CWA met FlexConnect AP's op een WLC met ISE configureren

Inhoud

Inleiding

Dit document beschrijft hoe u centrale webverificatie kunt configureren met FlexConnect AP's op een WLC ISE in lokale switchingmodus.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

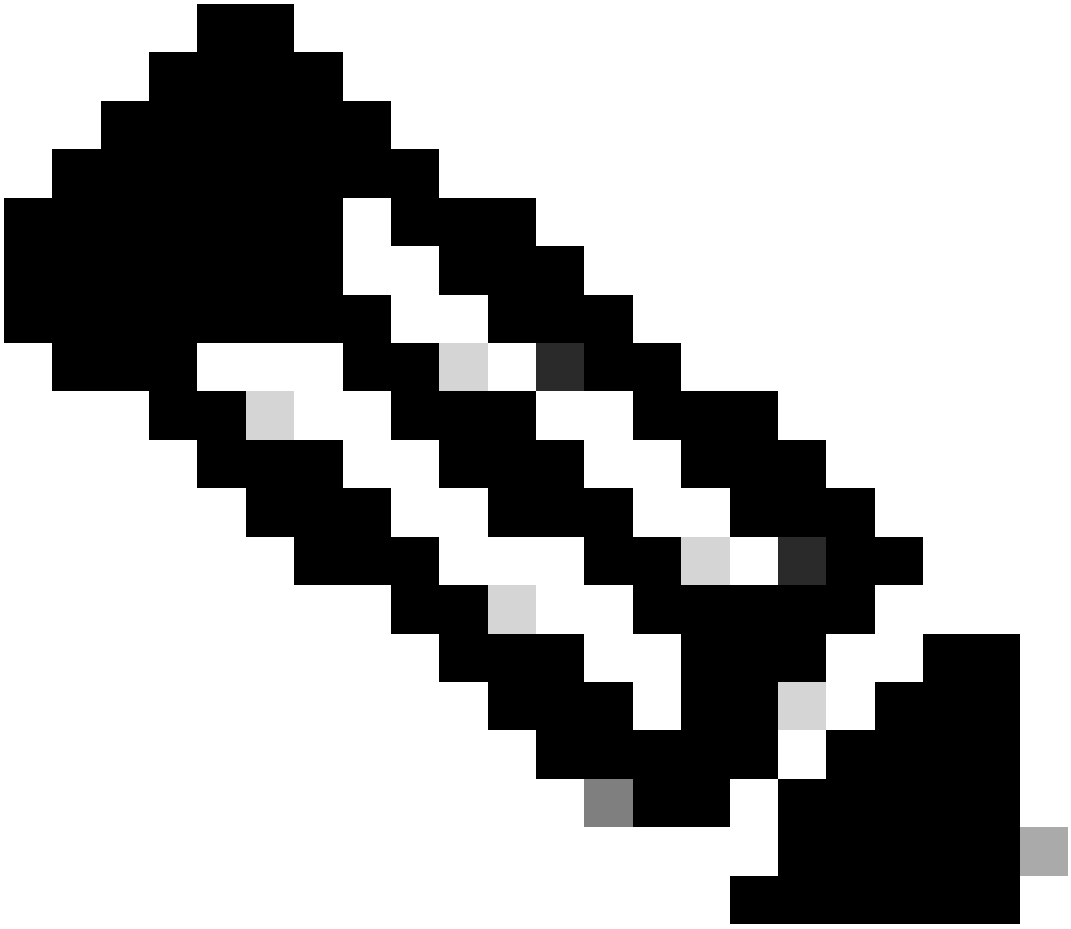
Gebruikte componenten

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

- Cisco Identity Services Engine (ISE), release 1.2.1
- Software voor draadloze LAN-controllers (WLC), release versie - 7.4.10.0
- Access points (AP)

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



> Opmerking: op dit moment wordt lokale verificatie op de FlexAP's niet ondersteund voor dit scenario.

Andere documenten in deze serie

- Configuratievoorbeeld van Central Web Verification met een Switch en Identity Services Engine
- Configuratievoorbeeld van centrale webverificatie op WLC en ISE

Configureren

Er zijn meerdere methoden om centrale webverificatie te configureren op de draadloze LAN-controller (WLC). De eerste methode is lokale webverificatie waarbij de WLC het HTTP-verkeer omleidt naar een interne of externe server waar de gebruiker wordt gevraagd om te verifiëren. De WLC haalt dan de referenties (teruggestuurd via een HTTP GET request in het geval van een externe server) en maakt een RADIUS-verificatie. In het geval van een gastgebruiker, is een externe server (zoals Identity Service Engine (ISE) of NAC Guest Server (NGS)) vereist, aangezien het portaal functies biedt zoals apparaatregistratie en zelfbevoorrading. Dit proces omvat de volgende stappen:

1. De gebruiker associeert met de web verificatie SSID.
2. De gebruiker opent zijn browser.
3. De WLC wordt omgeleid naar het guest portal (zoals ISE of NGS) zodra een URL is ingevoerd.
4. De gebruiker verifieert op het portaal.
5. Het gastportaal keert terug naar de WLC met de ingevoerde referenties.
6. De WLC authenticeert de gastgebruiker via RADIUS.
7. WLC keert terug naar de originele URL.

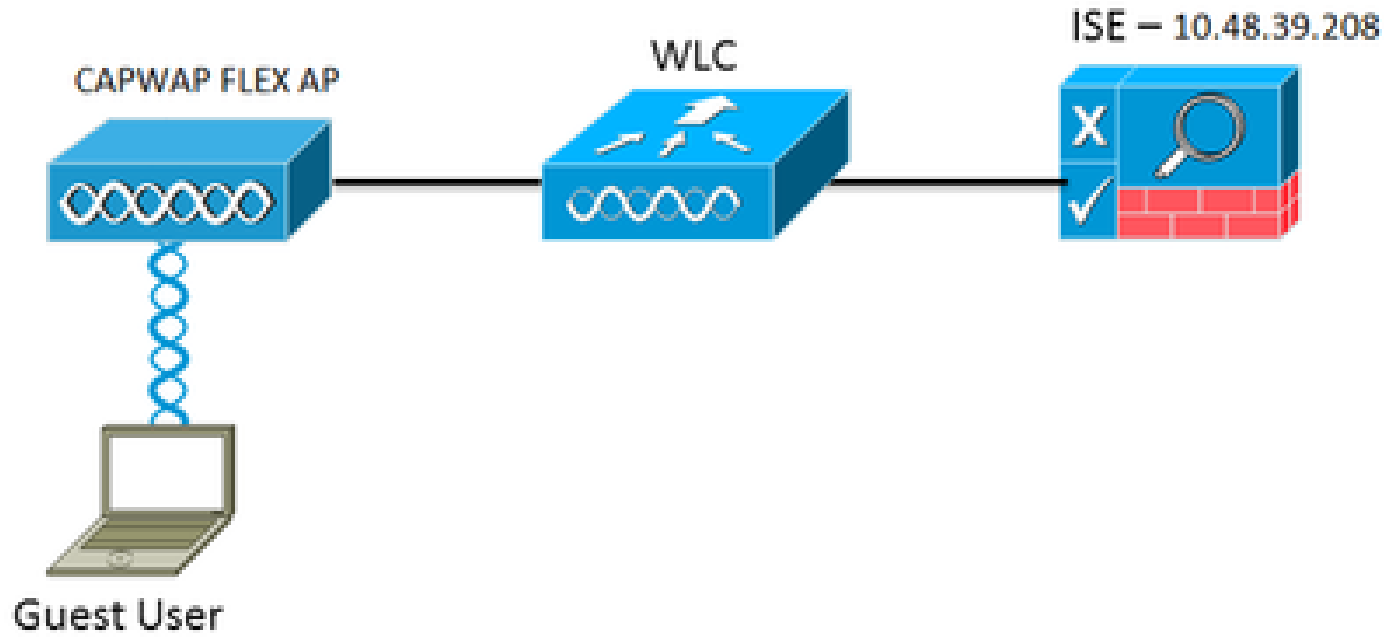
Dit proces omvat veel omleiding. De nieuwe benadering is om centrale webverificatie te gebruiken die werkt met ISE (versies later dan 1.1) en WLC (versies later dan 7.2). Dit proces omvat de volgende stappen:

1. De gebruiker associeert met de web verificatie SSID.
2. De gebruiker opent zijn browser.
3. De WLC wordt omgeleid naar de guest portal.
4. De gebruiker verifieert op het portaal.
5. De ISE verstuurt een RADIUS-wijziging van autorisatie (CoA - UDP-poort 1700) om de controller erop te wijzen dat de gebruiker geldig is en drukt uiteindelijk op RADIUS-kenmerken zoals de toegangscontrolelijst (ACL).
6. De gebruiker wordt gevraagd de oorspronkelijke URL opnieuw te proberen.

In deze sectie worden de stappen beschreven die nodig zijn om centrale webverificatie op WLC en ISE te configureren.

Netwerkdiagram

Deze configuratie gebruikt de volgende netwerkinstellingen:



