

Lokale webverificatie configureren met externe verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Webverificatie](#)

[Soorten authenticatie](#)

[Database voor verificatie](#)

[Lokale webverificatie](#)

[Lokale webverificatie met externe verificatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Lokale webverificatie configureren met externe verificatie op de CLI](#)

[AAA-server en -servergroep configureren](#)

[Lokale verificatie en autorisatie configureren](#)

[Parameterkaarten configureren](#)

[WLAN-beveiligingsparameters configureren](#)

[Beleidsprofiel voor draadloze verbindingen maken](#)

[Een beleidstag maken](#)

[Een beleidstag toewijzen aan een toegangspunt](#)

[Lokale webverificatie configureren met externe verificatie op de WebUI](#)

[AAA-configuratie op 9800 WLC](#)

[WebAuth-configuratie](#)

[WLAN-configuratie](#)

[Configuratie beleidsprofiel](#)

[Configuratie van beleidstag](#)

[Toewijzing van beleidstag](#)

[ISE-configuratie](#)

[Gastclient verbinden](#)

[Verifiëren](#)

[WLAN-overzicht weergeven](#)

[Parameterkaartconfiguratie weergeven](#)

[AAA-gegevens weergeven](#)

[Problemen oplossen](#)

[Veelvoorkomende problemen](#)

[Voorwaardelijke foutopsporing en Radio Active Trace en Embedded Packet Capture](#)

[Voorbeeld van een geslaagde poging](#)

Inleiding

In dit document wordt beschreven hoe u lokale webverificatie met externe verificatie configureert op een 9800 WLC en ISE.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van 9800 Wireless LAN Controllers (WLC)
- Lichte toegangspunten (LAP's)
- Hoe u een externe webserver Identity Services Engine (ISE) instelt en configureert.
- Hoe DHCP- en DNS-servers te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 9800-40 WLC Cisco IOS® XE, versie 17.18.4a met APSP1 en APSP2
- Identity Services Engine (ISE), versie 3.2.0.542
- Cisco® Wireless 9172I-reeks Wi-Fi 7-toegangspunt, versie 17.18.4.202

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Webverificatie

Webverificatie is een Layer 3-beveiligingsfunctie waarmee gastgebruikers toegang hebben tot het netwerk.

Deze functie is ontworpen om gasten eenvoudig en veilig toegang te bieden tot open SSID's, zonder dat een gebruikersprofiel hoeft te worden geconfigureerd, en het kan ook werken met beveiligingsmethoden van Layer 2.

Het doel van webverificatie is om niet-vertrouwde apparaten (gasten) toegang te geven tot het netwerk met beperkte netwerktoegangsrechten, via een gastnetwerk dat kan worden geconfigureerd met beveiligingsmechanismen en de beveiliging van het netwerk niet in gevaar wordt gebracht. Als gastgebruikers toegang tot het netwerk willen hebben, moeten ze met succes verifiëren, dat wil zeggen dat ze de juiste referenties moeten verstrekken of het Acceptable Use Policy (AUP) moeten accepteren om toegang tot het netwerk te krijgen.

Webauthenticatie is een voordeel voor bedrijven omdat het de loyaliteit van gebruikers bevordert, het bedrijf compliant maakt om een disclaimer te gebruiken die de gastgebruiker moet accepteren en het bedrijf in staat stelt om met bezoekers in contact te komen.

Om webverificatie te implementeren, moet rekening worden gehouden met de manier waarop het gastenportaal en de authenticatie worden behandeld. Er zijn twee gemeenschappelijke methoden:

- Lokale webverificatie (LWA): een methode om gastgebruikers rechtstreeks vanuit de WLC naar een portal te leiden. De omleiding en pre-WebAuth ACL zijn lokaal geconfigureerd op de WLC.
- Central web authentication (CWA): Een methode van omleiding van gastgebruikers waarbij de omleiding-URL en de omleiding-ACL centraal worden geconfigureerd op een externe server (bijvoorbeeld ISE) en via RADIUS aan de WLC worden gecommuniceerd. Bij centrale webverificatie bevinden de redirect URL en redirect ACL zich centraal op een externe server (zoals RADIUS). De RADIUS-server is degene die de verificatie afhandelt en stuurt instructies naar de WLC. In CWA vereist de WLC geen lokaal webauteurscertificaat, is slechts één certificaat nodig op het centrale webportaal en is een centrale verificatieserver vereist, zoals ISE. Navigeer voor meer informatie over CWA naar [Configure Central Web Authentication \(CWA\) op Catalyst 9800 WLC en ISE](#).

In Local Web Authentication kan het webportaal aanwezig zijn op de WLC of op een externe server. In LWA met Externe Authenticatie is het webportaal aanwezig op de WLC. In LWA met External Web Server is het webportaal aanwezig op een externe server (zoals Cisco DNA Spaces). Een voorbeeld van LWA met externe webserver wordt in detail beschreven op: [Configure DNA Spaces Captive Portal with Catalyst 9800 WLC](#).

Diagram van de verschillende webauthenticatiemethoden:

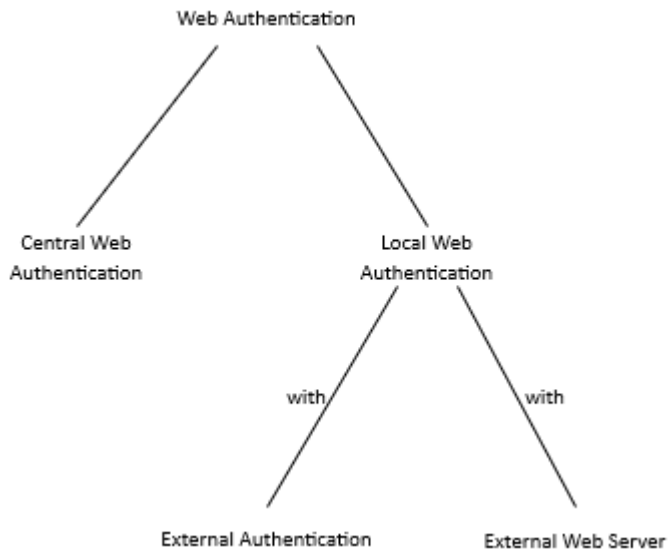


Diagram van de verschillende Web Authenticatie Methoden



Opmerking: Als u Wi-Fi 7 AP's met webverificatie implementeert op een 9800 WLC, moet u ervoor zorgen dat u een aanbevolen Cisco IOS XE-release zoals 17.18.4a of hoger uitvoert.

Soorten authenticatie

Er zijn vier soorten authenticatie om de gastgebruiker te verifiëren:

- Webauth: Voer gebruikersnaam en wachtwoord in.
- Toestemming (web-passthrough): accepteer AUP.
- Authbypass: Authenticatie op basis van het MAC-adres van het gastgebruikersapparaat.
- Webconsent: een mix tussen gebruikersnaam/wachtwoord en accepteer AUP.

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 soorten authenticatie om de gastgebruiker te verifiëren

Database voor verificatie

De referenties voor verificatie kunnen worden opgeslagen op een LDAP-server, lokaal op de WLC of op de RADIUS-server.

- Lokale database: De referenties (gebruikersnaam en wachtwoord) worden lokaal opgeslagen op de WLC.
- LDAP-database: De referenties worden opgeslagen in de LDAP-back-enddatabase. De WLC zoekt op de LDAP-server naar de referenties van een bepaalde gebruiker in de database.
- RADIUS-database: De referenties worden opgeslagen in de back-enddatabase van RADIUS. De WLC zoekt op de RADIUS-server naar referenties van een bepaalde gebruiker in de database.

