

Configureer de Captive Portal met Catalyst 9800 WLC voor DNA-ruimtes

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Sluit de 9800 controller aan op Cisco DNA-ruimtes](#)

[De SSID op DNA-ruimtes maken](#)

[Configuratie van ACL- en URL-filters op de 9800-controller](#)

[Captive Portal zonder RADIUS-server op DNA-ruimtes](#)

[Web Auth Parameter Map configuratie op de 9800 controller](#)

[De SSID op de 9800 controller maken](#)

[Policy Profile op de 9800-controller configureren](#)

[Policy Tag op de 9800 controller configureren](#)

[Captive Portal met RADIUS Server op DNA-ruimtes](#)

[Web Auth Parameter Map configuratie op de 9800 controller](#)

[RADIUS-serverconfiguratie op de 9800-controller](#)

[De SSID op de 9800 controller maken](#)

[Policy Profile op de 9800-controller configureren](#)

[Policy Tag op de 9800 controller configureren](#)

[De globale parameterkaart configureren](#)

[Maak het portaal op DNA-ruimtes](#)

[Configureer de Captive Portal Rules voor DNA-ruimtes](#)

[Krijg specifieke informatie van DNA Spaces](#)

[Wat zijn de IP-adressen die DNA-ruimtes gebruiken?](#)

[Wat is de URL die het inlogportal van DNA Spaces gebruikt?](#)

[Wat zijn de RADIUS-servergegevens voor DNA-ruimtes?](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Veelvoorkomende problemen](#)

[Altijd-AAN-traceren](#)

[Voorwaardelijke debugging en radio actieve tracersing](#)

[Voorbeeld van een geslaagde poging](#)

Inleiding

Dit document beschrijft hoe u interactieve portalen op Cisco DNA-ruimtes kunt configureren.

Voorwaarden

In dit document kunnen clients op de Catalyst 9800 draadloze LAN-controller (C9800 WLC) DNA-ruimtes gebruiken als een externe inlogpagina voor webverificatie.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de Command Line Interface (CLI) of Graphic User Interface (GUI) voor de 9800 draadloze controllers
- Cisco DNA-ruimtes

Gebruikte componenten

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

- Catalyst 9800-L controller versie 16.12.2s

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.

Achtergrondinformatie

Web Authenticatie is een eenvoudige Layer 3-verificatiemethode zonder dat er een applicatie of client-hulpprogramma nodig is. Dit kan worden gedaan

- a) Met de Interne Pagina op C9800 WLC als is of na wijzigingen
- b) Met aangepaste login bundel geüpload naar C9800 WLC
- c) Aangepaste login pagina gehost op een externe server

Om gebruik te maken van de captive portal van DNA Spaces is in wezen een manier om externe web authenticatie voor clients op C9800 WLC te implementeren.

Het proces van de externe website wordt in detail beschreven op:

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html>

Op C9800 WLC wordt het virtuele IP-adres gedefinieerd als de globale parameter-kaart en is doorgaans 192.0.2.1

Configureren

Netwerkdigram



Sluit de 9800 controller aan op Cisco DNA-ruimtes

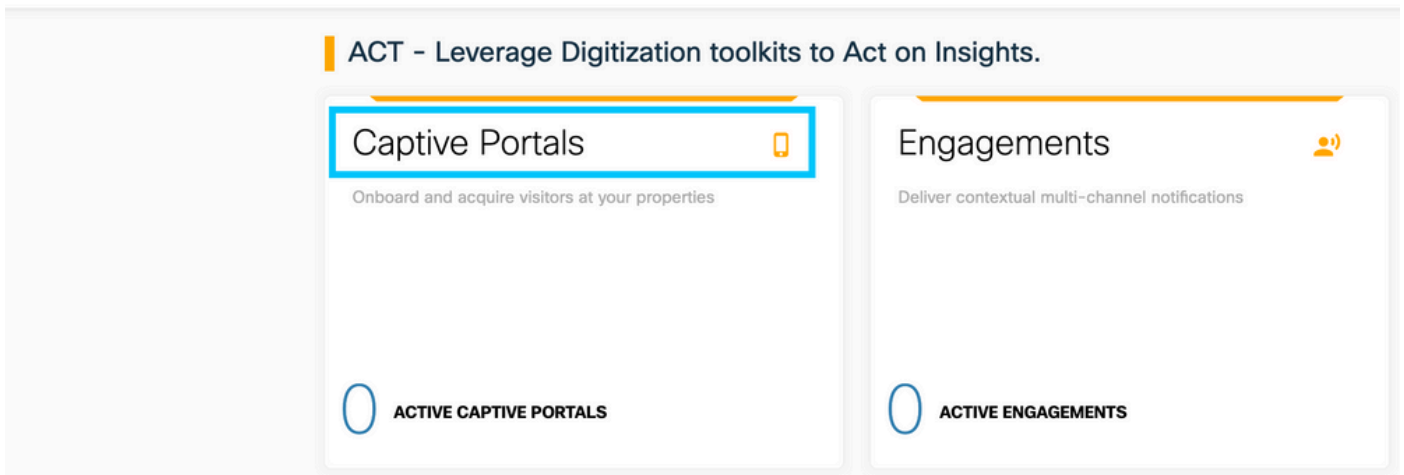
De controller moet worden aangesloten op DNA-ruimtes met een van de opties - Direct Connect, via DNA Spaces Connector of met CMX Tethering.

In dit voorbeeld is de Direct Connect optie in gebruik, hoewel captive portals op dezelfde manier zijn geconfigureerd voor alle instellingen.