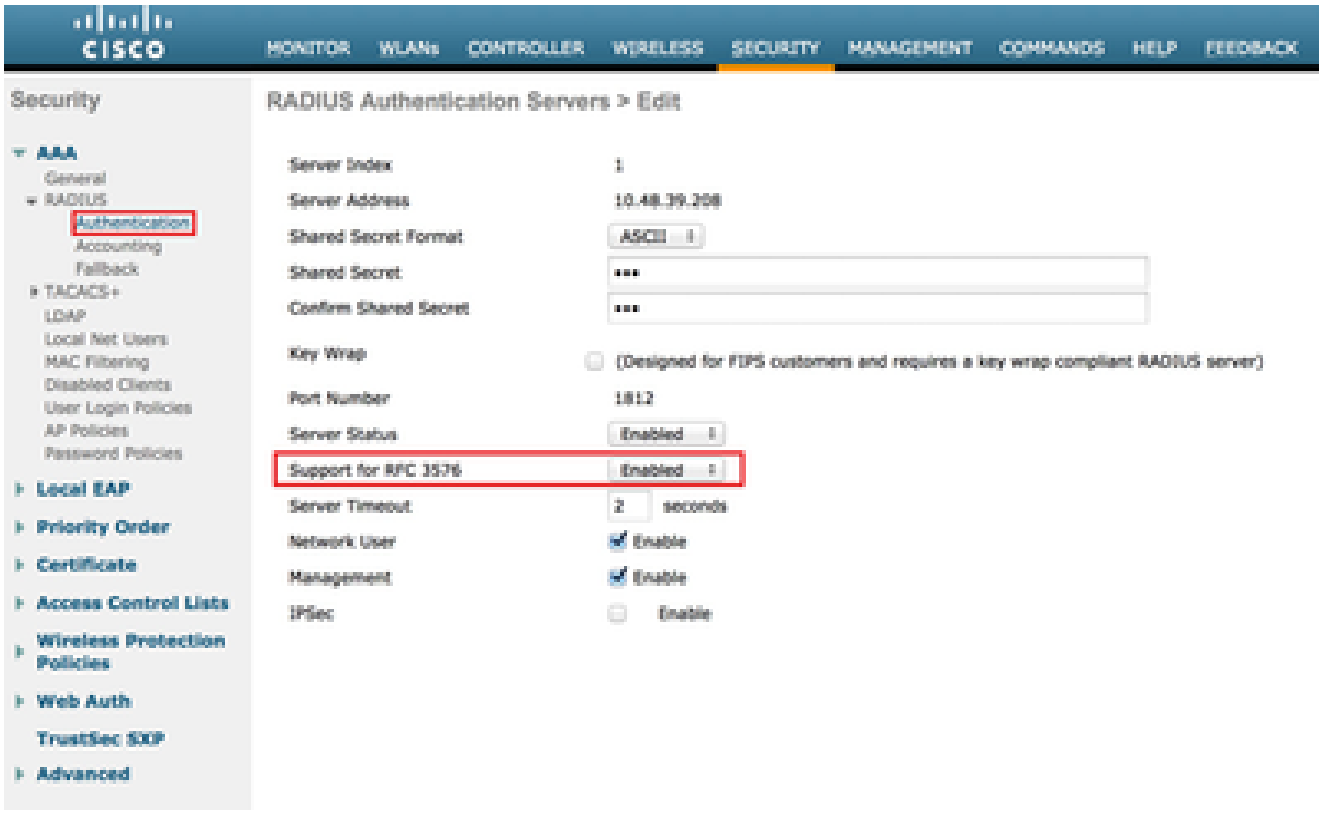
Netwerkinstelling

WLC-configuratie

De WLC-configuratie is vrij eenvoudig. Er wordt een trucje gebruikt (hetzelfde als bij switches) om de URL voor de dynamische verificatie van de ISE te verkrijgen (omdat er CoA wordt gebruikt, moet er een sessie worden aangemaakt omdat de sessie-id deel uitmaakt van de URL). De SSID is ingesteld om MAC-filtering te gebruiken en de ISE is ingesteld om een Access-Accept-bericht terug te sturen, zelfs als het MAC-adres niet wordt gevonden, zodat de omleiding URL voor alle gebruikers wordt verzonden.

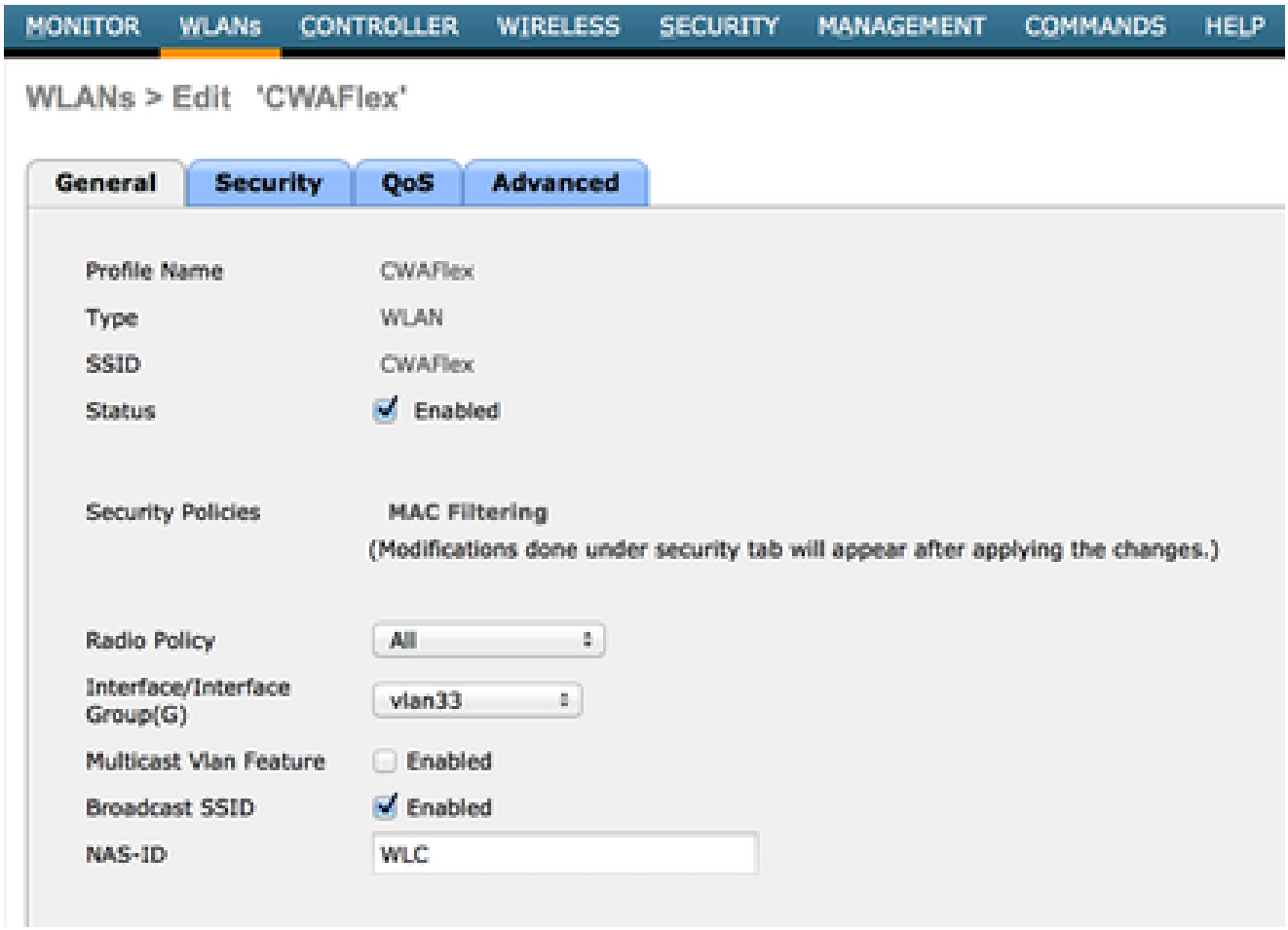
Daarnaast moeten RADIUS-netwerktoegangscontrole (NAC) en AAA-overschrijding zijn ingeschakeld. Met RADIUS NAC kan de ISE een CoA-verzoek verzenden dat aangeeft dat de gebruiker nu is geverifieerd en toegang heeft tot het netwerk. Het wordt ook gebruikt voor de beoordeling van de houding waarin de ISE het gebruikersprofiel wijzigt op basis van het resultaat van de houding.

1. Zorg ervoor dat op de RADIUS-server RFC3576 (CoA) is ingeschakeld, wat de standaardinstelling is.



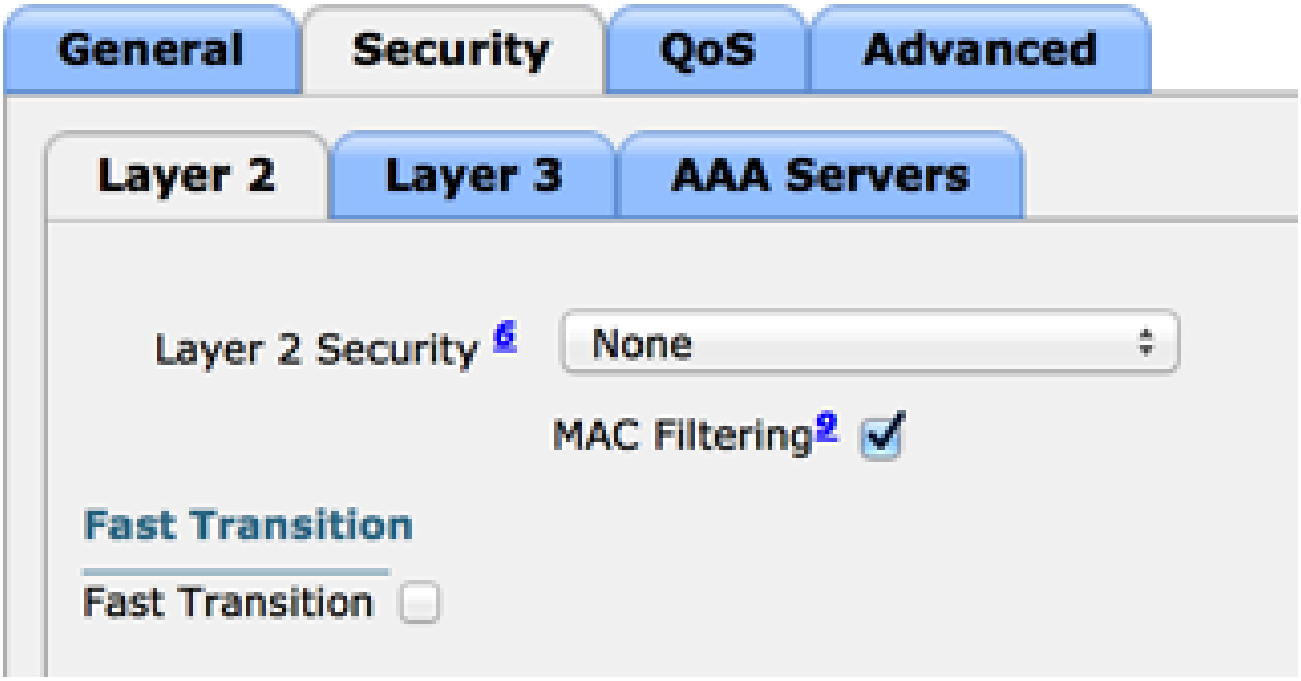
RADIUS-server heeft RFC3576

2. Maak een nieuw WLAN. Dit voorbeeld maakt een nieuw WLAN met de naam CWAFlex en wijst het toe aan vlan33. (Houd er rekening mee dat dit niet veel effect zal hebben aangezien het toegangspunt in de lokale switchingmodus staat.)