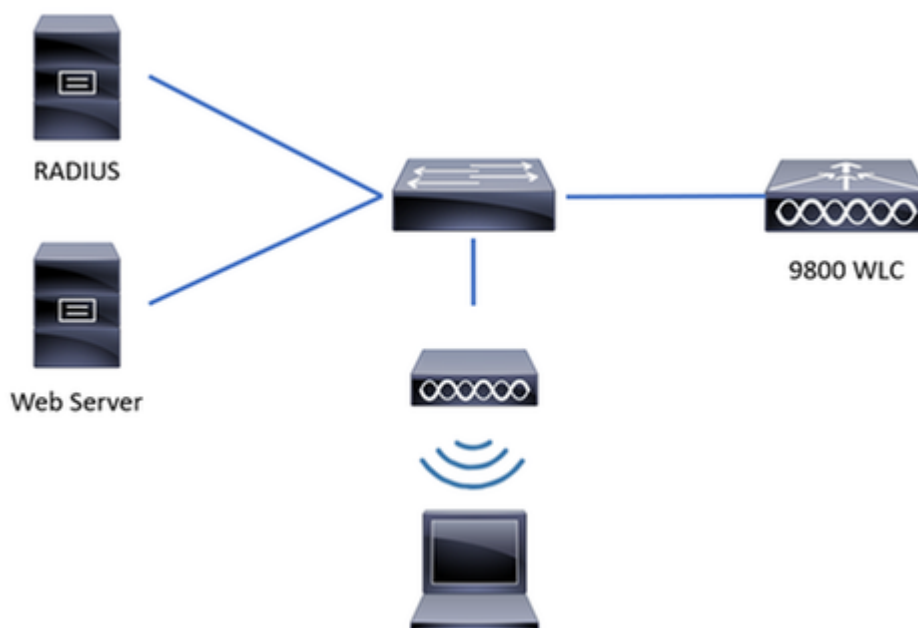
Lokale webverificatie

Bij lokale webverificatie wordt de gastgebruiker direct vanuit de WLC doorgestuurd naar een webportaal.

Het webportaal kan zich in de WLC of in een andere server bevinden. Wat het lokaal maakt, is het feit dat de redirect-URL en de ACL die overeenkomt met het verkeer op de WLC moeten staan (niet de locatie van het webportaal). In LWA, wanneer een gastgebruiker verbinding maakt met het gastnetwerk, onderschept de WLC de verbinding van de gastgebruiker en leidt deze door naar de

URL van het webportaal, waar de gastgebruiker wordt gevraagd om te verifiëren. Wanneer de gastgebruiker referenties invoert (gebruikersnaam en wachtwoord), legt de WLC de referenties vast. De WLC verifieert de gastgebruiker met een LDAP-server, RADIUS-server of lokale database (database lokaal aanwezig op de WLC). In het geval van een RADIUS-server (een externe server zoals ISE) kan deze niet alleen worden gebruikt om referenties op te slaan, maar ook om opties te bieden voor apparaatregistratie en zelfvoorziening. In het geval van een externe webserver, zoals Cisco DNA Spaces, is het webportaal daar aanwezig. In LWA is er één certificaat op de WLC en een ander op het webportaal.

De afbeelding vertegenwoordigt de algemene topologie van LWA:



Algemene topologie van LWA

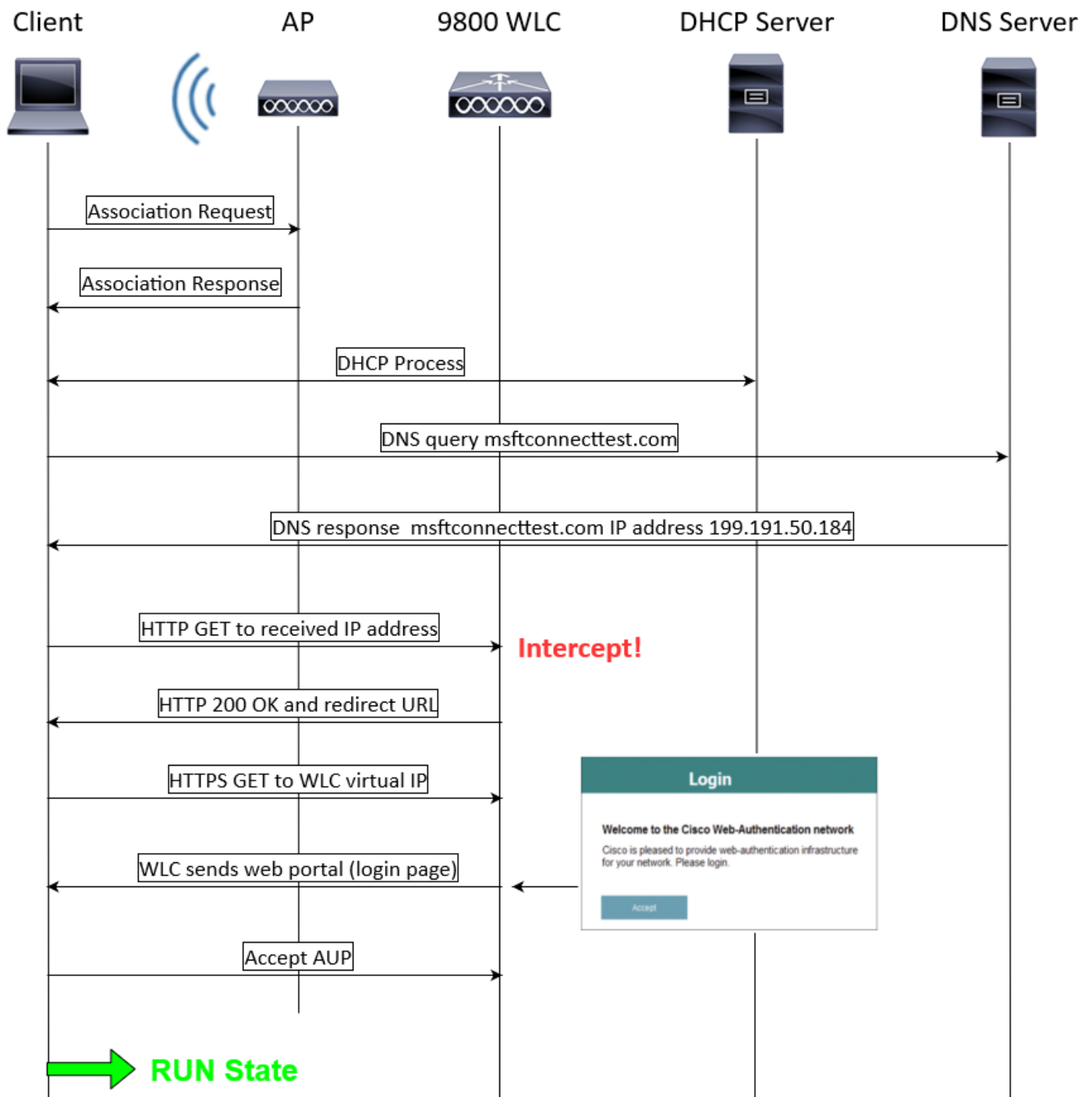
Apparaten in de netwerktopologie van LWA:

- Client: verzendt verzoeken naar DHCP- en DNS-server, vraagt toegang tot het gastnetwerk WLAN en reageert op verzoeken van de WLC.
- Toegangspunt: verbonden met een switch, zendt het gastnetwerk uit en biedt een draadloze verbinding met gastgebruikersapparaten. Het staat ook DHCP- en DNS-pakketten toe voordat de gastgebruiker is geverifieerd (voordat u geldige referenties invoert).
- WLC: Beheert de AP's en clients. De WLC host de redirect URL en de ACL die overeenkomt met het verkeer. Onderschept HTTP-verzoeken van de gastgebruikers, leidt ze door naar een webportaal (inlogpagina) waar gastgebruikers moeten verifiëren. Het registreert de referenties en verifieert de gastgebruikers, en het verzendt toegangsverzoeken naar een externe server, LDAP-server of lokale database om te bevestigen of de referenties geldig zijn.
- Verificatieserver: reageert op toegangsverzoeken van de WLC met toegang accepteren/weigeren. De verificatieserver valideert de referenties van de gastgebruiker en

stelt de WLC op de hoogte als de referenties geldig of ongeldig zijn. Als de referenties geldig zijn, heeft de gastgebruiker toegang tot het netwerk (de verificatieserver biedt opties voor apparaatregistratie en zelfvoorziening). Als de referenties niet geldig zijn, wordt de gastgebruiker de toegang tot het netwerk ontnomen.

