ISE Self Registered Guest Portal configureren

Inhoud

Inleiding

Dit document beschrijft hoe u deze functionaliteit kunt configureren en oplossen. Self Registered Guest Portal, staat gastgebruikers toe om zelf te registreren samen met medewerkers om hun AD-referenties te gebruiken om toegang te krijgen tot netwerkbronnen. Met deze portal kunt u meerdere functies configureren en aanpassen.

Voorwaarden

Vereisten

Cisco raadt u aan ervaring te hebben met ISE-configuratie en basiskennis van deze onderwerpen:

- ISE-implementaties en gaststromen
- Configuratie van draadloze LAN-controllers (WLC)

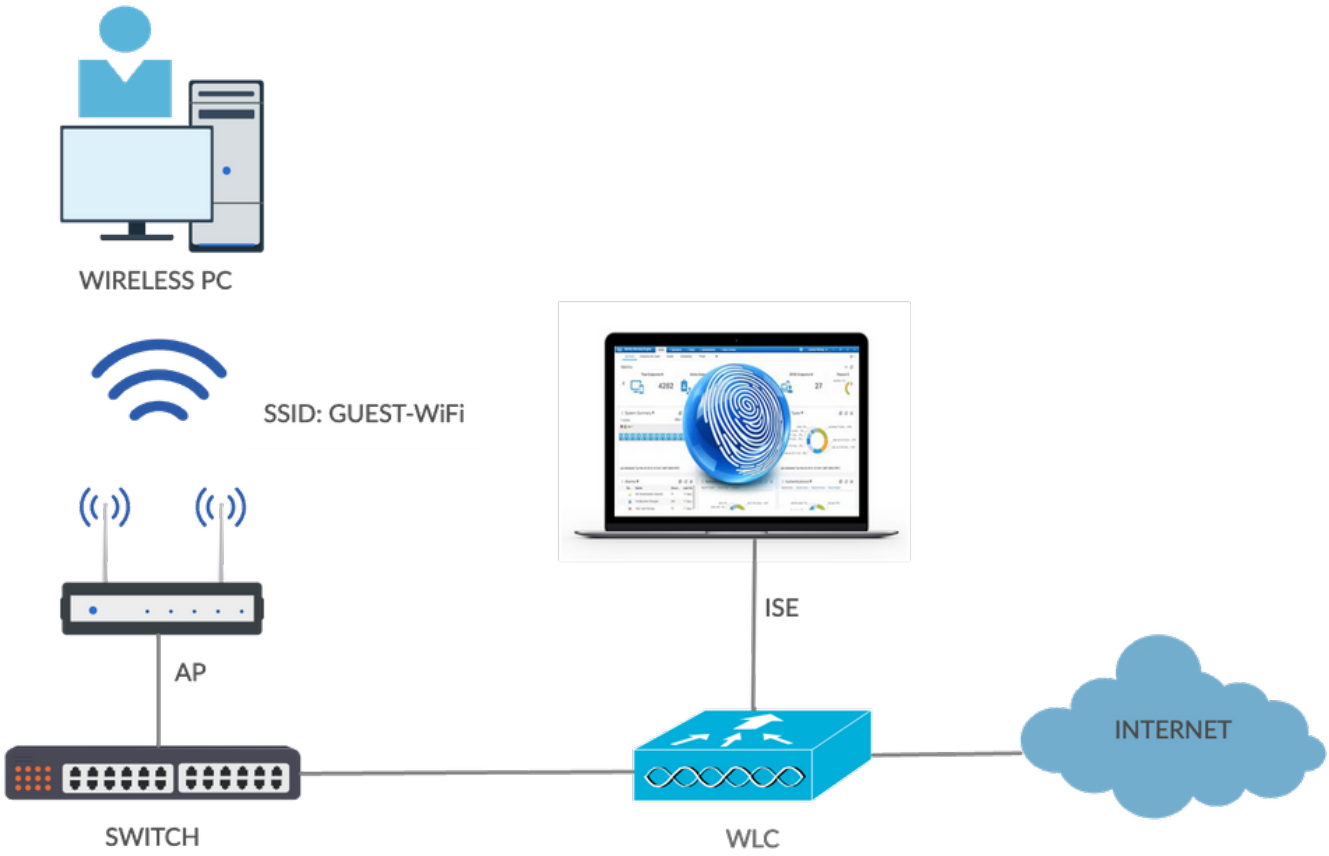
Gebruikte componenten

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

- Microsoft Windows 10 Pro
- Cisco WLC 5508 met versie 8.5.135.0
- ISE-software, versie 3.0

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 en gegevensstroom



Dit scenario presenteert meerdere opties die beschikbaar zijn voor gastgebruikers wanneer ze zelfregistratie uitvoeren.

Hier is de algemene stroom:

Stap 1. Gastgebruiker associeert met Service Set Identifier (SSID): Guest-WiFi. Dit is een open netwerk met MAC-filtering met ISE voor verificatie. Deze verificatie komt overeen met de tweede autorisatieregel op de ISE en het autorisatieprofiel wordt omgeleid naar het Guest Self Registered Portal. ISE retourneert een RADIUS access-Accept met twee cisco-av-paren:

- url-redirect-acl (het verkeer moet worden omgeleid en de naam van Access Control List (ACL) moet lokaal op de WLC worden gedefinieerd)

- url-redirect (waar dat verkeer naar ISE te leiden)

Stap 2. De gastgebruiker wordt omgeleid naar ISE. In plaats van referenties te verstrekken om in te loggen, klikt de gebruiker op **Register for Guest Access.** De gebruiker wordt doorgestuurd naar een pagina waar die account kan worden gemaakt. Een optionele geheime registratiecode kan worden ingeschakeld om het zelfregistratierecht te beperken tot mensen die die geheime waarde kennen. Nadat de account is aangemaakt, wordt de gebruiker geloofsbrieven (gebruikersnaam en wachtwoord) gegeven en logt hij in met deze referenties.

