DNA-ruimtes Captive Portal met AireOS Controller Configuration Voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u interactieve portalen kunt configureren met behulp van Cisco DNA Spaces met een AireOS-controller.

Bijgedragen door Andres Silva Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

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

- 5520 draadloze LAN-controller versie 8.10.12.0

Configureren

Netwerkdiagram

Configuraties

Sluit de WLC aan op Cisco DNA-ruimtes

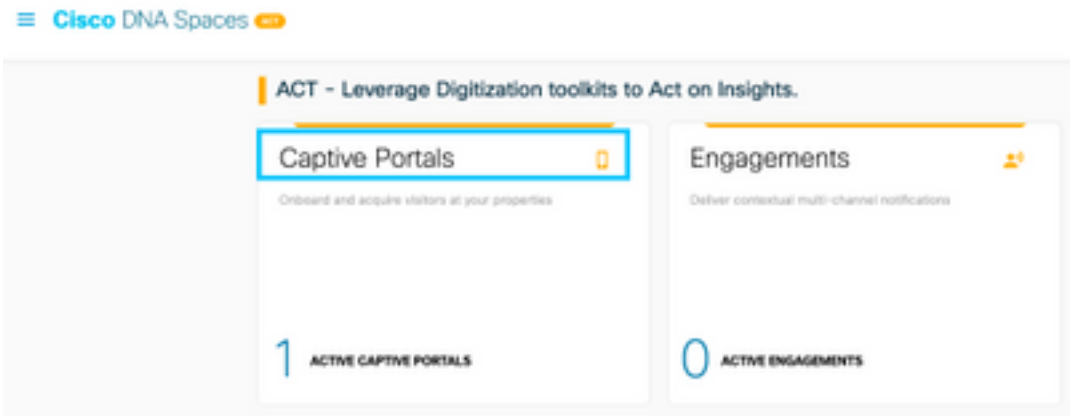
De controller moet worden aangesloten op DNA-ruimtes met behulp van een van de beschikbare instellingen, Direct Connect, via DNA Spaces Connector of met CMX Tethering.

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

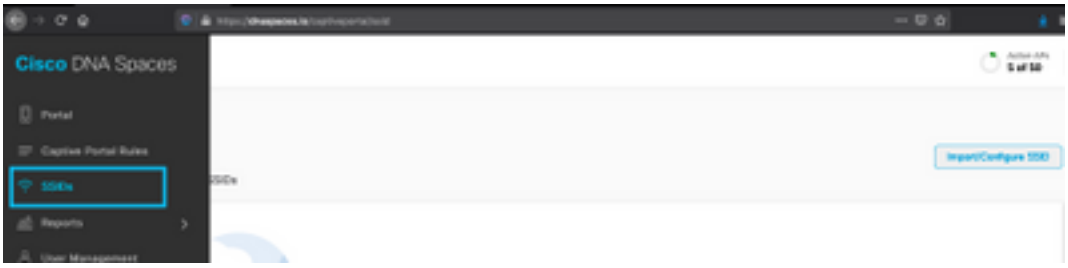
Om de controller te verbinden met Cisco DNA Spaces moet het in staat zijn om de Cisco DNA Spaces-cloud via HTTPS te bereiken. Voor meer informatie over het aansluiten van de controller op DNA-ruimtes, zie deze link: DNA-ruimtes Direct Connect Configuration Voorbeeld

De SSID op DNA-ruimtes maken

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



Stap 2. Open het menu van het toegangsportaal door op het pictogram van drie lijnen linksboven op de pagina te klikken en klik op **SSID's:**

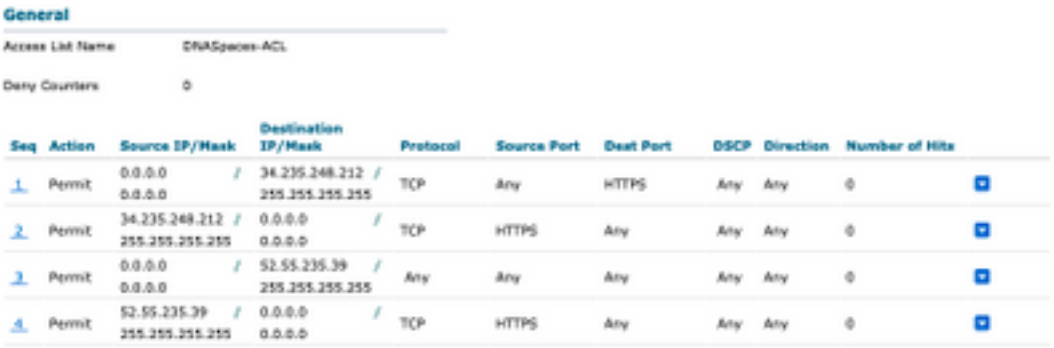


Stap 3. Klik op **SSID importeren/configureren**, selecteer **CUWN (CMX/WLC)** als het type "Draadloos netwerk" en voer de naam van de SSID in:

ACL-configuratie op de controller

Een pre-authenticatie ACL is vereist als dit een web verificatie SSID is, en zodra het draadloze apparaat verbinding maakt met de SSID en een IP-adres ontvangt, de staat van de beleidsmanager van het apparaat verplaatst naar de staat **Webauth_Reqd** en de ACL wordt toegepast op de client sessie om de bronnen te beperken die het apparaat kan bereiken.

