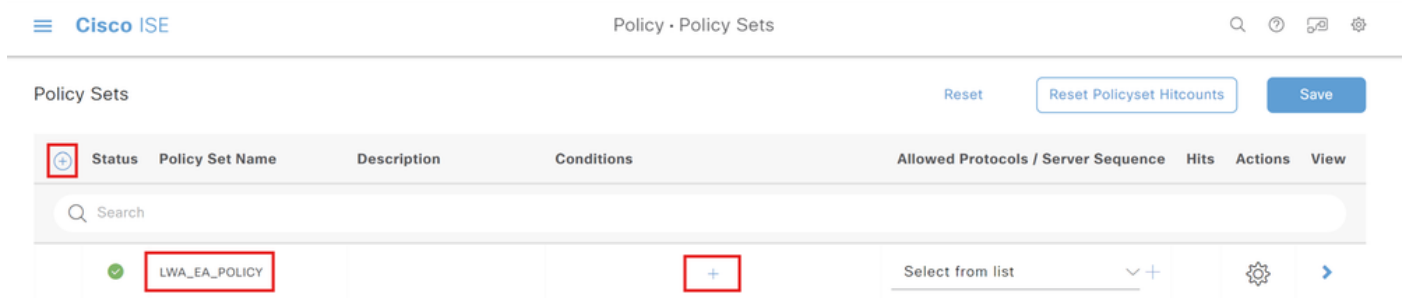
Konfiguration der Authentifizierungsregel

Schritt 1: Navigieren Sie zu Policy > Policy Sets.



ISE-Richtlinie - Policy Sets

Schritt 2. Wählen Sie das +-Zeichen, geben Sie den Namen des Policy Sets LWA_EA_POLICY ein. Klicken Sie auf die Spalte Bedingungen.



Konfiguration der Authentifizierungsregel

Schritt 3. Wählen Sie im Dictionary die Option Netzwerkzugriff. Wählen Sie für das Attribut die Option Benutzername aus.

Conditions Studio

Library

Search by Name



5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	

Editor

Network Access-UserName

Select attribute for condition

Dictionary Attribute ID Info

Network Access	Attribute	ID	
Network Access	Device IP Address		
Network Access	ISE Host Name		
Network Access	NetworkDeviceName		
Network Access	Protocol		
Network Access	UserName		
Network Access	VN		

Wörterbuch-Netzwerkzugriff

Schritt 4. Legen Sie Equals fest und geben Sie guest in das Textfeld ein (den Benutzernamen, der unter Administration > Identity Management > Identities > Users definiert ist). Klicken Sie auf Speichern, um die Änderungen zu speichern.

Search by Name



5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	
Wireless_Access	
Wireless_MAB	

Network Access-UserName

Equals guest

Set to 'Is not'