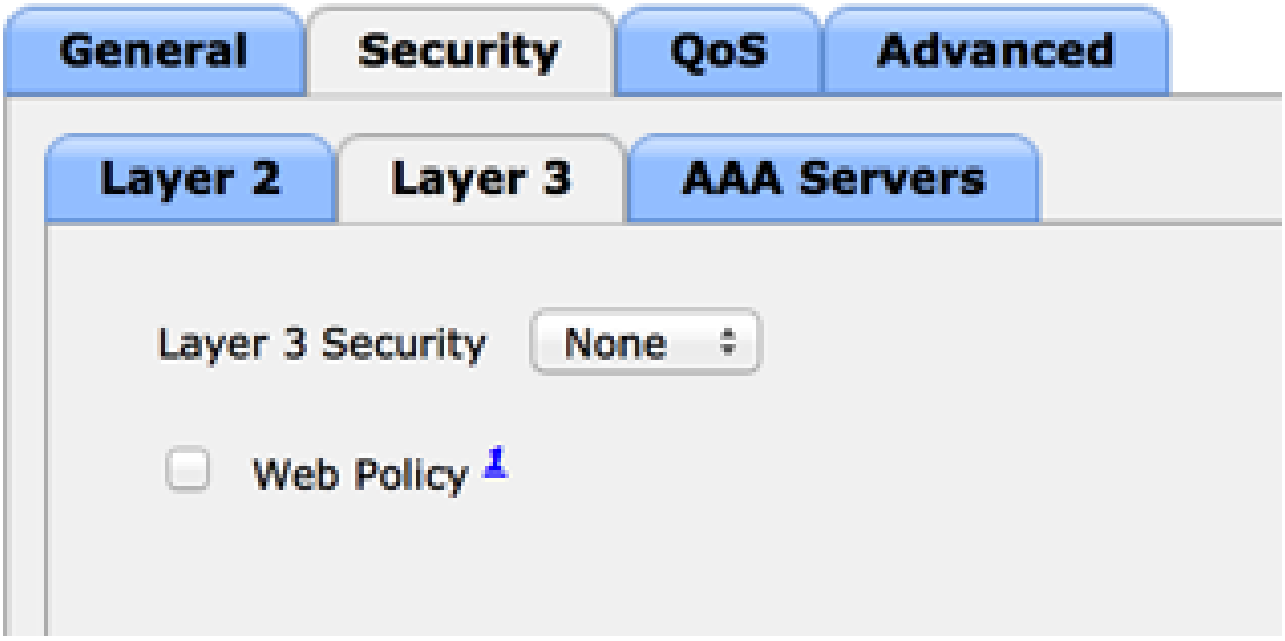
Een nieuw WLAN maken

3. Schakel op het tabblad Beveiliging MAC-filtering in als Layer 2-beveiliging.



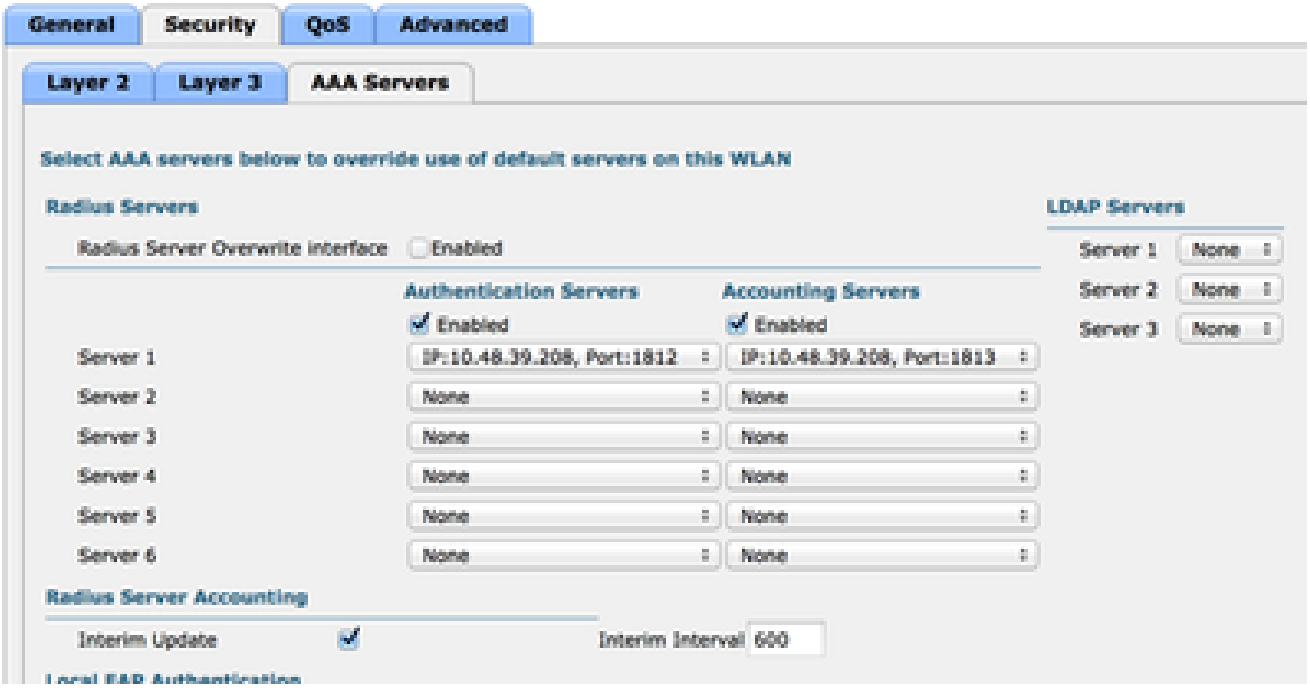
MAC-filtering inschakelen

4. Zorg ervoor dat op het tabblad Layer 3 de beveiliging is uitgeschakeld. (Als de webverificatie op Layer 3 is ingeschakeld, is lokale webverificatie ingeschakeld en niet centrale webverificatie.)



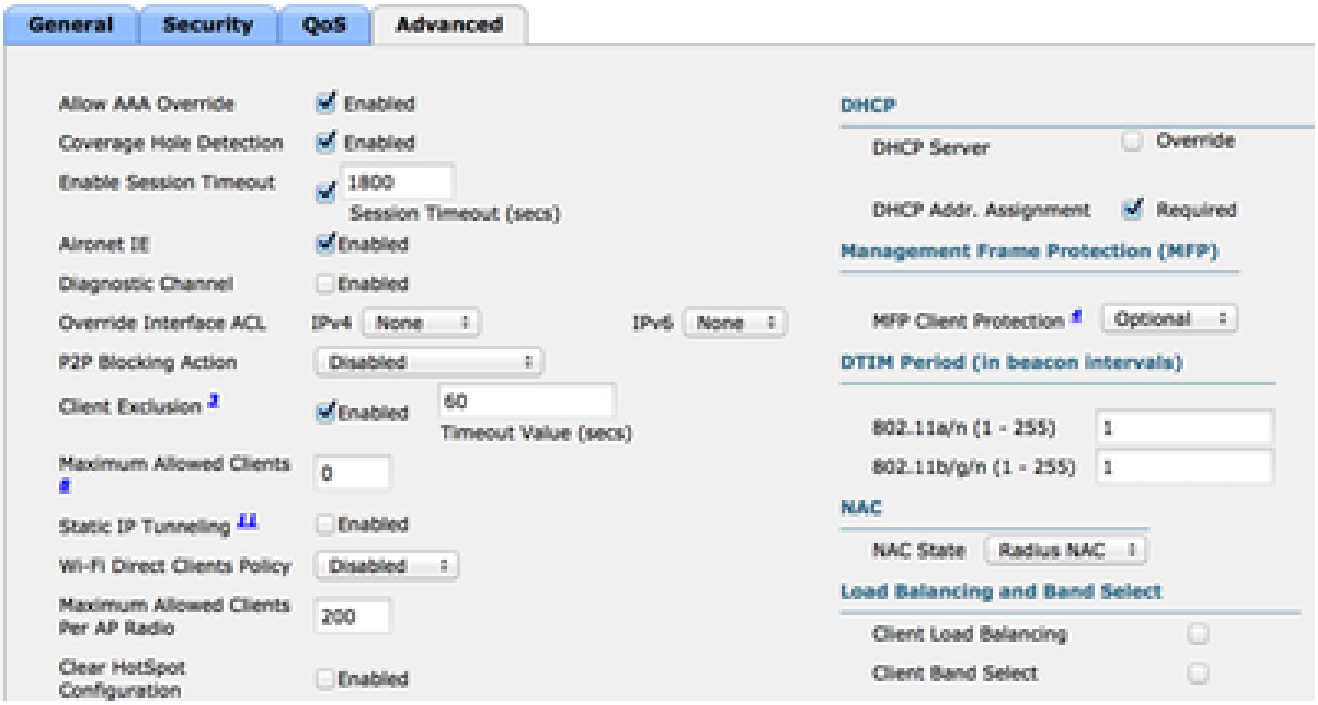
Zorg ervoor dat de beveiliging is uitgeschakeld

5. Selecteer in het tabblad AAA-servers de ISE-server als radiusserver voor het WLAN. U kunt deze optie ook selecteren voor accounting zodat u meer gedetailleerde informatie over ISE hebt.



Selecteer ISE-server

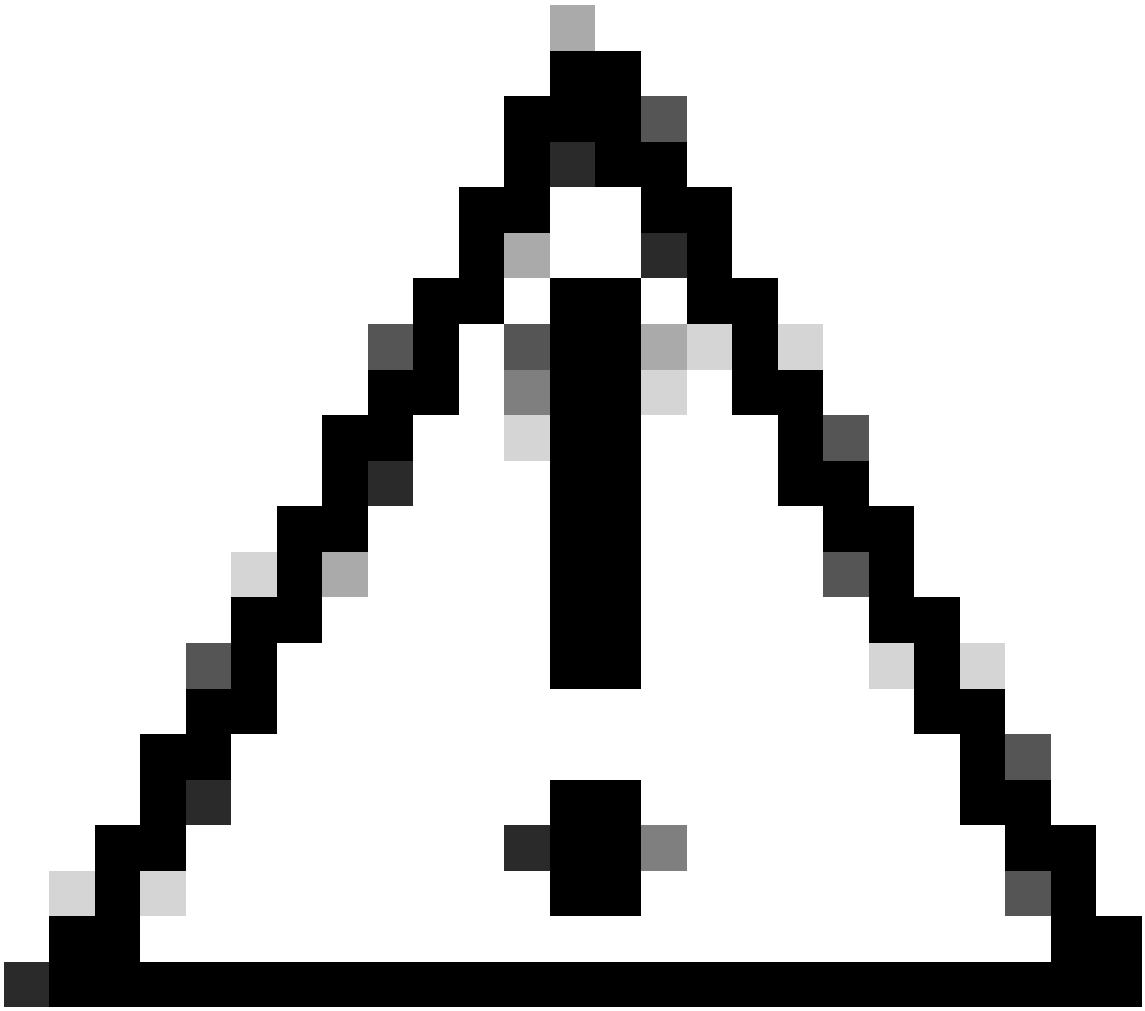
6. Zorg er in het tabblad Geavanceerd voor dat de optie AAA-negeren is ingeschakeld en dat Radius NAC is geselecteerd voor NAC-status.