Stap 1. Navigeer naar **Security > Access Control Lists > Access Control Lists,** klik op **New** en configureer de regels om communicatie tussen de draadloze clients mogelijk te maken naar DNA-ruimtes als volgt. Vervang de IP-adressen door de door DNA Spaces opgegeven adressen voor de account in gebruik:



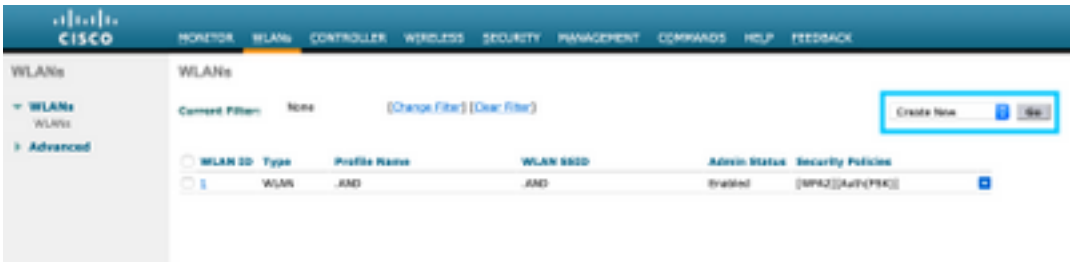
> **Opmerking**: Om de IP-adressen van DNA-ruimtes in de ACL toe te staan, klikt u op de optie **Handmatig configureren** uit de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** onder de sectie ACL-configuratie.

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.

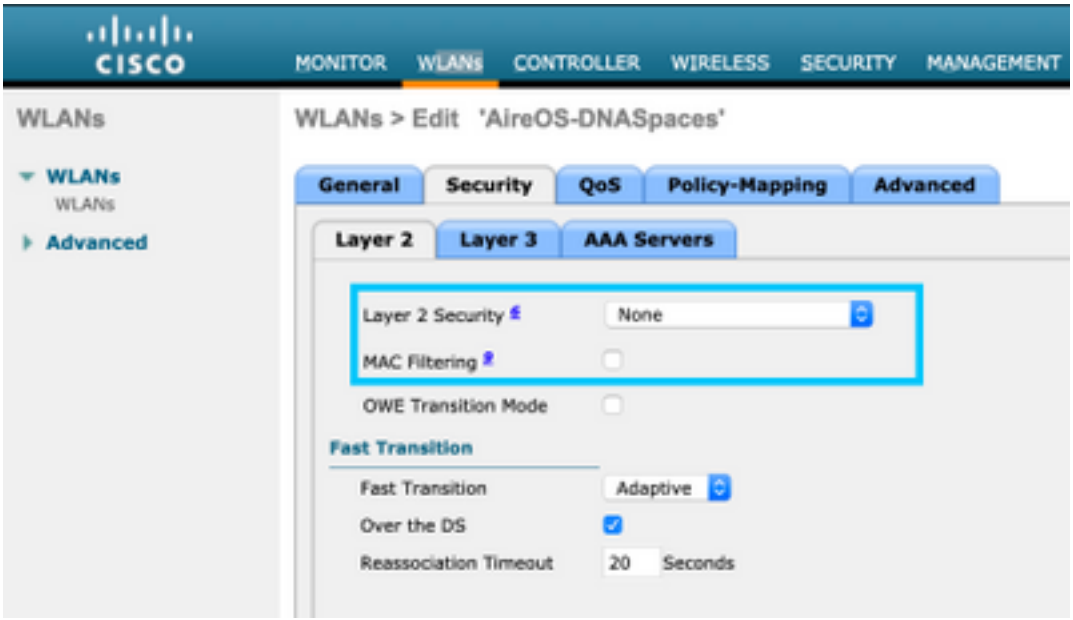
Captive Portal zonder RADIUS-server op DNA-ruimtes

SSID-configuratie op de controller

Stap 1. Navigeren naar **WLAN's > WLAN's.** Maak een nieuw WLAN. Configureer de profielnaam en de SSID. Zorg ervoor dat de SSID-naam hetzelfde is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken.**



Stap 2. Layer 2-beveiliging configureren. Navigeer naar het tabblad **Security > Layer 2** in het tabblad WLAN-configuratie en selecteer als **Geen** in het vervolgkeuzemenu van Layer 2 Security**.** Zorg ervoor dat MAC Filtering is uitgeschakeld.



Stap 3. Layer 3-beveiliging configureren. Navigeer naar het tabblad Security > Layer 3 in het tabblad WLAN-configuratie, vorm Web **Policy als de Layer 3-beveiligingsmethode, Passthrough inschakelen, configureer de voorverificatie-ACL, Override Global Config inschakelen** zoals het **Web Auth Type** als **Extern is ingesteld,** en stel de Redirect URL in.

Opmerking: om de URL te verplaatsen, klikt u op de optie **Handmatig configureren**, van de SSID die is gemaakt in stap 3 van de sectie **De SSID maken op DNA-ruimtes,** onder de sectie SSID configuratie.