Duplicate Save

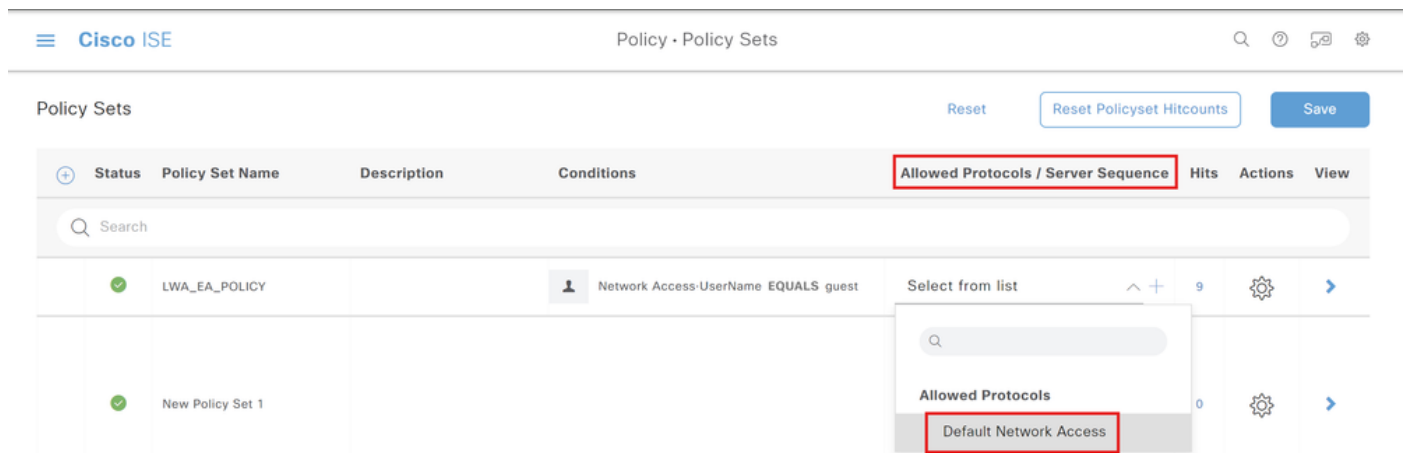
NEW AND OR

Close

Use

Benutzername Gast

Schritt 5: Navigieren Sie zu Policy > Policy Sets. Wählen Sie im von Ihnen erstellten Richtlinienatz in der Spalte Zugelassene Protokolle/Serversequenz die Option Standard-Netzwerkzugriff aus.



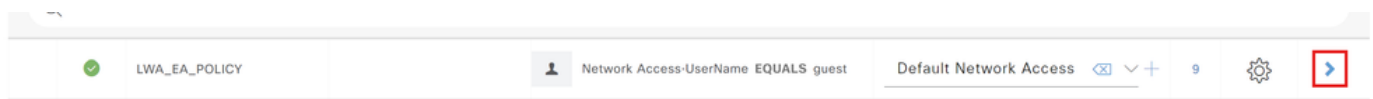
Policy Sets

Schritt 6: Klicken Sie auf Speichern, um die Änderungen zu speichern.

Konfiguration der Authentifizierungsregeln

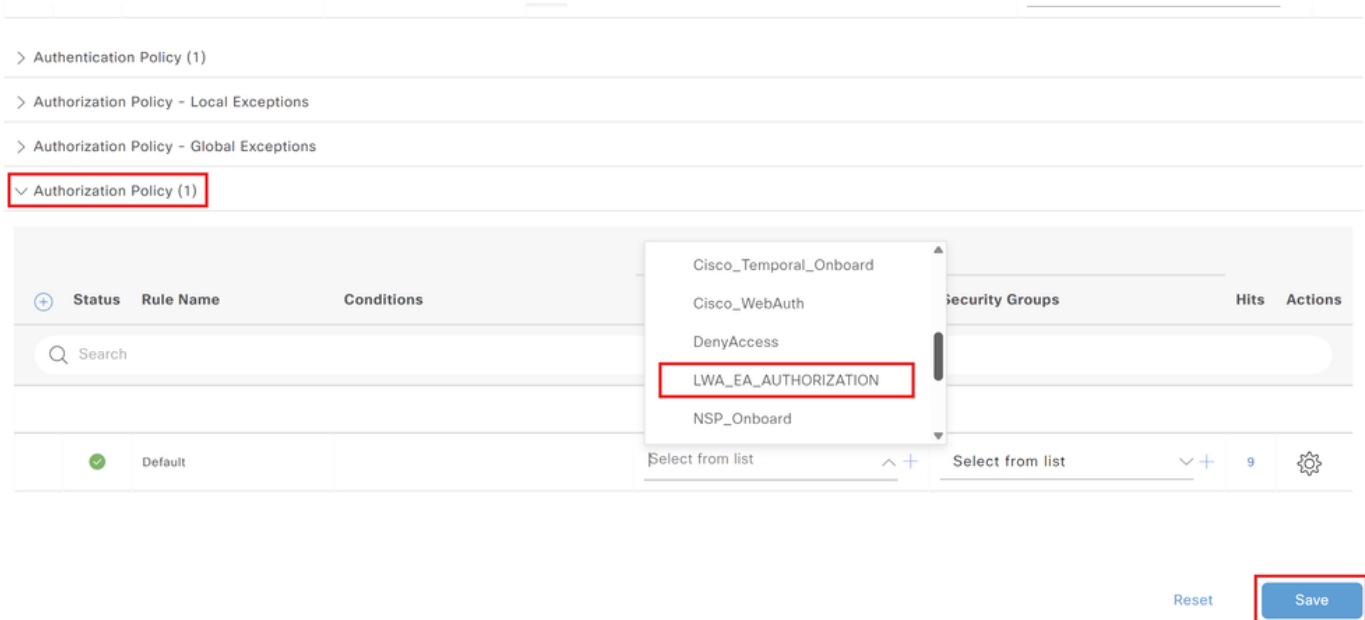
Die Autorisierungsregel bestimmt, welche Berechtigungen (welches Autorisierungsprofil) auf den Client angewendet werden.

