Centrale webverificatie configureren op SD-Access

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Topologie

Overzicht

CWA configureren in Cisco Catalyst Center

- Het netwerkprofiel maken
- De SSID maken
- Fabric Provisioning

De configuratie bekijken die aan Cisco ISE is geleverd

- Autorisatieprofiel
- Beleidssets
- Configuratie van gastportal

De configuratie bekijken die aan de WLC is geleverd

- SSID-configuratie
- Configuratie van draadloos beleidsprofiel
- Beleidstag-configuratie
- ACL-configuratie omleiden

ACL omleiden op het toegangspunt

Inleiding

In dit document wordt een stapsgewijze handleiding beschreven voor het configureren van centrale webverificatie (CWA) en worden de verificatieprocedures voor alle onderdelen beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Catalyst 9800 draadloze controllerarchitectuur
- Authenticatie, autorisatie en boekhouding (AAA)

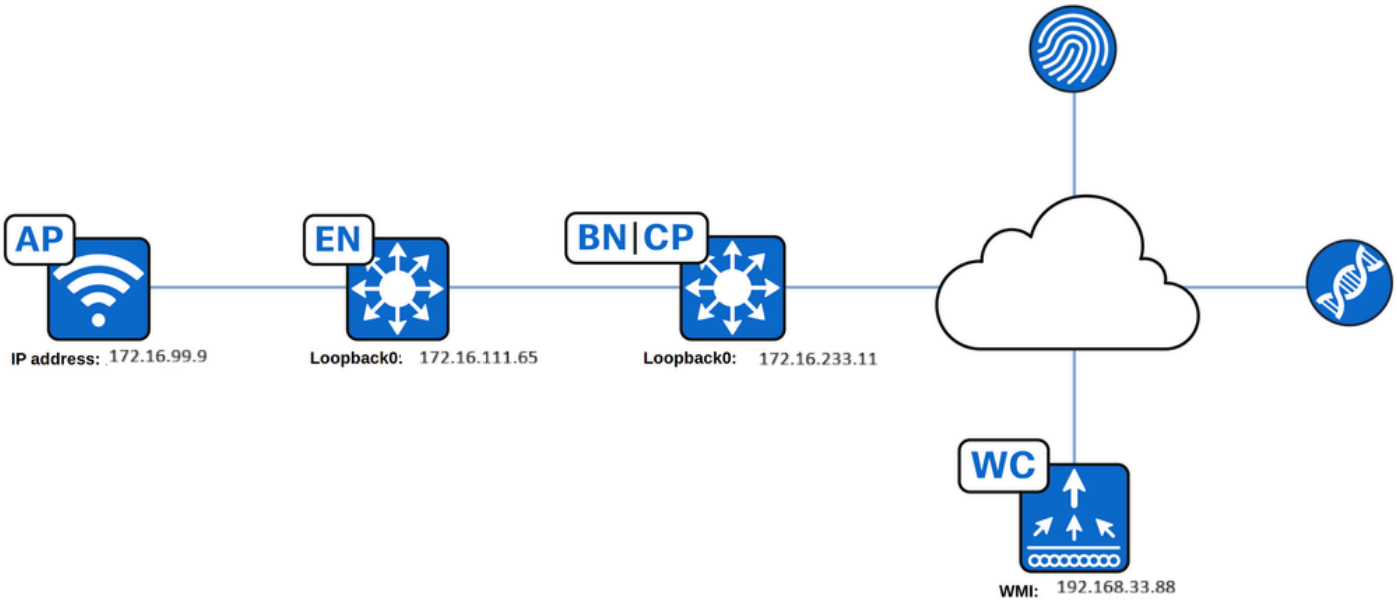
Gebruikte componenten

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

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - Versie 2.3.7.7
- Cisco Identity Services Engine (ISE) - Versie 3.0.0.458
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA Border Node/Control Plane - C9500-48P, Cisco IOS® XE17.12.05
- Cisco Access Point - C9130AXI-A, versie 17.9.5.47

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.

Topologie



Overzicht

Central Web Authentication (CWA) gebruikt een SSID van het gasttype om de webbrowser van de gebruiker om te leiden naar een captive portal gehost door Cisco ISE, met behulp van een geconfigureerde omleiding ACL. Met het interne portaal kan de gebruiker zich registreren en verifiëren en na succesvolle verificatie past de draadloze LAN-controller (WLC) de juiste machtiging toe om volledige netwerktoegang te verlenen. Deze handleiding bevat stapsgewijze instructies voor het configureren van CWA met Cisco Catalyst Center.

CWA configureren in Cisco Catalyst Center

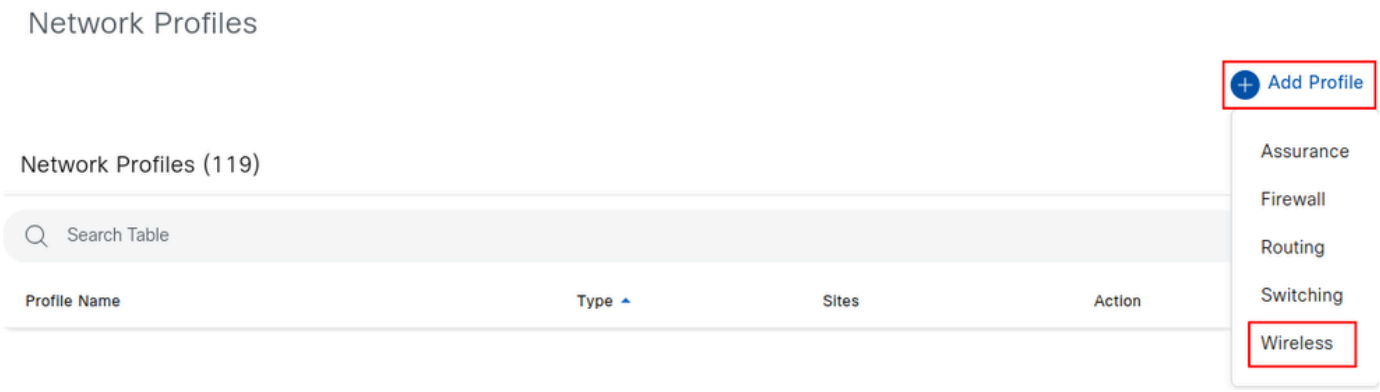
Het netwerkprofiel maken

Met een netwerkprofiel kunnen instellingen worden geconfigureerd die op een specifieke site kunnen worden toegepast. Netwerkprofielen kunnen worden gemaakt voor verschillende elementen in Cisco Catalyst Center, waaronder:

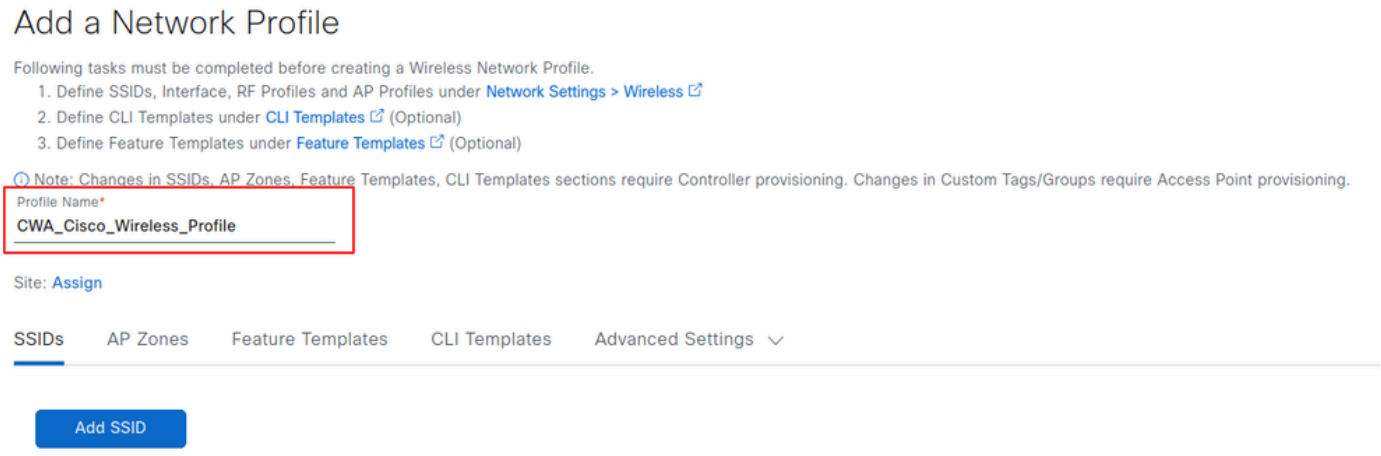
- verzekering
- firewall
- routering
- omschakeling
- telemetrieapparaat
- Draadloos

Voor CWA moet een draadloos profiel worden geconfigureerd.

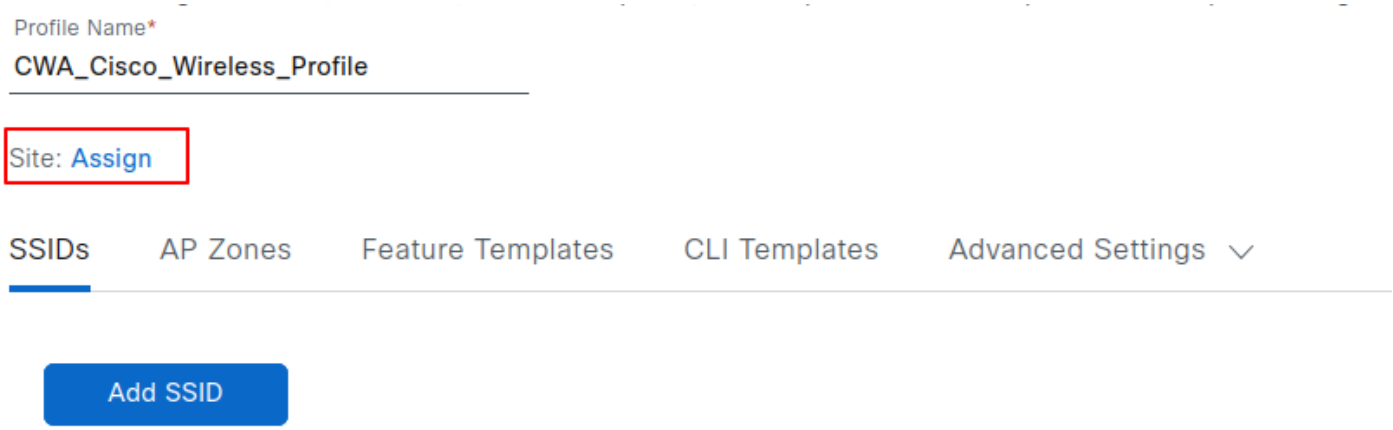
Als u een draadloos profiel wilt configureren, gaat u naar Ontwerpen > Netwerkprofielen, klikt u op Profiel toevoegen en selecteert u Draadloos.



Noem het profiel zoals vereist. In dit voorbeeld wordt het profiel voor het draadloze netwerk CWA_Cisco_Wireless_Profile genoemd. U kunt bestaande SSID's aan dit profiel toevoegen door SSID toevoegen te selecteren. Het maken van SSID's wordt behandeld in de volgende sectie.