Captive Portal met RADIUS Server op DNA-ruimtes

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

Configuratie RADIUS-servers op de controller

Stap 1. Navigeer naar **Security > AAA > RADIUS > Verificatie,** klik op **New** en voer de RADIUS-serverinformatie in. Cisco DNA Spaces fungeert als de RADIUS-server voor gebruikersverificatie

en kan reageren op twee IP-adressen. Beide RADIUS-servers configureren:

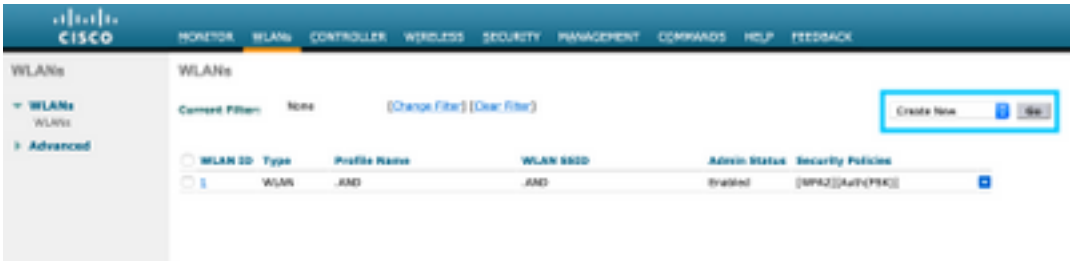
> **Opmerking**: om het IP-adres en de geheime sleutel van RADIUS voor zowel primaire als secundaire servers te verkrijgen, klikt u op de optie **Handmatig configureren** van de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** en naar de sectie **RADIUS Server Configuration**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

Stap 2. Configureer de RADIUS-server voor accounting. Navigeer naar **Security > AAA > RADIUS > Accounting** en klik op **New**. Configureer de twee RADIUS-servers als volgt:

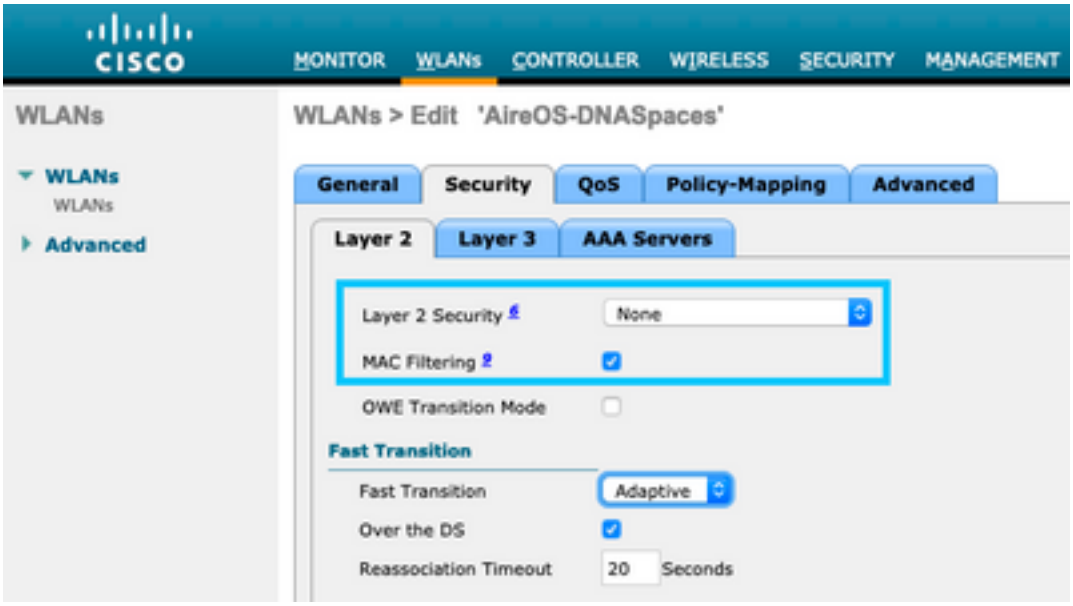
SSID-configuratie op de controller

> **Belangrijk**: Alvorens met de configuratie van SSID te beginnen, zorg ervoor dat de **Verificatie van de Radius van het Web** aan "PAP"onder Controlemechanisme > Algemeen wordt geplaatst.