Stap 3. ISE stuurt een RADIUS-wijziging van autorisatie (CoA) opnieuw naar de WLC. De WLC verifieert de gebruiker opnieuw wanneer deze het RADIUS-toegangsverzoek verstuurt met het kenmerk Alleen autoriseren. ISE reageert met Access-Accept en Airrespace ACL die lokaal is gedefinieerd op de WLC, die alleen toegang tot het internet biedt (definitieve toegang voor gastgebruikers is afhankelijk van het autorisatiebeleid).

> **Opmerking:** EAP-sessies (Extensible Verification Protocol), ISE moet een CoA-terminate verzenden om opnieuw verificatie te starten, omdat de EAP-sessie tussen de aanvrager en de ISE loopt. Maar voor MAB (MAC filtering), CoA Reauthenticate is genoeg; het is niet nodig de-associatie of de-authenticatie van de draadloze client ongedaan te maken.

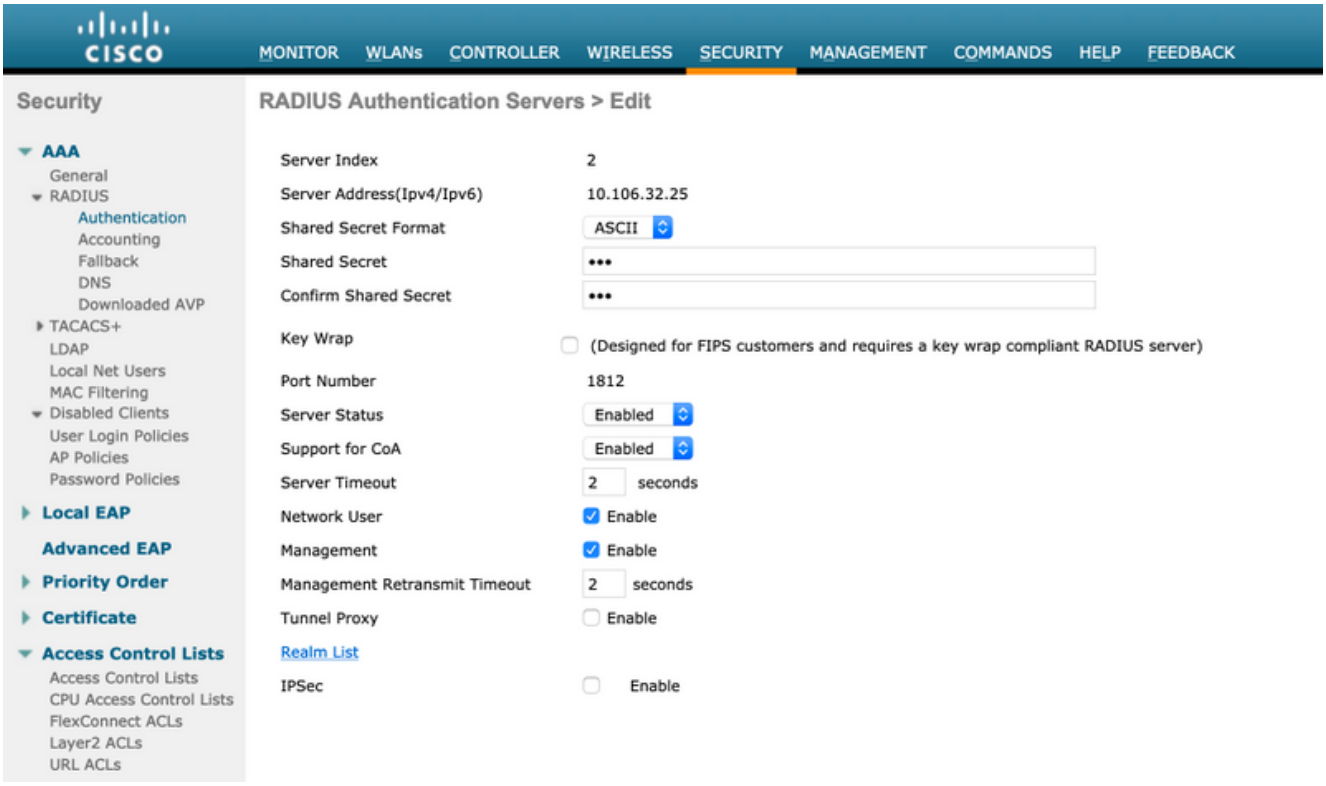
Stap 4. De gastgebruiker heeft toegang tot het netwerk gewenst.

Meerdere extra functies zoals postuur en Bring Your Own Device (BYOD) kunnen worden ingeschakeld (later besproken).