Schritt 1: Navigieren Sie zu Policy > Policy Sets. Klicken Sie auf den Pfeil des erstellten Richtlinienatzes.



Pfeil für Richtlinienatz

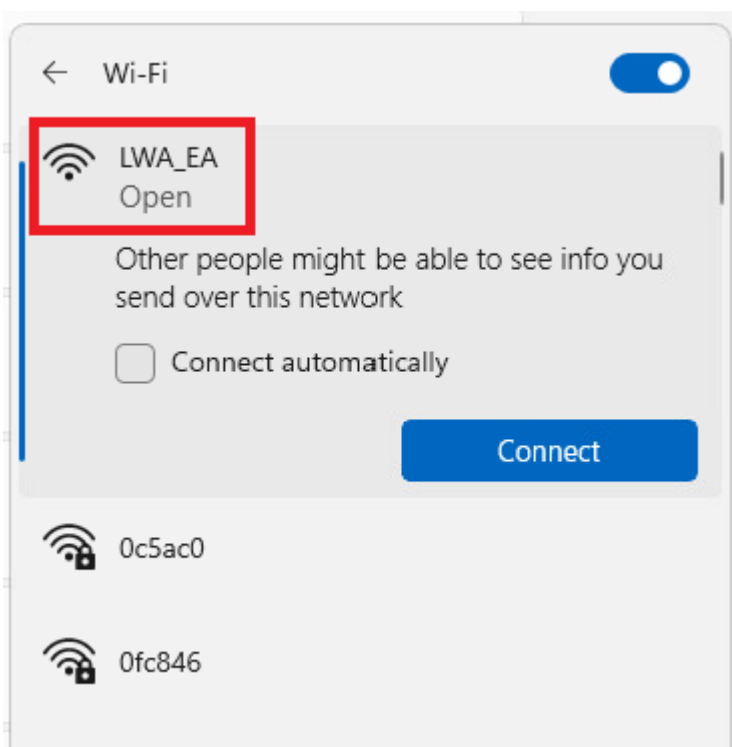
Schritt 2. Erweitern Sie auf derselben Seite mit dem Richtlinienatz die Option Autorisierungsrichtlinie, wie im Bild dargestellt. Löschen Sie in der Spalte Profile DenyAccess, und fügen Sie LWA_EA_AUTHORIZATION hinzu. Klicken Sie auf Speichern, um die Änderungen zu speichern.



Autorisierungsrichtlinie

Gastclient verbinden

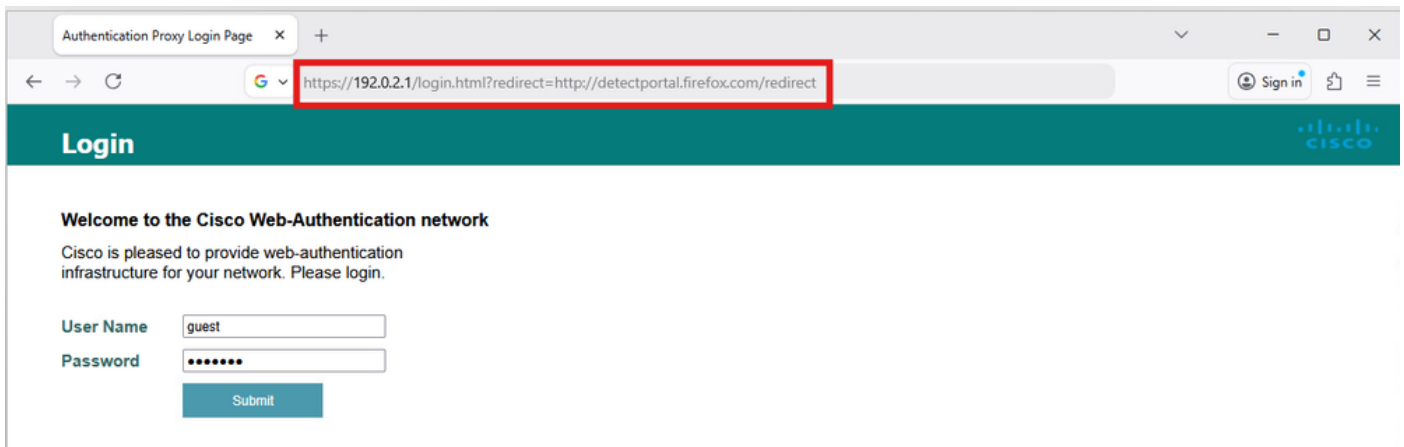
Schritt 1: Navigieren Sie auf Ihrem Computer/Telefon zu den Wi-Fi-Netzwerken, suchen Sie die SSID LWA_EA und wählen Sie Verbinden.