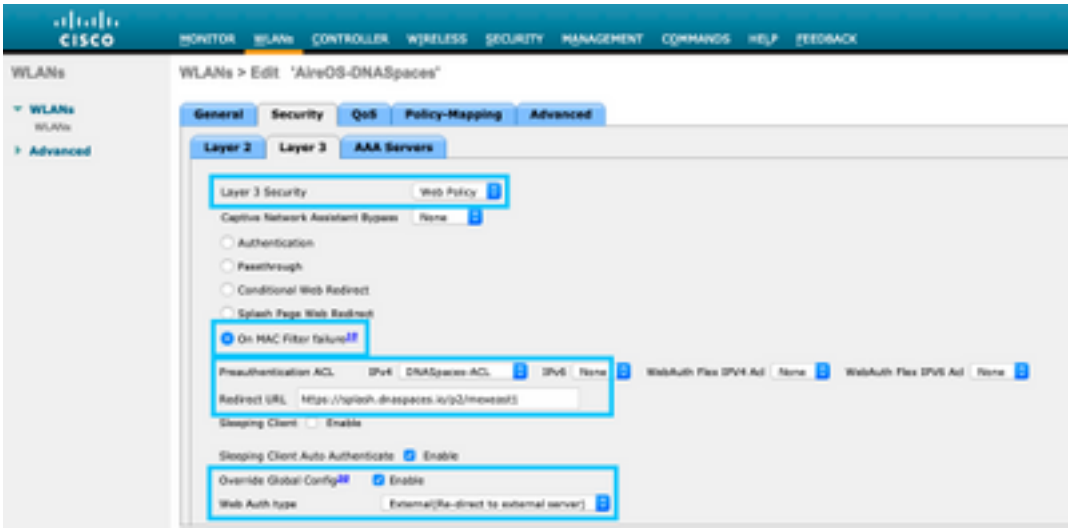
Stap 1. Navigeren naar **WLAN's > WLAN's.** Maak een nieuw WLAN. Configureer de profielnaam en de SSID. Zorg ervoor dat de SSID-naam hetzelfde is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken.**



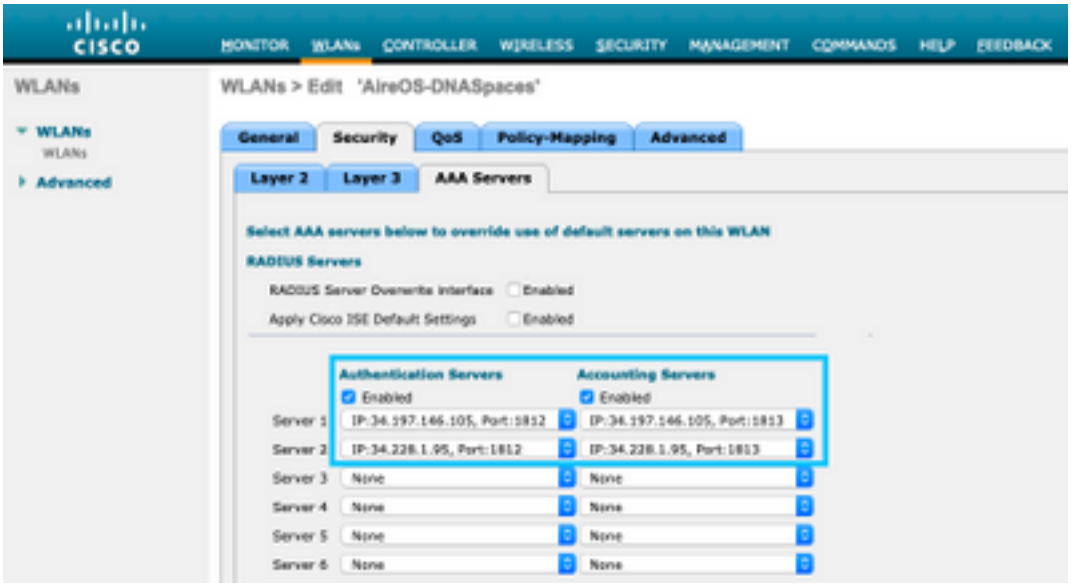
Stap 2. Layer 2-beveiliging configureren. Navigeer naar het tabblad **Security > Layer 2** in het tabblad WLAN-configuratie. Layer 2-beveiliging als **geen** configureren. Schakel Mac-filtering in.



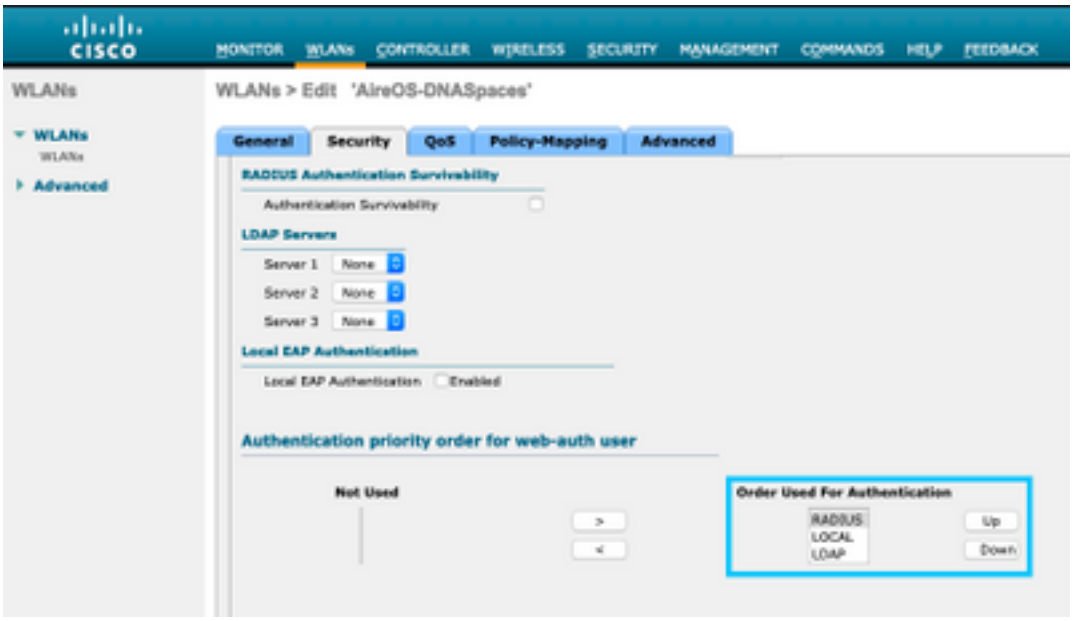
Stap 3. Layer 3-beveiliging configureren. Navigeer naar het tabblad Security > Layer 3 in het tabblad WLAN-configuratie, configureer Web **Policy als de Layer 3-beveiligingsmethode, Inschakelen op fouten in Mac-filter, configureer de voorverificatie-ACL, Override Global Config inschakelen** zoals het **Web Auth Type** als **Extern is**, configureer de Redirect URL.