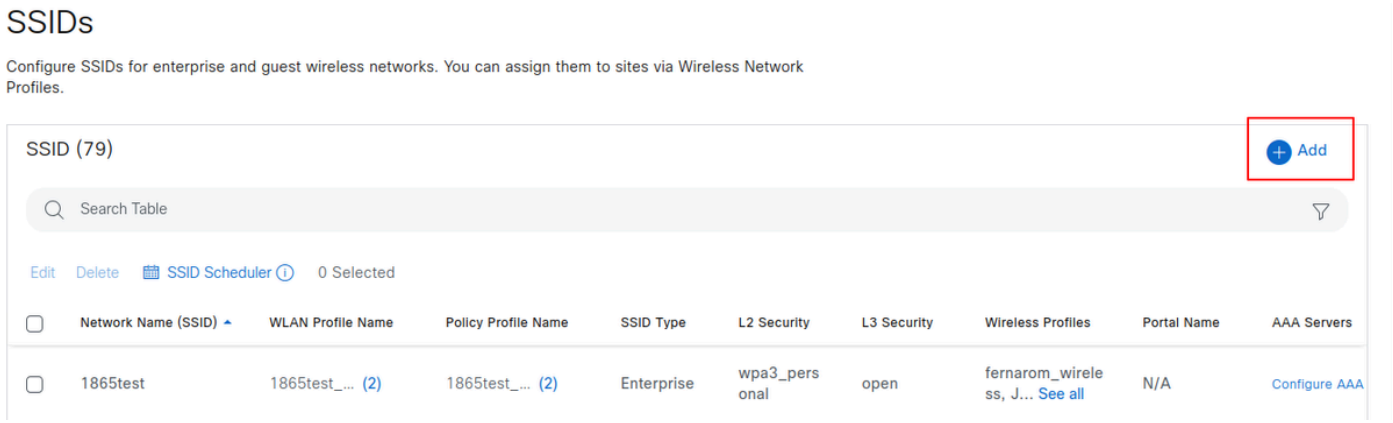


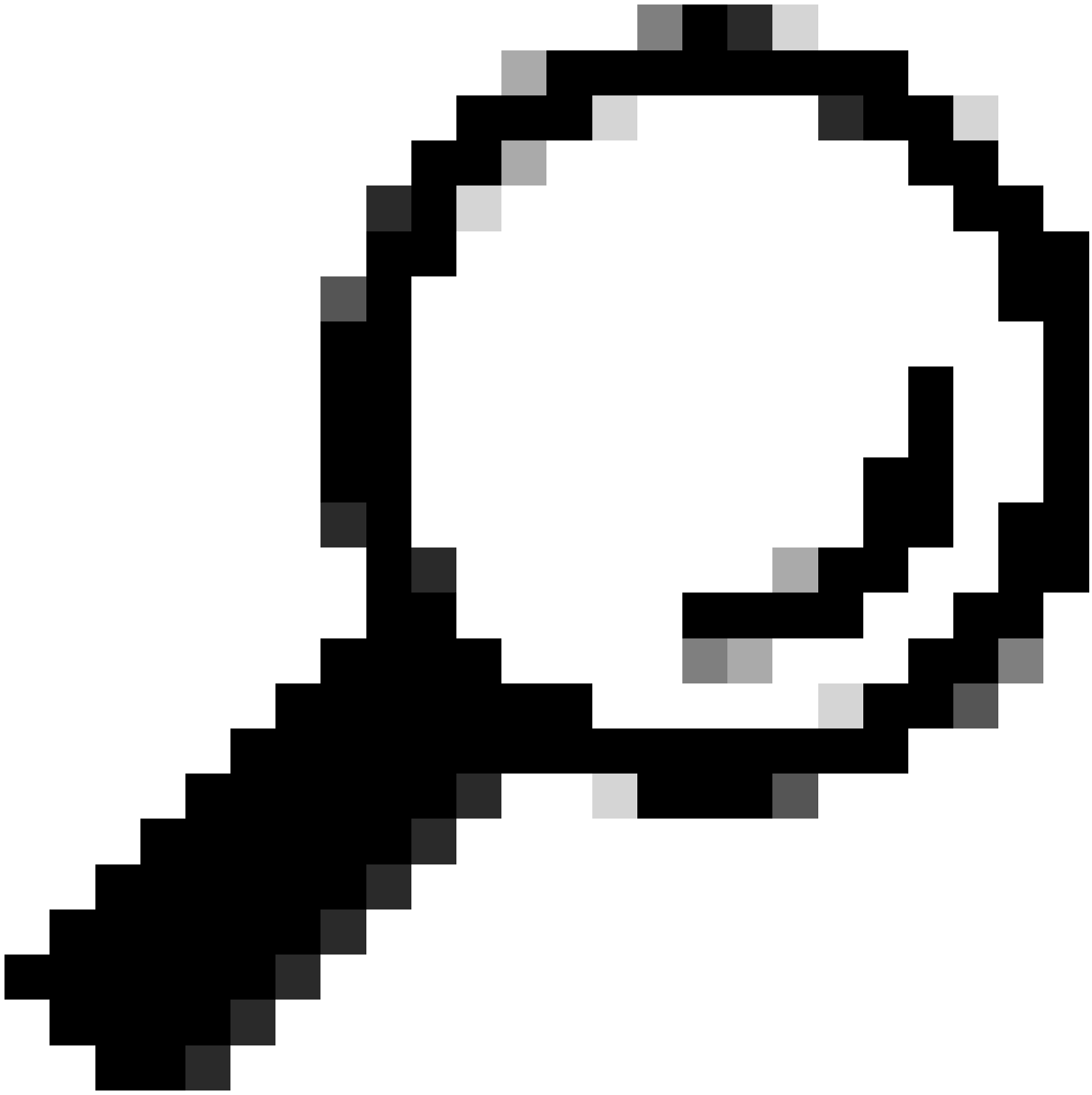
Selecteer Toewijzen om de site te kiezen waarop dit profiel moet worden toegepast en selecteer vervolgens de gewenste site. Nadat u de sites hebt geselecteerd, klikt u op Opslaan.



De SSID maken

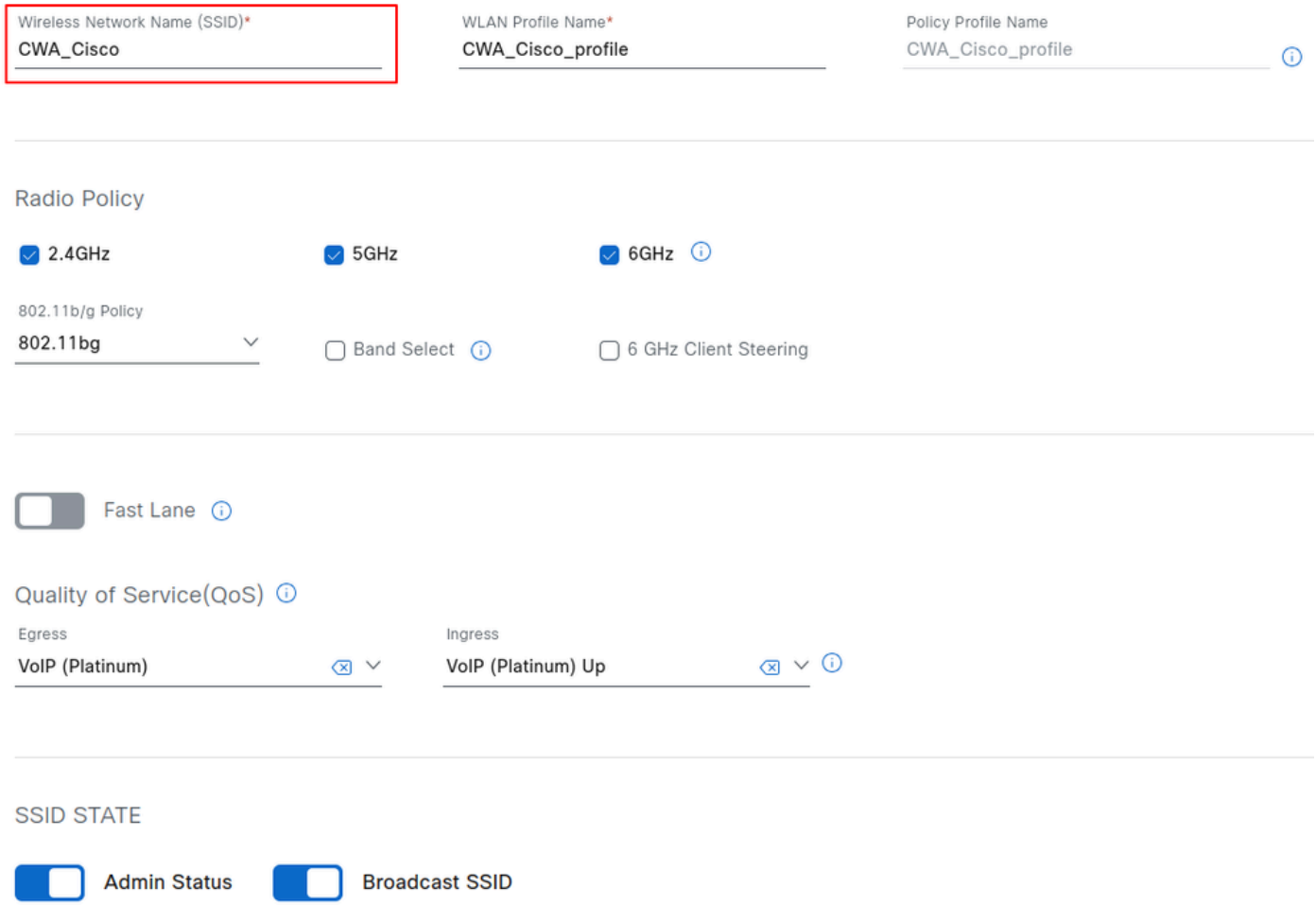
Navigeer naar Ontwerp > Netwerkinstellingen > Draadloos > SSID's en klik op Toevoegen.



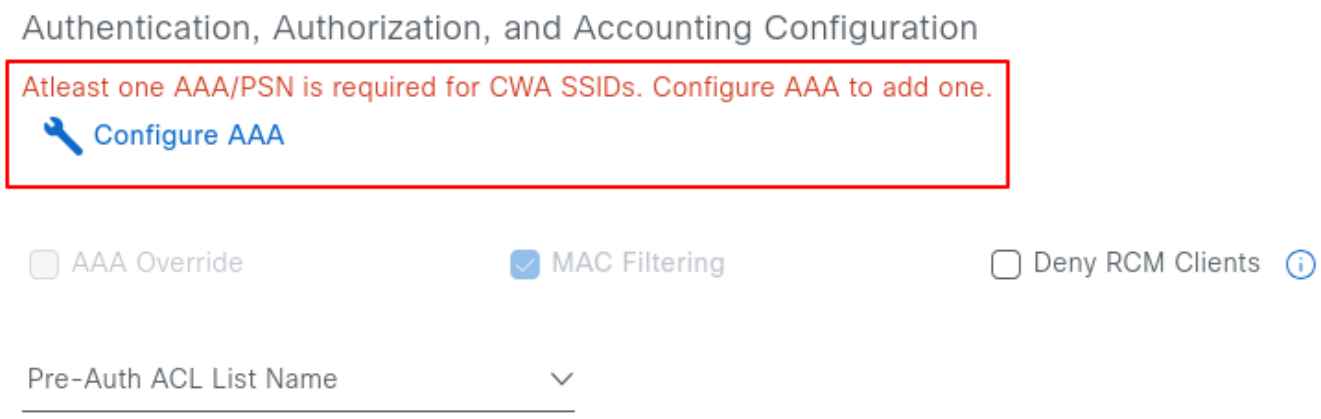


Tip: bij het maken van een SSID voor CWA is het essentieel om het gasttype te selecteren. Deze selectie voegt een opdracht toe aan het draadloze beleidsprofiel van de SSID op de WLC - de opdracht nac - waarmee CoA kan worden gebruikt voor herverificatie nadat de gebruiker zich heeft geregistreerd op het interne portaal. Zonder deze configuratie kunnen gebruikers een eindeloze lus ervaren van registreren en herhaaldelijk worden doorgestuurd naar de portal.

Nadat u Toevoegen hebt geselecteerd, gaat u verder met de SSID-configuratieworkflow. Op de eerste pagina, configureer de SSID-naam, kunt u ook de radiobeleidsband selecteren en de SSID-status definiëren, inclusief beheerdersstatus en broadcast-instellingen. Voor deze configuratiehandleiding wordt de SSID CWA_Cisco genoemd.



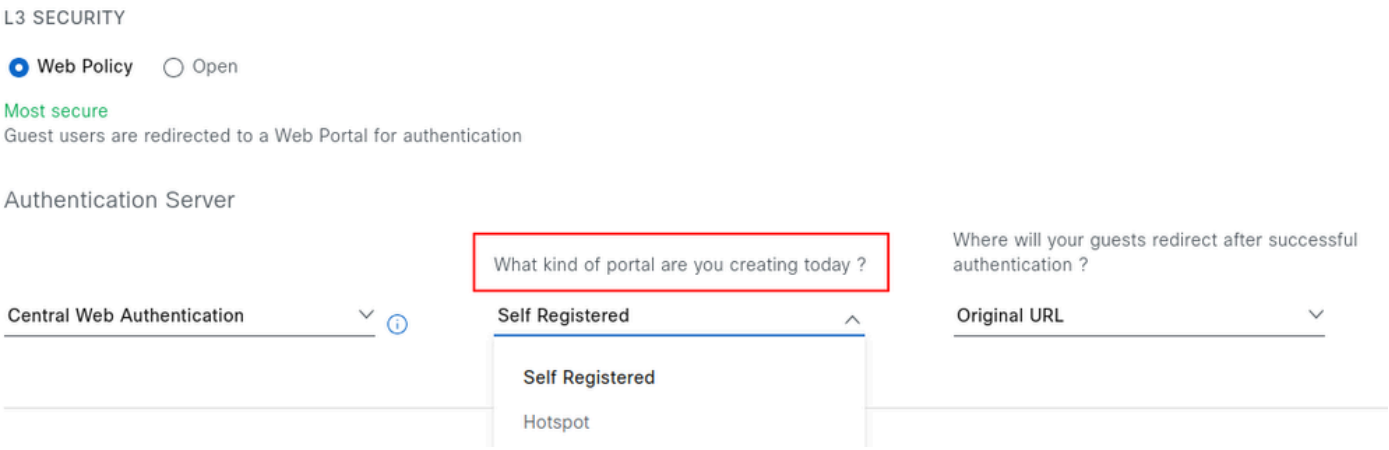
Nadat u de SSID-naam hebt ingevoerd, worden de naam van het WLAN-profiel en de naam van het beleidsprofiel automatisch gegenereerd. Selecteer Volgende om door te gaan.
Ten minste één AAA/PSN moet worden geconfigureerd voor CWA-SSID's. Als er geen is geconfigureerd, selecteert u AAA configureren en kiest u het IP-adres van de PSN in de vervolgkeuzelijst.