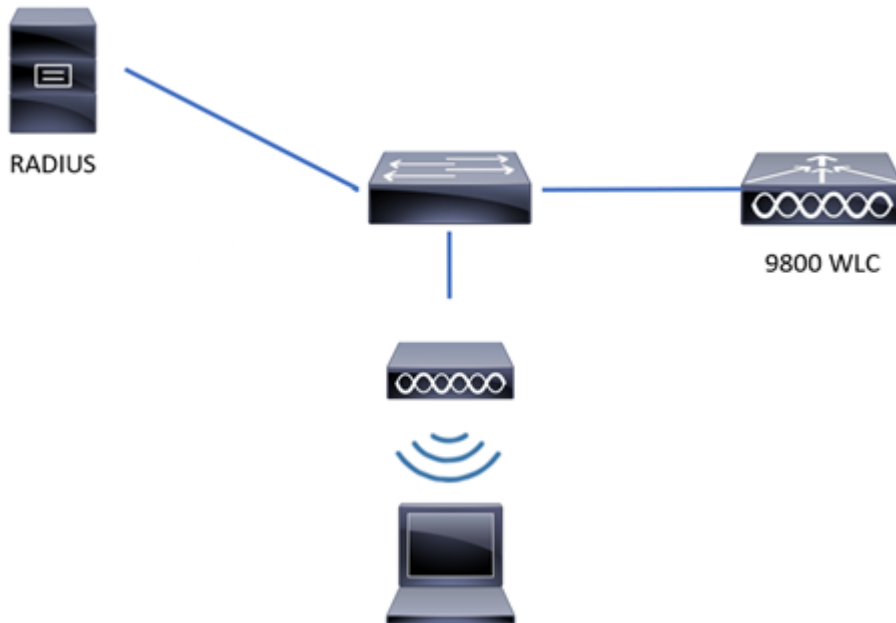
LWA-stroom:

- De gastgebruiker wordt geassocieerd met een toegangspunt dat het gastnetwerk WLAN uitzendt.
- De gastgebruiker doorloopt het DHCP-proces om een IP-adres te krijgen.
- De gastgebruiker wil een internetconnectiviteitscontrole uitvoeren naar het captive-portaal. Als het een Apple-apparaat is, probeert het de Apple captive-portal; als het een Android-apparaat is, probeert het de Android captive-portal; als het een Windows-apparaat is, probeert het de Windows connect-testportal.
- De gastgebruiker stuurt een DNS-query om het IP-adres van de captive portal te vragen. De DNS-server reageert op de zoekopdracht met het IP-adres van de correspondent.
- De gastgebruiker stuurt een HTTP GET-bericht naar het IP-adres van het captive-portaal.
- De WLC onderschept dat bericht en antwoordt op de gastgebruiker met HTTP 200 OK en de redirect-URL.
- De gastgebruiker stuurt een HTTPS GET-bericht naar het virtuele IP-adres van de WLC en de WLC reageert met het webportaal.
- De gastgebruiker wordt gevraagd om verificatiegegevens in te voeren op het webportaal.
- Het webportaal leidt de gebruiker terug naar de WLC met de verstrekte referenties (als een extern webportaal wordt gebruikt).
- De WLC verifieert de gastgebruiker via een lokale database of stuurt een query naar de RADIUS- of LDAP-server om te bevestigen of de referenties correct zijn (als het verificatietype webconsent of webauth is).
- Als de referenties correct zijn, verifieert de WLC de gastgebruiker en gaat deze naar de staat RUN. Als de inloggegevens onjuist zijn, wordt de gastgebruiker verwijderd.
- De WLC leidt de client terug naar de oorspronkelijke URL die is ingevoerd in de webbrowser.