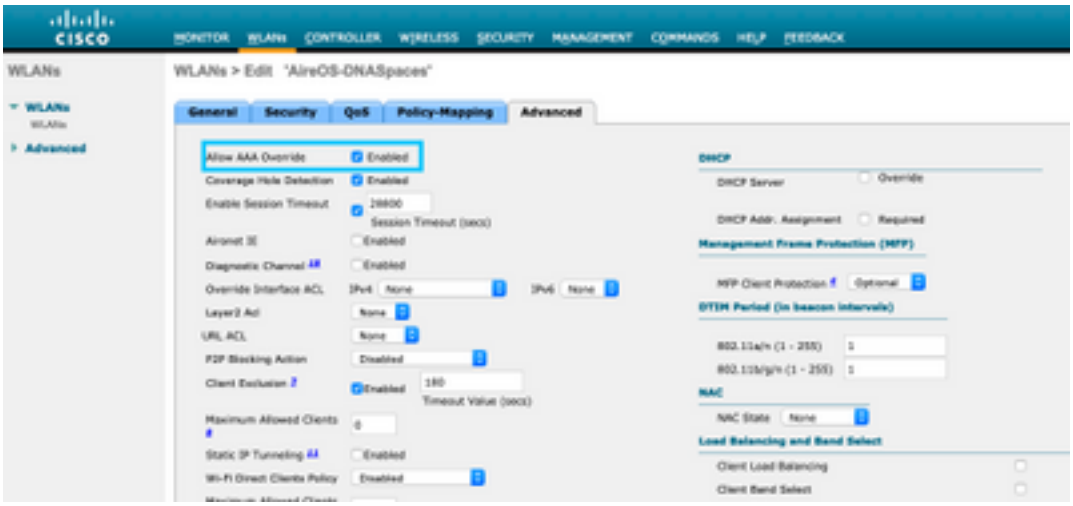
Stap 4. AAA-servers configureren. Navigeer naar het tabblad **Security > AAA-servers** in het tabblad WLAN-configuratie, **laat verificatieservers** en **accountingservers** toe en kies in het vervolgkeuzemenu de twee RADIUS-servers:



Stap 6. Configureer de **prioriteitsvolgorde voor verificatie voor webautoregebruikers**. Navigeer naar het tabblad **Security > AAA-servers** in het tabblad WLAN-configuratie en stel RADIUS als eerste in volgorde.

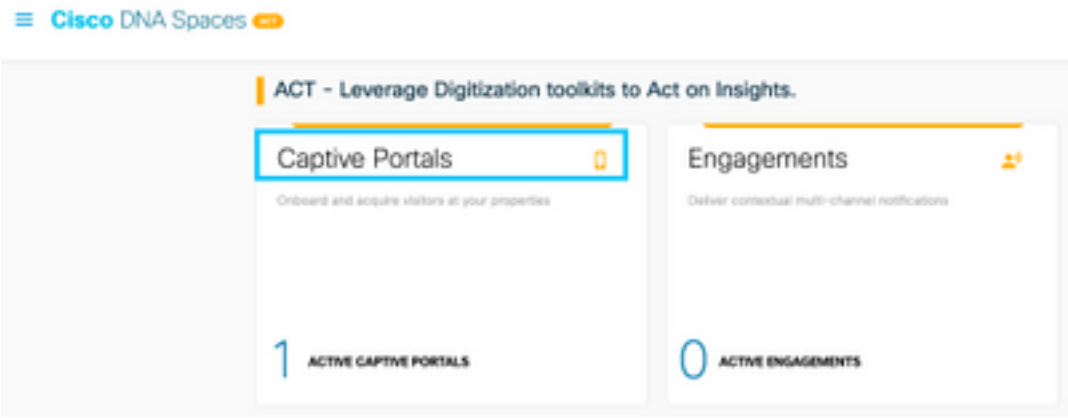


Stap 7. Navigeer naar het tabblad **Advanced** in het tabblad WLAN-configuratie en schakel **AAA-overbrugging** in.