Gastclient verbinden

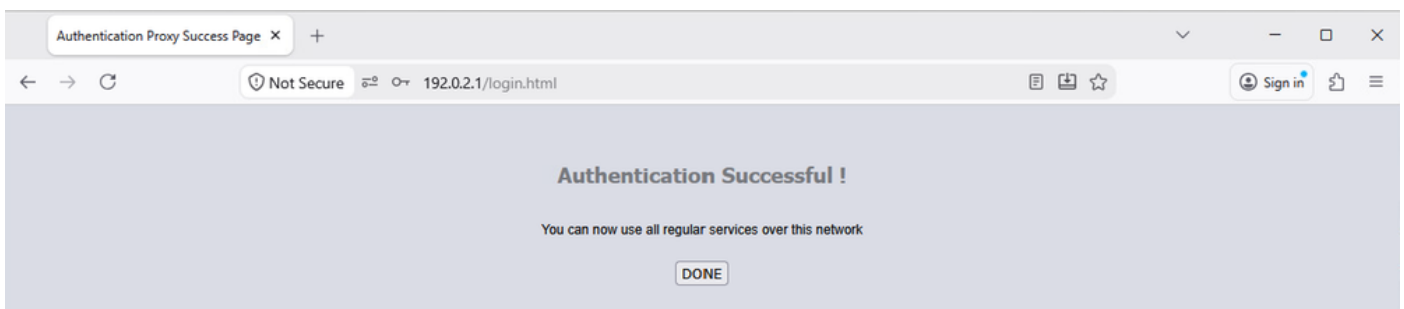
Schritt 2: Ein Browserfenster mit der Anmeldeseite wird angezeigt. Die Umleitungs-URL befindet

sich im URL-Feld, und Sie müssen den Benutzernamen und das Kennwort eingeben, um Zugriff auf das Netzwerk zu erhalten. Wählen Sie dann Senden.