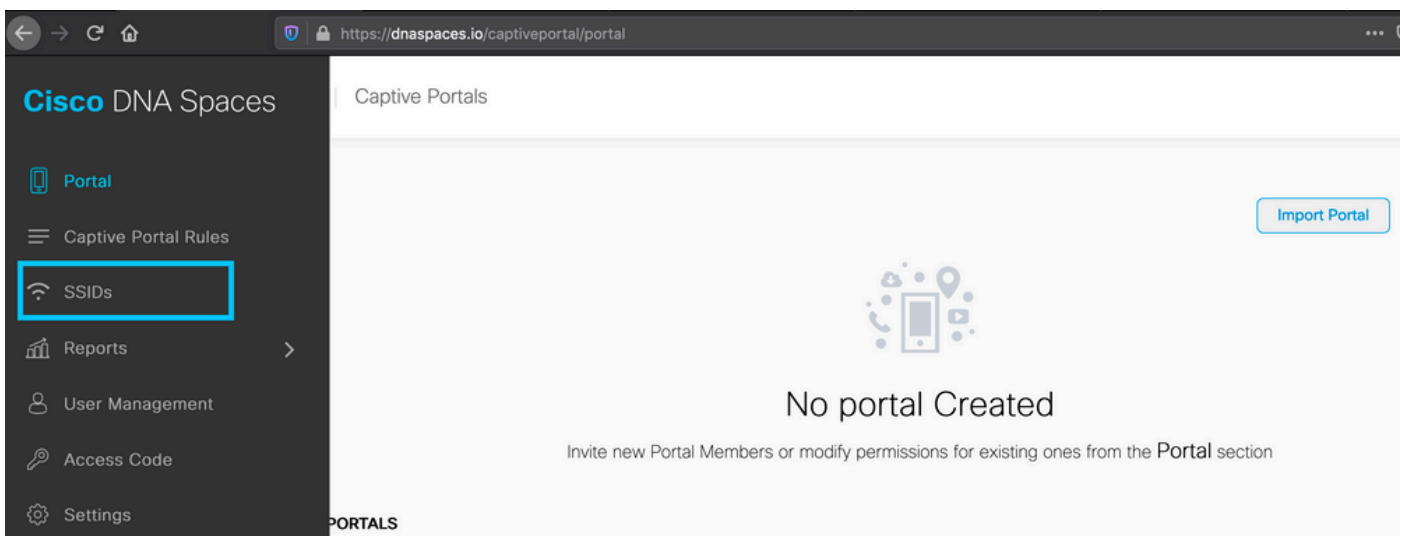
Om de controller te kunnen aansluiten op Cisco DNA-ruimtes, moet de controller de Cisco DNA Spaces Cloud via HTTPS kunnen bereiken. Voor meer informatie over het aansluiten van de 9800 controller op DNA-ruimtes, zie deze link: [DNA-ruimtes - 9800 Controller Direct Connect](#)

De SSID op DNA-ruimtes maken

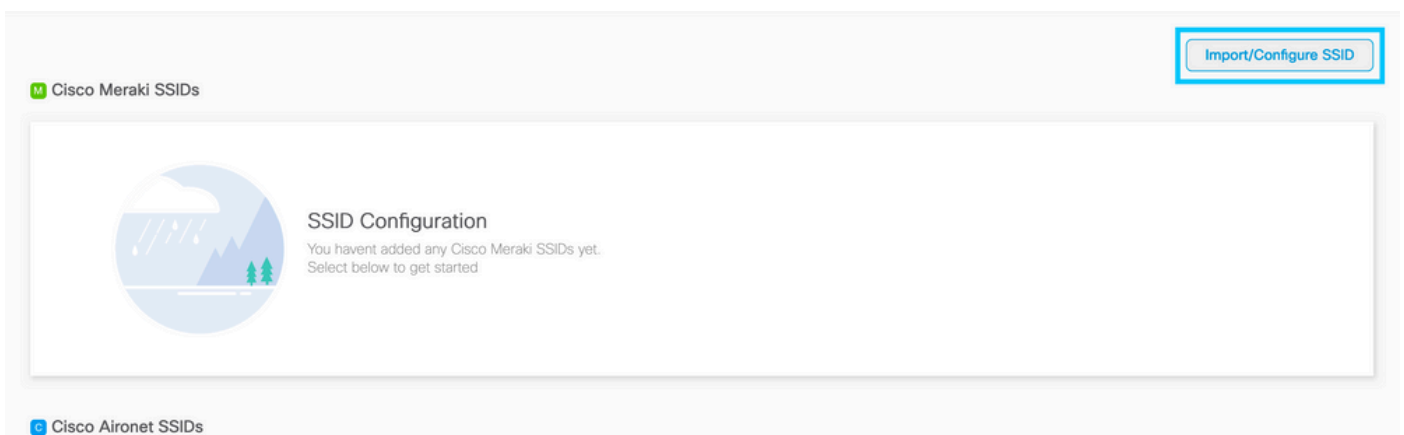
Stap 1. Klik op **Captive Portals** in het dashboard van DNA Spaces:



Stap 2. Open het intiem portaalspecifieke menu, klik op het pictogram met drie lijnen in de linkerbovenhoek van de pagina en klik op **SSID's**:



Stap 3. Klik op **SSID importeren/configureren**, selecteer **CUWN (CMX/WLC)** als het type "Draadloos netwerk" en voer de naam van de SSID in:



Configuratie van ACL- en URL-filters op de 9800-controller

Verkeer van een draadloze client is niet toegestaan op het netwerk totdat de verificatie is voltooid. In het geval van web authenticatie, om het te voltooien, een draadloze client verbindt met deze

SSID, ontvangt een IP-adres en dan wordt de client policy manager status verplaatst naar **Webauth_reqd** staat. Aangezien de client nog niet is geverifieerd, wordt alle traffic sourcing van het IP-adres van de client verwijderd, behalve DHCP en DNS en HTTP (die worden onderschept en omgeleid).

Standaard maakt de 9800 vooraf gecodeerde ACL's wanneer we een WLAN-webserver instellen. Deze hardcoded ACL's maken DHCP, DNS en verkeer naar de externe webautorisatieserver mogelijk. Al de rest wordt omgeleid zoals elk http traffic.

Als u echter een specifiek niet-HTTP-verkeerstype moet toestaan, kunt u een pre-auth ACL configureren. U zou dan de inhoud van de bestaande hardcoded pre-auth ACL (van stap 1 van deze sectie) moeten imiteren en het aan uw behoeften vergroten.