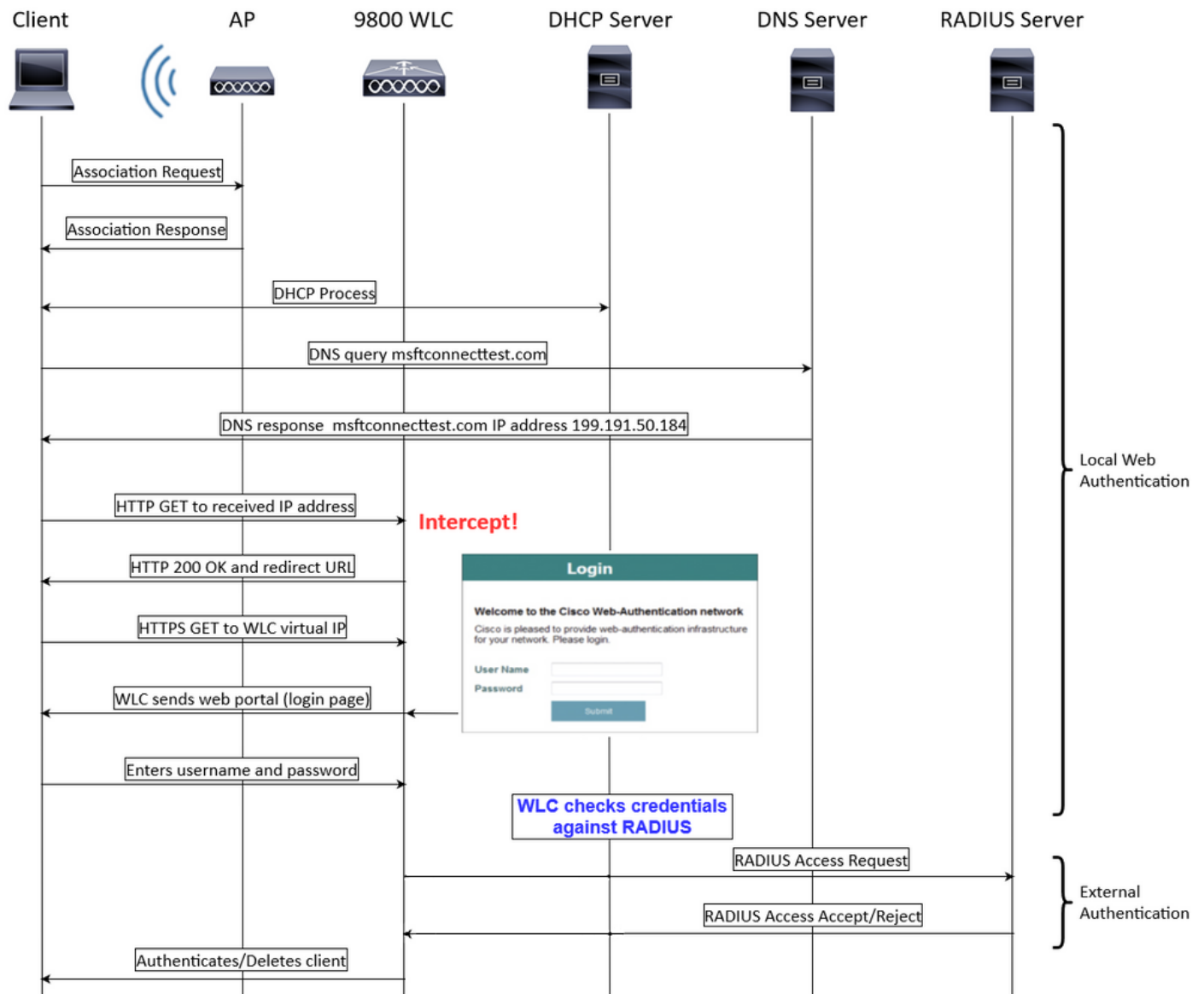
LWA-stroom

Lokale webverificatie met externe verificatie



Algemene topologie van LWA-EA

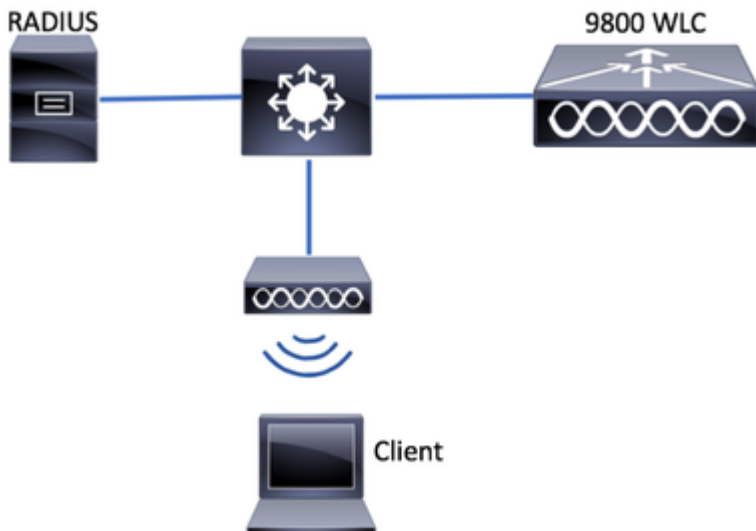
LWA-EA is een methode van LWA waarbij het webportaal en de omleidings-URL zich op de WLC bevinden en de referenties worden opgeslagen op een externe server, zoals ISE. De WLC legt de referenties vast en verifieert de client via een externe RADIUS-server. Wanneer de gastgebruiker inloggegevens invoert, controleert de WLC de inloggegevens op RADIUS, verzendt deze een RADIUS Access Request en ontvangt deze een RADIUS Access Accept/Reject van de RADIUS-server. Als de referenties correct zijn, gaat de gastgebruiker vervolgens naar de staat RUN. Als de referenties onjuist zijn, wordt de gastgebruiker verwijderd door de WLC.



LWA-EA-stroom

Configureren

Netwerkdigram



Netwerkdigram



Opmerking: dit configuratievoorbeeld heeft alleen betrekking op centrale switching/verificatie. De configuratie voor flex local switching stelt enigszins andere eisen aan de configuratie van webverificatie.

Lokale webverificatie configureren met externe verificatie op de CLI

AAA-server en -servergroep configureren

```
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 verificatie en autorisatie configureren

```
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-beveiligingsparameters configureren

```
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
```

Beleidsprofiel voor draadloze verbindingen maken

```
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
```

Een beleidstag maken

```
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
```

Een beleidstag toewijzen aan een toegangspunt

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

Als u de configuratie aan de ISE-zijde wilt voltooien, springt u naar het gedeelte ISE Configuration.

Lokale webverificatie configureren met externe verificatie op de WebUI

AAA-configuratie op 9800 WLC

Stap 1. Voeg de ISE-server toe aan de 9800 WLC-configuratie.

Navigeer naar Configuratie > Beveiliging > AAA > Servers/groepen > RADIUS > Servers > +
Toevoegen en voer de RADIUS-servergegevens in zoals in de afbeelding wordt weergegeven:

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-configuratie op 9800 WLC

Stap 2. Voeg de RADIUS-servergroep toe.

Navigeer naar Configuratie > Beveiliging > AAA > Servers/groepen > RADIUS > Servergroep > + Toevoegen en voer de RADIUS-servergroepgegevens in:

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

De RADIUS-servergroep toevoegen

Stap 3. Maak een lijst met verificatiemethoden.

Navigeer naar Configuratie > Beveiliging > AAA > Lijst met AAA-methoden > Verificatie > +
Toevoegen:

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

Cancel

Apply to Device

Een lijst met verificatiemethoden maken

Stap 4. Maak een lijst met autorisatiemethoden.

Navigeer naar Configuratie > Beveiliging > AAA > Lijst met AAA-methoden > Autorisatie > +
Toevoegen:

Quick Setup: AAA Authorization

Method List Name*

LWA_AUTHORIZATION

Type*

network

i

Group Type

group

i

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

Een lijst met autorisatiemethoden maken

WebAuth-configuratie

Een parameterkaart maken of bewerken. Selecteer het type als webauth, het virtuele IPv4-adres moet een adres zijn dat niet op het netwerk wordt gebruikt om IP-adresconflicten te voorkomen en voeg een Trustpoint toe.

Navigeer naar Configuratie > Beveiliging > Web Auth > + Toevoegen of selecteer een parameterkaart:

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-configuratie

WLAN-configuratie

Stap 1. Maak het WLAN.

Navigeer naar Configuration > Tags & Profiles > WLAN's > + Add en configureer het netwerk naar behoefte.

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

Het WLAN maken

Stap 2. Navigeer naar Beveiliging > Layer2 en selecteer Geen in de Beveiligingsmodus van Layer 2.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'Layer2' sub-tab, the 'None' security mode is chosen. The 'MAC Filtering', 'OWE Transition Mode', and 'Lobby Admin Access' options are all unchecked.

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

De WLAN-beveiliging maken

Stap 3. Navigeer naar Beveiliging > Laag3 en vink op Webbeleid het vakje aan, op Web Auth Parameter Map selecteer de parameter naam en op Authentication List selecteer de eerder gemaakte verificatielijst.

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Web Policy

☒

Show Advanced Settings >>>

Web Auth Parameter Map

global

Authentication List

LWA_AUTHENTIC...

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

De WLAN-verificatielijst maken

Het WLAN wordt weergegeven in de WLAN-lijst:

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

Gemaakt WLAN

Configuratie beleidsprofiel

In een beleidsprofiel kunt u onder andere het VLAN selecteren dat de clients toewijst.

U kunt uw standaardbeleidsprofiel gebruiken of u kunt een nieuw profiel maken.

Stap 1. Maak een nieuw beleidsprofiel aan.

Navigeer naar Configuratie > Tags en profielen > Beleid en configureer uw standaardbeleidsprofiel of maak een nieuw profiel.

Zorg ervoor dat het profiel is ingeschakeld.

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

Een nieuw beleidsprofiel maken

Stap 2. Selecteer het VLAN.

Blader naar het tabblad Toegangsbeleid en selecteer de VLAN-naam in de vervolgkeuzelijst of typ handmatig de VLAN-ID.

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 x ⓘ

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

Selecteer het VLAN

Configuratie van beleidstag

Binnen de Policy Tag is waar u uw SSID koppelt aan uw Beleidsprofiel. U kunt een nieuwe beleidstag maken of de standaardbeleidstag gebruiken.

Navigeer naar Configuratie > Tags & Profielen > Tags > Beleid en voeg indien nodig een nieuwe toe, zoals weergegeven in de afbeelding.

Selecteer + Toevoegen:

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

Configuratie van beleidstag

Koppel uw WLAN-profiel aan het gewenste beleidsprofiel:

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
✓

> WLAN-POLICY Maps : 0

Cancel
Apply to Device

Configuratie van beleidstag

Toewijzing van beleidstag

Wijs de beleidstag toe aan de benodigde toegangspunten.

Als u de tag aan één toegangspunt wilt toewijzen, navigeert u naar Configuratie > Draadloos > Toegangspunten > Naam toegangspunt > Algemene tags, maakt u de gewenste toewijzing en klikt u vervolgens op Bijwerken en toepassen op apparaat.