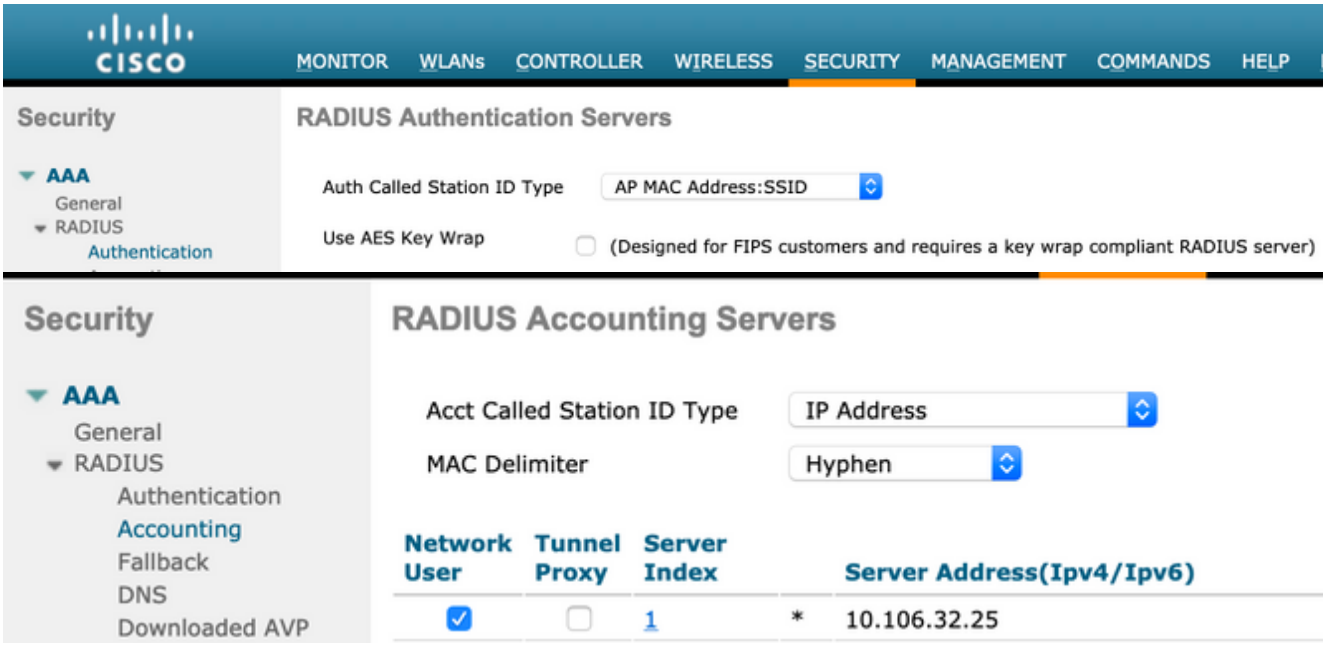
Configureren

WLC

1. Voeg de nieuwe RADIUS-server voor verificatie en accounting toe. Ga naar **Security > AAA > Radius > Verificatie** om RADIUS CoA in te schakelen (RFC 3576).



Er is een vergelijkbare configuratie voor accounting. Het is ook aan te raden om de WLC te configureren om SSID te verzenden in het kenmerk Call Station ID, waarmee de ISE flexibele regels kan configureren op basis van SSID:



2. Voer op het tabblad WLAN's de Wireless LAN (WLAN) Guest-WiFi in en configureer de juiste interface. Stel Layer 2-beveiliging in op **Geen** met MAC-filtering. Selecteer in Beveiligings-/verificatie-, autorisatie- en accounting (AAA) servers het ISE-IP-adres voor zowel verificatie als accounting. Schakel in het tabblad Advanced de **AAA Override in** en stel de status Network Admission Control (NAC) in op ISE NAC (CoA-ondersteuning).

3. Navigeer naar **Beveiliging > Toegangscontrolelijsten > Toegangscontrolelijsten** en maak twee toegangslijsten aan:

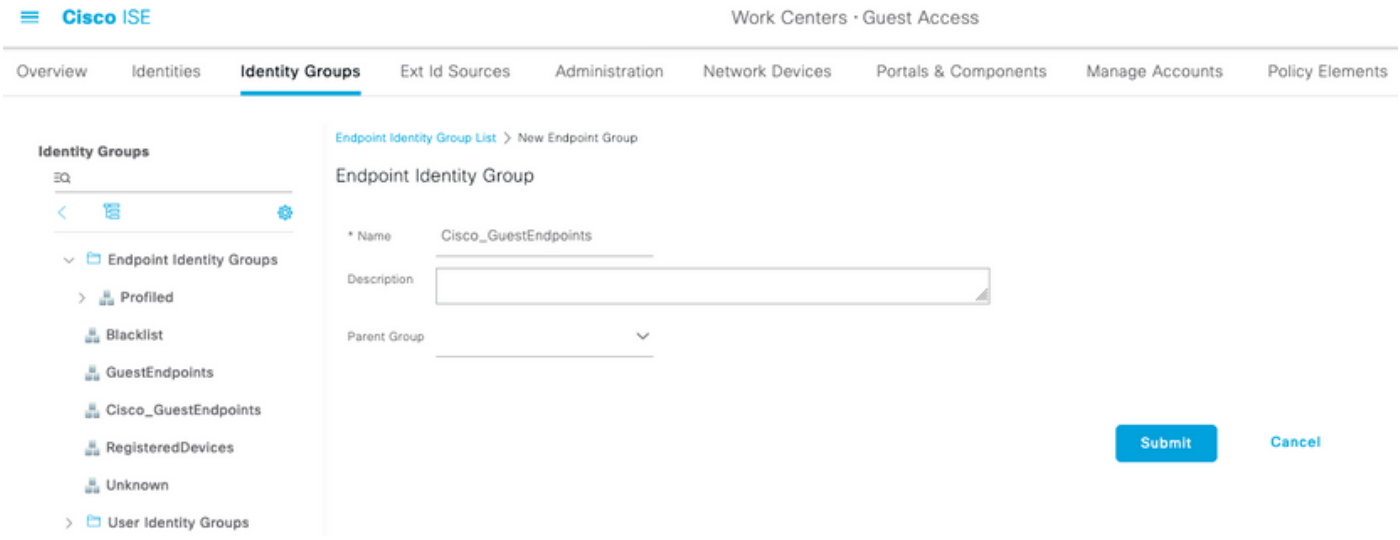
   GuestRedirect, die verkeer toestaat dat niet moet worden omgeleid en omleidt al ander

verkeerInternet, dat voor collectieve netwerken wordt ontkend en voor alle anderen toegelaten