Zorg ervoor dat AAA-opheffing is ingeschakeld

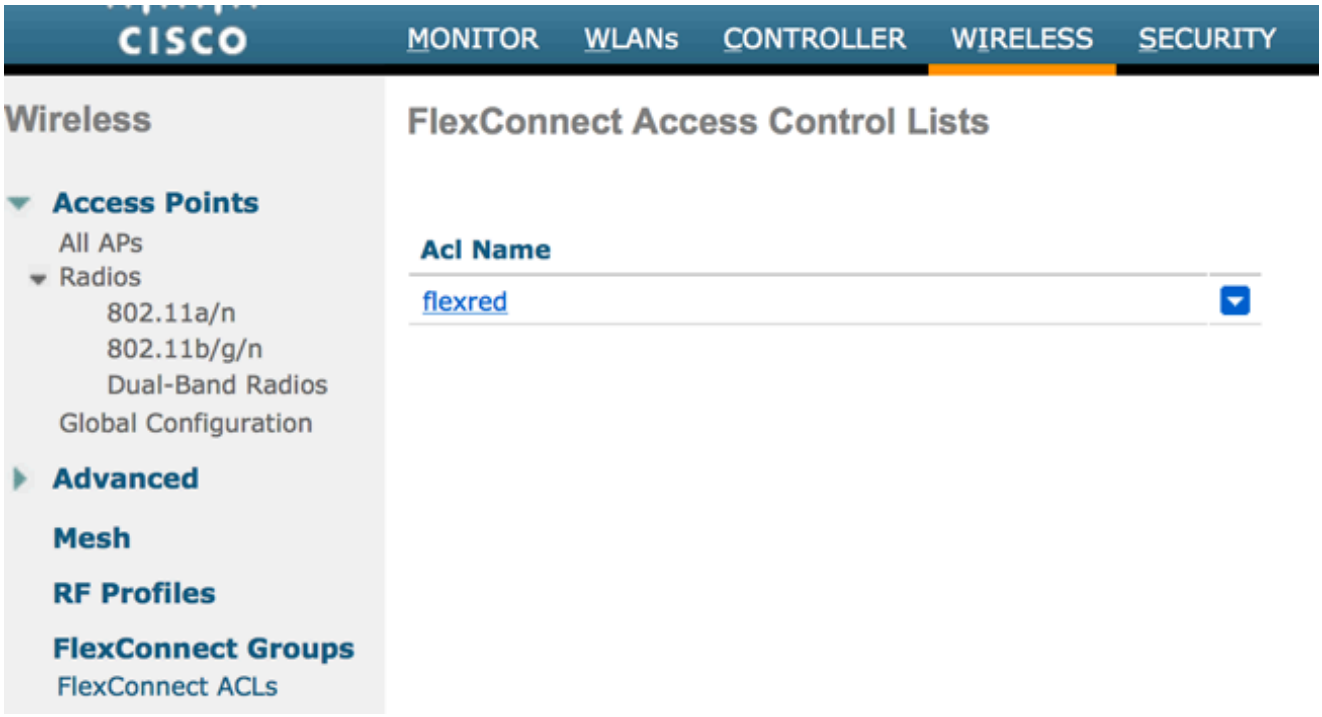
7. Maak een omleiding van ACL.

   Deze ACL wordt in het bericht Access-Accept van de ISE als referentie gebruikt en definieert welk verkeer moet worden omgeleid (ontkend door de ACL) en welk verkeer niet moet worden omgeleid (toegestaan door de ACL). In principe moeten DNS en verkeer van/naar de ISE worden toegestaan



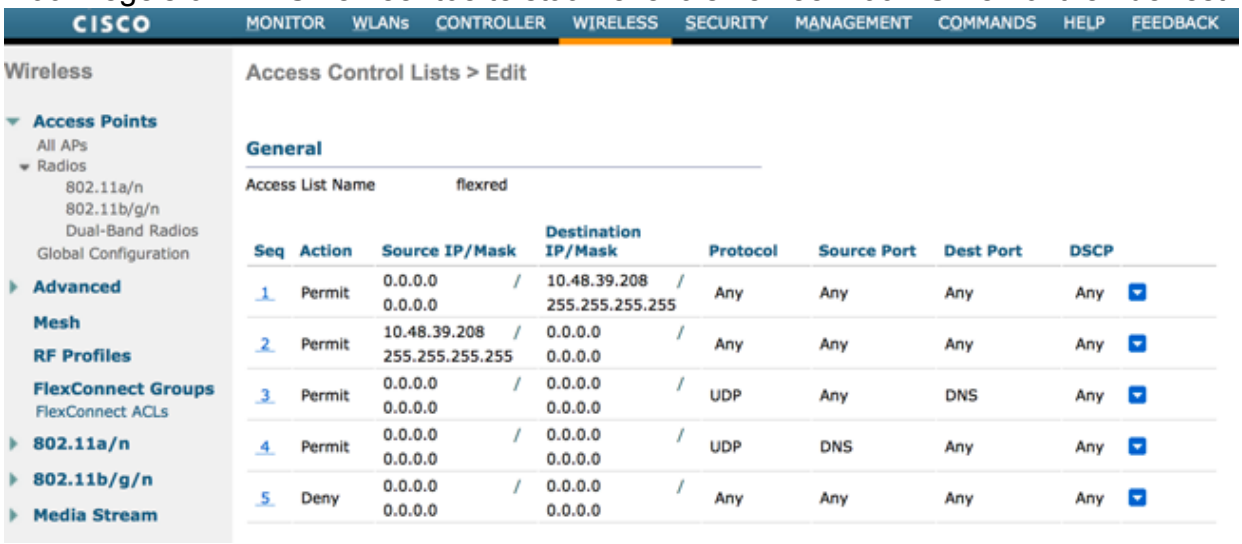
Waarschuwing: een probleem met FlexConnect AP's is dat u een FlexConnect ACL moet maken die losstaat van uw normale ACL. Dit probleem is gedocumenteerd in Cisco bug-id CSCue68065 en is opgelost in release 7.5. In WLC 7.5 en hoger is alleen een FlexACL vereist en is geen standaard ACL nodig. De WLC verwacht dat de door ISE geretourneerde omgestuurde ACL een normale ACL is. Om er echter zeker van te zijn dat het werkt, hebt u dezelfde ACL nodig als de FlexConnect ACL. (Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.)

Dit voorbeeld laat zien hoe u een FlexConnect ACL met de naam flexred kunt maken:



Een FlexConnect-ACL met de naam Flexred maken

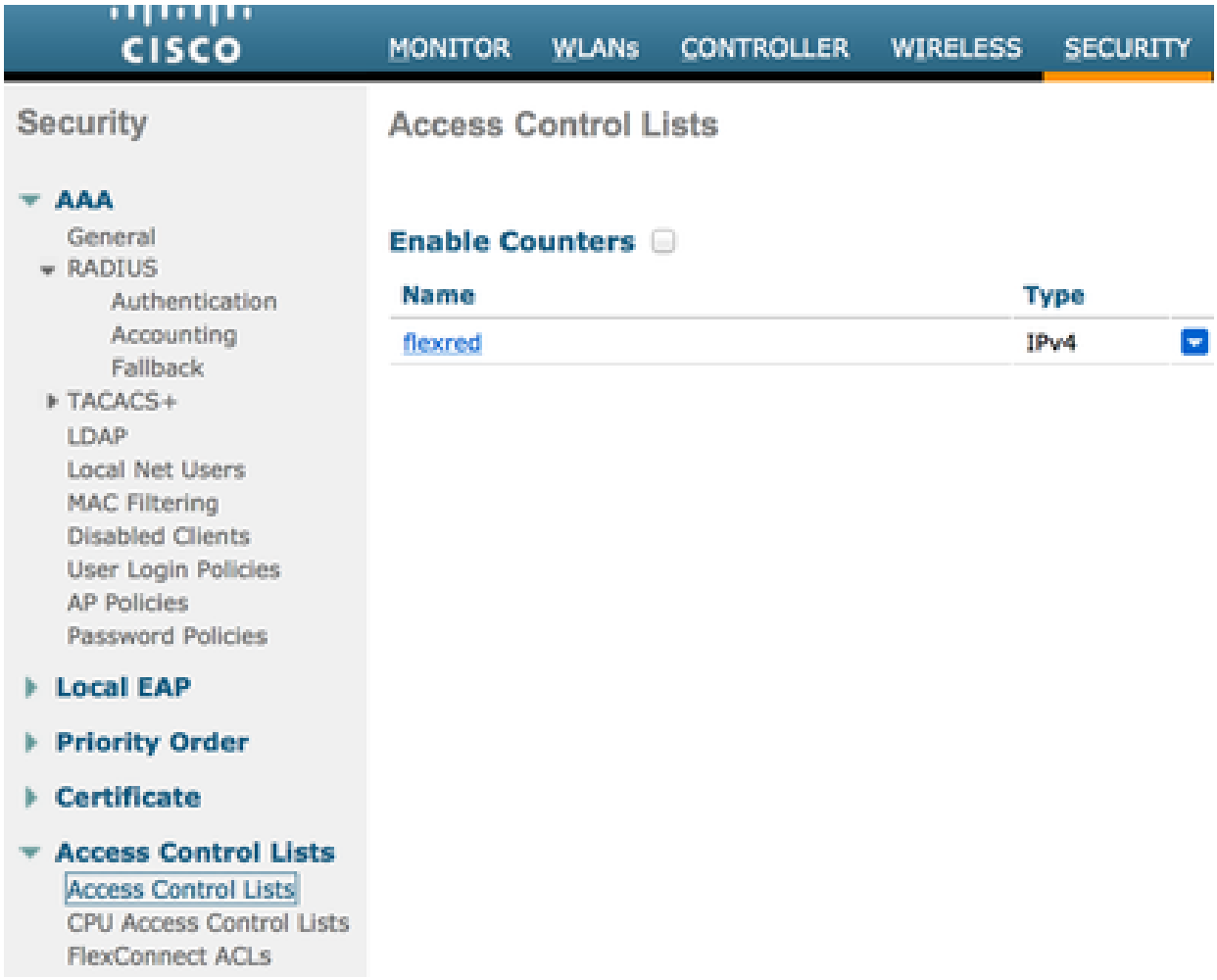
a. Maak regels om DNS-verkeer toe te staan evenals verkeer naar ISE en ontken de rest.