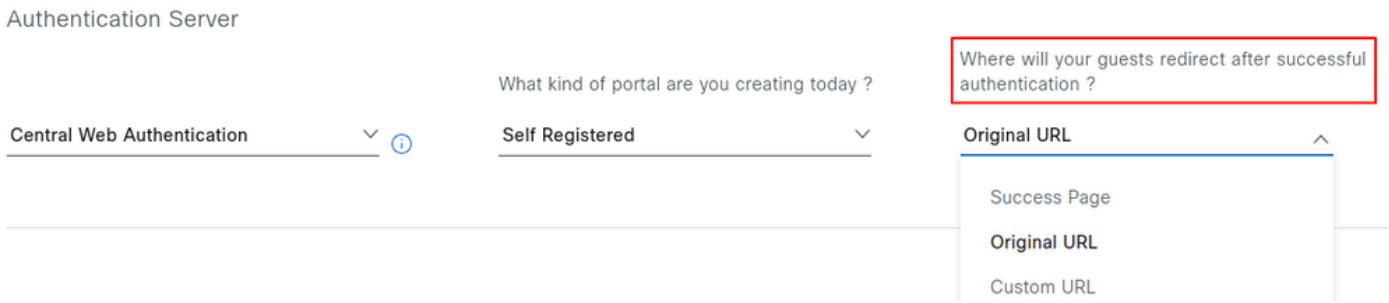
Nadat u de AAA-server hebt geselecteerd, stelt u de beveiligingsparameters voor Layer 3 in en selecteert u het portaaltype: Zelfregistratie of Hotspot.

Hotspot-gastenportalen: een hotspot-gastenportaal biedt gasten toegang tot het netwerk zonder dat ze gebruikersnamen en wachtwoorden nodig hebben. Hier moeten gebruikers een Acceptable

Use Policy (AUP) accepteren om toegang te krijgen tot het netwerk, wat leidt tot latere internettoegang. Gastportalen met referenties: toegang via een geaccrediteerd gastportaal vereist dat gasten een gebruikersnaam en wachtwoord hebben.



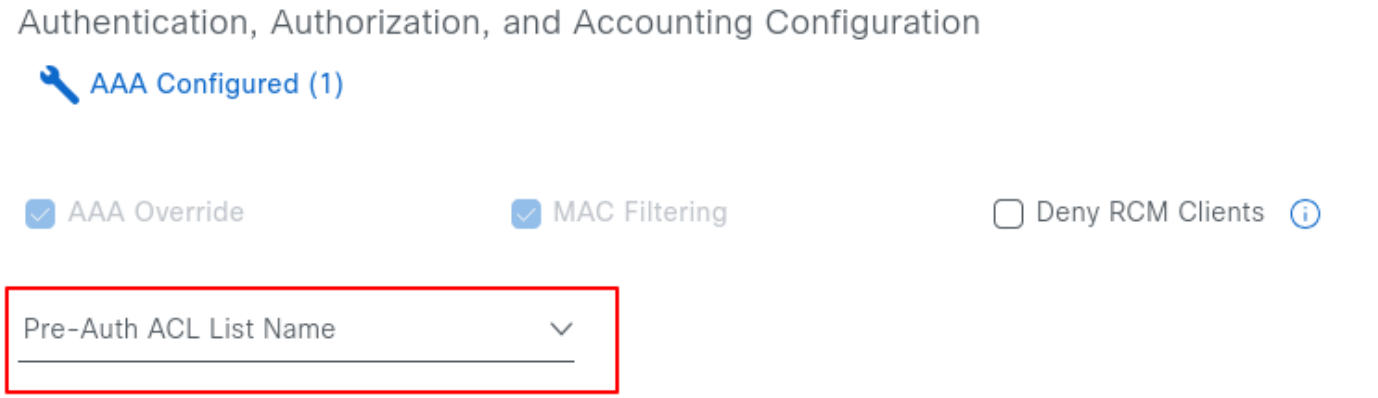
De actie die plaatsvindt nadat de gebruiker zich registreert of het gebruiksbeleid accepteert, kan ook worden geconfigureerd. Er zijn drie opties beschikbaar: Succespagina, Oorspronkelijke URL en Aangepaste URL.



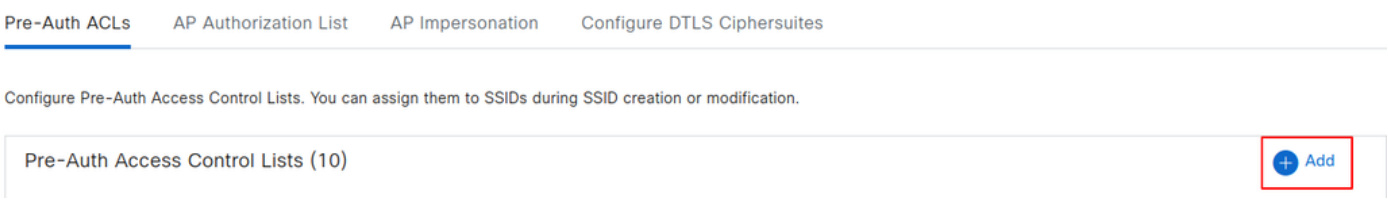
Hieronder wordt het gedrag van elke optie beschreven:

Succespagina: hiermee wordt de gebruiker omgeleid naar een bevestigingspagina die aangeeft dat de verificatie is geslaagd.
Oorspronkelijke URL: verwijst de gebruiker door naar de oorspronkelijke URL die werd aangevraagd voordat deze werd onderschept door de portal.
Aangepaste URL: hiermee wordt de gebruiker omgeleid naar een opgegeven aangepaste URL. Als u deze optie selecteert, wordt in een extra veld de bestemmings-URL gedefinieerd

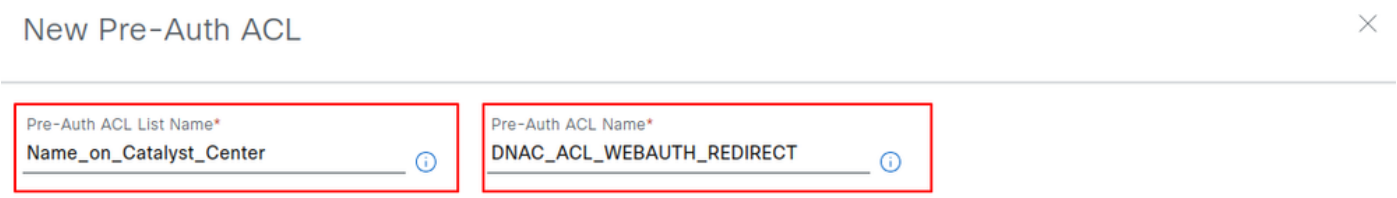
Op dezelfde pagina, onder Authenticatie, Autorisatie en Boekhoudconfiguratie, kan ook een Pre-Authenticatie ACL worden geconfigureerd. Met deze ACL kunnen extra vermeldingen worden toegevoegd voor protocollen die verder gaan dan DHCP-, DNS- of PSN-IP-adressen, die worden verkregen uit de netwerkinstellingen en tijdens de provisioning aan de ACL-omleiding worden toegevoegd. Deze functie is beschikbaar in Cisco Catalyst Center versie 2.3.3.x en hoger.



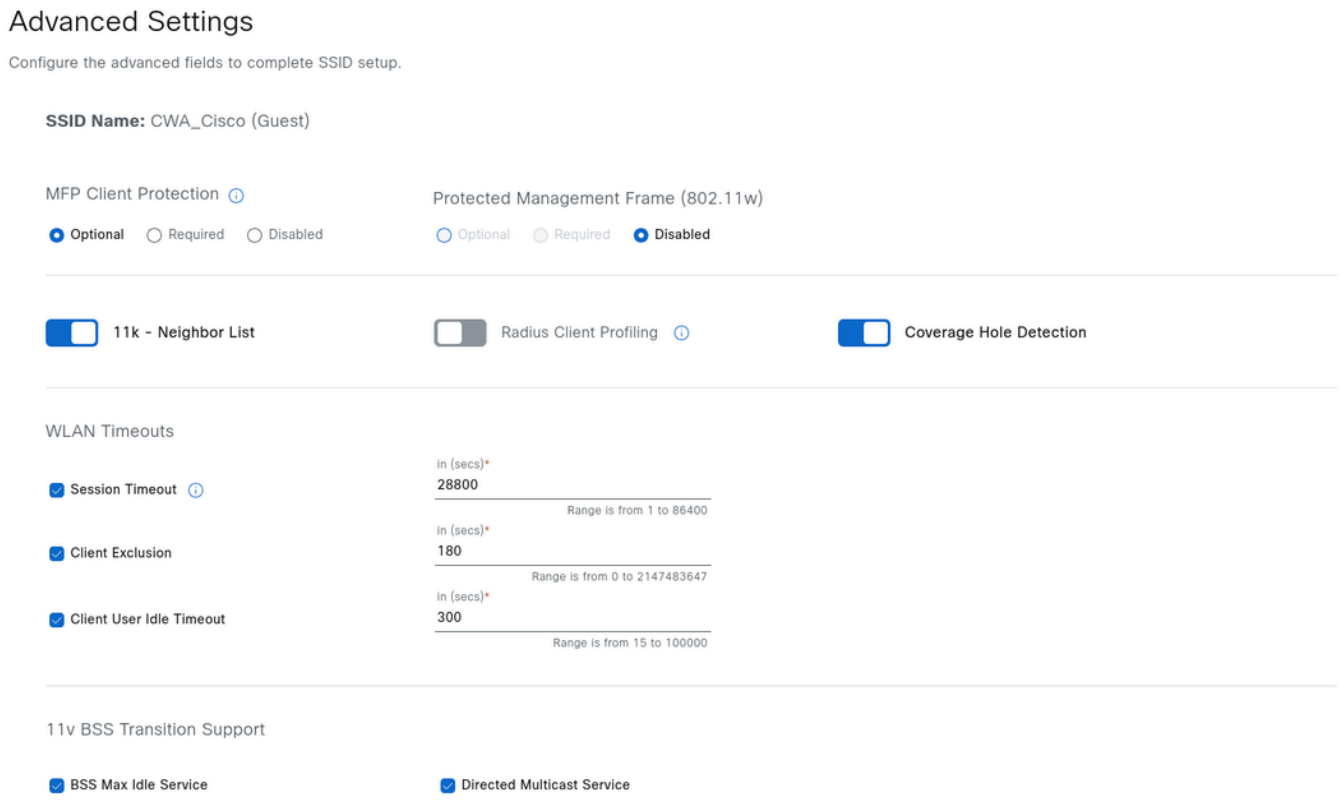
Om een Pre-Auth ACL te configureren, gaat u naar Ontwerp > Netwerkinstellingen > Draadloos > Beveiligingsinstellingen en klikt u op Toevoegen.



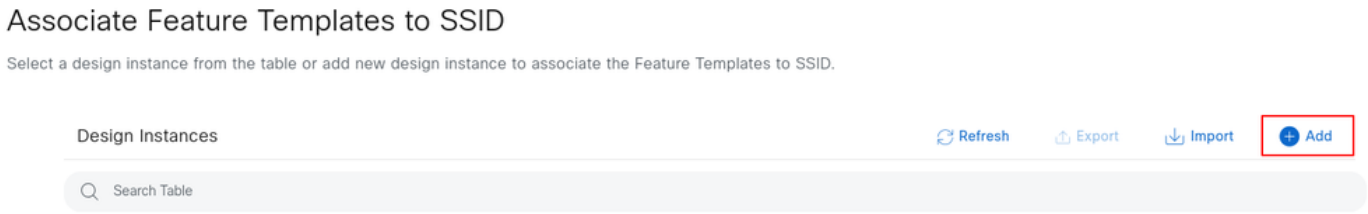
De voornaam identificeert de ACL in Catalyst Center, terwijl de tweede naam overeenkomt met de ACL-naam op de WLC. De tweede naam kan overeenkomen met de bestaande omleiding ACL geconfigureerd op de WLC. Als referentie, Catalyst Center levert de naam Cisco DNA_ACL_WEBAUTH_REDIRECT aan de WLC. Inzendingen van de Pre-Auth ACL worden toegevoegd na de bestaande items.