Anmeldeseite mit Umleitungs-URL

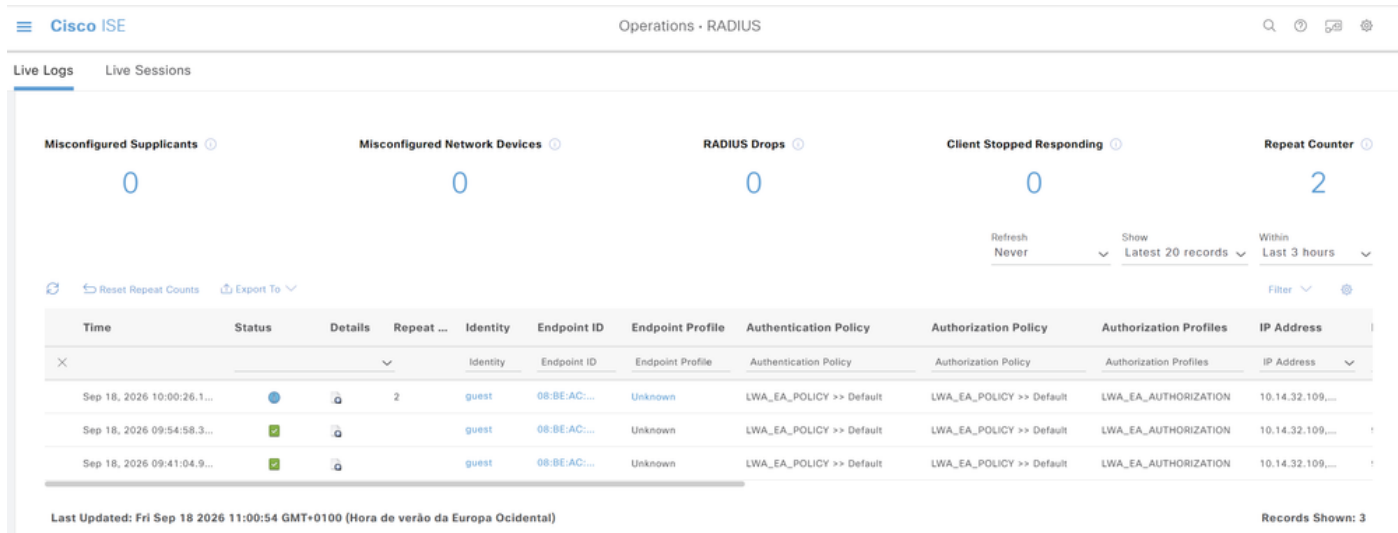
Wenn die Anmeldeinformationen korrekt sind, wird eine Seite für die erfolgreiche Authentifizierung angezeigt:



Seite "Authentifizierung erfolgreich"

 Anmerkung: Die angegebene URL wurde vom WLC bereitgestellt. Sie enthält die virtuelle WLC-IP und die Umleitung für die Windows-Verbindungstest-URL.

Schritt 3: Navigieren Sie zu Operations > RADIUS > Live Logs. Sie sehen das authentifizierte Client-Gerät sowie die Authentifizierungs- und Autorisierungsrichtlinien.



Radius Live-Protokolle

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Show WLAN Summary

<#root>

```
9800WLC#show wlan summary
```

```
Number of WLANs: 1
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----
```

```
1 LWA_EA LWA_EA UP [open],[Web Auth]
```

```
9800WLC#
```

```
show wlan name LWA_EA
```

```
WLAN Profile Name : LWA_EA
=====
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
```

Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security

Web Based Authentication : Enabled

OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

(...)
Security-2.4GHz/5GHz

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
```

```
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

```
9800WLC#show aaa method-lists authentication
```

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

```
name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP
```

```
authen queue=AAA_ML_AUTHEN_ENABLE
```

```
authen queue=AAA_ML_AUTHEN_PPP
```

```
authen queue=AAA_ML_AUTHEN_SGBP
```

```
(...)
```

```
9800WLC#show aaa method-lists authorization
```

```
author queue=AAA_ML_AUTHOR_SHELL
```

```
author queue=AAA_ML_AUTHOR_NET
```

```
name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP
```

```
author queue=AAA_ML_AUTHOR_CONN
```

```
author queue=AAA_ML_AUTHOR_IPMOBILE
```

```
author queue=AAA_ML_AUTHOR_RM
```

```
(...)
```

```
9800WLC#show aaa servers
```

```
RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS
```

```
State: current UP, duration 8421s, previous duration 0s
```

```
Dead: total time 0s, count 0
```

```
Platform State from SMD: current UP, duration 8421s, previous duration 0s
```

```
SMD Platform Dead: total time 0s, count 0
```

```
Platform State from WNCd (0) : current UP
```

```
(...)
```

Fehlerbehebung

Häufige Probleme

Nachfolgend finden Sie eine Reihe von Anleitungen zur Behebung von Web-Authentifizierungsproblemen, wie z. B.:

- Benutzer können sich nicht authentifizieren.
- Zertifikatprobleme.
- Die Umleitungs-URL funktioniert nicht.
- Gastbenutzer können keine Verbindung zum Gast-WLAN herstellen.
- Benutzer erhalten keine IP-Adresse.
- Die Umleitung zur Seite "Web Authentication Log in Page" ist fehlgeschlagen.
- Nach erfolgreicher Authentifizierung erhalten Gastbenutzer keinen Zugriff auf das Internet.