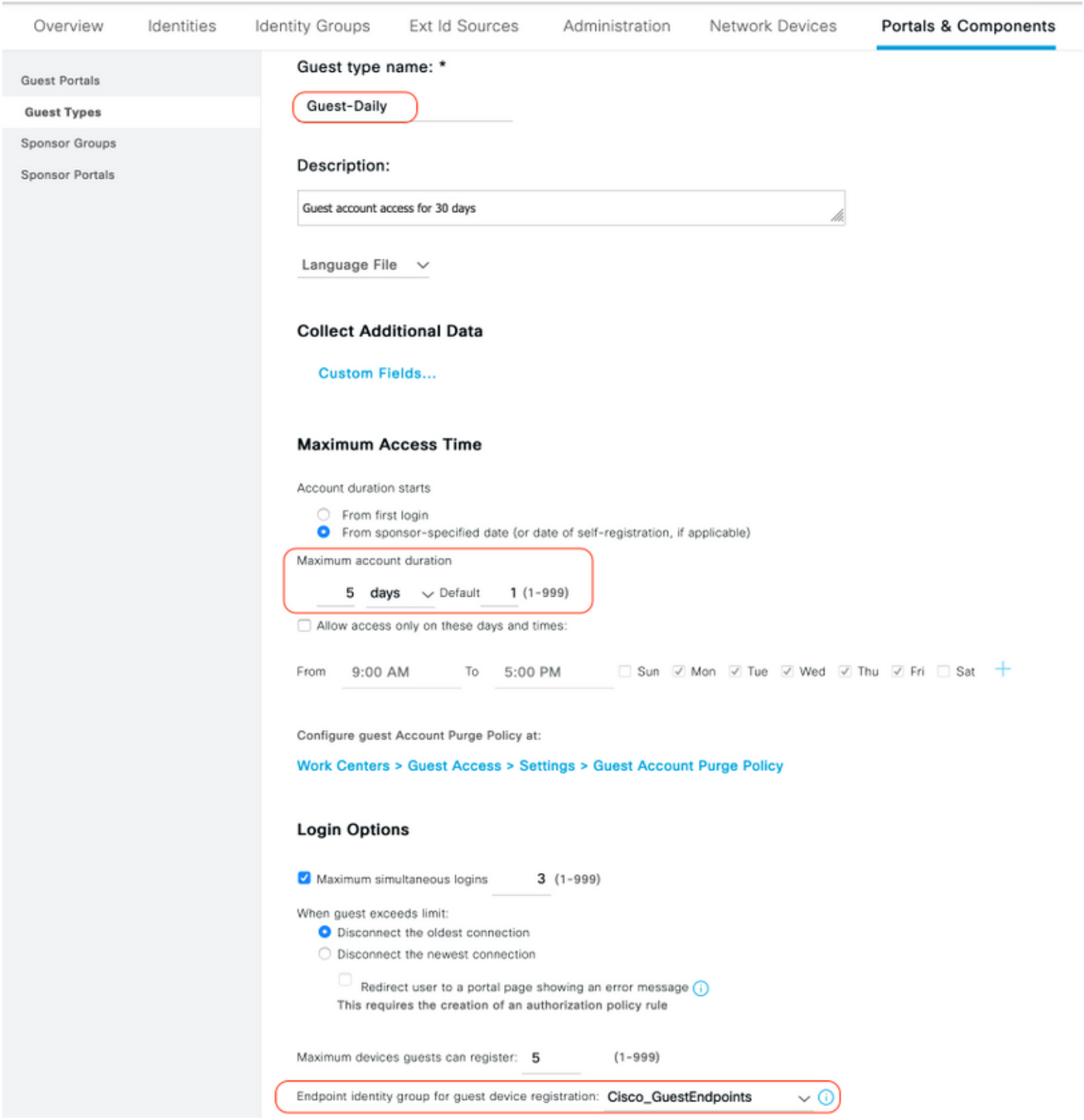
Hier is een voorbeeld voor GuestRedirect ACL (verkeer naar/van ISE moet worden uitgesloten van omleiding):

ISE

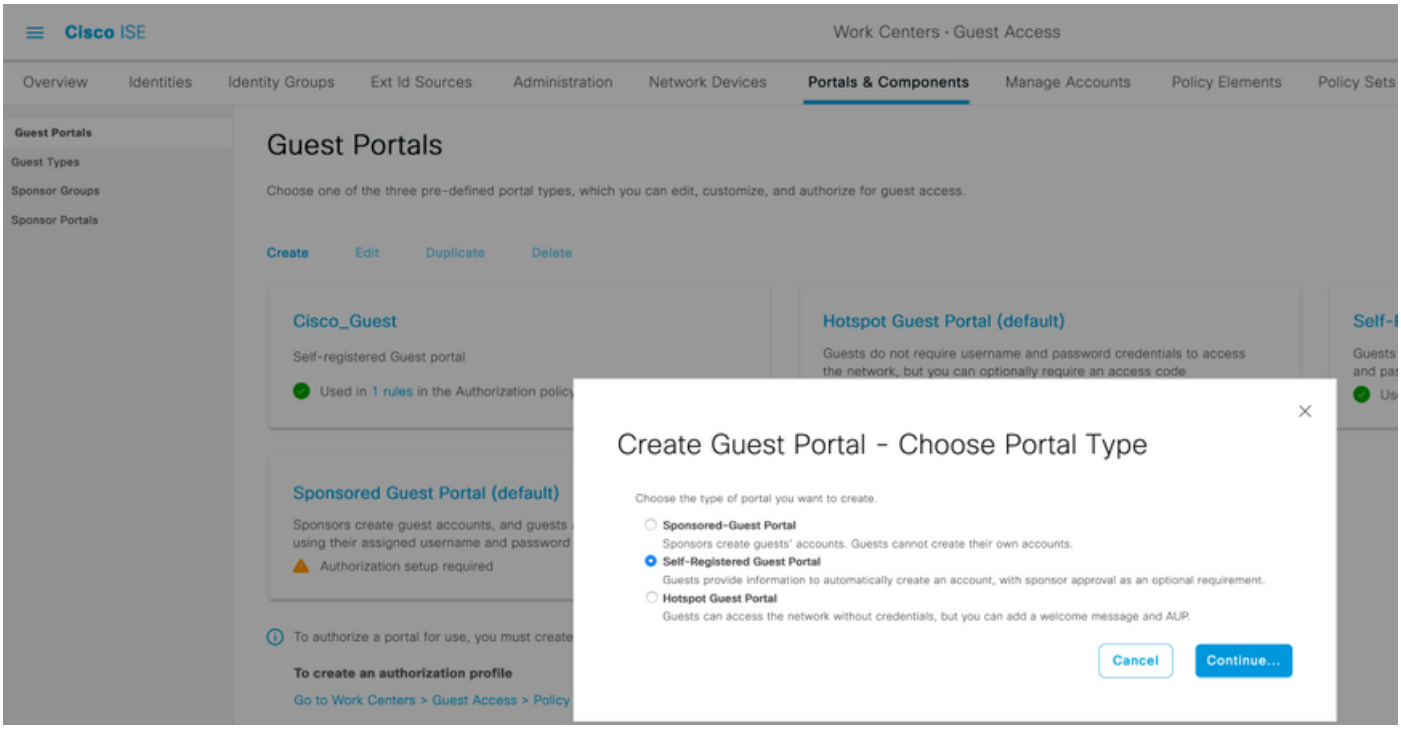
1. Voeg de WLC toe als een Network Access Device van **Work Centers > Guest Access > Network Devices**.
2. Een endpointgroep maken. Navigeren naar **werkcentra > Gasttoegang > Identiteitsgroepen > Endpoint Identity Groups.**