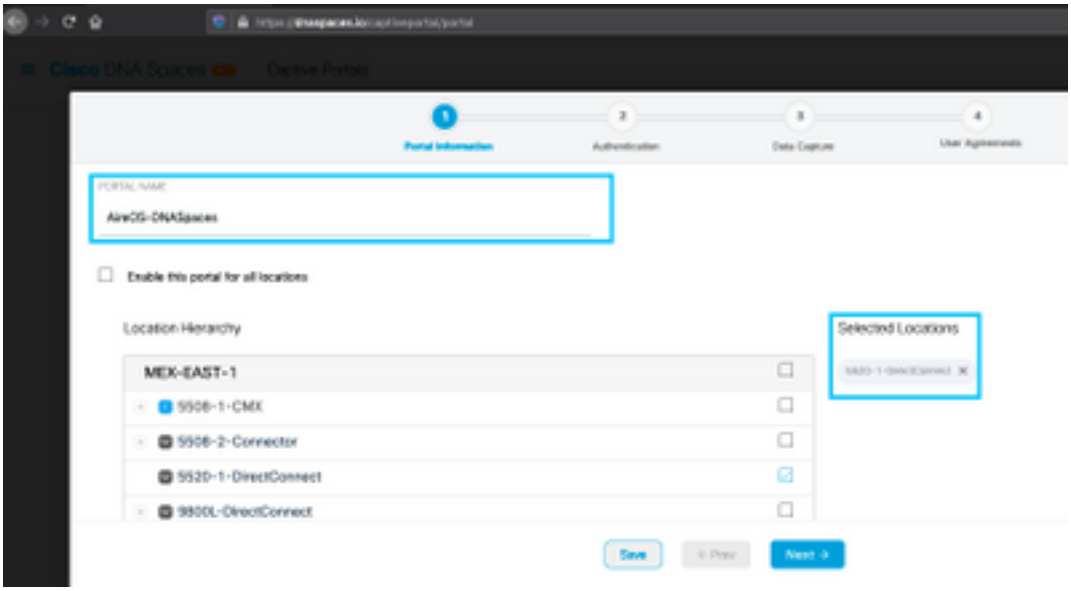


Maak het portaal op DNA-ruimtes

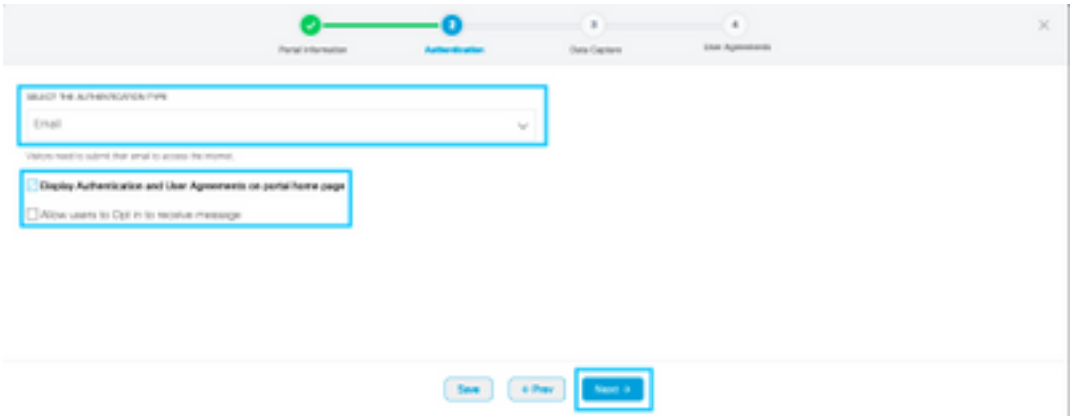
Stap 1. Klik op **Captive Portals** in het dashboard van DNA Spaces:



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

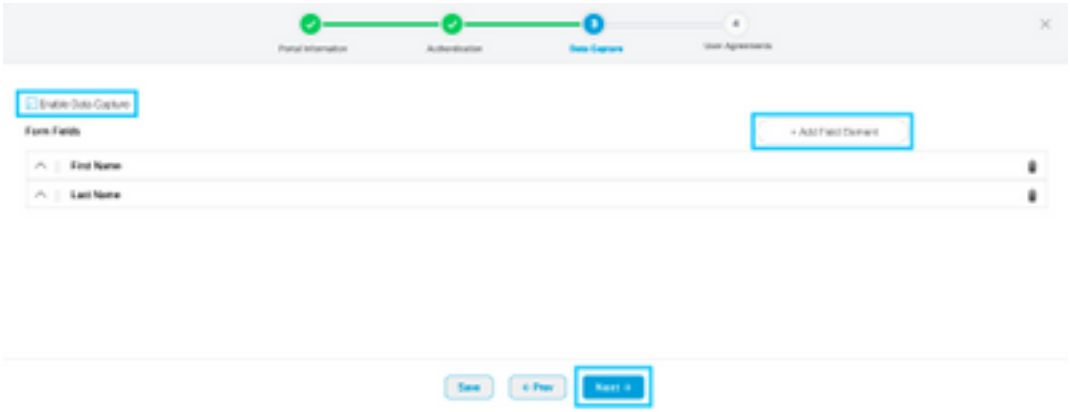


Stap 3. Selecteer het verificatietype, kies als u gegevensvastlegging en gebruikersovereenkomsten op de portal-startpagina wilt weergeven en als gebruikers mogen inloggen om een bericht te ontvangen. Klik op **Volgende**:



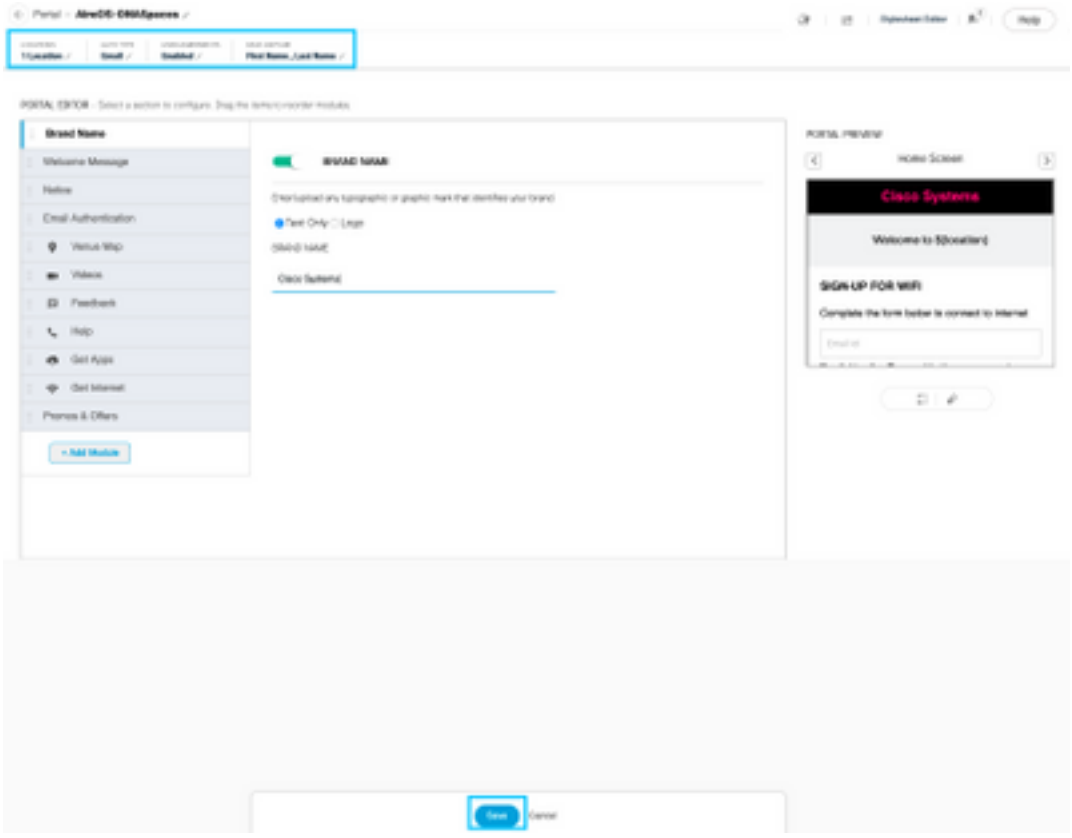
Stap 4. Configureer de gegevensopnameelementen. Als u gegevens van de gebruikers wilt opnemen, schakelt u het vakje **Enable Data Capture in** en klikt u op **+Add Field Element** om de

gewenste velden toe te voegen. Klik op **Volgende**:



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

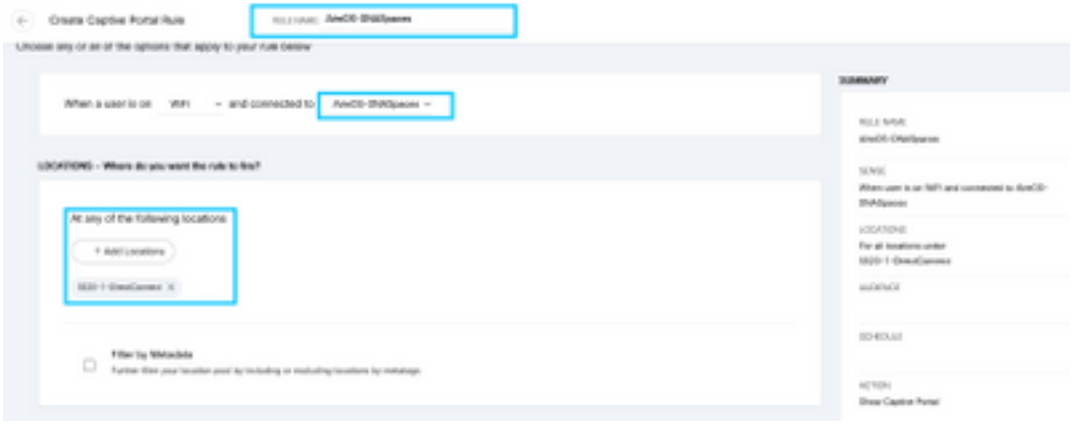
Stap 6. Bewerk het portal zoals nodig, klik op **Opslaan:**