In diesen Handbüchern werden die einzelnen Schritte zur Fehlerbehebung ausführlich beschrieben:

- [Beheben gängiger Probleme bei der Webauthentifizierung](#)
- [Andere Situationen, in denen Fehler behoben werden müssen](#)

Bedingtes Debuggen und Radio Active Trace und eingebettete Paketerfassung

Sie können bedingtes Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debyebeine für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Um das bedingte Debuggen zu aktivieren, verwenden Sie die Schritte im Handbuch, [Conditional Debug und RadioActive trace](#).

Sie können auch Embedded Packet Capture (EPC) sammeln. EPC ist eine Paketerfassungseinrichtung, die einen Überblick über Pakete ermöglicht, die an die Catalyst 9800 WLCs gerichtet sind, von diesen stammen und diese durchlaufen, nämlich DHCP-, DNS- und HTTP GET-Pakete in LWA. Diese Aufzeichnungen können zur Offline-Analyse mit Wireshark exportiert werden. Weitere Informationen hierzu finden Sie unter [Embedded Packet Capture](#).

Beispiel eines erfolgreichen Versuchs

Dies ist die Ausgabe von RA_traces für einen erfolgreichen Versuch, jede der Phasen beim Zuordnungs-/Authentifizierungsprozess in Verbindung mit einer Gast-SSID mit dem RADIUS-Server zu identifizieren.

802.11-Zuordnung/Authentifizierung:

```
[client-orch-sm] [17062]: (Hinweis): MAC: 08be.ac3f-Zuordnung empfangen. BSSID cc70.edcf.552f,
WLAN LWA_EA, Steckplatz 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f: Zuordnungsanforderung für Punkt 11 empfangen.
Verarbeitung gestartet, SSID: LWA_EA, Richtlinienprofil: POLICY_PROFILE, AP-Name: CW9172I-LAB, AP
MAC-Adresse: 2ce3.8eb4BSSID MAC000.0000.0000wlan-ID: 1RSSI: -49, SNR 46
[Client-Orch-State] [17062]: (Hinweis): MAC: 08be.ac3f Client-Zustandsübergang: S_CO_INIT ->
S_CO_ASSOCIATION
[dot11-validate] [17062]: (Info): MAC: 08be.ac3f Dot11 dh die ext/supp Raten zu validieren. Validierung
für unterstützte Raten durchlaufen radio_type 2
```

[dot11-validate] [17062]: (Info): MAC: 08be.ac3f WiFi Direct: Dot11 validieren P2P IE. P2P IE nicht vorhanden.

[dot11] [17062]: (debug): MAC: 08be.ac3f dot11 Zuordnungsantwort senden. Framing-Zuordnungsantwort mit resp_status_code: 0

[dot11] [17062]: (debug): MAC: 08be.ac3f Dot11 Funktionsinfo byte1 1, Byte2: 11

[dot11-frame] [17062]: (Info): MAC: 08be.ac3f WiFi Direct: Assoc Resp. mit P2P IE überspringen: Direkte Wi-Fi-Richtlinie deaktiviert

[dot11] [17062]: (Info): MAC: 08be.ac3f dot11 Zuordnungsantwort senden. ASSOC-Antwort der Länge: 130 mit resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS

[dot11] [17062]: (Hinweis): MAC: 08be.ac3f Zuordnungserfolg. AID 1, Roaming = Falsch, WGB = Falsch, 11r = Falsch, 11w = Falsch Schnelles Roaming = Falsch

[dot11] [17062]: (Info): MAC: 08be.ac3f DOT11-Zustandsübergang: S_DOT11_INIT -> S_DOT11_ASSOCIATED

[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Station Dot11-Zuordnung erfolgreich.