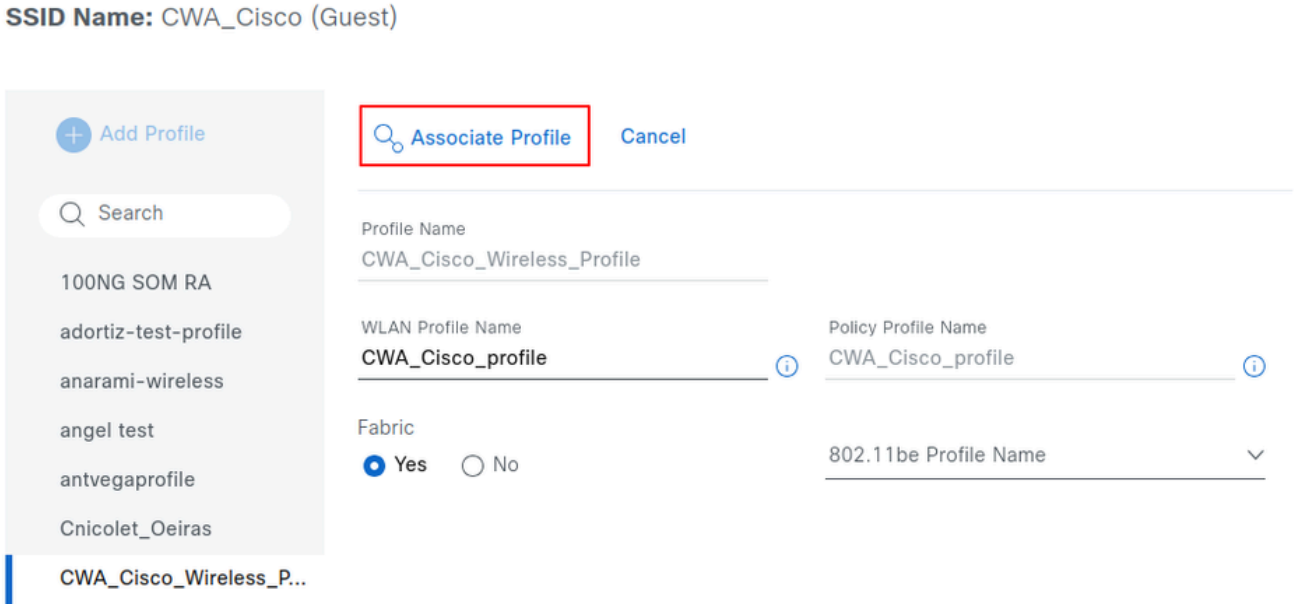
Wanneer u terugkeert naar de werkstroom voor het maken van de SSID, geeft het selecteren van Volgende de geavanceerde instellingen weer, waaronder snelle overgang, time-out van sessies, time-out van clientgebruikers en snelheidsbeperking. Pas de parameters aan zoals vereist en selecteer vervolgens Volgende om door te gaan. In het kader van deze configuratiehandleiding worden in het voorbeeld de standaardinstellingen behouden.



Nadat u Volgende hebt geselecteerd, wordt een prompt weergegeven om functiesjablonen aan de SSID te koppelen. Selecteer de gewenste sjablonen door op Toevoegen te klikken en klik als u klaar bent op Volgende.

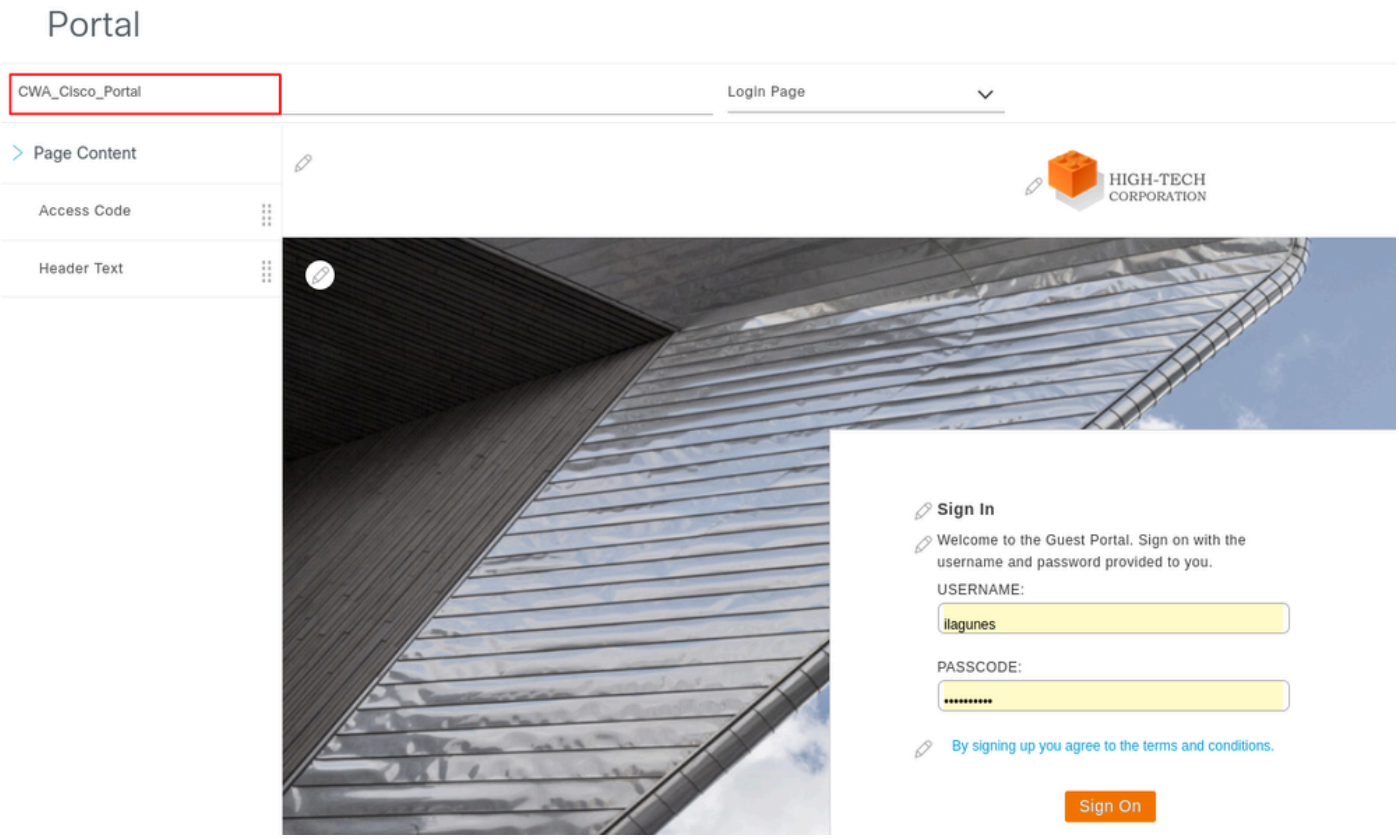


Koppel de SSID aan het eerder gemaakte draadloze profiel. Zie het gedeelte Profiel voor draadloos netwerk maken voor meer informatie. In deze sectie kunt u ook selecteren of de SSID-structuur is ingeschakeld of niet. Als u klaar bent, klikt u op Profiel koppelen.

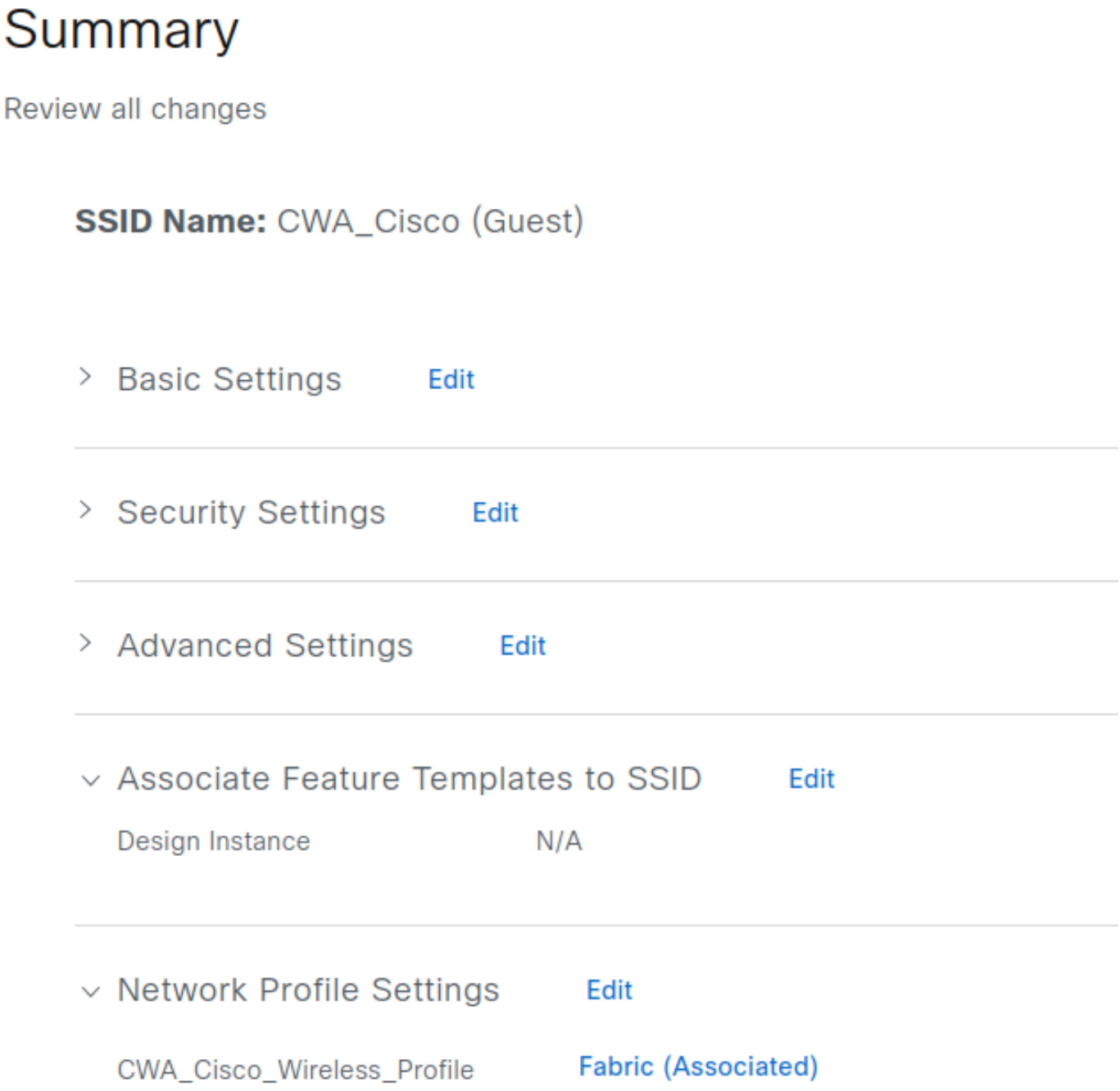


Wireless Management TrustPoint weergeven
Zodra het profiel aan de SSID is gekoppeld, klikt u op Volgende om het interne portaal te maken en te ontwerpen. Klik vervolgens op Portaal maken.

De portaalnaam definieert de domeinnaam in de FQDN en de naam van de beleidsset op ISE. Klik op Opslaan als u klaar bent. Het portaal blijft bewerkbaar en kan indien nodig worden verwijderd.