3. Maak een gastentype door te navigeren naar **werkcentra > Gasttoegang > Portal en componenten > Gasttypes.** Raadpleeg de eerder gemaakte Endpoint Identity Group onder dit nieuwe gasttype en Opslaan.



4. Maak een nieuw type gastenportal: Gastenportaal met eigen registratie. Navigeren naar **werkcentra > Gasttoegang > Gastenportalen.**

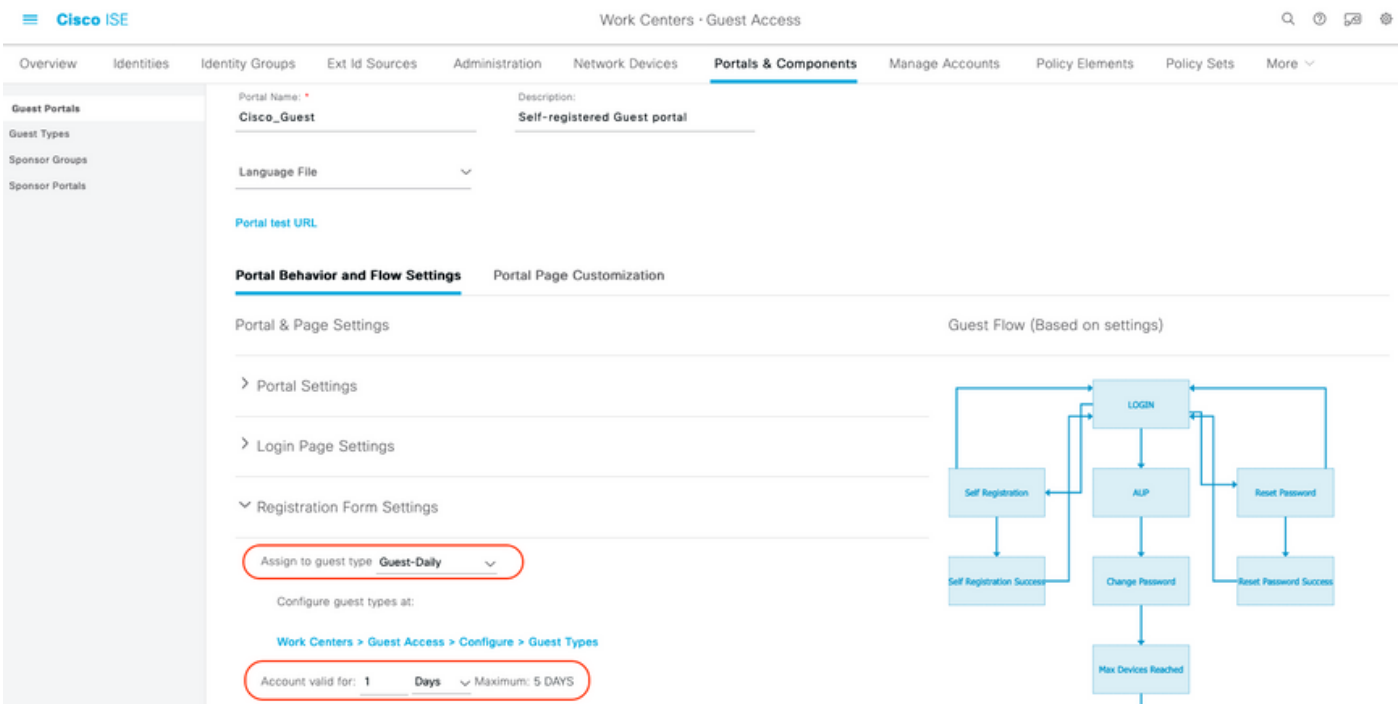


5. Kies de portaalnaam, verwijs naar het Gasttype dat eerder is gemaakt en verstuur de aanmeldingsinstellingen onder Registratieformulier instellingen om de aanmeldingsgegevens via e-mail te versturen.