Stap 1. Controleer huidige geharde ACL's

CLI-configuratie:

```
Andressi-9800L#show ip access list
```

```
Extended IP access list WA-sec-34.235.248.212
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any
```

```
Extended IP access list WA-v4-int-34.235.248.212
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212 wordt als zodanig genoemd omdat het een automatische Web Audio (WA) security (sec) ACL of portal ip "34.235.248.212" is. Beveiligings-ACL's definiëren wat is toegestaan (op vergunning) of gevallen (op ontkennen)

Wa-v4-int is een onderschepping ACL, dat is een punt ACL of omleiden ACL en bepaalt wat wordt verzonden naar CPU voor omleiding (op vergunning) of wat wordt verzonden naar dataplane (op ontkennen).

WAP-v4-int34.235.248.212 wordt eerst toegepast op verkeer dat van de klant komt en houdt HTTP(s)-verkeer naar DNA Spaces-portal IP 34.235.248.212 op het dataplane (niet drop of voorwaartse actie nog, gewoon overhandigen aan dataplane). Het stuurt naar CPU (voor omleiding behalve virtueel IP-verkeer dat wordt onderhouden door de webserver) al het HTTP(s)-verkeer. Andere soorten verkeer worden gegeven aan het dataplane.

WAP-sec-34.235.248.212 maakt HTTP- en HTTPS-verkeer naar de DNA-ruimte IP 34.235.248.212 mogelijk die u in de webverificatie-parameterkaart hebt geconfigureerd en het staat ook DNS- en DHCP-verkeer toe en laat de rest vallen. HTTP-verkeer dat moet worden onderschept, is al onderschept voordat het deze ACL bereikt en hoeft daarom niet door deze ACL te worden bestreken.

Opmerking: Om de IP-adressen van DNA-ruimtes in de ACL toe te staan, klikt u op de optie **Handmatig configureren** uit de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** onder de sectie ACL-configuratie. Een voorbeeld vindt u in de sectie "Wat zijn de IP-adressen die de DNA-ruimtes gebruiken" aan het einde van het document.

DNA-ruimtes gebruikt 2 IP-adressen en het mechanisme in stap 1 laat slechts één portaal IP toe. Om pre-authenticatie toegang tot meer HTTP-bronnen toe te staan, moet u URL-filters gebruiken die dynamisch gaten maken in de onderschepping (omleiden) en beveiliging (voorbestemmen) ACL's voor de IP's gerelateerd aan de website waarvan u de URL in het URL-filter invoert. DNS-verzoeken worden dynamisch gesnooped voor de 9800 om het IP-adres van die URL's te leren en dynamisch aan de ACL's toe te voegen.

Stap 2. Configureer het URL-filter om het DNA Spaces-domein toe te staan. Navigeer naar Configuration > Security > URL Filters, klik op **+Add** en configureer de lijstnaam, selecteer **PRE-AUTH** als het type, actie als **PERMIT** en de URL **splash.dnaspaces.io** (of .eu als u het EMEA-portal gebruikt):

The screenshot shows the 'Add URL Filter' configuration window. The 'List Name*' field is set to 'DNASpaces'. The 'Type' dropdown is set to 'PRE-AUTH'. The 'Action' is set to 'PERMIT' with a checked checkbox. The 'URLs' field contains 'splash.dnaspaces.io'. The window has a 'Cancel' button and an 'Apply to Device' button.

CLI-configuratie:

```
Addresssi-9800L(config)#urlfilter list
```

```
Addresssi-9800L(config-urlfilter-params)#action permit
```

```
Addresssi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

De SSID kan worden geconfigureerd om een RADIUS-server te gebruiken of zonder de SID. Als die sessieduur, bandbreedterimiet of naadloos provisioninginternet is geconfigureerd in de sectie **Acties** van de configuratie Captive Portal Rule, moet de SSID worden geconfigureerd met een RADIUS-server, anders is het niet nodig om de RADIUS-server te gebruiken. Alle soorten portals op DNA-ruimtes worden op beide configuraties ondersteund.

Captive Portal zonder RADIUS-server op DNA-ruimtes

Web Auth Parameter Map configuratie op de 9800 controller

Stap 1. Navigeer naar **Configuration > Security > Web Auth**, klik op **+Add** om een nieuwe parameterkaart te maken. In het venster dat pop-up vormt de naam van de parameterkaart, en selecteert **Toestemming** als type:

The screenshot shows a 'Create Web Auth Parameter' dialog box. The title bar is dark blue with a close button (X) on the right. The main area is white with a light blue border. It contains four input fields, each with a label and a value:

- Parameter-map name***: DNASpaces-PM
- Maximum HTTP connections**: 1-200
- Init-State Timeout(secs)**: 60-3932100
- Type**: consent (dropdown menu)

At the bottom, there is a 'Close' button with an X icon and an 'Apply to Device' button with a checkmark icon.

Stap 2. Klik op de parameterkaart die in de vorige stap is geconfigureerd, navigeer naar het tabblad **Advanced** en voer de Redirect for log-in URL, Add for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID en portal IPv4 Address in zoals geïllustreerd Klik op **Update & Apply**:

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address


Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page

Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

Opmerking: om de splash pagina URL en het IPv4 omleiden adres, klik op de optie **Handmatig configureren** in de SSID-pagina van DNA-ruimtes. Dit wordt geïllustreerd in "Wat is de URL die het portaal van DNA-ruimten gebruikt?" aan het eind van het document

Opmerking: Cisco DNA Spaces portal kan twee IP-adressen, maar de 9800 controller maakt het mogelijk om slechts één IP-adres te configureren, een van die IP-adressen te kiezen en het op de parameterkaart te configureren als het Portal IPv4-adres.

Opmerking: zorg ervoor dat zowel de virtuele IPv4- als de IPv6-adressen worden geconfigureerd in de algemene webautoriteitsparameterkaart. Als de Virtual IPv6 niet is geconfigureerd, worden de clients soms omgeleid naar het interne portal in plaats van naar het geconfigureerde DNA Spaces-portal. Daarom moet een virtueel IP altijd worden geconfigureerd. "192.0.2.1" kan worden geconfigureerd als Virtual IPv4 en FE80:0:0:0:903A::11E4 als Virtual IPV6. Er zijn weinig tot geen redenen om andere IP's te gebruiken dan deze.

CLI-configuratie:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

De SSID op de 9800 controller maken

Stap 1. Navigeer naar **Configuratie > Tags en profielen > WLAN's** en klik op **+Add**. Configureer de profielnaam, SSID en schakel het WLAN in. Zorg ervoor dat de SSID-naam dezelfde naam is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken**.

Add WLAN

General Security Advanced

Profile Name* 9800DNASpaces

SSID* 9800DNASpaces

WLAN ID* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Cancel Apply to Device

Stap 2. Navigeer naar **Security > Layer 2**. Stel Layer 2 Security Mode in op **Geen** en zorg ervoor dat MAC-filtering is uitgeschakeld.

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

Transition Mode WLAN ID 0

Fast Transition Adaptive Enabled

Over the DS

Reassociation Timeout 20

Cancel Apply to Device

Stap 3. Navigeer naar **Security > Layer 3**. Schakel webbeleid in en configureer de webautoriteitparameterkaart. Klik op **Toepassen op apparaat**.

Edit WLAN ✕

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

[Show Advanced Settings >>>](#)

Web Policy

Web Auth Parameter Map

Authentication List ⓘ

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

Policy Profile op de 9800-controller configureren

Stap 1. Navigeer naar **Configuratie > Tags & profielen > Beleid** en maak een nieuw beleidsprofiel of gebruik het standaard beleidsprofiel. In het tabblad Toegangsbeleid moet u de client-VLAN configureren en het URL-filter toevoegen.