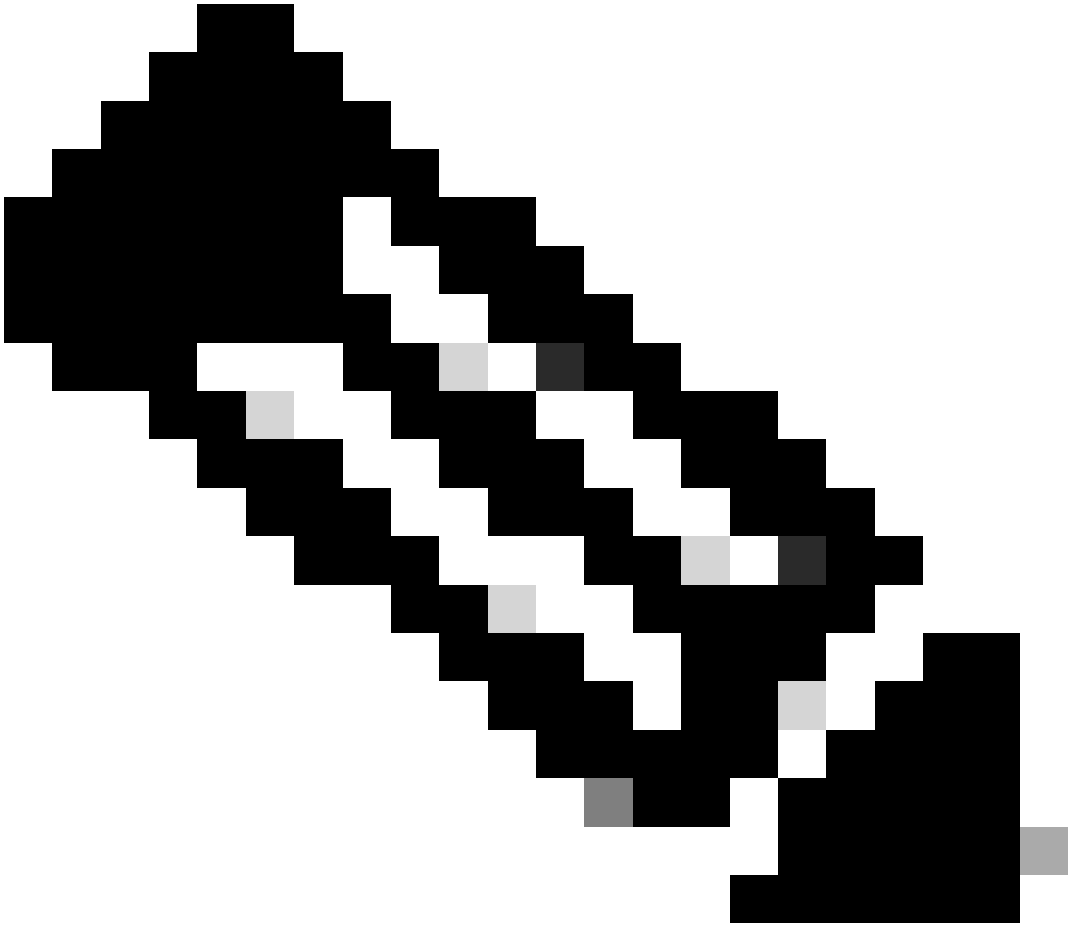
Selecteer Volgende om een overzicht weer te geven van alle configuratieparameters die in de vorige stappen zijn gedefinieerd.



Bevestig de configuratiedetails en selecteer vervolgens Opslaan om de wijzigingen toe te passen.

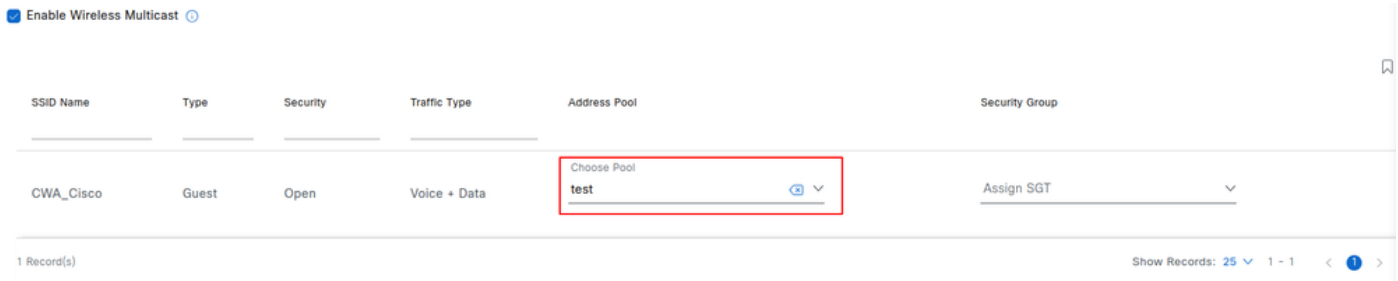
Fabric Provisioning

Nadat het profiel van het draadloze netwerk is gekoppeld aan de verbindingssite, wordt de SSID weergegeven onder Voorzieningen > Verbindingssites > (Uw site) > Draadloze SSID's.

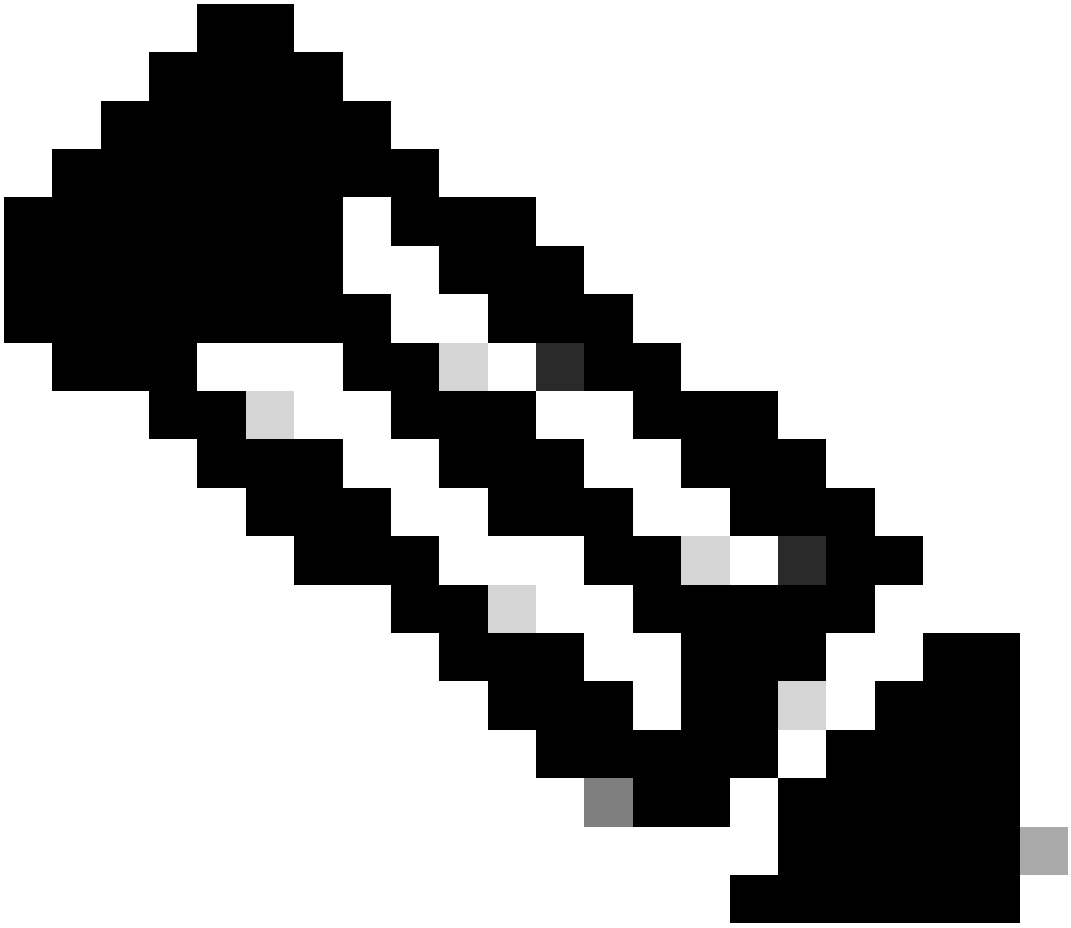


Opmerking: u moet de draadloze netwerkcontroller voor de site beschikbaar maken zodat de SSID's onder de draadloze SSID's kunnen worden weergegeven

Kies de SSID-pool, koppel optioneel een beveiligingsgroeptag en klik op Implementeren. De SSID wordt alleen door toegangspunten uitgezonden als er een pool is toegewezen.



Op AirOS- en Catalyst 9800-controllers moet u de draadloze LAN-controller opnieuw inrichten nadat de SSID-configuratie is gewijzigd in Netwerkinstellingen.



Opmerking: als er geen pool is toegewezen aan de SSID, wordt verwacht dat de toegangspunten deze niet uitzenden. De SSID wordt alleen uitgezonden nadat een pool is toegewezen. Zodra de pool is toegewezen, hoeft de controller niet opnieuw te worden ingericht.

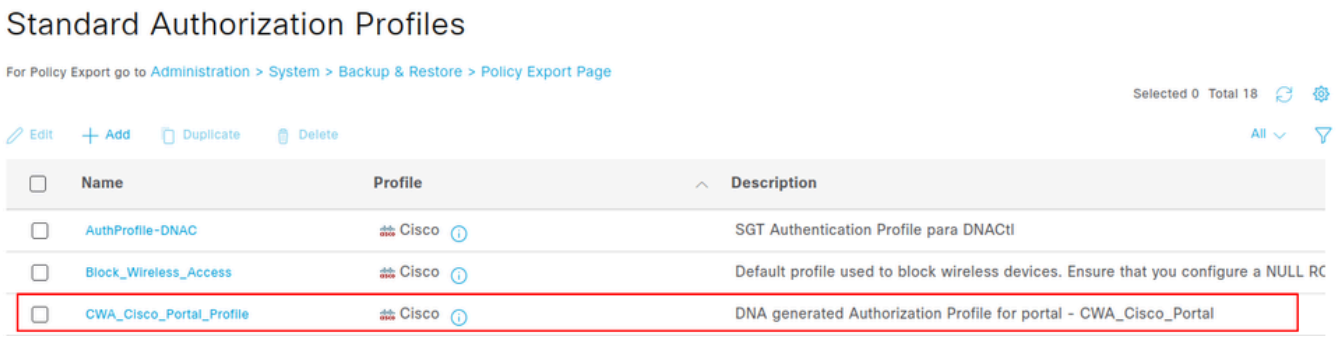
Controleer de configuratie die aan Cisco ISE is geleverd

In dit gedeelte wordt de configuratie onderzocht die door Catalyst Center aan Cisco ISE is geleverd.

Autorisatieprofiel

Onderdeel van de configuratie die Catalyst Center voor Cisco ISE biedt, is een machtigingsprofiel. Dit profiel definieert het resultaat dat aan een client is toegewezen op basis van de parameters en kan specifieke instellingen bevatten, zoals VLAN-toewijzing, ACL's of URL-omleidingen.
Als u het machtigingsprofiel in ISE wilt bekijken, gaat u naar Beleid > Beleidselementen > Resultaten. Als de portalnaam CWA_Cisco_Portal is, is de profielnaam

CWA_Cisco_Portal_Profile. In het veld Beschrijving wordt de tekst weergegeven: Door DNA gegenereerd autorisatieprofiel voor portal - CWA_Cisco_Portal.



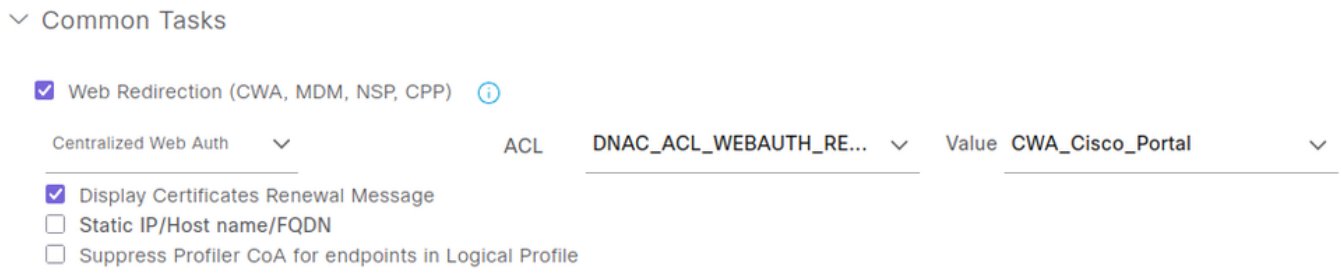
Als u de kenmerken wilt bekijken die met dit machtigingsprofiel naar de draadloze netwerkcontroller zijn verzonden, klikt u op de naam van het machtigingsprofiel en gaat u naar de sectie Algemene taken.
Dit autorisatieprofiel levert de Redirect ACL en de Redirect URL.

Het attribuut Web Redirection bevat twee parameters:

1. ACL-naam: ingesteld op Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Waarde: Verwijst naar de naam van de captive portal, in dit voorbeeld CWA_Cisco_Portal.

Met de optie Bericht voor verlenging van certificaten weergeven kan het portaal worden gebruikt voor het vernieuwen van certificaten die het eindpunt momenteel gebruikt.

Een extra optie, Statische IP/hostnaam/FQDN, is beschikbaar onder Bericht voor vernieuwing van weergavecertificaten. Deze functie maakt het mogelijk om het IP-adres van het portaal te leveren in plaats van het FQDN, wat handig is wanneer het portaal in gevangenschap niet kan worden geladen vanwege het onvermogen om de DNS-server te bereiken.