IP-Lernprozess:

[Client-Orch-State] [17062]: (Hinweis): MAC: 08be.ac3f Client-Zustandsübergang: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [17062]: (Info): MAC: 08be.ac3f Übergang zum IP-Lernstatus: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

[client-auth] [17062]: (Info): MAC: 08be.ac3f Zustandsübergang der Client-Authentifizierungsschnittstelle: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

[client-iplearn] [17062]: (Hinweis): MAC: 08be.ac3f Client-IP erfolgreich lernen. Methode: DHCP-IP: 10.14.32.109

[client-iplearn] [17062]: (Info): MAC: 08be.ac3f Übergang zum IP-Lernstatus: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Erhaltene IP-Lernantwort. Methode: IPLEARN_METHODE_DHCP

Layer-3-Authentifizierung:

[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Ausgelöste L3-Authentifizierung. Status = 0x0, Erfolg

[Client-Orch-State] [17062]: (Hinweis): MAC: 08be.ac3f Client-Zustandsübergang: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

[client-auth] [17062]: (Hinweis): MAC: 08be.ac3f L3-Authentifizierung initiiert. LWA

[client-auth] [17062]: (Info): MAC: 08be.ac3f Zustandsübergang der Client-Authentifizierungsschnittstelle: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd when in LOGIN state

[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET-Anforderung

[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]GET analysieren, src [10.14.32.109] dst [10.107.221.82] url [<http://firefox.detect.portal/>]

[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]Vollständige Informationen: parse_request return 8

[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 E/A-Zustand LESEN -> SCHREIBEN

[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 E/A-Zustand SCHREIBEN -> LESEN

[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 E/A-Zustand NEU -> LESEN

[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Lesevorgang, Nachricht bereit

[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd, wenn sich der Status LOGIN befindet

Layer-3-Authentifizierung erfolgreich. Verschieben Sie den Client in den RUN-Status:

```
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] Gast-Benutzername für Client 08be.ac3f
empfangen
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is
received for attr auth-domain(954)
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] Webauth-Methode wechselt den Zustand von
'Wird ausgeführt' zu 'Erfolg erstellen'
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] Kontext ändert Status von 'Wird ausgeführt' in
'Erfolg authentifizieren'
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is
received for attr method(757)
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] Ausgelöstes Ereignis AUTHZ_SUCCESS (11)
[auth-mgr] [17062]: (Info): [08be.ac3f:capwap_90000004] Kontext-Statusänderung von 'Erfolg
authentifizieren' zu 'Erfolg authentifizieren'
[webauth-acl] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]Anwenden der IPv4-
Abmelde-ACL über SVM, Name: IP-Adm-V4-LOGOUT-ACL, Priorität: 51, IIF-ID: 0
[Webauth-sess] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]Verwendete Param-Map:
global
[Webauth-State] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]Verwendete Param-Map:
global
[Webauth-State] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]Status AUTHC_SUCCESS
-> AUTHZ
[Webauth-Seite] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]Senden der Webauth-
Erfolgsseite
[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]56539/218 E/A-Zustand
AUTHENTIFIZIEREN -> SCHREIBEN
[Webauth-io] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]56539/218 E/A-Zustand
SCHREIBEN -> ENDE
[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.14.32.109]56539/218 Entfernen Sie
IO ctx und schließen Sie den Sockel, ID [99000029]
[client-auth] [17062]: (Hinweis): MAC: 08be.ac3f L3-Authentifizierung erfolgreich. ACL[:]
[client-auth] [17062]: (Info): MAC: 08be.ac3f Zustandsübergang der Client-Authentifizierungsschnittstelle:
S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[Webauth-httpd] [17062]: (Info): capwap_90000004[08be.ac3f][ 10.48.39.243]56538/219 Entfernen von
IO ctx und Schließen des Sockels, ID [D7000028]
[errmsg] [17062]: (Info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd:
Benutzernamen-Eintrag (Gast) verbunden mit ssid (LWA_EA) für Gerät mit MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (Info): [ Angewandtes Attribut :bsn-vlan-interface-name 0 "VLAN0039" ]
[aaa-attr-inf] [17062]: (Info): [Angewendetes Attribut: Timeout 0 1800 (0x708) ]
[aaa-attr-inf] [17062]: (Info): [Angewendetes Attribut: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL" ]
[ewlc-qos-client] [17062]: (Info): MAC: 08be.ac3f QoS-Ausführungsstatushandler für Clients
[rog-proxy-capwap] [17062]: (debug): RUN-Statusbenachrichtigung für verwalteten Client: 08be.ac3f
[Client-Orch-State] [17062]: (Hinweis): MAC: 08be.ac3f Client-Zustandsübergang:
S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN
```

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

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.