Edit Policy Profile ✕

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

RADIUS Profiling

Local Subscriber Policy Name

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

HTTP TLV Caching

DHCP TLV Caching

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Policy Tag op de 9800 controller configureren

Stap 1. Ga naar **Configuration > Tags & profielen > Policy**. Maak een nieuwe beleidstag of gebruik de standaardbeleidstag. Breng het WLAN aan in het beleidsprofiel in de beleidstag.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Stap 2. Pas de Policy Tag toe op het toegangspunt om de SSID uit te zenden. Navigeer naar **Configuration > Wireless > Access points**, selecteer het toegangspunt in kwestie en voeg de beleidstag toe. Hierdoor start het toegangspunt de CAPWAP-tunnel opnieuw op en voegt het zich bij de 9800 controller:

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI-configuratie:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>  
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

Captive Portal met RADIUS Server op DNA-ruimtes

Opmerking: DNA Spaces RADIUS-server ondersteunt alleen PAP-verificatie die van de controller komt.

Web Auth Parameter Map configuratie op de 9800 controller

Stap 1. Maak een web auth parameter map. Navigeer naar **Configuration > Security > Web Auth**, klik op **+Add**, configureer de naam van de parametermap en selecteer **webauth** als het type:

Create Web Auth Parameter ✕

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

✕ Close ✓ Apply to Device

Stap 2. Klik op de parameterkaart die in stap 1 is geconfigureerd, klik op **Advanced** en voer de

Redirect for log-in in, Add for AP MAC Address, Add for Client MAC Address, Add for WLAN SSID en portal IPv4 Address. Klik op **Bijwerken en toepassen:**

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address


Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page

Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

Opmerking: Om de splash pagina URL en het IPv4 omleiden adres te verkrijgen, klik op de **Handmatig instellen** optie van de SSID gemaakt in stap 3 van de sectie **Maak de SSID op DNA-ruimtes** onder de sectie **Creëren van de SSID's in WLC Direct Connect** sectie **Creëer de configuratie van de toegangscontrolelijst** sectie.

Opmerking: Cisco DNA Spaces Portal kan twee IP-adressen oplossen, maar de 9800 controller staat slechts toe dat één IP-adres wordt geconfigureerd, één case kiest een van die IP-adressen die op de parameterkaart moeten worden geconfigureerd als het Portal IPv4-adres.

Opmerking: Zorg ervoor dat zowel de virtuele IPv4- als de IPv6-adressen zijn geconfigureerd in de algemene webautoriteitsparameterkaart. Als de virtuele IPv6 niet is geconfigureerd, worden de clients soms omgeleid naar het interne portal in plaats van naar het geconfigureerde DNA-portaal. Daarom moet een virtueel IP altijd worden geconfigureerd. "192.0.2.1" kan worden geconfigureerd als Virtual IPv4 en FE80:0:0:0:903A::11E4 als Virtual IPV6. Er zijn weinig tot geen redenen om andere IP's te gebruiken dan deze.

CLI-configuratie:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

RADIUS-serverconfiguratie op de 9800-controller

Stap 1. Configureer de RADIUS-servers. Cisco DNA Spaces fungeert als de RADIUS-server voor gebruikersverificatie en kan reageren op twee IP-adressen. Navigeer naar **Configuration > Security > AAA**, klik op **+Add** en configureer beide RADIUS-servers:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

Servers Server Groups

TACACS+

Create AAA Radius Server

Name*	DNASpaces1
IPv4 / IPv6 Server Address*	34.197.146.105
PAC Key	<input type="checkbox"/>
Key Type	0
Key*	*****
Confirm Key*	*****
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

Cancel Apply to Device

Opmerking: om het IP-adres en de geheime sleutel van RADIUS voor zowel primaire als secundaire servers te verkrijgen, klikt u op de optie **Handmatig configureren** van de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** en naar de sectie **RADIUS Server Configuration** navigeren.

Stap 2. Configureer de RADIUS-servergroep en voeg beide RADIUS-servers toe. Navigeer naar **Configuratie > Beveiliging > AAA > servers / groepen > RADIUS > servergroepen**, klik op **+add**, configureer de naam van de servergroep, MAC-scheidingsteken als **koppelteken**, MAC-filtering als **MAC**, en wijs de twee RADIUS-servers toe:

[+ AAA Wizard](#)[Servers / Groups](#)[AAA Method List](#)[AAA Advanced](#)[+ Add](#)[- Delete](#)**RADIUS**

TACACS+

LDAP

Servers

Server Groups

Name

Server 1

Server 2

0 10 items per page

Create AAA Radius Server Group

Name*

DNASpaces

Group Type

RADIUS

MAC-Delimiter

hyphen

MAC-Filtering

mac

Dead-Time (mins)

1-1440

Available Servers

Assigned Servers

>

<

DNASpaces1
DNASpaces2[Cancel](#)[Apply to Device](#)

Stap 3. Configureer een lijst met verificatiemethoden. Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie**. Klik op **+Add**. Configureer de naam van de methodelijst, selecteer de **aanmelding** als het type en wijs de servergroep toe:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication
Authorization
Accounting

+ Add - Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> default	dot1x	local	N/A	N/A

10 items per page

Quick Setup: AAA Authentication

Method List Name* DNASpaces

Type* login

Group Type group

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- DNASpaces

Cancel Apply to Device

Stap 4. Configureer een lijst met autorisatiemethoden. Blader naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie** en klik op **+add**. Configureer de naam van de methodelijst, selecteer het **network** als het type en wijs de servergroep toe:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add - Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> MeshAP	credential-download	local	N/A	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name* **DNASpaces**

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- DNASpaces**

Cancel Apply to Device

De SSID op de 9800 controller maken

Stap 1. Navigeer naar **Configuratie > Tags en profielen > WLAN's** en klik op **+Add**. Configureer de profielnaam, SSID en schakel het WLAN in. Zorg ervoor dat de SSID-naam dezelfde naam is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken**.

Add WLAN ✕

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID

WLAN ID*

Status

Stap 2. Navigeer naar **Security > Layer 2**. Stel Layer 2 Security Mode in op **Geen**, schakel MAC-filtering in en voeg de autorisatielijst toe:

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Transition Mode WLAN ID Reassociation Timeout

Authorization List*

Stap 3. Navigeer naar **Security > Layer 3**. Schakel webbeleid in, configureer de webautoriteitparameterkaart en de verificatielijst. Schakel de optie Inschakelen op Mac-filterfout in en voeg de ACL voor verificatie toe. Klik op **Toepassen op apparaat**.

Add WLAN



General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map DNASpaces-PM ▼

Authentication List DNASpaces ▼

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

<< Hide

On Mac Filter Failure

Splash Web Redirect DISABLED

Preauthentication ACL

IPv4 DNASpaces-ACL ▼

IPv6 None ▼

Cancel

Apply to Device

Policy Profile op de 9800-controller configureren

Stap 1. Navigeer naar **Configuratie > Tags & profielen > Beleid** en maak een nieuw beleidsprofiel of gebruik het standaard beleidsprofiel. In het tabblad Toegangsbeleid moet u de client-VLAN configureren en het URL-filter toevoegen.