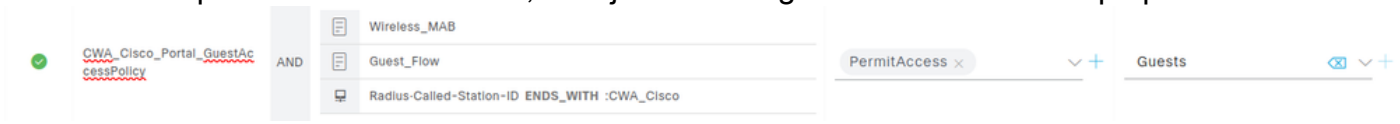


Beleidssets

Navigeer naar Beleid > Beleidsreeksen > Standaard > Autorisatiebeleid om de twee beleidsreeksen te bekijken die zijn gemaakt voor het portaal met de naam CWA_Cisco_Portal. Deze beleidssets zijn:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

Het CWA_Cisco_Portal_GuestAccessPolicy wordt toegepast wanneer de client het webverificatieproces al heeft voltooid, hetzij door zelfregistratie of via het hotspotportaal.

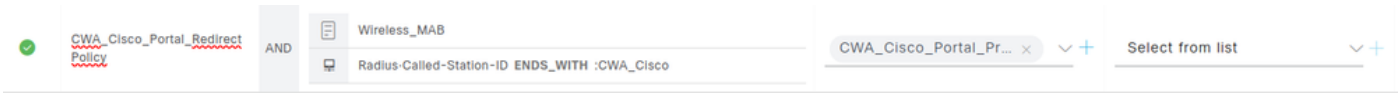


Deze beleidsset voldoet aan drie criteria:

- Wireless_MAB: Wordt gebruikt wanneer Cisco ISE een verificatieaanvraag voor MAC Authentication Bypass (MAB) ontvangt van een draadloze LAN-controller.
- Guest_Flow: verwijst naar ISE die het MAC-adres van het eindpunt controleert in vergelijking met de identiteitsgroep GuestEndpoints. Als het MAC-adres van het eindpunt niet aanwezig is in deze groep, wordt het beleid niet toegepast.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: De Called-Station-ID is een RADIUS-kenmerk in ISE dat het bridge of Access Point MAC-adres opslaat in ASCII-indeling en de SSID toevoegt die wordt geopend, gescheiden door een puntkomma (:). In dit voorbeeld vertegenwoordigt CWA_Cisco de SSID-naam.

Onder de kolomprofielen ziet u de naam PermitAccess, dit is een gereserveerd autorisatieprofiel dat niet kan worden bewerkt, dat volledige toegang geeft tot het netwerk en u kunt ook een SGT toewijzen onder de kolom Beveiligingsgroepen, in dit geval Gasten.

Het profiel PermitAccess wordt gebruikt. Dit is een gereserveerd autorisatieprofiel dat niet kan worden bewerkt en dat volledige toegang tot het netwerk biedt. Een SGT kan ook worden toegewezen onder de kolom Beveiligingsgroepen; in dit geval is de SGT ingesteld op Gasten. Het volgende beleid dat moet worden beoordeeld, is CWA_Cisco_Portal_RedirectPolicy.



Deze beleidsset voldoet aan de volgende twee criteria:

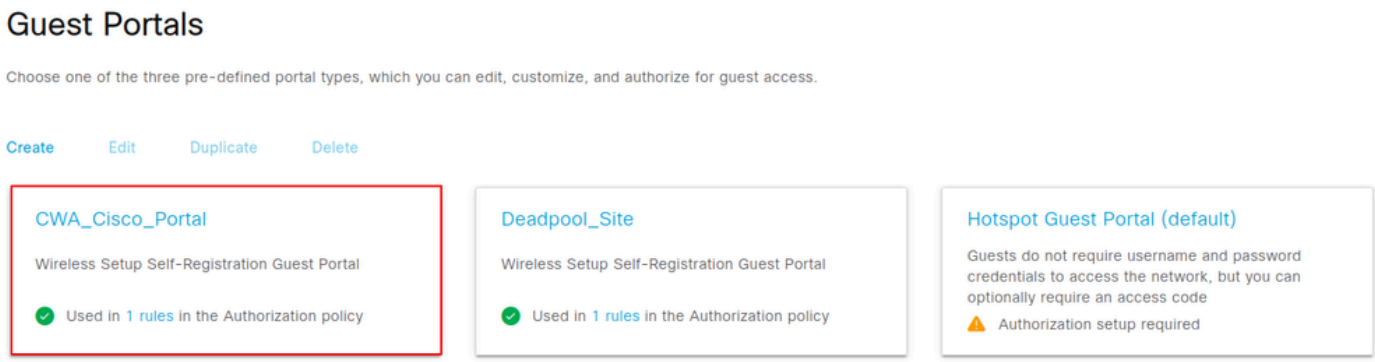
- Wireless_MAB: Wordt gebruikt wanneer Cisco ISE een MAB-verificatieverzoek ontvangt van een draadloze LAN-controller.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: De Called-Station-ID is een RADIUS-kenmerk in ISE dat het bridge of Access Point MAC-adres opslaat in ASCII-indeling en de SSID toevoegt die wordt geopend, gescheiden door een puntkomma (:). In dit voorbeeld vertegenwoordigt :CWA_Cisco de SSID-naam.

De volgorde van dit beleid is cruciaal. Als CWA_Cisco_Portal_RedirectPolicy als eerste in de lijst wordt weergegeven, komt dit alleen overeen met MAB-verificatie en de SSID-naam met behulp van het RADIUS-kenmerk Called-Station-ID ENDS_WITH :CWA_Training. In deze configuratie zal het eindpunt, zelfs als het al is geverifieerd via het portaal, voor onbepaalde tijd aan dit beleid

blijven voldoen. Als gevolg hiervan wordt nooit volledige toegang verleend via het PermitAccess-profiel en blijft de client vastzitten in een continue lus van authenticatie en omleiding naar het portaal.

Configuratie van gastportal

Navigeer naar Werkcentra > Gasttoegang > Portalen en onderdelen om het portaal te bekijken. Het gastenportaal dat hier is gemaakt, gebruikt dezelfde naam als in Catalyst Center CWA_Cisco_Portal. Selecteer de naam van het portaal als u meer details wilt bekijken.

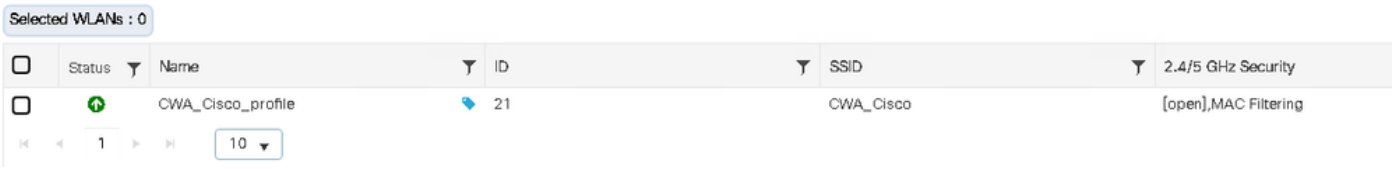


Controleer de configuratie die aan de WLC is geleverd

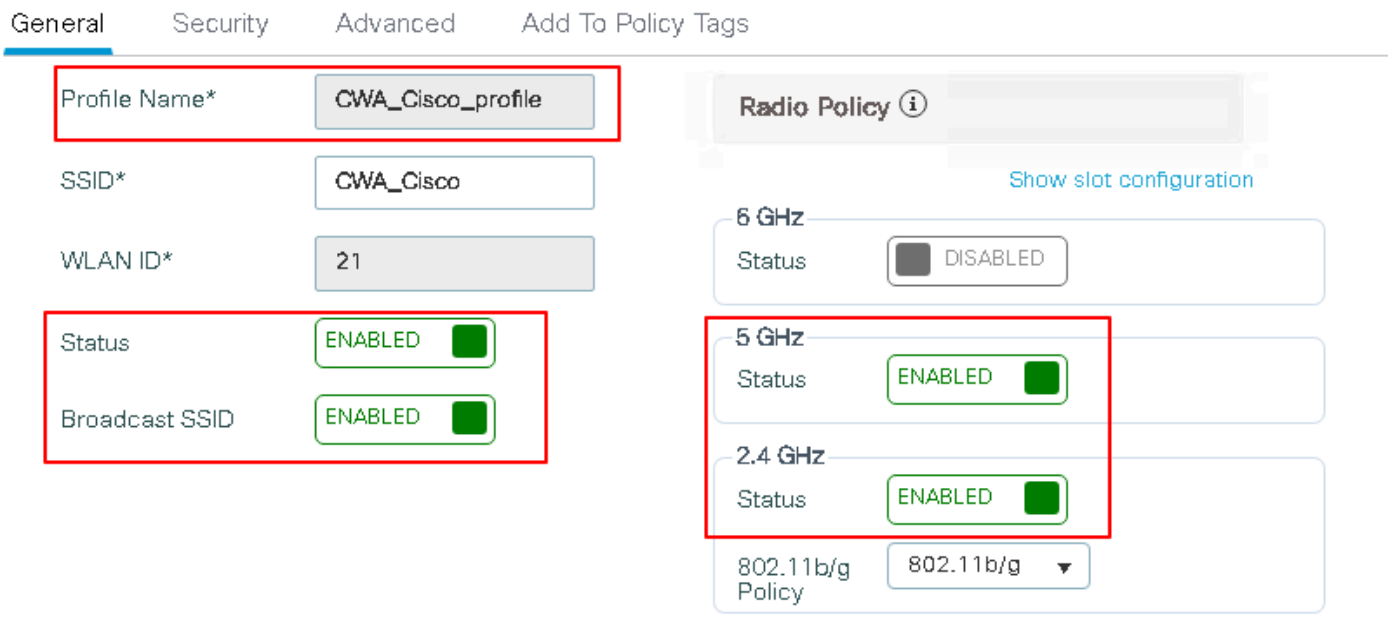
In dit gedeelte wordt de configuratie onderzocht die door Catalyst Center wordt geleverd aan de draadloze LAN-controller.

SSID-configuratie

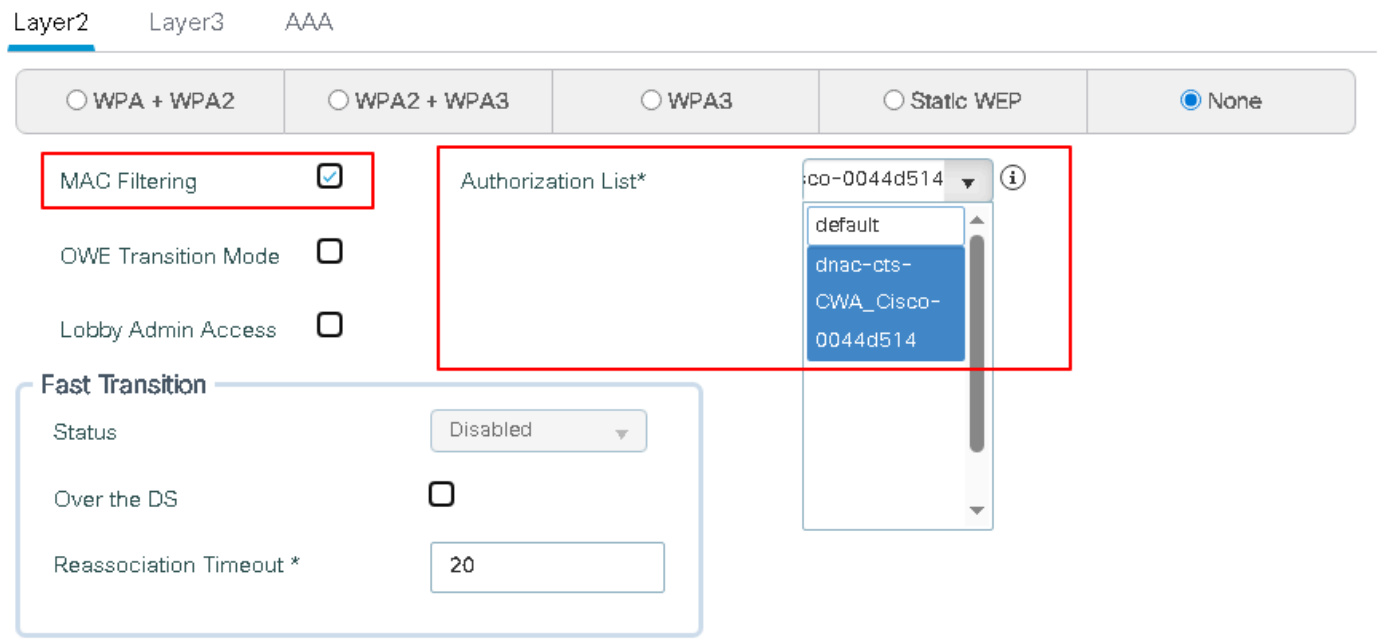
Navigeer in de WLC GUI naar Configuratie > Tags en profielen > WLAN's om de SSID-configuratie te bekijken.