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

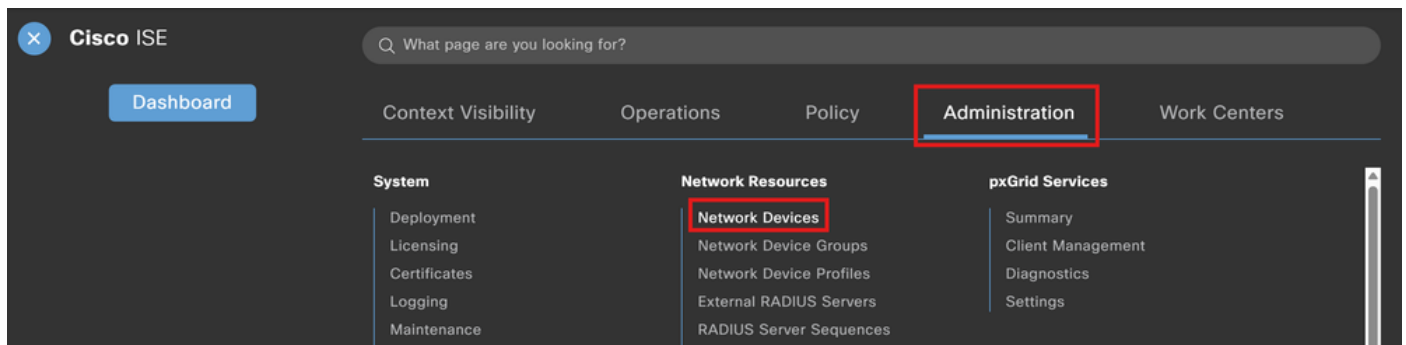
Cancel Update & Apply to Device

Toewijzing van beleidstag

ISE-configuratie

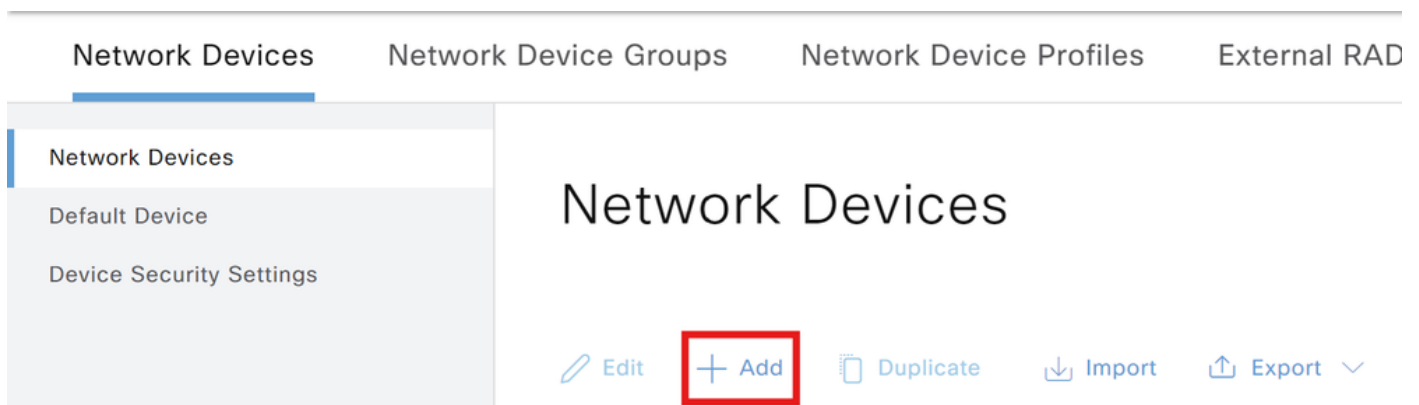
9800 WLC toevoegen aan ISE

Stap 1. Navigeer naar Beheer > Netwerkbronnen > Netwerkkapparaten zoals weergegeven in de afbeelding.



9800 WLC toevoegen aan ISE

Stap 2. Klik op +Toevoegen.



Netwerkkaparameters toevoegen

Optioneel kan het een gespecificeerde modelnaam, softwareversie, beschrijving en netwerkkaparaatgroepen toewijzen op basis van apparaattypen, locatie of WLC's.

Stap 3. Voer de 9800 WLC-instellingen in, zoals weergegeven in de afbeelding. Voer dezelfde RADIUS-sleutel in die is gedefinieerd bij het maken van de server aan de WLC-zijde. Klik vervolgens op Indienen.

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](#)

netwerkkapparaten bekijken.

Network Devices

Selected 0 Total 6  

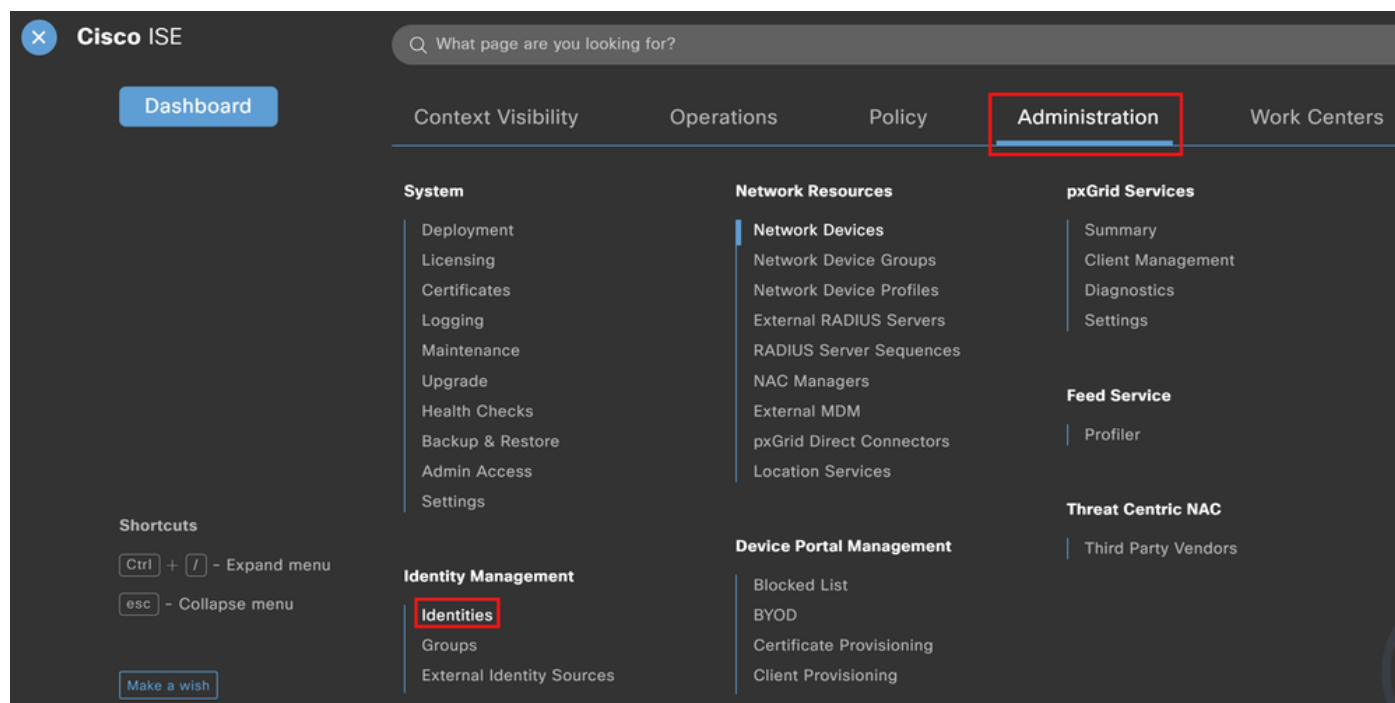
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

☐	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

Lijst met netwerkkapparaten

Nieuwe gebruiker maken op ISE

Stap 1. Navigeer naar Beheer > Identiteitsbeheer > Identiteiten:



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'. The 'Administration' section is expanded, showing a sidebar with 'System', 'Network Resources', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Network Resources' section is further expanded, showing 'Network Devices' (highlighted with a red box), 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', 'pxGrid Direct Connectors', and 'Location Services'. The 'Network Devices' section is further expanded, showing 'Blocked List', 'BYOD', 'Certificate Provisioning', and 'Client Provisioning'. The 'Identities' link in the 'Identity Management' section is also highlighted with a red box.