Edit Policy Profile



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

RADIUS Profiling

Local Subscriber Policy Name Search or Select ▼

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

VLAN

VLAN/VLAN Group VLAN2672 ▼

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ▼

IPv6 ACL Search or Select ▼

URL Filters

Pre Auth DNASpaces ▼

Post Auth Search or Select ▼

Stap 2. In het tabblad Geavanceerd, AAA negeren inschakelen en naar keuze de lijst met boekhoudmethoden configureren:

Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input type="text" value="default-aaa-policy x"/>
Accounting List	<input type="text" value="DNASpaces x"/>

Fabric Profile	<input type="checkbox"/> <input type="text" value="Search or Select"/>
Umbrella Parameter Map	<input type="text" value="Not Configured"/>
mDNS Service Policy	<input type="text" value="default-mdns-service"/> Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input type="text" value="Search or Select"/>

Air Time Fairness Policies

2.4 GHz Policy	<input type="text" value="Search or Select"/>
5 GHz Policy	<input type="text" value="Search or Select"/>

Policy Tag op de 9800 controller configureren

Stap 1. Ga naar **Configuration > Tags & profielen > Policy**. Maak een nieuwe beleidstag of gebruik de standaardbeleidstag. Breng het WLAN aan in het beleidsprofiel in de beleidstag.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Stap 2. Pas de Policy Tag toe op het toegangspunt om de SSID uit te zenden. Navigeer naar **Configuration > Wireless > Access points**, selecteer het toegangspunt in kwestie en voeg de beleidstag toe. Hierdoor start het toegangspunt de CAPWAP-tunnel opnieuw op en voegt het zich bij de 9800 controller:

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI-configuratie:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering
```

```
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list
```

```
Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

De globale parameterkaart configureren

Onaanbevolen stap: voer deze opdrachten uit om HTTPS-omleiding toe te staan, maar houd er rekening mee dat omleiding in client-HTTPS-verkeer niet nodig is als client-besturingssysteem de detectie van een interfaceportaal doet en een zwaarder CPU-gebruik veroorzaakt en altijd een certificaatwaarschuwing geeft. Het wordt daarom aanbevolen te vermijden om het te configureren, tenzij dit nodig is voor een zeer specifieke toepassing.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

Opmerking: u moet een geldig SSL-certificaat hebben voor de virtuele IP die in Cisco Catalyst 9800 Series draadloze controller is geïnstalleerd.

Stap 1. Kopieer een ondertekend gecertificeerd bestand met de extensie .p12 naar een TFTP-server en voer deze opdracht uit om het certificaat over te dragen en te installeren in de 9800 controller:

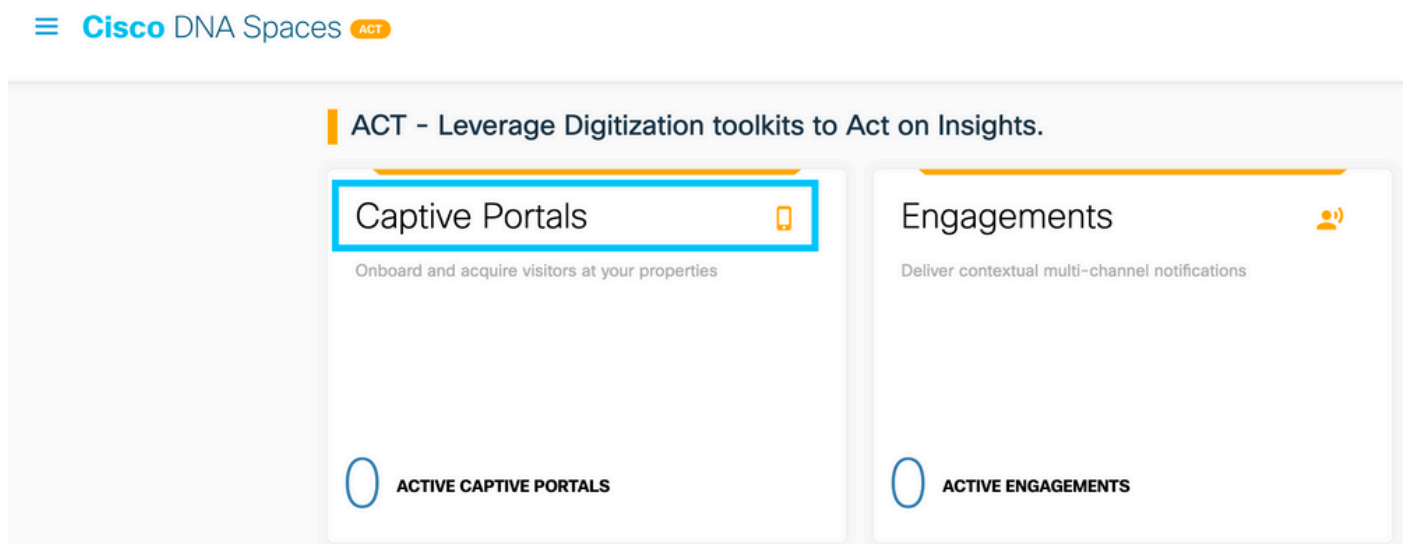
```
Andressi-9800L(config)#crypto pki import
```

Stap 2. Om het geïnstalleerde certificaat in kaart te brengen aan de kaart van de webauth-parameter, voert u deze opdrachten uit:

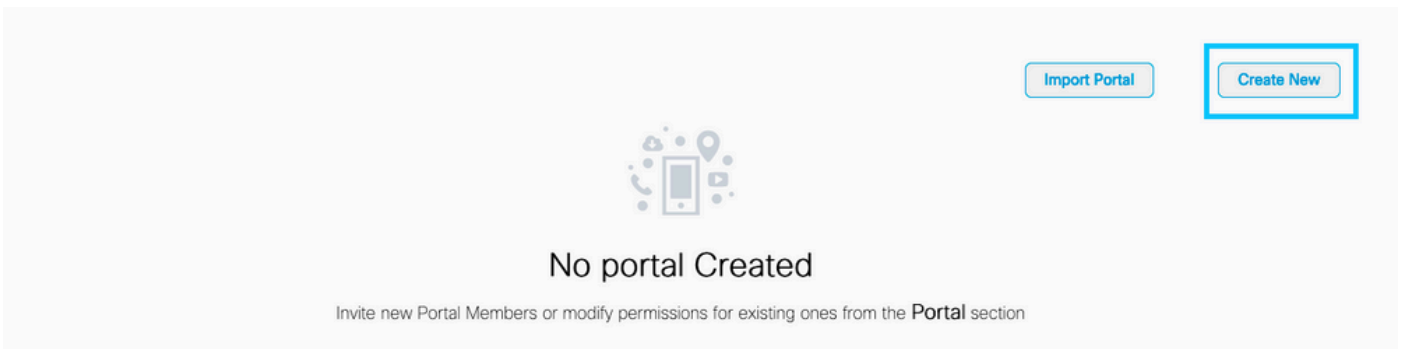
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