Raadpleeg dit document over de configuratie van de SMTP-server op ISE:

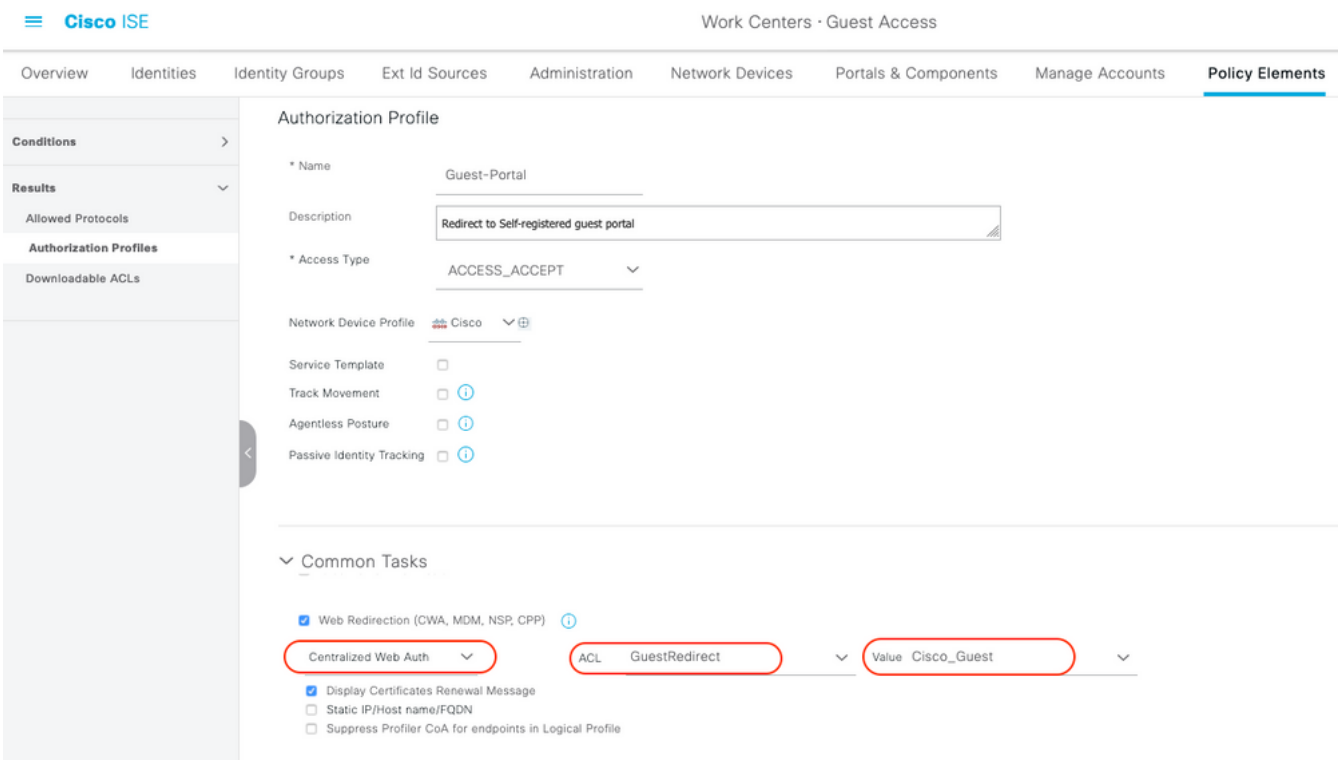
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

Standaardwaarde voor alle andere instellingen Onder Portal Page Personalisatie, kunnen alle pagina's die worden gepresenteerd worden aangepast. Standaard is het gastaccount 1 dag geldig en kan het worden uitgebreid naar het aantal dagen dat is ingesteld onder het specifieke gasttype.