DNS-verkeer toestaan

Als u de maximale beveiliging wilt, kunt u alleen poort 8443 naar ISE toestaan. (Als u zich positioneert, moet u typische poortpoorten toevoegen, zoals 8905,8906,8909,8910.)

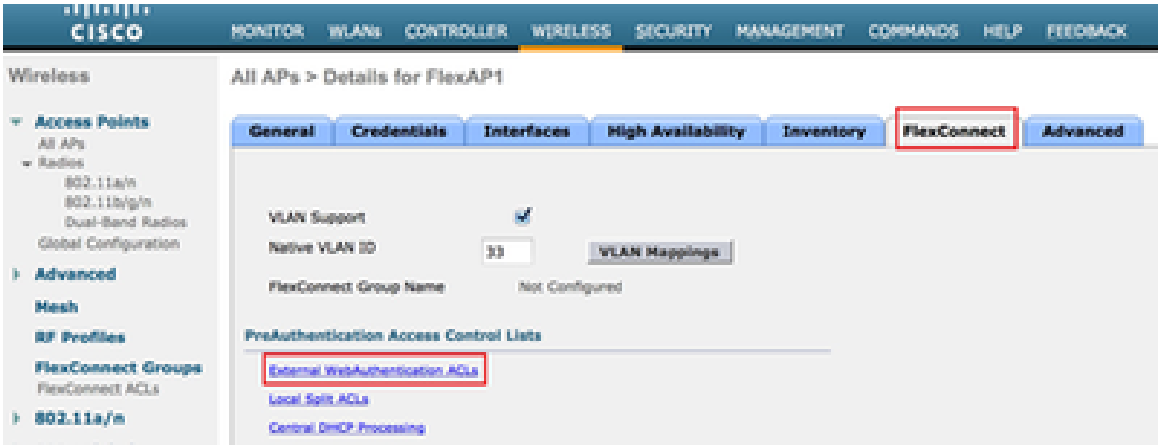
b. (Alleen op code vóór versie 7.5 vanwege Cisco-bug IDCue68065) Kies Beveiliging > Toegangscontrolelijsten om een identieke ACL met dezelfde naam te maken.



Dezelfde ACL maken

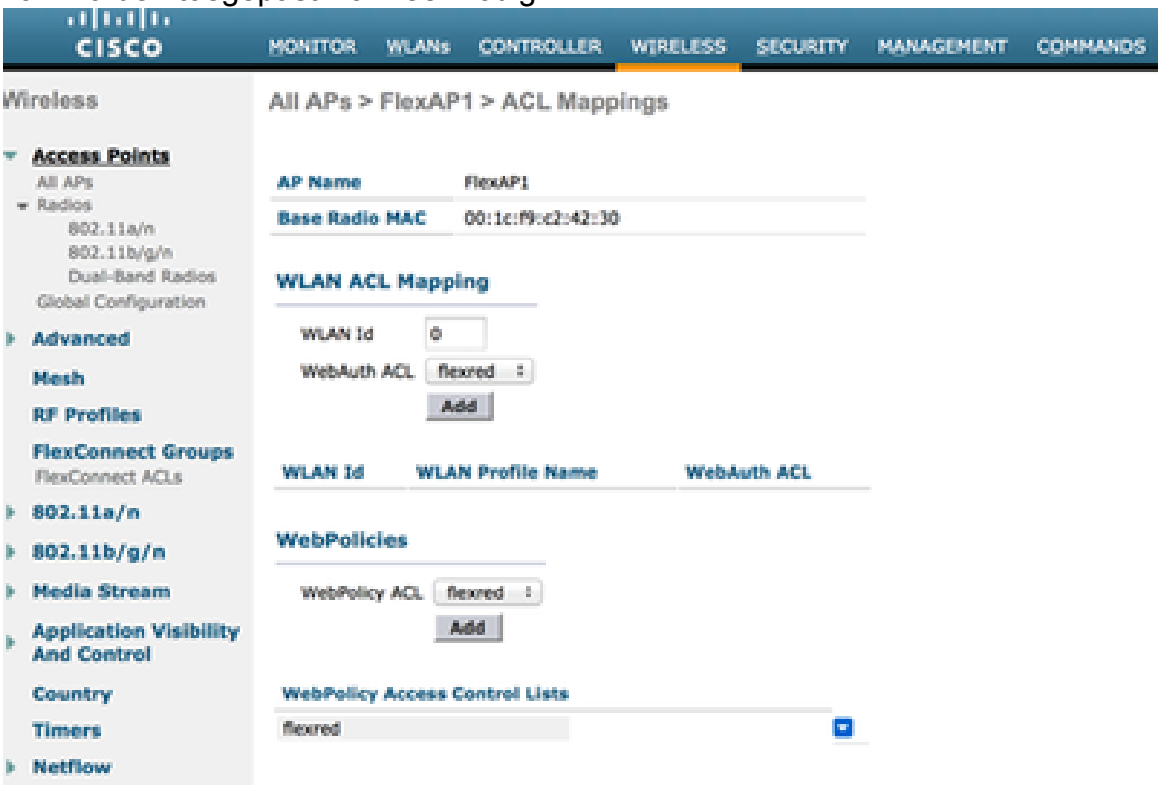
c. Bereid de specifieke FlexConnect AP voor. Merk op dat u voor een grotere implementatie doorgaans FlexConnect-groepen zou gebruiken en om schaalbaarheidsredenen deze items niet per AP zou uitvoeren.

1. Klik op Draadloos en selecteer het specifieke toegangspunt.
2. Klik op het tabblad FlexConnect en klik op Externe webverificatie-ACL's . (Vóór versie 7.4 werd deze optie webbeleid genoemd.)



Klik op FlexConnect Tab

3. Voeg de ACL (in dit voorbeeld genoemd) toe aan het gebied van webbeleid. Hiermee wordt de ACL op het access point gedrukt. Het wordt nog niet toegepast, maar de ACL-inhoud wordt aan het toegangspunt gegeven, zodat het kan worden toegepast wanneer nodig.



ACL toevoegen aan webbeleidsgebied

De WLC-configuratie is nu voltooid.

ISE-configuratie

Het autorisatieprofiel maken

Voltooi de volgende stappen om het autorisatieprofiel te maken:

1. Klik op Beleid en klik vervolgens op Beleidselementen.
2. Klik op Resultaten.
3. Breid Autorisatie uit en klik vervolgens op Autorisatieprofiel.

4. Klik op de knop Toevoegen om een nieuw autorisatieprofiel voor de centrale webauth te maken.

5. Typ in het veld Naam een naam voor het profiel. Dit voorbeeld gebruikt CentralWebauth.

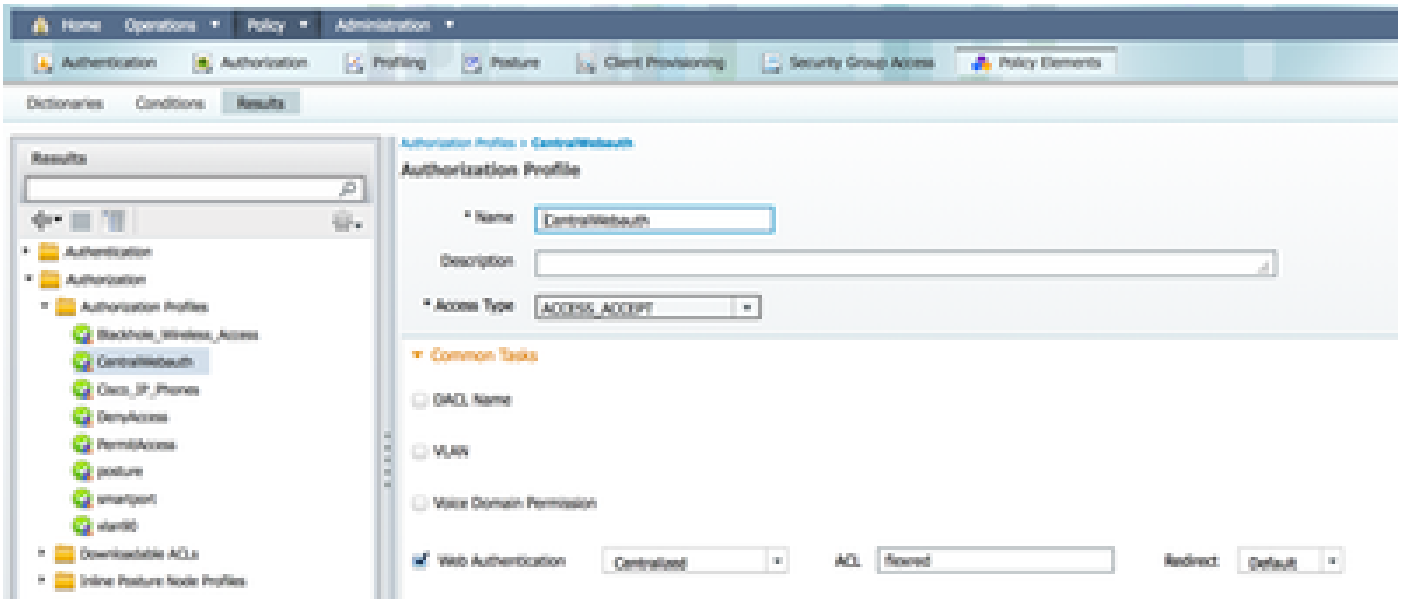
6. Kies ACCESS_ACCEPTEREN in de vervolgkeuzelijst Toegangstype.

7. Schakel het aanvinkvakje Web Verification in en kies Gecentraliseerde webautorisatie in de vervolgkeuzelijst.

8. Voer in het veld ACL de naam in van de ACL op de WLC die het verkeer definieert dat wordt omgeleid. Dit voorbeeld gebruikt flexred.