Maak het portaal op DNA-ruimtes

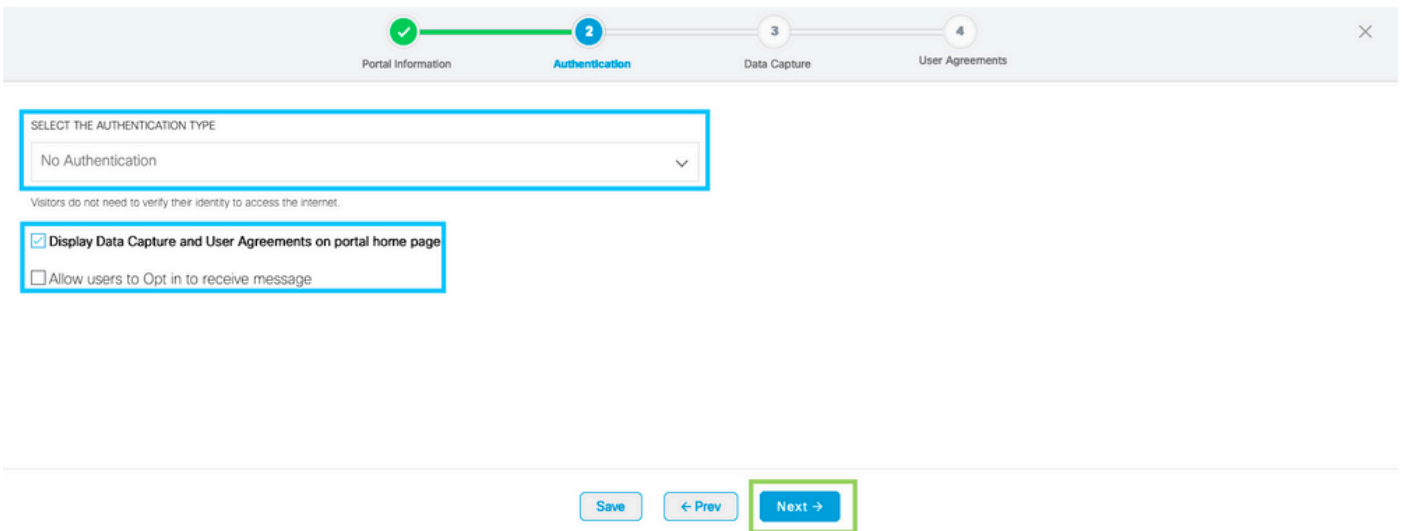
Stap 1. Klik op **Captive Portals** in het dashboard van DNA Spaces:



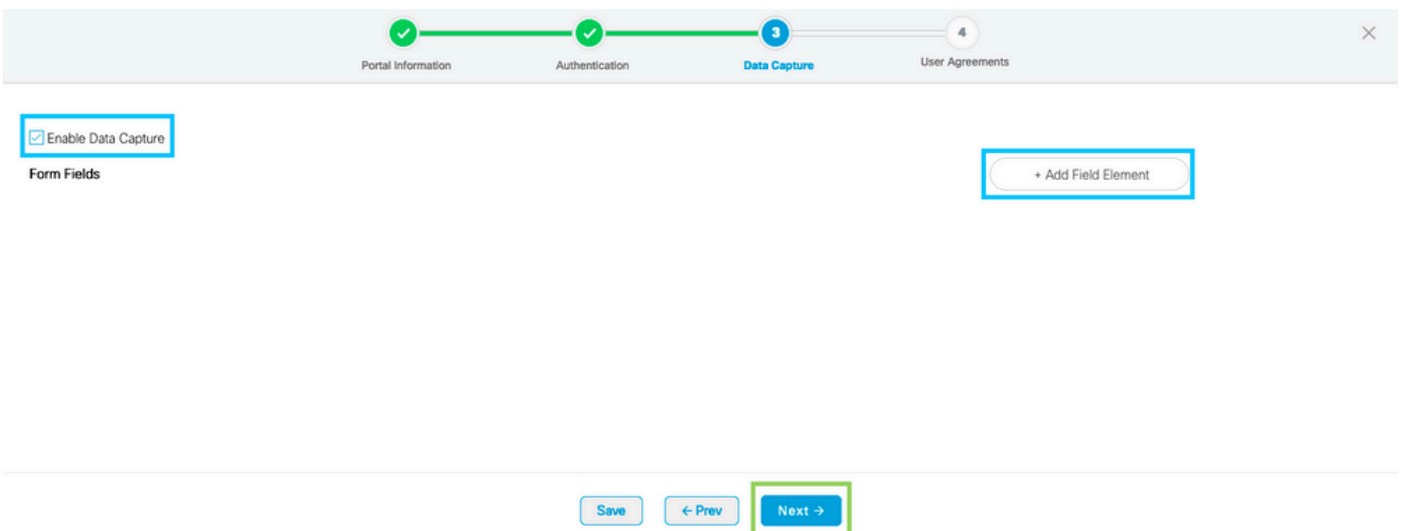
Stap 2. Klik op **Nieuw maken**, voer de portalnaam in en selecteer de locaties die de portal kunnen gebruiken:



Stap 3. Selecteer het verificatietype, kies als u gegevensvastlegging en gebruikersovereenkomsten op de portal-startpagina wilt weergeven en als gebruikers mogen inloggen om een bericht te ontvangen. Klik op **Volgende**:



Stap 4. Configureer de gegevensopnameelementen. Als u gegevens van de gebruikers wilt opnemen, schakelt u het vakje **Enable Data Capture** in en klikt u op **+Add Field Element** om de gewenste velden toe te voegen. Klik op **Volgende**:



Stap 5. Controleer de voorwaarden en bepalingen inschakelen en klik op **Portal opslaan en configureren**:

✓ Portal Information
 ✓ Authentication
 ✓ Data Capture
 4 User Agreements

This section allows you to enable and configure Terms & Conditions and Privacy policy Statements.

Enable Terms & Conditions

TERMS & CONDITION MESSAGE English

Wi-Fi Terms of Use, Last updated: September 27, 2013.
 These Wi-Fi Terms & Conditions Of Use (the Wi-Fi Terms) together with the TERMS OF USE govern your use of the Wi-Fi service.
 Description of the Service
 The Service provides you with wireless access to the Internet within the premises. We do not, as an ordinary practice, proactively monitor the activities of those who use the Service or exercise any editorial control over any material transmitted, hosted or posted using the Service to ensure that users comply with these Wi-Fi Terms and/or the law, although it reserves the right to do so.