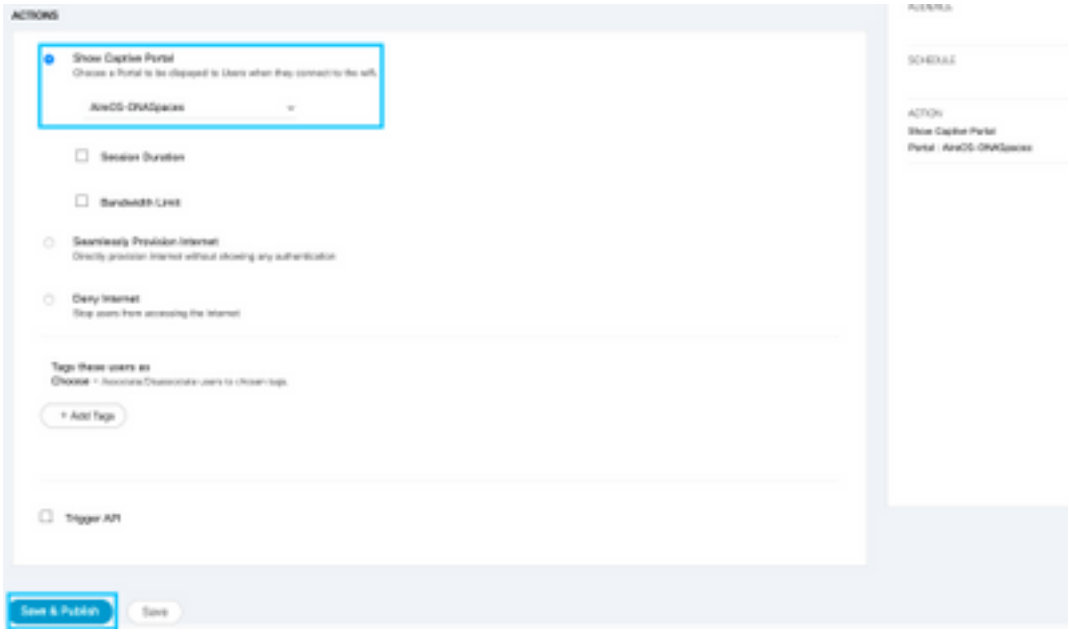
Configureer de Captive Portal Rules voor DNA-ruimtes

Stap 1. Open het menu van het interactieve portaal en klik op **Captive Portal Rules:**

Stap 2. Klik op **+ Nieuwe regel maken**. Voer de regelnaam in, kies de eerder geconfigureerde SSID en selecteer de locaties waar deze poortregel beschikbaar is voor:



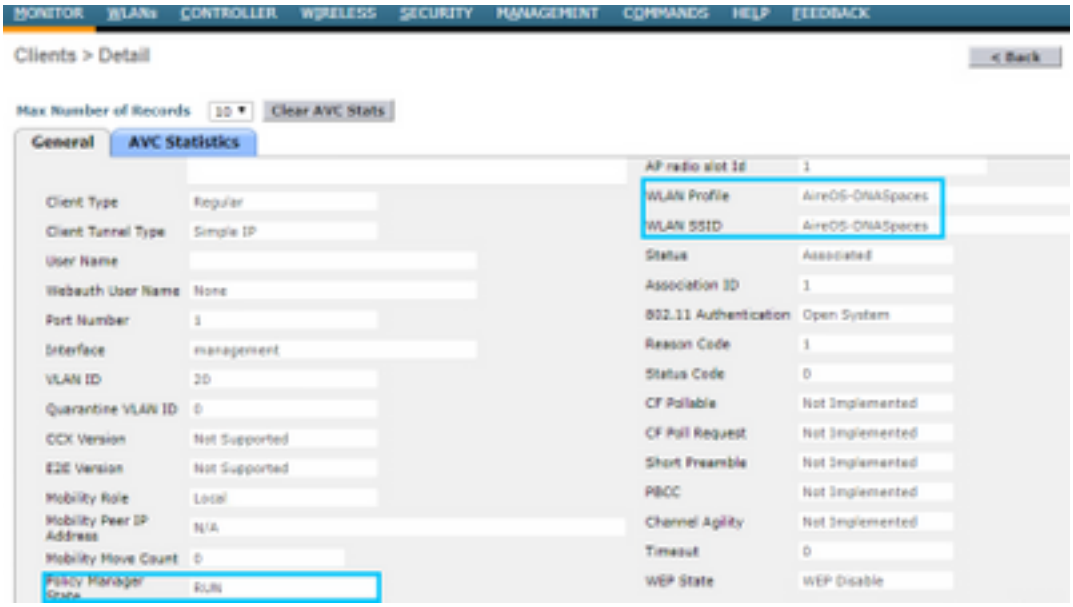
Stap 3. Kies de actie van het portaal voor gevangenschap. In dit geval, wanneer de regel wordt geraakt, wordt het portaal getoond. Klik op **Opslaan en publiceren.**



Verifiëren

Om de status te bevestigen van een client die is aangesloten op de SSID, navigeer naar **Monitor >**

Clients, klik op het MAC-adres en zoek naar Policy Manager-status:



Problemen oplossen

De volgende opdracht kan in de controller worden ingeschakeld voordat wordt getest om het associatie- en verificatieproces van de client te bevestigen.

```
(5520-Andressi) >debug client
```

```
(5520-Andressi) >debug web-auth redirect enable mac
```

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

802.11 koppeling/authenticatie:

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

DHCP- en Layer 3-verificatie:

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN
ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using
URL:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-
Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

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

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
```

```
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255,URL ACL ID 255,URL ACL
Action 0)

*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user
```

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.