9. Kies Standaard in de vervolgkeuzelijst Omleiden.

Het kenmerk Redirect bepaalt of de ISE de standaard webportal ziet of een aangepaste webportal die de ISE-beheerder heeft gemaakt. Bijvoorbeeld, leidt de gebogen ACL in dit voorbeeld tot een omleiding op HTTP-verkeer van de client naar overal.



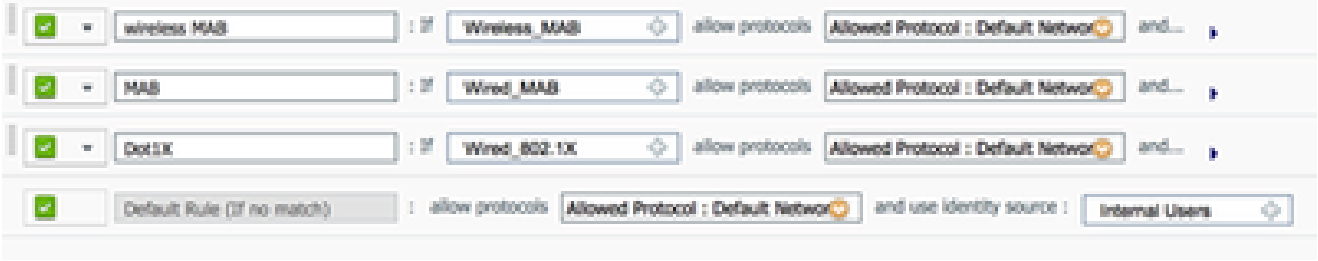
ACL activeert een omleiding op HTTP-verkeer van de client naar elke locatie

Een verificatieregel maken

Voltooi de volgende stappen om het verificatieprofiel te gebruiken om de verificatieregel te maken:

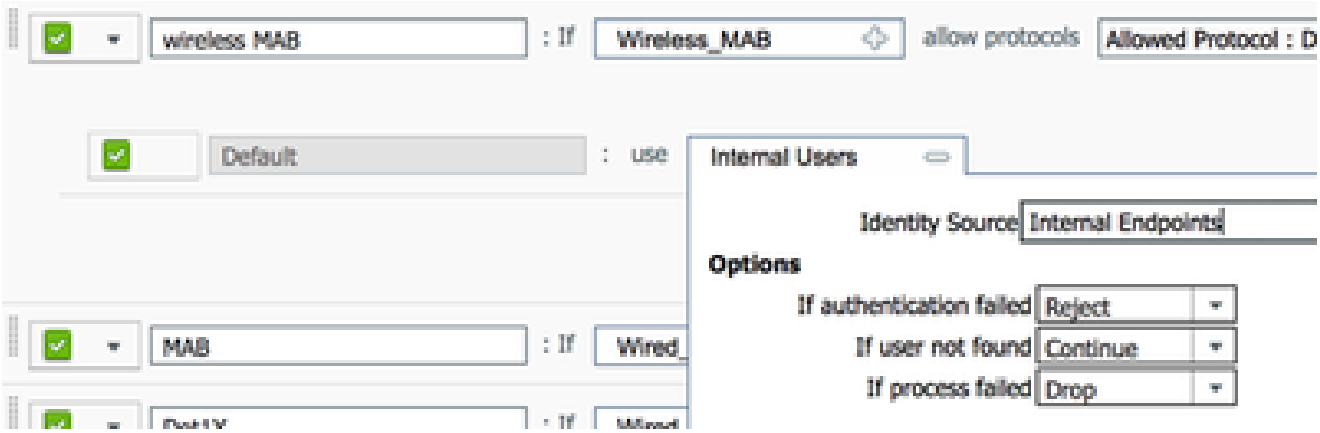
1. Klik in het menu Beleid op Verificatie.

   Deze afbeelding toont een voorbeeld van hoe de verificatieregelgeving te configureren. In dit voorbeeld wordt een regel ingesteld die wordt geactiveerd wanneer MAC-filtering wordt gedetecteerd.



Hoe te om beleidsregel te vormen

2. Voer een naam in voor de verificatieregel. In dit voorbeeld wordt het gebruik van het draadloze tabblad gebruikt .
3. Selecteer het plusteken (+) in het veld Als.
4. Kies Samengestelde voorwaarde en kies dan Wireless_MAB .
5. Kies standaard netwerktoegang zoals toegestaan protocol.
6. Klik op de pijl naast en ... om de regel verder uit te vouwen.
7. Klik op het pictogram + in het veld Identity Source en kies Interne endpoints.
8. Kies Doorgaan in de vervolgkeuzelijst Indien gebruiker niet gevonden.

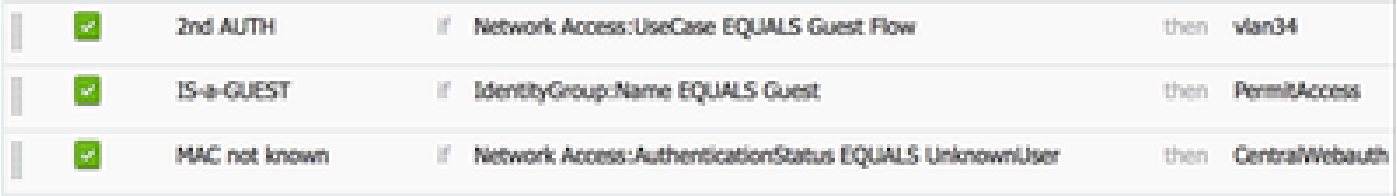


Klik op Continue (Doorgaan)

Deze optie maakt het mogelijk om een apparaat te authenticeren (via webauth) zelfs als het MAC-adres niet bekend is. Dot1x-clients kunnen nog steeds authenticeren met hun referenties en moeten niet betrokken zijn bij deze configuratie.

Een autorisatieregel aanmaken

Er zijn nu verscheidene regels in het vergunningsbeleid te vormen. Wanneer de PC is gekoppeld, zal het door mac filtering gaan; er wordt aangenomen dat het MAC-adres niet bekend is, dus de webauth en ACL worden teruggegeven. Deze niet bekende MAC-regel wordt in de volgende afbeelding getoond en wordt in deze sectie geconfigureerd.

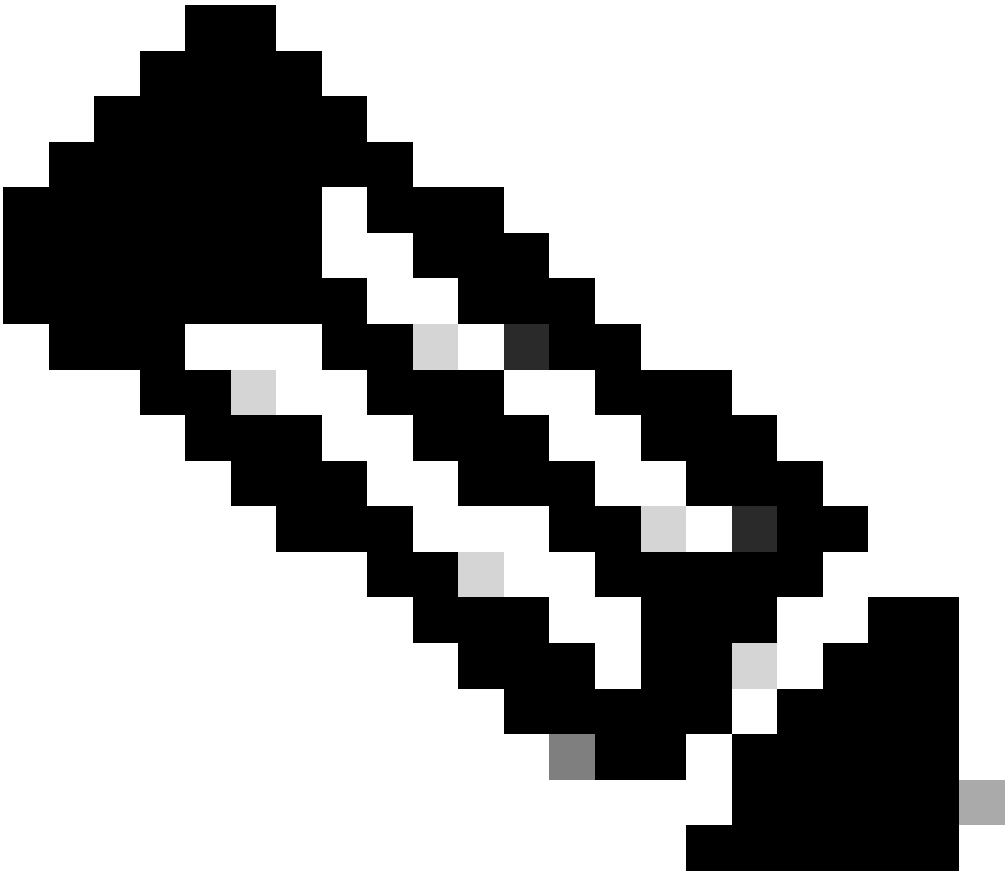


Voltooi de volgende stappen om de autorisatieregel te maken:

1. Maak een nieuwe regel en voer een naam in. Dit voorbeeld gebruiktMAC niet bekend.
2. Klik op het pictogram plus (+) in het veld Voorwaarden en kies om een nieuwe voorwaarde te maken.
3. Breid de vervolgkeuzelijst expressie uit.
4. Kies Netwerktoegang en breid deze uit.
5. Klik op Verificatiestatus en kies de operator Gelijk.
6. Kies Onbekende gebruiker in het rechterveld.
7. Kies op de pagina Algemene autorisatie CentralWebauth (Autorisatieprofiel) in het veld rechts van het woord dan .

   Met deze stap kan de ISE doorgaan, ook al is de gebruiker (of de MAC) niet bekend.

   Onbekende gebruikers krijgen nu de inlogpagina te zien. Echter, zodra ze hun referenties invoeren, worden ze opnieuw gepresenteerd met een authenticatieverzoek op de ISE; daarom moet een andere regel worden geconfigureerd met een voorwaarde die wordt voldaan als de gebruiker een gastgebruiker is. In dit voorbeeld, Als UseridentiteitsGroup gelijk is aan Guestis gebruikt, en er wordt aangenomen dat alle gasten tot deze groep behoren.
8. Klik op de knop Acties aan het einde van de MAC onbekende regel en kies ervoor om een nieuwe regel toe te voegen.