Stap 6. Bewerk het portal zoals nodig, klik op Opslaan:

LOCATIONS: 1 Location ✓
 AUTH TYPE: No Authentication ✓
 USER AGREEMENTS: Enabled ✓
 DATA CAPTURE: Email, Mobile Number ✓

PORTAL EDITOR - Select a section to configure. Drag the items to reorder modules.

- Brand Name
- Welcome Message**
- Notice
- Data Capture
- Venue Map
- Videos
- Feedback
- Help
- Get Apps
- Get Internet
- Promos & Offers

[+ Add Module](#)

WELCOME MESSAGE

First time visitor welcome text

Welcome to Cisco Mexico

Add a custom message for Repeat visitors

Hi \${firstName} \${lastName}, Welcome to \$location x

Note
If any variables used in the message above are not available. We will default to the message shown for first time visitors.

PORTAL PREVIEW

Home Screen

ACME Company

Welcome to Cisco Mexico

SIGN-UP FOR WIFI

Email Address

Mobile Number

 Cancel

Configureer de Captive Portal Rules voor DNA-ruimtes

Stap 1. Klik op **Captive Portals** in het dashboard van DNA Spaces:

ACT - Leverage Digitization toolkits to Act on Insights.

Captive Portals 📱

Onboard and acquire visitors at your properties

0

ACTIVE CAPTIVE PORTALS

Engagements 👤

Deliver contextual multi-channel notifications

0

ACTIVE ENGAGEMENTS

Stap 2. Open het menu van het interactieve portaal en klik op **Captive Portal Rules**:

The screenshot shows the Cisco DNA Spaces interface. On the left, a dark sidebar menu is open, with 'Captive Portal Rules' highlighted in blue. The main content area shows the 'Captive Portals' section with a table of rules. The table has columns for NAME, STATUS, and LAST MODIFIED. One rule is visible: '9800DNASpaces1' with a status of 'Draft' and a last modified date of 'Feb 18, 2020'. There are 'Import Portal' and 'Create New' buttons at the top right of the table.

Stap 3. Klik op **+ Nieuwe regel maken**. Voer de regelnaam in en kies de eerder ingestelde SSID.

The screenshot shows the 'Create Captive Portal Rule' form. At the top, there is a back arrow and the title 'Create Captive Portal Rule'. Below it, a text input field contains 'RULE NAME: 9800DNASpaces' and is highlighted with a blue box. Underneath, there is a section titled 'Choose any or all of the options that apply to your rule below'. In this section, there is a dropdown menu for 'When a user is on' set to 'WiFi', and another dropdown menu for 'and connected to' set to '9800-DNASpaces1', which is also highlighted with a blue box. Below this is a section titled 'LOCATIONS - Where do you want the rule to fire?' with the text 'At any of the following locations' and a '+ Add Locations' button. At the bottom of this section, it says 'Please select at-least one location'.

Stap 4. Selecteer de locaties waar de portal beschikbaar is. Klik op **+ Locaties toevoegen** in de sectie **LOCATIES**. Kies de gewenste uit de Locatie Hiërarchie.

Choose Locations

Location Hierarchy

MEX-EAST-1	<input type="checkbox"/>
+ 5508-1-CMX	<input type="checkbox"/>
+ 5508-2-Connector	<input type="checkbox"/>
+ 5520-1-DirectConnect	<input type="checkbox"/>
9800L-DirectConnect	<input checked="" type="checkbox"/>

Selected Locations

9800L-DirectConnect X

Stap 5. Kies de actie van het portaal voor gevangenschap. In dit geval, wanneer de regel wordt geraakt, wordt het portaal getoond. Klik op **Opslaan en publiceren**.

ACTIONS

- Show Captive Portal**
Choose a Portal to be displayed to Users when they connect to the wifi.
9800DNASpaces1
- Session Duration
- Bandwidth Limit
- Seamlessly Provision Internet
Directly provision internet without showing any authentication
- Deny Internet
Stop users from accessing the internet

Tags these users as
Choose - Associate/Disassociate users to chosen tags.
+ Add Tags

Trigger API

Save & Publish Save

SCHEDULE

ACTION
Show Captive Portal
Portal : 9800DNASpaces1

Krijg specifieke informatie van DNA Spaces

Wat zijn de IP-adressen die DNA-ruimtes gebruiken?

Om te verifiëren welke IP-adressen DNA-ruimtes voor het portaal in uw regio worden gebruikt, gaat u naar de pagina Captival Portal op de DNA Space home. Klik op **SSID** in het linkermenu en klik vervolgens op **handmatig configureren** onder uw SSID. De IP-adressen worden in het voorbeeld van de ACL genoemd. Dat zijn de IP-adressen van het portaal voor gebruik in ACL's en webauth parameterkaart. DNA-ruimtes gebruiken andere IP-adressen voor de algehele NMSP/cloud-connectiviteit van het besturingsplane.



In de eerste sectie van de pop-up die wordt weergegeven, toont stap 7 de IP-adressen die in de ACL-definitie worden vermeld. U hoeft die instructies niet te doen en geen ACL te maken, neem gewoon nota van de IP-adressen. Dat zijn de IP's die door de portal in uw omgeving worden gebruikt

Configure



Creating the Access Control List

To create the access control list, perform the following steps:

- 1 Log in to the WLC Direct Connect with your WLC Direct Connect credentials.
- 2 Choose **Security > Access Control Lists > Access Control Lists**.
For FlexConnect local mode, choose **Security > Access Control Lists > FlexConnect ACLs**.
- 3 To add an ACL, click **New**.
- 4 In the **New** page that appears, enter the following:
 - a. In the **Access Control List Name** field, enter a name for the new ACL.

Note:

You can enter up to 32 alphanumeric characters.

- b. Choose the ACL type as **IPv4**.

Note:

This option is not available for FlexConnect ACLs.

- c. Click **Apply**.

- 5 When the **Access Control Lists** page reappears, click the name of the new ACL.
- 6 In the **Edit** page that appears, click **Add New Rule**. The **Rules > New** page appears.
- 7 Configure a rule for this ACL with the following wall garden ranges.

No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

Wat is de URL die het inlogportal van DNA Spaces gebruikt?

Om te verifiëren welke login portal URL DNA Spaces gebruikt voor de portal in uw regio, ga naar de Captival Portal pagina op de DNA Space home. Klik op **SSID** in het linkermenu en klik vervolgens op **handmatig configureren** onder uw SSID.



Scroll omlaag in de pop-up die verschijnt en in de tweede sectie, stap 7 toont u de URL die u moet configureren in uw parametermap op de 9800.

Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

- 1 In the WLC Direct Connect main window, click the **WLANS** tab.
- 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
- 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
- 4 Click **Apply**.
The WLAN added appears in the WLANS page.
- 5 Click the WLAN you have newly created.
- 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.
- 7 In the **Layer 3 tab**, do the following configurations:
 - a. From the Layer 3 security drop-down list, choose **Web Policy**.
 - b. Choose the **Passthrough** radio button.
 - c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.
 - d. Select the Enable check box for the Sleeping Client.
 - e. Select the Enable check box for the Override Global Config.
 - f. From the Web Auth Type drop-down list, choose **External**.
 - g. In the URL field that appears, enter the Cisco DNA Spaces splash URL.

<https://splash.dnaspaces.eu/p2/emeabru2>

Wat zijn de RADIUS-servergegevens voor DNA-ruimtes?

Om te weten te komen wat de RADIUS-server IP-adressen zijn die u moet gebruiken en wat het gedeelde geheim is, gaat u naar de pagina Captival Portal op het DNA Space home. Klik op **SSID** in het linkermenu en klik vervolgens op **handmatig configureren** onder uw SSID.



In het pop-upvenster dat wordt weergegeven, scrollt u omlaag in de derde sectie (RADIUS) en stap 7 geeft u het IP/poort en gedeeld geheim voor radiusverificatie. Accounting is optioneel en wordt behandeld in stap 12.

- 7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvJK

- 8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

- 9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

- 10 From the MAC Delimiter drop-down list, choose **Hyphen**.

- 11 Click **New**.

- 12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvJK

Verifiëren

Om de status te bevestigen van een client die is aangesloten op de SSID, navigeer naar **Monitoring > Clients**, klik op het MAC-adres van het apparaat en zoek naar Policy Manager-status:

Client	
360 View General QOS Statistics ATF Statistics Mobility History Call Statistics	
Client Properties AP Properties Security Information Client Statistics QOS Properties	
Wireless LAN Id	1
WLAN Profile Name	9800-DNASpaces1
Wireless LAN Network Name (SSID)	9800-DNASpaces1
BSSID	10b3.d694.00ef
Uptime(sec)	64 seconds
Session Timeout	1800 sec (Remaining time: 1762 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m2 ss1
Supported Rates	9.0,18.0,36.0,48.0,54.0
Join Time Of Client	03/11/2020 17:47:25 Central
Policy Manager State	Run

Problemen oplossen

Veelvoorkomende problemen

1. Als de virtuele interface op de controller geen IP-adres heeft geconfigureerd, worden de clients omgeleid naar het interne portal in plaats van naar het omleiden portal dat in de parameterkaart is geconfigureerd.
2. Als de cliënten een *fout 503* ontvangen terwijl omgeleid naar het portaal op de ruimten van DNA, zorg ervoor de controlemechanisme in de **Hiërarchie** van de **Plaats** op Ruimten van DNA wordt gevormd.

Altijd-AAN-traceren

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle aan de client gerelateerde fouten, waarschuwingen en meldingen op het niveau constant worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

Opmerking: afhankelijk van het volume van de logbestanden die worden gegenereerd, kunt u enkele uren teruggaan naar meerdere dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en deze stappen uitvoeren (Zorg ervoor dat u de sessie vastlegt aan een tekstbestand).

Stap 1. Controleer de huidige controllertijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

```
# show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals die door de systeemconfiguratie wordt gedictieerd. Dit geeft een snel overzicht van de gezondheid van het systeem en eventuele fouten.

```
# show logging
```

Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
Cisco IOS-XE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                                     Port
-----|-----
```

Opmerking: als u een van de vermelde voorwaarden ziet, betekent dit dat de sporen worden aangemeld om het debug-niveau te bereiken voor alle processen die de ingeschakelde voorwaarden ervaren (mac-adres, IP-adres, etc.). Dit zou het volume van de boomstammen doen toenemen. Daarom wordt aanbevolen alle voorwaarden te wissen wanneer niet actief debuggen

Stap 4. Als het mac-adres dat getest wordt niet als voorwaarde vermeld is in Stap 3, verzamel dan de altijd beschikbare informatie voor het specifieke mac-adres.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Voorwaardelijke debugging en radio actieve tracering

Als de altijd-on sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug level traces biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Voer deze stappen uit om voorwaardelijke debugging in te schakelen.

Stap 1. Zorg ervoor dat de debug-voorwaarden niet zijn ingeschakeld.

```
# clear platform condition all
```

Stap 2. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdrachten wordt het opgegeven MAC-adres 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Opmerking: als u meer dan één client tegelijk wilt bewaken, voert u de opdracht `debug wireless mac <aaaa.bbbb.ccc>` per mac-adres uit.

Opmerking: U ziet de output van de client activiteit niet op de terminal sessie, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 3. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 4. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Zodra de monitor-tijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

```
ra_trace_MAC_aabbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 5. Verzamel het bestand van de mac-adresactiviteit. U kunt het spoor `.log` naar een externe server kopiëren of de uitvoer direct op het scherm weergeven.

Controleer de naam van het RA traces bestand

```
# dir bootflash: | inc ra_trace
```

Kopieert het bestand naar een externe server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Geef de inhoud weer:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 6. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer breedsprakige mening van debug niveaulogboeken zijn. U hoeft niet opnieuw te debuggen de client als we alleen een verdere gedetailleerde kijk op debug logs die al zijn verzameld en intern opgeslagen.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
```

to-file ra-internal-<FILENAME>.txt

Opmerking: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem contact op met Cisco TAC om te helpen bij het doorlopen van deze sporen.

U kunt de Ra-internal-FILENAME.txt kopiëren naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Kopieert het bestand naar een externe server:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Geef de inhoud weer:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Stap 7. Verwijder de debug-voorwaarden.

```
# clear platform condition all
```

Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossing sessie.

Voorbeeld van een geslaagde poging

Dit is de output van RA_traces voor een succesvolle poging om elk van de fasen tijdens het vereniging/authenticatieproces te identificeren terwijl het verbinden met een SSID zonder server van de RADIUS.

802.11 koppeling/authenticatie:

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0, 2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile: DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

IP-leerproces:

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

Layer 3-verificatie:

Triggered L3 authentication. status = 0x0, Success
Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
L3 Authentication initiated. LWA
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in INIT state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src [10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in LOGIN state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src [10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in LOGIN state

Layer 3-verificatie gelukt, verplaats de client naar de status RUN:

[34e1.2d23.a668:capwap_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668
L3 Authentication Successful. ACL:[]
Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entry (34E1.2D23.A668) joined with ssid (9800DNASpaces) for device with MAC: 34e1.2d23.a668
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU

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.