ISE Administratie - Identiteiten

Stap 2. Navigeer naar Gebruikers, klik op +Toevoegen.

Users

Latest Manual Network Scan Res...

Network Access Users

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

Status

Username ^

Description

First Name

Last Name

Em:

Gebruiker toevoegen

Stap 3. Voer de gebruikersnaam en het wachtwoord voor de gastgebruiker in en klik op Indienen.

[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

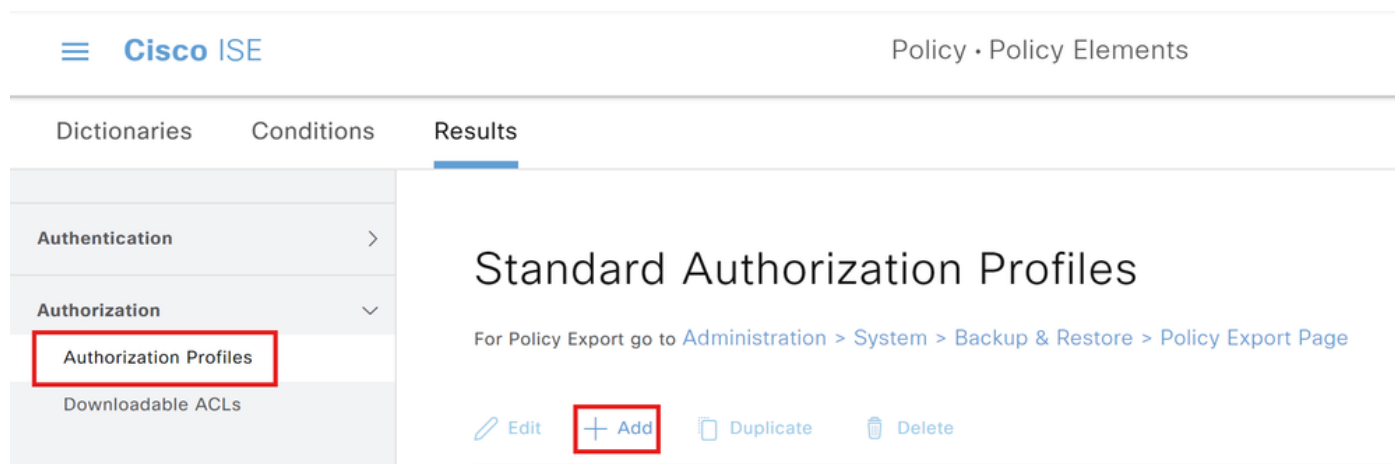
Enable Password

[Generate Password](#)

i

Nieuwe gebruiker maken op ISE

Stap 2. Ga naar Autorisatie > Autorisatieprofielen. Klik op +Toevoegen om een autorisatieprofiel te maken.



Cisco ISE Policy • Policy Elements

Dictionaryes Conditions Results

Authentication >

Authorization v

Authorization Profiles

Downloadable ACLs

Standard Authorization Profiles

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

Edit + Add Duplicate Delete

Autorisatieprofiel toevoegen

Stap 3. Maak het autorisatieprofiel LWA_EA_AUTHORISATION aan. De details van de attributen moeten Access Type=ACCESS_ACCEPT zijn. Klik op Verzenden.

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  Cisco v ⊕

Service Template ☐

Track Movement ☐ 

Agentless Posture ☐ 

Passive Identity Tracking ☐ 

Autorisatieprofiel maken

Stap 4. Navigeer naar Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen, u kunt de autorisatieprofielen bekijken.

DictionariesConditionsResults

Authentication >Authorization >Authorization ProfilesDownloadable ACLsProfiling >Posture >Client Provisioning >

Standard Authorization Profiles

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

EditAddDuplicateDelete

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

Lijst met autorisatieprofielen

Verificatieregel configureren

Stap 1. Navigeer naar Beleid > Beleidssets.

Cisco ISE

Dashboard

Recent Pages

- Results
- Policy Sets
- Identities
- Network Devices

Q What page are you looking for?

Context VisibilityOperationsPolicyAdministration

Policy Sets

Posture

Policy Elements

- Dictionaries
- Conditions
- Results

Profiling

Client Provisioning

ISE-beleid - Beleidssets

Stap 2. Selecteer het +-teken en typ de naam van de beleidsset LWA_EA_POLICY. Klik op de kolom Voorwaarden.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	LWA_EA_POLICY		+	Select from list			

Verificatieregel configureren

Stap 3. Bij Woordenboek selecteert u Netwerkttoegang. Selecteer in Attriboot de gebruikersnaam.

Conditions Studio

Library

Search by Name

5G

Catalyst_Switch_Local_Web_Auth entication

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

Woordenboek netwerkttoegang

Stap 4. Stel Equals in en typ guest in het tekstvak (de gebruikersnaam is gedefinieerd in Beheer > Identiteitsbeheer > Identiteiten > Gebruikers). Klik op Opslaan om de wijzigingen op te slaan.

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

Gebruikersnaam Gast

Stap 5. Navigeer naar **Beleid > Beleidssets**. In de beleidsset die u hebt gemaakt, in de kolom **Toegestane protocollen/serverreeks** selecteert u **Standaardnetwerktoegang**.

Cisco ISE

Policy - Policy Sets

Policy Sets

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	LWA_EA_POLICY		Network Access-UserName EQUALS guest	Select from list	9	⚙️	➡️
✓	New Policy Set 1			Allowed Protocols	0	⚙️	➡️
				Default Network Access			

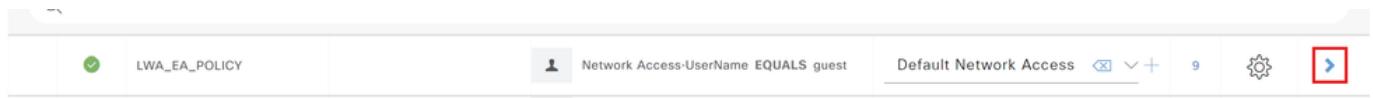
Beleidssets

Stap 6. Klik op **Opslaan** om de wijzigingen op te slaan.

Machtigingsregels configureren

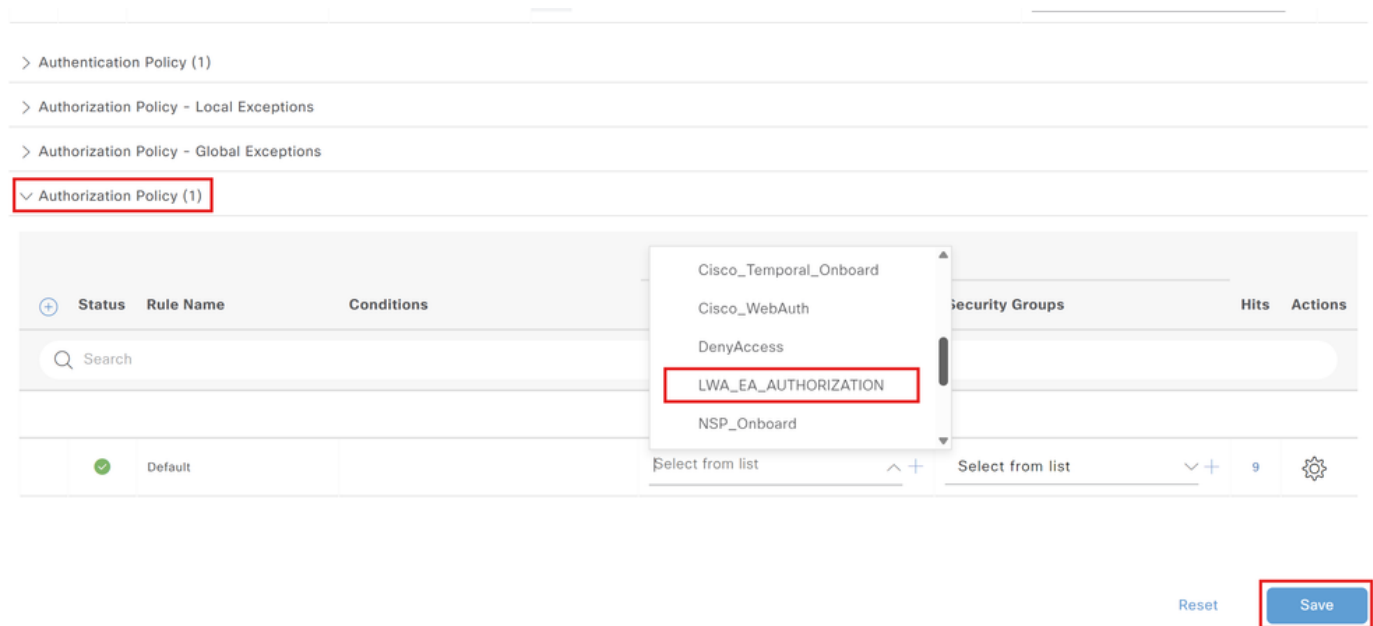
De autorisatieregel is degene die verantwoordelijk is om te bepalen welke toestemmingen (welk autorisatieprofiel) op de klant worden toegepast.