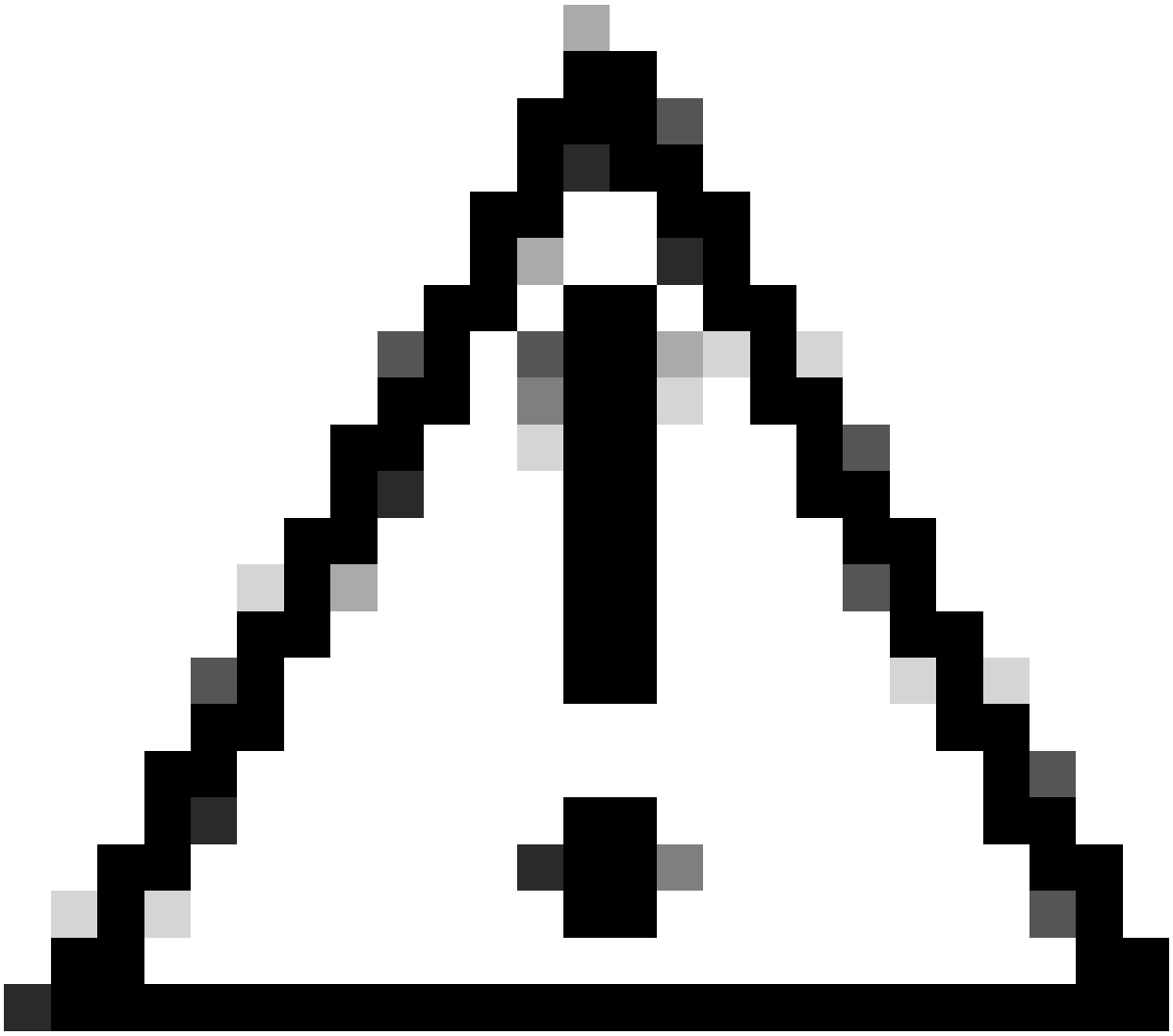
Opmerking: het is heel belangrijk dat deze nieuwe regel vóór de onbekende regel van de MAC komt.

9. Voer in het veld Naam 2e AUTH in.
10. Selecteer een identiteitsgroep als voorwaarde. Dit is een voorbeeld van Guest.
11. Klik in het veld Voorwaarde op het plusteken (+) en kies om een nieuwe voorwaarde te maken.
12. Kies Netwerktoegang en klik op UseCase .
13. Kies Gelijk als de operator.
14. Kies GuestFlow als de juiste operand. Dit betekent dat je gebruikers die net ingelogd zijn op de webpagina zal vangen en terugkomen na een wijziging van de autorisatie (het gastenstroomdeel van de regel) en alleen als ze behoren tot de gastenidentiteitsgroep.
15. Klik op de autorisatiepagina op het plusteken (+) (naast toen) om een resultaat voor uw

regel te kiezen.

In dit voorbeeld wordt een voorgeconfigureerd profiel (vlan34) toegewezen; deze configuratie wordt niet in dit document weergegeven.

U kunt een Permit Access-optie kiezen of een aangepast profiel maken om het VLAN of de kenmerken die u wilt, te retourneren.



Waarschuwing: in ISE versie 1.3, afhankelijk van het type webverificatie, kan de Guest Flow-gebruikscase niet meer worden gevonden. De autorisatieregel zou dan de gastgebruikersgroep als enige mogelijke voorwaarde moeten bevatten.

IP-verlenging inschakelen (optioneel)

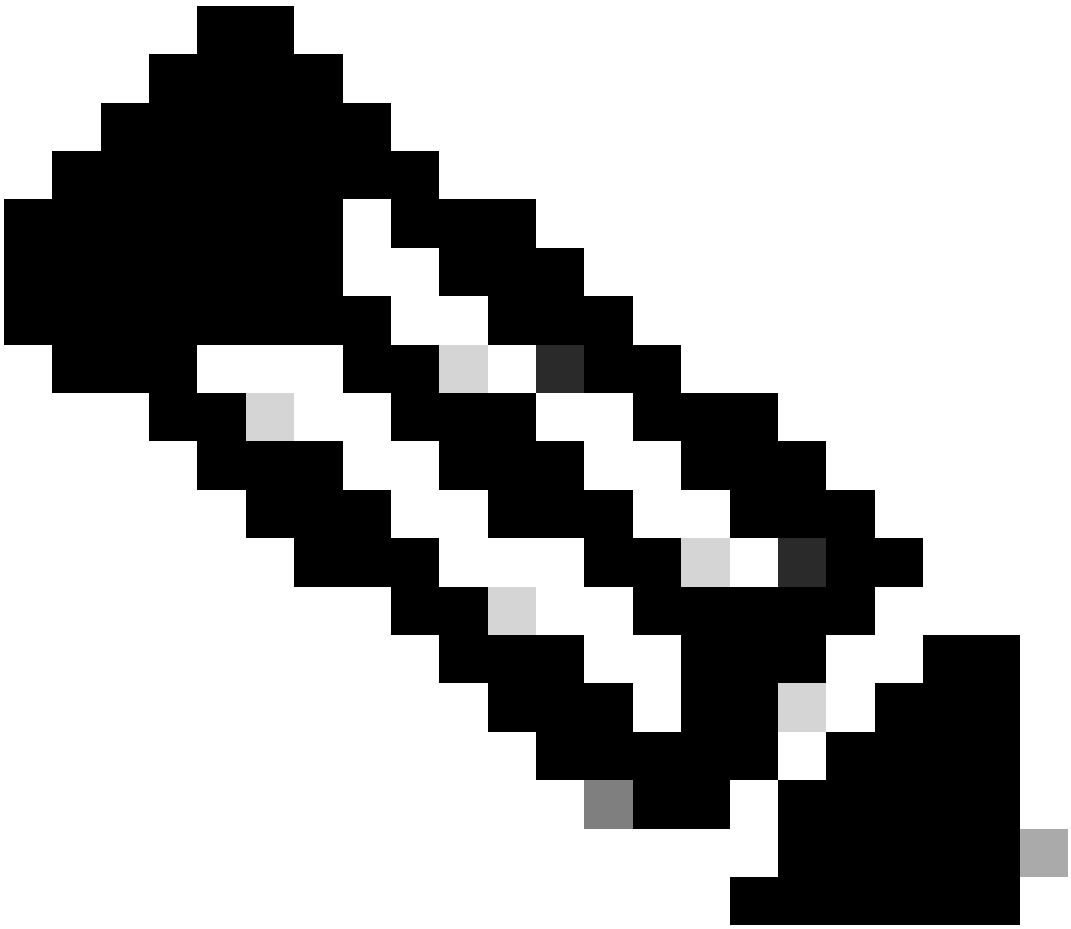
Als u een VLAN toewijst, is de laatste stap voor de client-pc om zijn IP-adres te vernieuwen. Deze stap wordt bereikt door het gastportaal voor Windows-clients. Als u geen VLAN hebt ingesteld

voor de 2e AUTH-regel eerder, kunt u deze stap overslaan.

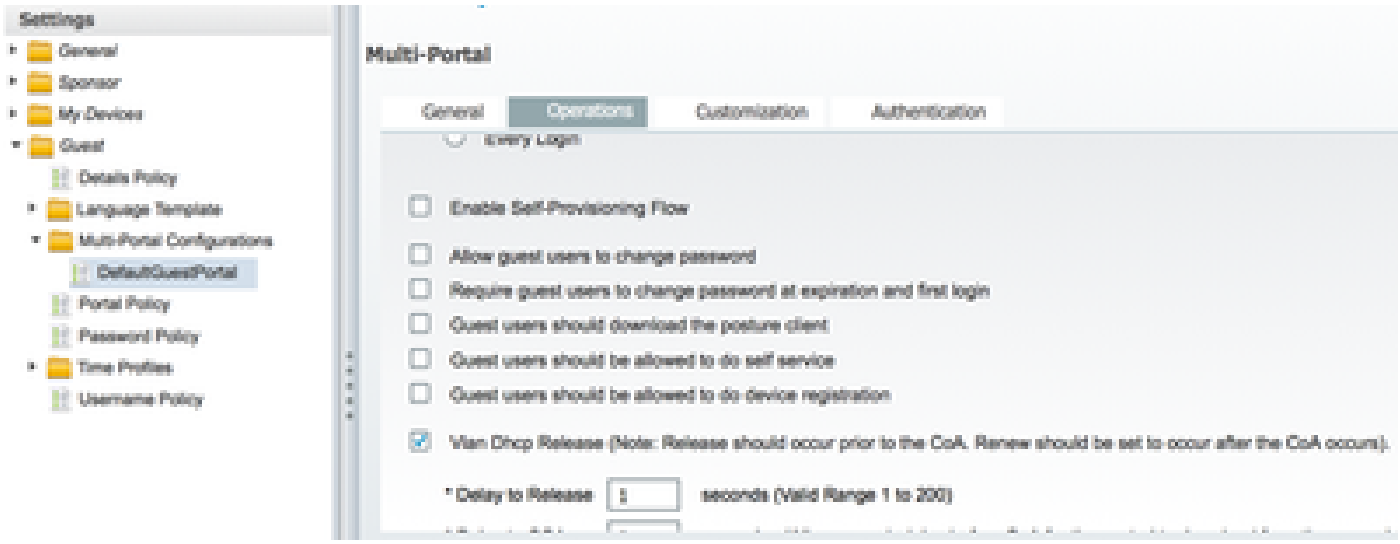
Merk op dat op FlexConnect AP's het VLAN vooraf op het AP zelf moet bestaan. Daarom als het niet, kunt u een VLAN-ACL-afbeelding op AP zelf of op de flex groep tot stand brengen waar u geen ACL voor het nieuwe VLAN toepast u wilt creëren. Dat maakt feitelijk een VLAN (zonder ACL).