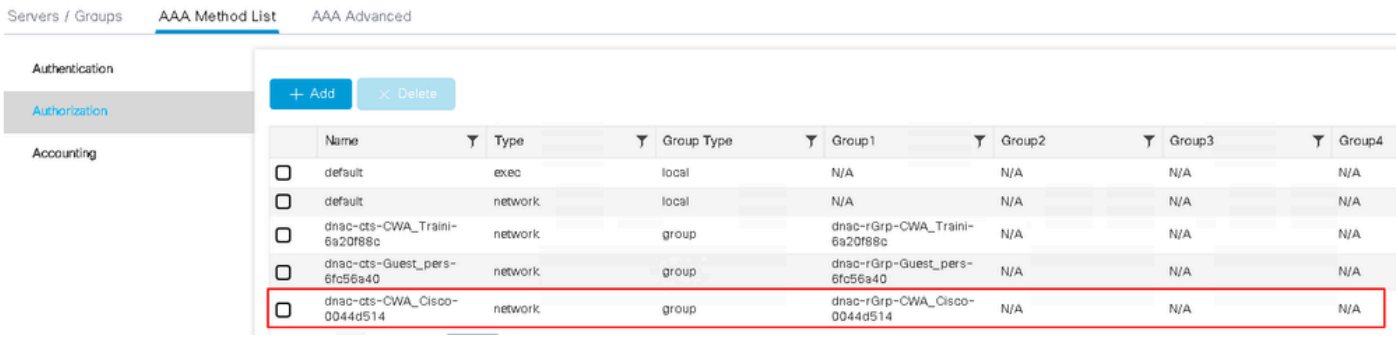
De SSID CWA_Cisco heeft de naam CWA_Cisco_profile op de WLC, met ID 21 en een Open beveiligingstype met MAC-filtering. Dubbelklik op de SSID om de configuratie te bekijken.



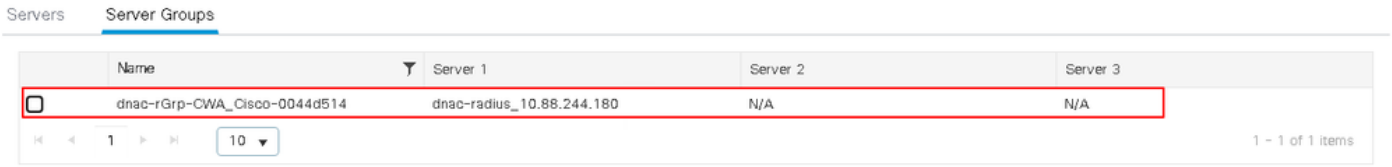
De SSID is UP en zendt uit op zowel 5 GHz- als 2,4 GHz-kanalen en is gekoppeld aan het beleidsprofiel CWA_CIsco_Profile. Klik op het tabblad Beveiliging om de instellingen te bekijken.



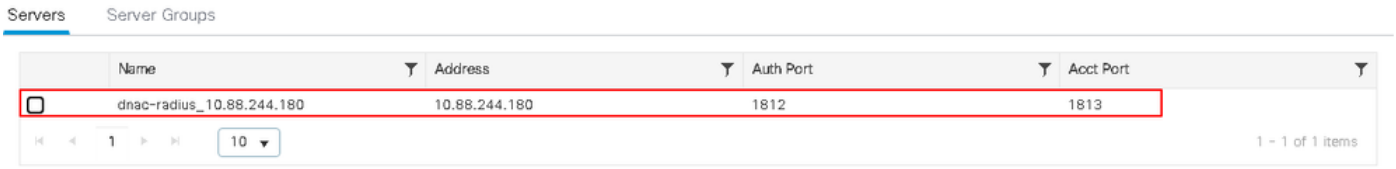
Belangrijke instellingen zijn de Layer 2-beveiligingsmethode (MAC-filtering) en de AAA-autorisatielijst (Cisco DNA-cts-CWA_Cisco-0044d514). Om de configuratie te bekijken, gaat u naar Configuratie > Beveiliging > AAA > Methodenlijst AAA > Autorisatie.



De methodenlijst verwijst naar de RADIUS-groep Cisco DNA-rGrp-CWA_Cisco-0044d514in de kolom Groep1. Als u de configuratie wilt bekijken, gaat u naar Configuratie > Beveiliging > AAA > Server/Groepen > Servergroepen.



De servergroep Cisco DNA-rGrp-CWA_Cisco-0044d514 wijst in de kolom Server 1 naar Cisco DNA-radius_10.88.244.180. Bekijk de configuratie op het tabblad Servers.



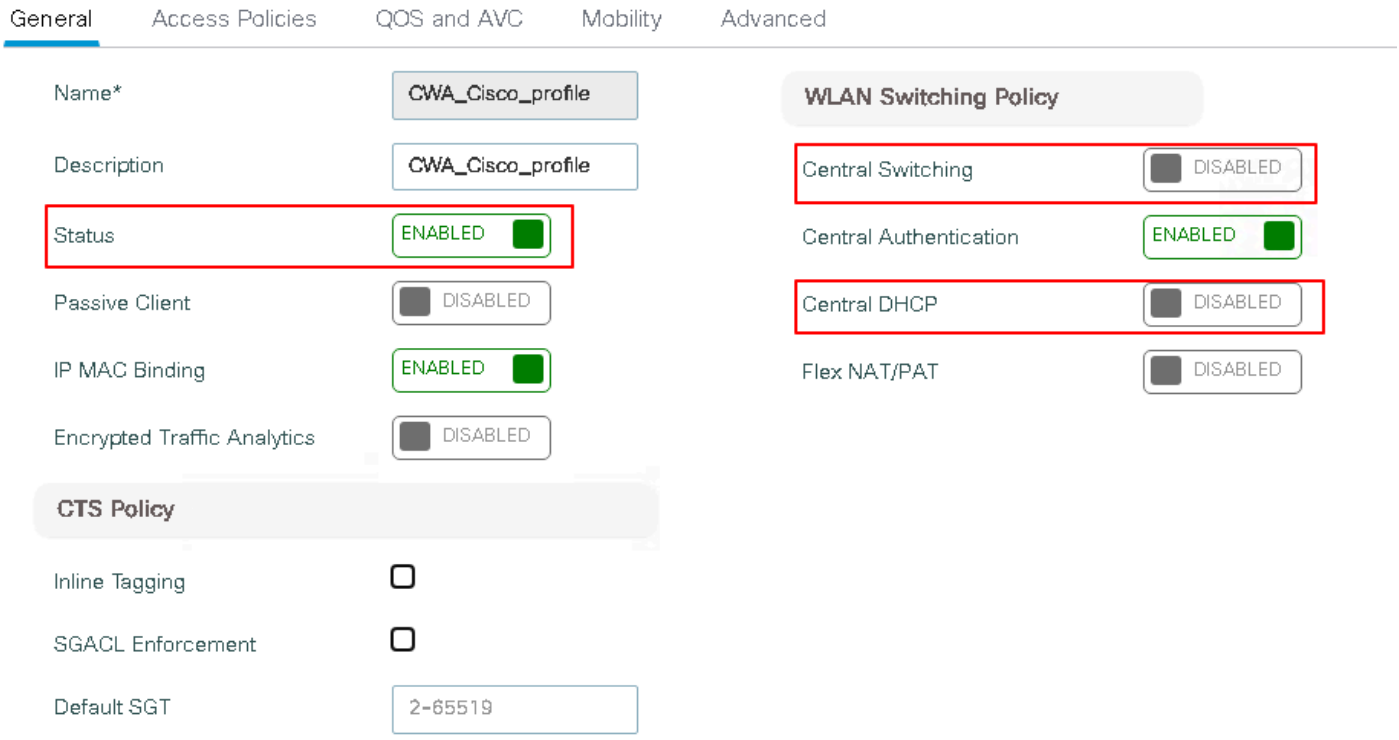
De server Cisco DNA-radius_10.88.244.180 heeft het IP-adres 10.88.244.180, Klik op de naam om de configuratie te bekijken

Een kritieke configuratie is Change of Authorization (CoA), dat een mechanisme biedt om de kenmerken van een verificatie-, autorisatie- en boekhoudsessie (AAA) te wijzigen nadat deze is geverifieerd op het interne portaal. Zonder deze functie blijft het eindpunt in een web-auth-status, zelfs na het voltooien van de registratie op het portaal.

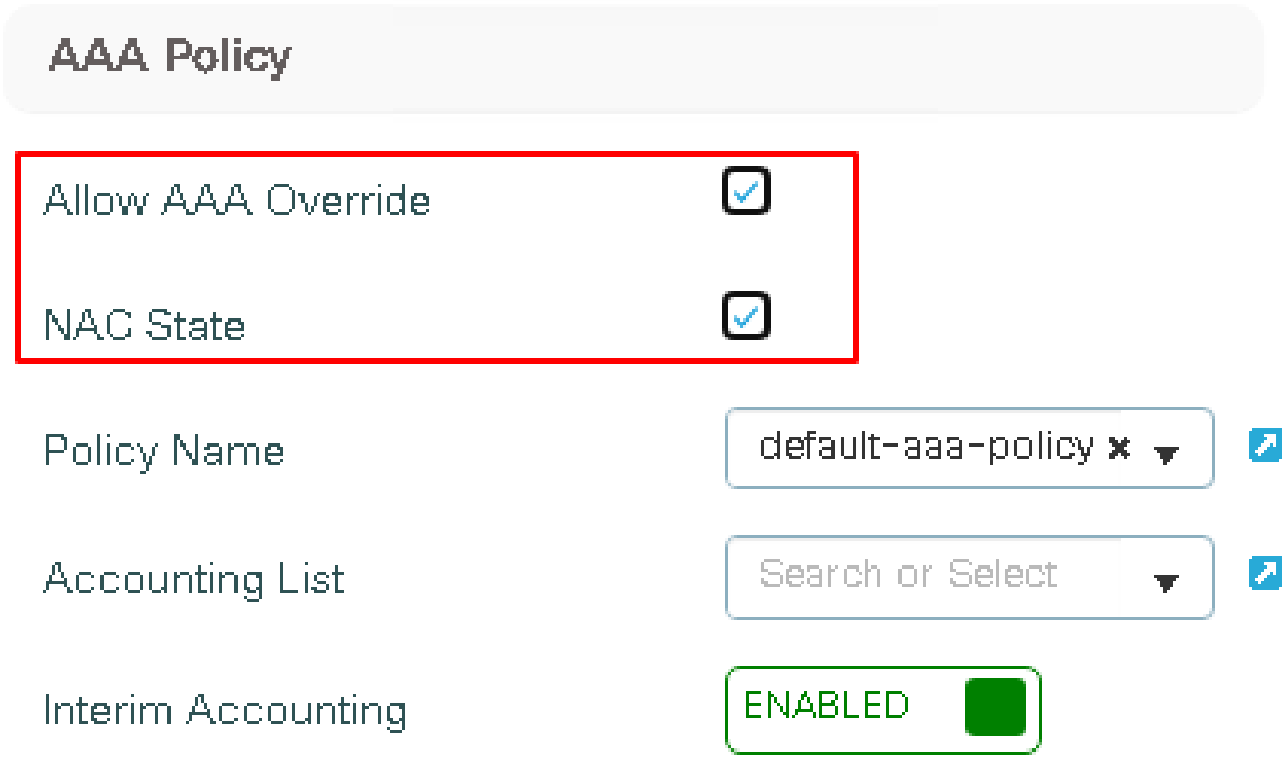
Configuratie van draadloos beleidsprofiel

In het beleidsprofiel kunnen aan clients instellingen worden toegewezen zoals VLAN, ACL's, QoS, Mobiliteitsanker en timers. Als u de configuratie voor het beleidsprofiel wilt bekijken, gaat u naar Configuratie > Codes en profielen > Beleid.

Klik op de naam van het beleid om de configuratie te bekijken.



De status van het beleid is ingeschakeld en zoals bij elke SSID van de verbinding zijn centrale switching en centrale DHCP uitgeschakeld. Klik op het tabblad Geavanceerd en navigeer vervolgens naar het gedeelte AAA-beleid om aanvullende configuratiedetails te bekijken.