Stap 1. Navigeer naar **Beleid > Beleidssets**. Klik op het pijlpictogram in de beleidsset die u hebt gemaakt.



Pijl voor beleidsset

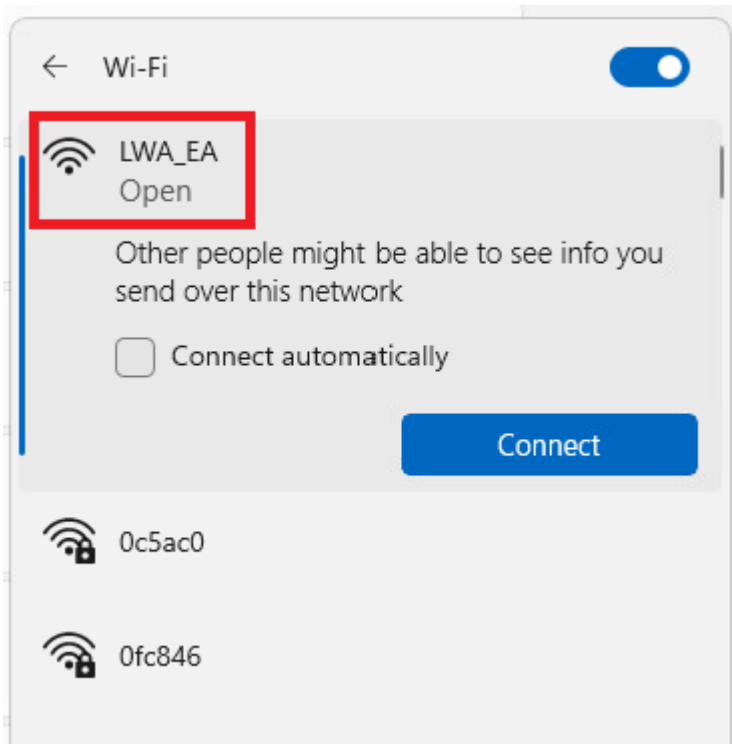
Stap 2. Vouw op dezelfde pagina Beleidsset het Autorisatiebeleid uit zoals in de afbeelding wordt weergegeven. In de kolom Profielen verwijdert u DenyAccess en voegt u LWA_EA_AUTHORISATION toe. Klik op Opslaan om de wijzigingen op te slaan.



machtingingsbeleid

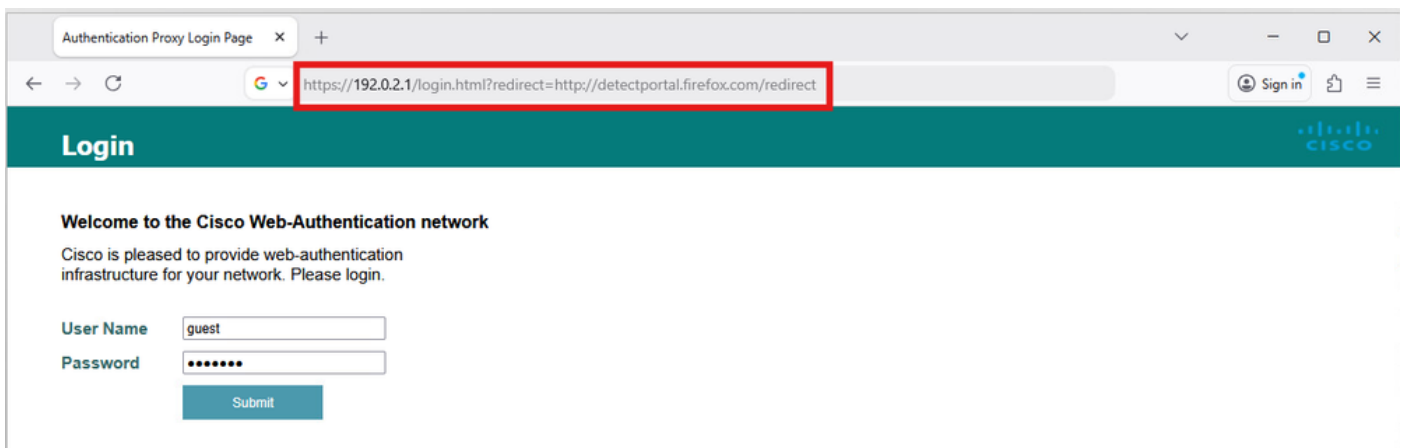
Gastclient verbinden

Stap 1. Op uw computer/telefoon navigeert u naar de Wi-Fi-netwerken, zoekt u de SSID LWA_EA en selecteert u Verbinden.



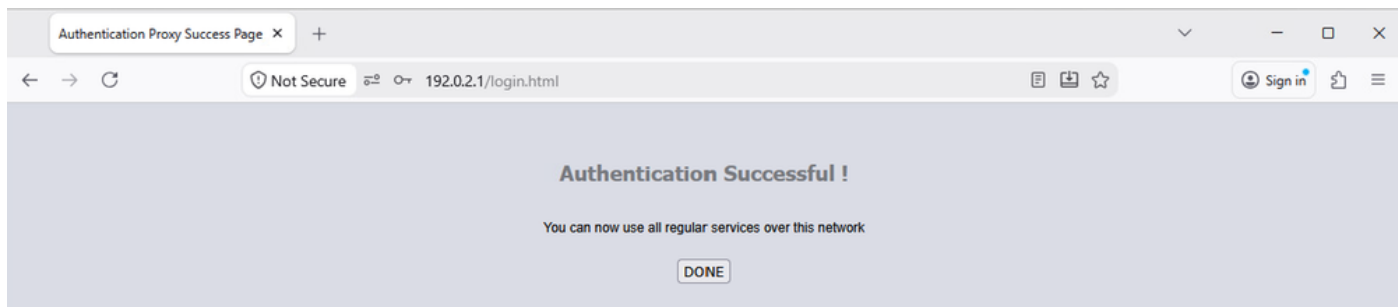
Gastclient verbinden

Stap 2. Er verschijnt een browservenster met de inlogpagina. De redirect-URL bevindt zich in het URL-vak en u moet de gebruikersnaam en het wachtwoord typen om toegang te krijgen tot het netwerk. Selecteer vervolgens Verzenden.



Login pagina met redirect URL

Als de referenties correct zijn, wordt een pagina met een geslaagde verificatie weergegeven:



Verificatie Succesvolle inlogpagina

 **Opmerking:** de URL die is weergegeven, is geleverd door de WLC. Het bevat de WLC Virtual IP en de redirect voor de Windows connect test URL.

Stap 3. Navigeer naar **Bewerkingen > RADIUS > Live Logs**. U kunt zien dat het clientapparaat is geverifieerd, samen met het verificatie- en autorisatiebeleid.