Als u een VLAN hebt toegewezen, moet u deze stappen uitvoeren om IP-vernieuwing in te schakelen:

1. Klik op Beheer en klik vervolgens op Gastbeheer.
2. Klik op Instellingen.
3. Breid Gast uit en breid dan Multi-Portal Configuration uit.
4. Klik op DefaultGuestPortal of de naam van een aangepaste portal die u hebt gemaakt.
5. Klik op het aankruisvakje VLAN DHCP release.



Opmerking: deze optie werkt alleen voor Windows-clients.



Klik op het vakje VLAN DHCP release

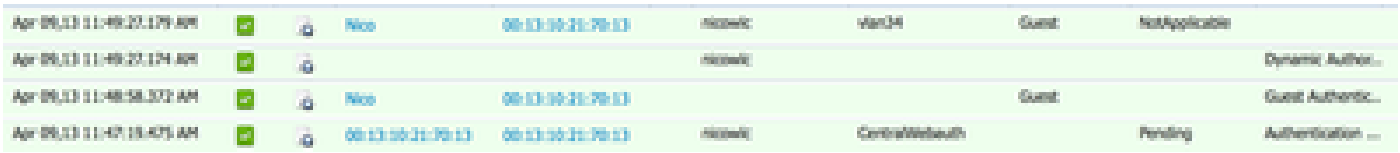
Traffic Flow

Het kan moeilijk lijken te begrijpen welk verkeer in dit scenario naar waar wordt gestuurd. Hier is een snelle beoordeling:

- De client stuurt een associatieverzoek via de ether voor de SSID.
- De WLC behandelt de MAC filtering authenticatie met ISE (waar het de omleiding attributen ontvangt).
- De client ontvangt alleen een assoc-respons nadat de MAC-filtering is voltooid.
- De client dient een DHCP-verzoek in en dat wordt LOKAAL geschakeld door het toegangspunt om een IP-adres van de externe site te verkrijgen.
- In de staat Central_webauth, wordt het verkeer dat gemarkeerd is voor deny op de omleiding ACL (dus HTTP is doorgaans) CENTRAAL geschakeld. Zo is het niet de AP die de omleiding maar de WLC doet; bijvoorbeeld, wanneer de klant vraagt om een website, de AP stuurt dit naar de WLC ingekapseld in CAPWAP en de WLC spoofs die website IP adres en omleidingen naar ISE.
- De client wordt omgeleid naar de ISE-URL voor omleiding. Dit wordt LOKAAL opnieuw geschakeld (omdat het op vergunning op flex redirect ACL raakt).
- Eenmaal in de RUN staat, wordt het verkeer lokaal geschakeld.

Verifiëren

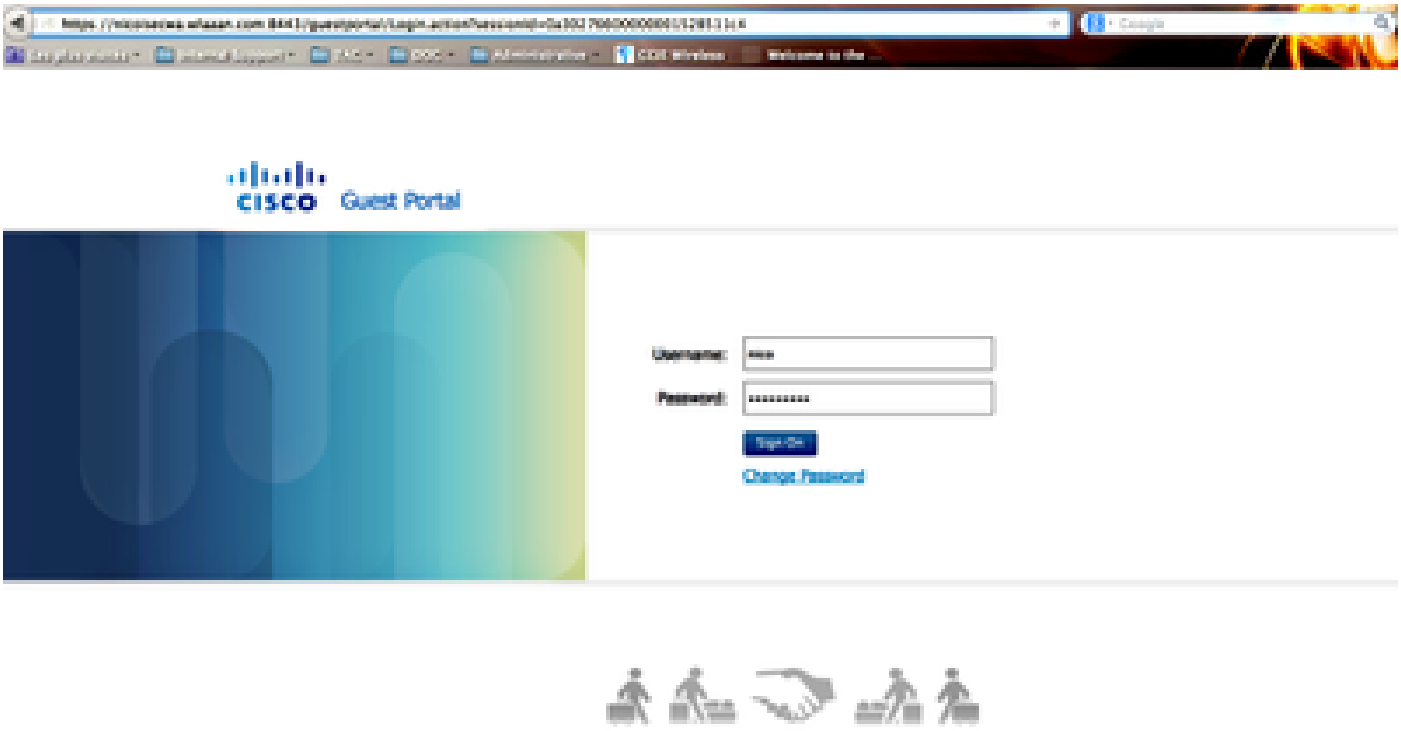
Zodra de gebruiker aan de SSID is gekoppeld, wordt de autorisatie weergegeven op de ISE-pagina.



De autorisatie wordt weergegeven

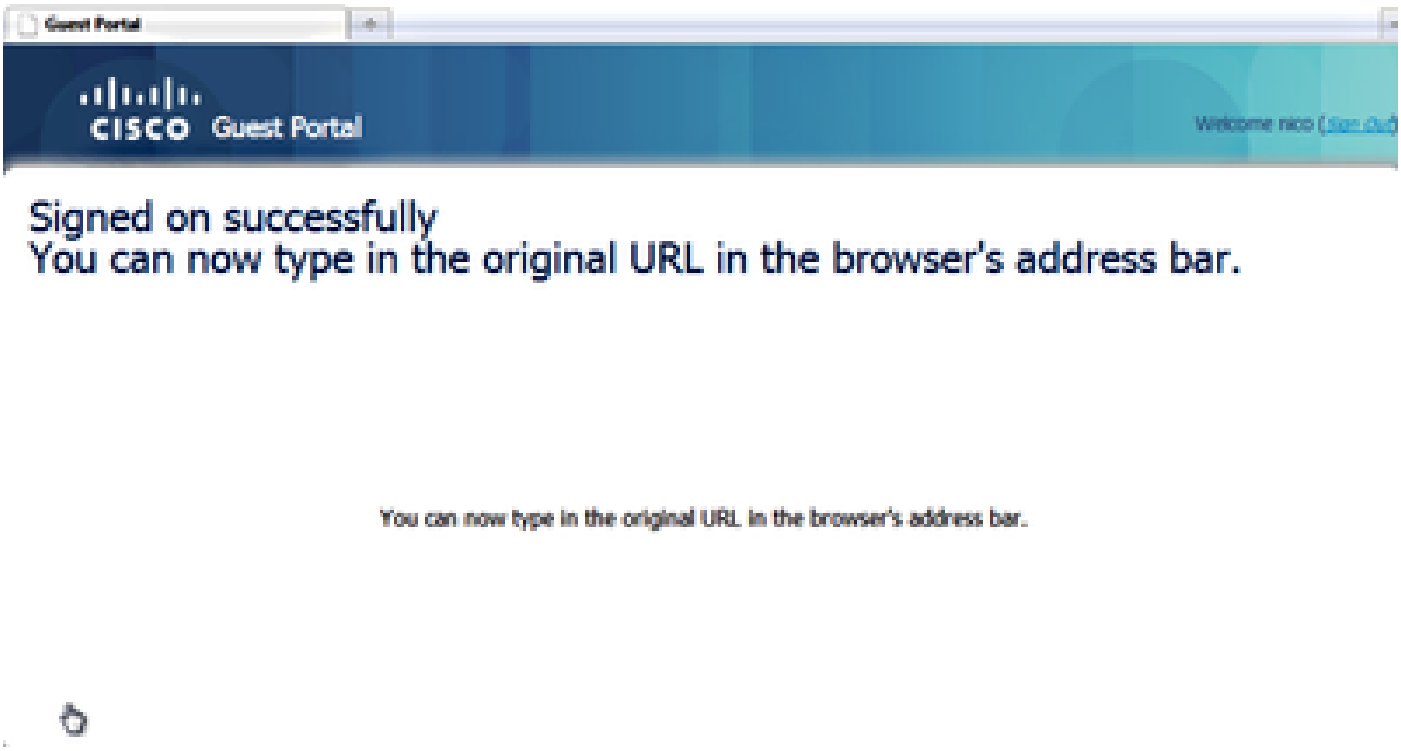
Vanaf de basis kunt u de MAC-adresfiltering-verificatie zien die de CWA-kenmerken retourneert. Vervolgens wordt de portal ingelogd met de gebruikersnaam. De ISE stuurt dan een CoA naar de WLC en de laatste verificatie is een Layer 2 mac filtering-verificatie aan de WLC-kant, maar ISE onthoudt de client en de gebruikersnaam en past het benodigde VLAN toe dat we in dit voorbeeld hebben geconfigureerd.

Wanneer een adres wordt geopend op de client, wordt de browser omgeleid naar de ISE. Zorg ervoor dat Domain Name System (DNS) correct is geconfigureerd.



Doorverwezen naar ISE

Netwerktoegang wordt verleend nadat de gebruiker het beleid heeft aanvaard.



Netwerktoegang verleend

Op de controller veranderen de Policy Manager-status en de RADIUS NAC-status van POSTURE_REQD naar RUN.

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

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