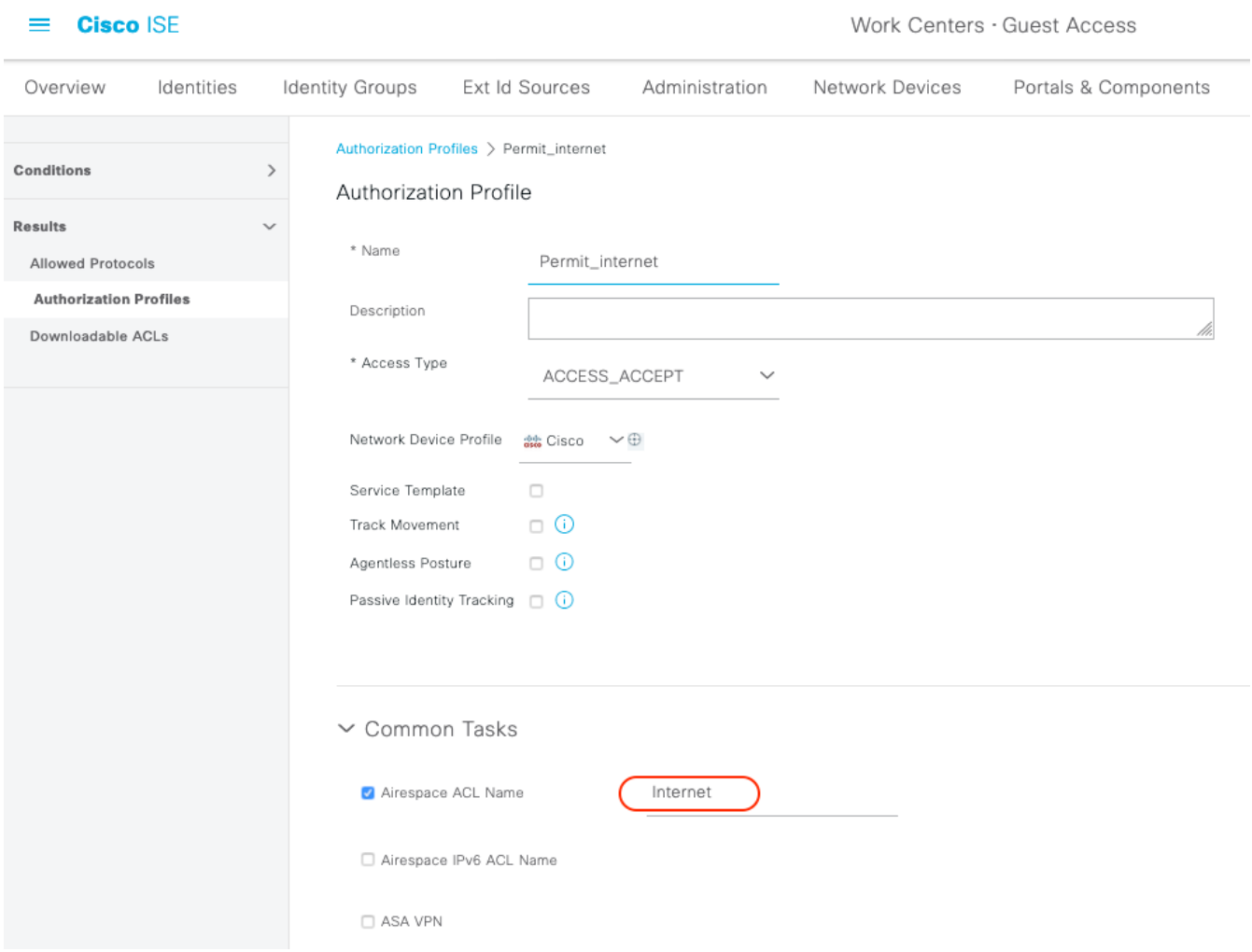


6. Configureer deze twee autorisatieprofielen door te navigeren naar **werkcentra > Toegang voor gasten > Beleidselementen > Resultaten > Autorisatieprofielen**.

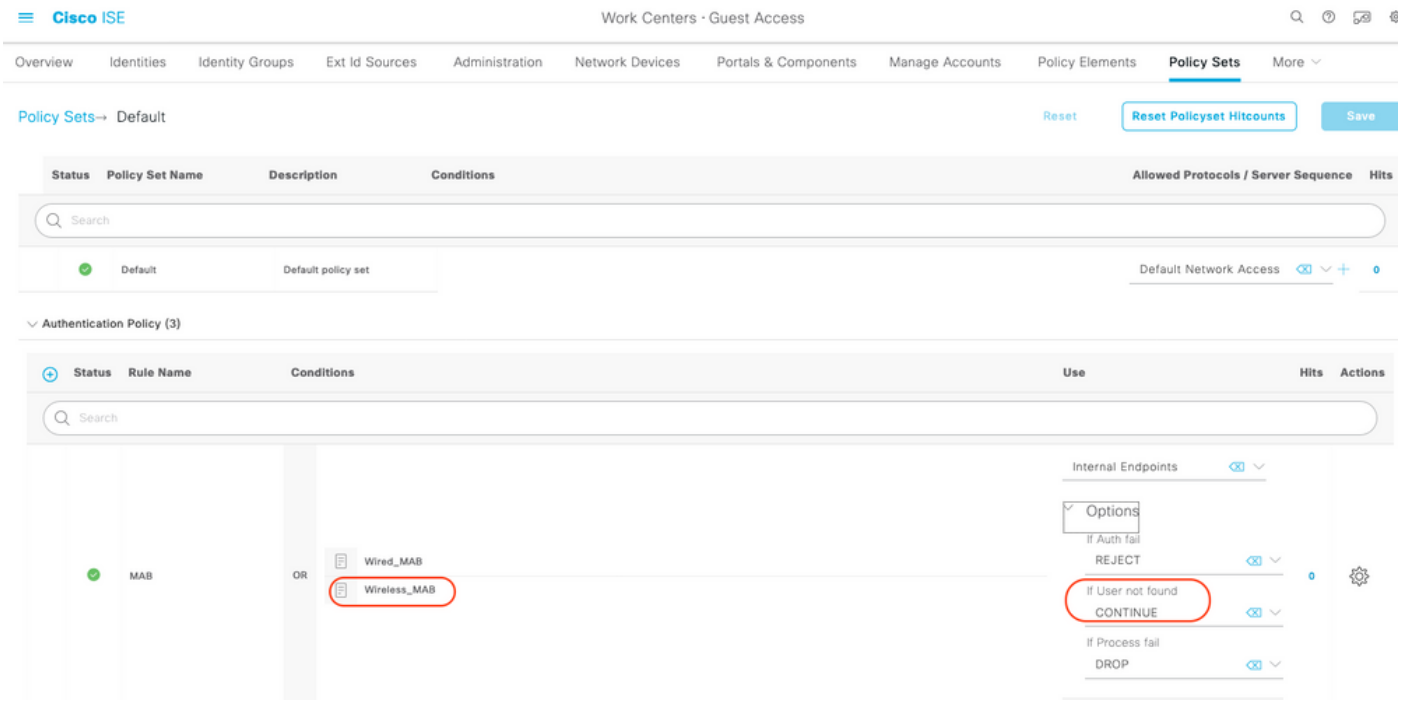
- Guest-Portal (met omleiding naar Guest portal **Cisco_Guest** en een Redirect ACL met de naam **GuestRedirect**). Deze GuestRedirect ACL is eerder gemaakt op WLC.