Zowel AAA Override als Network Access Control (NAC) kunnen worden ingeschakeld. Met AAA Override kan de controller attributen accepteren die door de RADIUS-server worden geretourneerd, zoals ACL's of URL's, en deze attributen toepassen op clients. NAC maakt een wijziging van de autorisatie (CoA) mogelijk nadat de klant zich heeft geregistreerd op het portaal. Deze configuratie kan ook worden bekeken via de CLI op de WLC.
Als u het beleidsprofiel wilt verifiëren, wordt de SSID gekoppeld om de opdracht uit te voeren:

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
CWA_Cisco_profile
  CWA_Cisco  UP
```

Voer de volgende opdracht uit om de configuratie voor het beleidsprofiel CWA_Cisco_profile te bekijken:

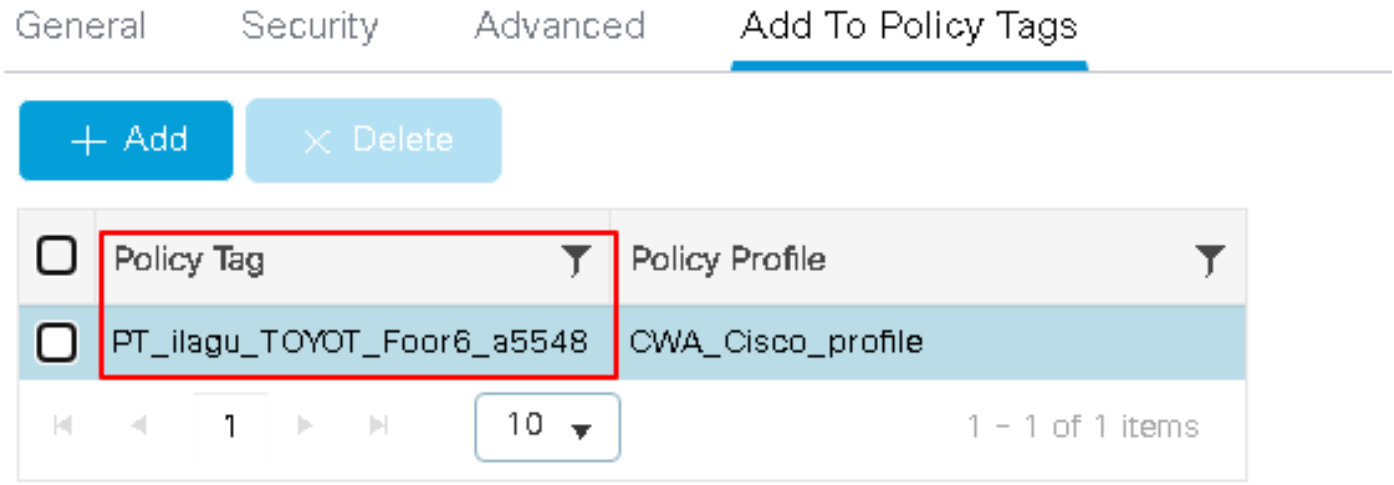
<#root>

```
WLC#show running-config | section policy CWA_Cisco_profile


wireless profile policy CWA_Cisco_profile
```

```
aaa-override


no central dhcp


no central switching


description CWA_Cisco_profile
dhcp-tlv-caching
exclusionlist timeout 180
fabric CWA_Cisco_profile
http-tlv-caching
nac


service-policy input platinum-up
service-policy output platinum
no shutdown
```

Beleidstag-configuratie

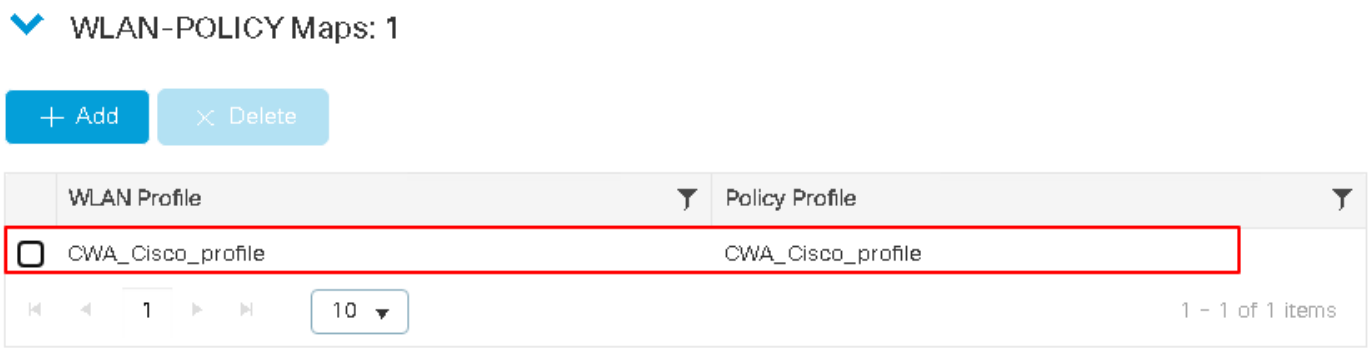
De tag policy is de manier waarop u het WLAN koppelt aan het beleidsprofiel, navigeert naar Configuratie > Codes en profielen > WLAN's, klikt u op de WLAN-naam en navigeert u naar Toevoegen aan beleidscodes om de tag policy te identificeren die aan de SSID is toegewezen.



Voor het SSID CWA_Cisco_profile wordt de beleidstag PT_ilagu_TOYOT_Foor6_a5548 gebruikt om de configuratie te verifiëren en te navigeren naar Configuratie > Tags & profielen > Tags > Beleid.

Klik op de naam om de details te bekijken. De beleidstag PT_ilagu_TOYOT_Foor6_a5548 koppelt de WLAN CWA_Cisco die is gekoppeld aan de naam CWA_Cisco_profile op de WLC (zie de

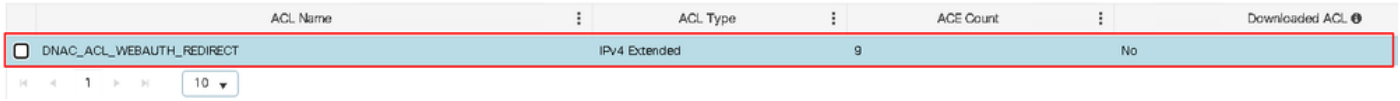
WLANs-pagina voor meer informatie) aan het beleidsprofiel CWA_Cisco_profile.



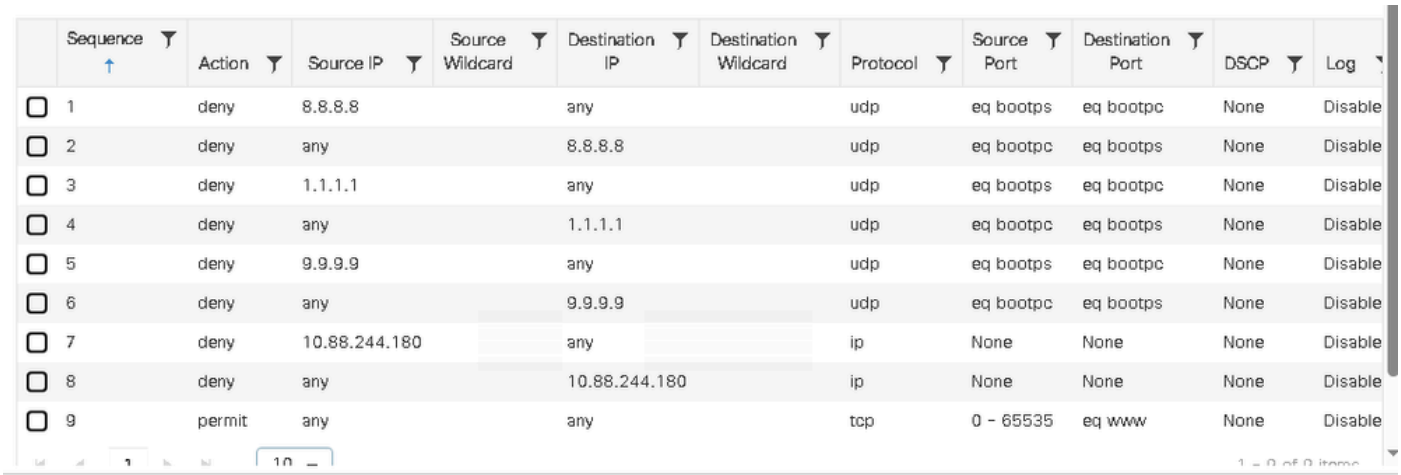
De WLAN-naam CWA_Cisco_profile verwijst naar de WLAN CWA_Cisco.

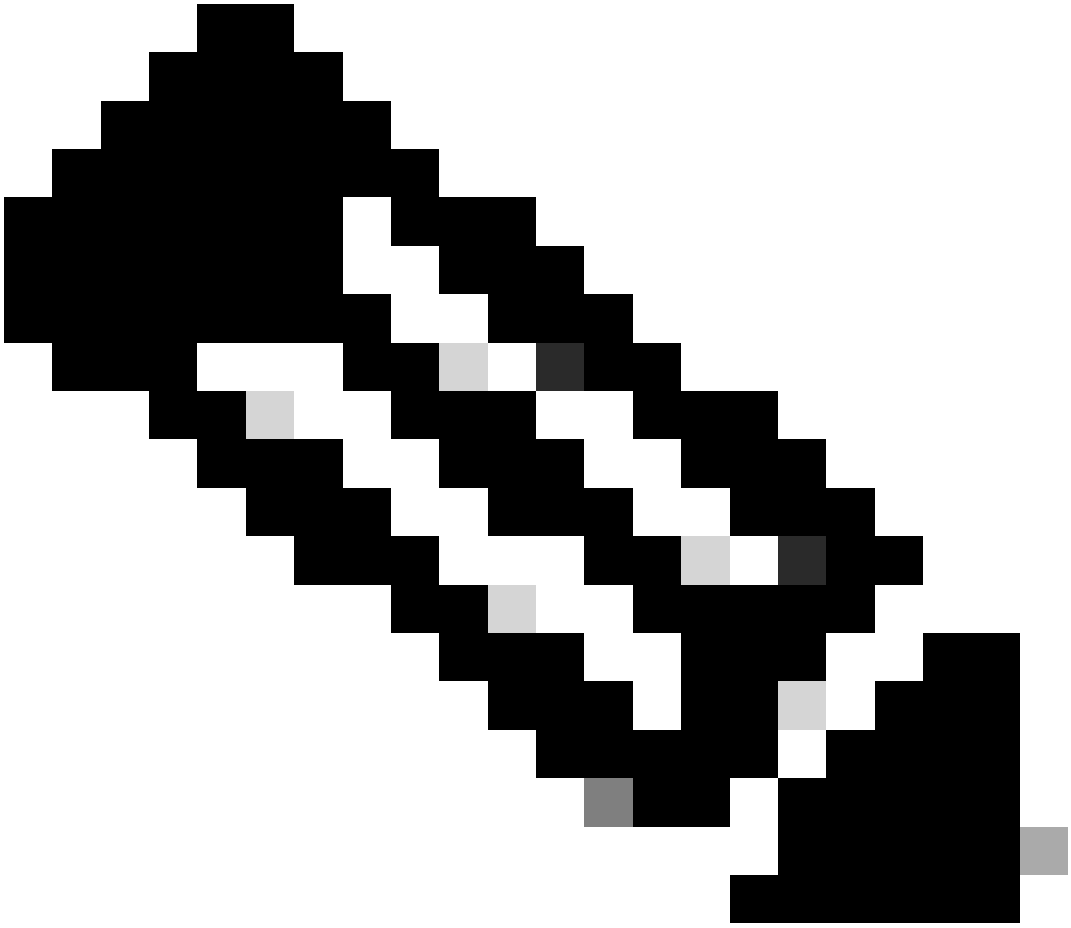
ACL-configuratie omleiden

In CWA definieert een Redirect Access Control List welk verkeer wordt omgeleid naar de WLC voor verdere verwerking en welk verkeer omzeilt omleiding
Deze configuratie wordt naar de WLC gepusht nadat de SSID is gemaakt en de WLC vanuit Inventory is geleverd. Om het te bekijken, navigeert u naar Configuratie > Beveiliging >ACL, De naam van de ACL die Catalyst Center gebruikt voor de omleiding ACL is Cisco DNA_ACL_WEBAUTH_REDIRECT.



Klik op de naam om de configuratie te bekijken. De waarden zijn afgeleid van de netwerkinstellingen van de site in Catalyst Center.





Opmerking: deze waarden worden verkregen uit de netwerkinstellingen van de site die zijn geconfigureerd in Catalyst Center en de DHCP/DNS-waarden worden afkomstig uit de pool die is geconfigureerd in het WLAN. Het IP-adres van het ISE-PSN wordt vermeld in de AAA-configuratie in de SSID-workflow.

Voer deze opdracht uit om de ACL-omleiding op de WLC CLI te bekijken:

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

De omleiding ACL kan worden toegepast op het Flex-profiel, zodat het kan worden verzonden naar de toegangspunten. Voer deze opdracht uit om deze configuratie te bevestigen

<#root>

```
WLC#show running-config | section flex


wireless profile flex default-flex-profile

 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT



central-webauth



urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

ACL omleiden op het toegangspunt

Op het toegangspunt worden de machtigings- en weigeringswaarden omgedraaid: vergunning geeft doorstuurverkeer aan en weigering geeft omleiding aan. Voer de volgende opdracht uit om de configuratie voor het omleiden van de ACL op het toegangspunt te bekijken:

<#root>

```
AP#sh ip access-lists


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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.