Cisco ISE Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 2

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Sep 18, 2026 10:00:26.1...			2	guest	08-BE-AC...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:54:58.3...				guest	08-BE-AC...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:41:04.9...				guest	08-BE-AC...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...

Last Updated: Fri Sep 18 2026 11:00:54 GMT+0100 (Hora de verão da Europa Ocidental) Records Shown: 3

Radius Live-logboeken

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

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 WNCN (0) : current UP
(...)

Problemen oplossen

Veelvoorkomende problemen

Dit zijn verschillende handleidingen voor het oplossen van problemen met webverificatie, zoals:

- Gebruikers kunnen niet verifiëren.
- Certificaatproblemen.
- Redirection URL werkt niet.
- Gastgebruikers kunnen geen verbinding maken met het gastnetwerk.
- Gebruikers krijgen geen IP-adres.
- Omleiding naar de webverificatielogpagina mislukt.
- Na een succesvolle verificatie krijgen gastgebruikers geen toegang tot internet.

In deze handleidingen worden de stappen voor probleemoplossing gedetailleerd beschreven:

- [Problemen oplossen met veelvoorkomende problemen voor webverificatie](#)
- [Andere situaties om problemen op te lossen](#)

Voorwaardelijke foutopsporing en Radio Active Trace en Embedded Packet Capture

U kunt voorwaardelijke foutopsporing inschakelen en Radio Active (RA) trace vastleggen, die foutopsporingsniveausporen biedt voor alle processen die interageren met de opgegeven voorwaarde (in dit geval client-mac-adres). Als u voorwaardelijke foutopsporing wilt inschakelen, gebruikt u de stappen in de handleiding, [Voorwaardelijke foutopsporing en RadioActive-tracering](#).

U kunt ook Embedded Packet Capture (EPC) verzamelen. EPC is een packet capture-faciliteit die een overzicht biedt van pakketten die bestemd zijn voor, afkomstig zijn van en door de Catalyst 9800 WLC's gaan, namelijk DHCP, DNS, HTTP GET-pakketten in LWA. Deze opnames kunnen

worden geëxporteerd voor offline analyse met Wireshark. Raadpleeg [Embedded Packet Capture voor](#) gedetailleerde stappen over hoe u dit kunt doen.

Voorbeeld van een geslaagde poging

Dit is de uitvoer van de RA_traces voor een geslaagde poging om elk van de fasen van het associatie-/verificatieproces te identificeren, terwijl deze in verbinding staat met een gast-SSID met RADIUS-server.

802.11 Associatie/authenticatie:

```
[client-orch-sm] [17062]: (noot): MAC: 08be.ac3f Association received. BSSID cc70.edcf.552f, WLAN LWA_EA, sleuf 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Ontvangen Dot11-assocatieverzoek. De verwerking is gestart, SSID: LWA_EA, Beleidsprofiel: POLICY_PROFILE, AP Naam: CW9172I-LAB, Ap Mac Adres: 2ce3.8eb4BSSID MAC0000.0000.0000wlan ID: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (noot): MAC: 08be.ac3f Overgang van clientstatus: S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (info): MAC: 08be.ac3f Dot11 ie validate ext/supp rates. Validatie geslaagd voor ondersteunde snelheden radio_type 2
[dot11-validate] [17062]: (info): MAC: 08be.ac3f WiFi direct: Dot11 validate P2P IE. P2P IE niet aanwezig.
[dot11] [17062]: (debug): MAC: 08be.ac3f dot11 Verzend associatierespons. Framing associatie reactie met resp_status_code: 0
[dot11] [17062]: (debug): MAC: 08be.ac3f Dot11 Capability info byte1 1, byte2: 11
[dot11-frame] [17062]: (info): MAC: 08be.ac3f WiFi direct: bouw assoc Resp met P2P IE: WiFi direct beleid uitgeschakeld
[dot11] [17062]: (info): MAC: 08be.ac3f dot11 Verzend associatierespons. Verzenden assoc antwoord van lengte: 130 met resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
[dot11] [17062]: (noot): MAC: 08be.ac3f Association succes. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
[dot11] [17062]: (info): MAC: 08be.ac3f DOT11 statusovergang: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Station Dot11 is een succes.
```

IP Learn-proces:

```
[client-orch-state] [17062]: (noot): MAC: 08be.ac3f Overgang van clientstatus: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (info): MAC: 08be.ac3f IP-leren statusovergang: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (info): MAC: 08be.ac3f Overgang van status client-auth-interface: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (opmerking): MAC: 08be.ac3f Client IP learn successful. Methode: DHCP IP: 10.14.32.109
[client-iplearn] [17062]: (info): MAC: 08be.ac3f IP-leren statusovergang: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Ontvangen ip-learn response. methode: IPLEARN_METHOD_DHCP
```

Layer 3-verificatie:

```
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Geactiveerde L3-verificatie. status = 0x0, succes
[client-orch-state] [17062]: (noot): MAC: 08be.ac3f Overgang van clientstatus: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (opmerking): MAC: 08be.ac3f L3 Verificatie gestart. LWA
```

[client-auth] [17062]: (info): MAC: 08be.ac3f Overgang status client-auth-interface:
S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[WebAuth-httpd] [17062]: (info): CAPWAP_90000004[08be.ac3f][10.14.32.109]GET RCvd bij
AANMELDING

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET request

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, 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]Lees volledig:
parse_request return 8

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO state READING
-> SCHRIJVEN

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO state WRITING
-> READING

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO-status NIEUW -
> LEZING

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Lees evenement,
Bericht gereed

[WebAuth-httpd] [17062]: (info): CAPWAP_90000004[08be.ac3f][10.14.32.109]POST RCvd bij
AANMELDING

Layer 3-verificatie is geslaagd. Verplaats de client naar de status RUN:

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Ontvangen gebruikersnaam voor gast client
08be.ac3f

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Auth mgr attr Melding van toevoeging/wijziging
wordt ontvangen voor attr auth-domain(954)

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Methode webauth waarbij de status wordt
gewijzigd van 'Running' in 'Authc Success'

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Context status wijzigen van 'Running' in 'Authc
Success'

[AUTH-MGR] [17062]: (info): [08be.ac3f:capwap_90000004] Auth Mgr attr Melding van
toevoeging/wijziging wordt ontvangen voor de methode attr(757)

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Gestegen gebeurtenis AUTHZ_SUCCESS (11)

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Context status wijzigen van 'Authc Success' in
'Authz Success'

[webauth-acl] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Toepassing van IPv4 logout
ACL via SVM, naam: IP-Adm-V4-LOGOUT-ACL, prioriteit: 51, IIF-ID: 0

[webauth-sess] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Gebruikte paramkaart:
wereldwijd

[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Gebruikte paramkaart:
wereldwijd

[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS ->
AUTHZ

[webauth-page] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Webauth-succespagina
verzenden

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO-statusverificatie
-> SCHRIJVEN

[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state WRITING
-> END

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO ctx
verwijderen en socket sluiten, id [99000029]

[client-auth] [17062]: (noot): MAC: 08be.ac3f L3 Authenticatie geslaagd. ACL:[]

[client-auth] [17062]: (info): MAC: 08be.ac3f Overgang status client-auth-interface:
S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 IO ctx verwijderen en socket sluiten, id [D7000028]
[errmsg] [17062]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: gebruikersnaamvermelding (gast) gekoppeld aan SSID (LWA_EA) voor apparaat met MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (info): [Toegepast attribuut :bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: (info): [Toegepast attribuut: timeout 0 1800 (0x708)]
[aaa-attr-inf] [17062]: (info): [Toegepast attribuut: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (info): MAC: 08be.ac3f Client QoS run state handler
[rog-proxy-capwap] [17062]: (debug): Beheerde client RUN state notification: 08be.ac3f
[client-orch-state] [17062]: (noot): MAC: 08be.ac3f Overgang van clientstatus: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.