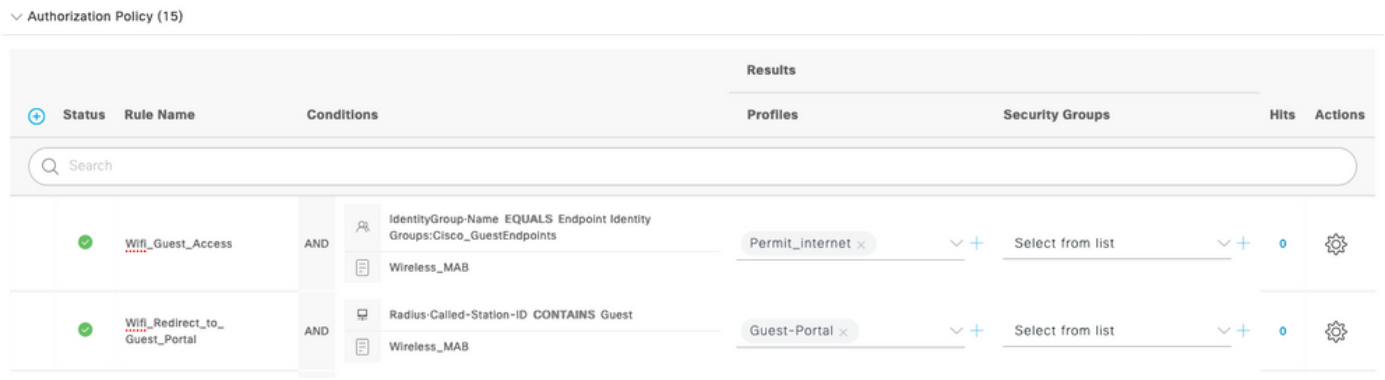
- Permit_Internet (met Airespace ACL gelijk internet)



7. Wijzig de Policy Set met de naam Default. De standaardbeleidsset is vooraf geconfigureerd voor toegang via het gastportal. Er is een **verificatiebeleid** met de naam MAB, waarmee de MAC-verificatie-omzeiling (MAB) voor een onbekend Mac-adres kan worden voortgezet (niet geweigerd).



8. Navigeer naar **het autorisatiebeleid** op dezelfde pagina. Maak deze autorisatieregels, zoals in deze afbeelding.



Nieuwe gebruikers wanneer associate met de Guest SSID zijn nog geen deel van een identiteitsgroep en dus overeenkomen met de tweede regel en worden doorgestuurd naar Guest Portal.

Nadat de gebruiker met succes inlogt, stuurt ISE een RADIUS CoA en voert WLC opnieuw verificatie uit. Ditmaal wordt de eerste autorisatieregel gematched (als eindpunt onderdeel wordt van een gedefinieerde endpointgroep) en krijgt de gebruiker een Permit_Internet autorisatieprofiel.

9. We kunnen ook tijdelijke toegang tot de gasten bieden door gebruik te maken van de voorwaarde Guest flow. Die voorwaarde controleert actieve zittingen op ISE en het wordt toegeschreven. Als die sessie het kenmerk heeft dat aangeeft dat de vorige gastgebruiker met succes geauthenticeerd heeft, wordt de voorwaarde aangepast. Nadat ISE de Radius Accounting Stop-melding ontvangt van Network Access Device (NAD), wordt de sessie beëindigd en later verwijderd. Op dat moment is de voorwaarde Network Access:UseCase = Guest Flow niet meer vervuld. Dientengevolge, raken alle verdere authentificaties van dat eindpunt generische regel die voor gastauthentificatie opnieuw richt.

> **Opmerking:** In een tijd, kunt u of de Tijdelijke Gasttoegang of de Permanente Gasttoegang maar niet beide gebruiken.

Raadpleeg dit document voor gedetailleerde informatie over de tijdelijke en permanente toegangsconfiguratie van ISE Guest.

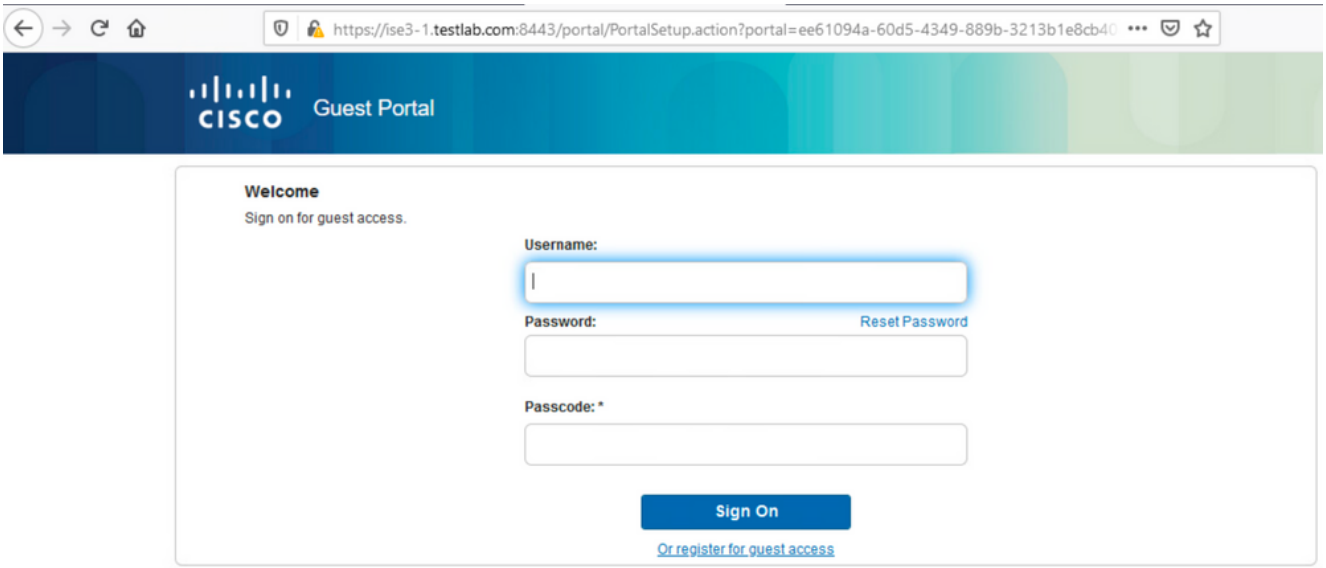
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html

Verifiëren

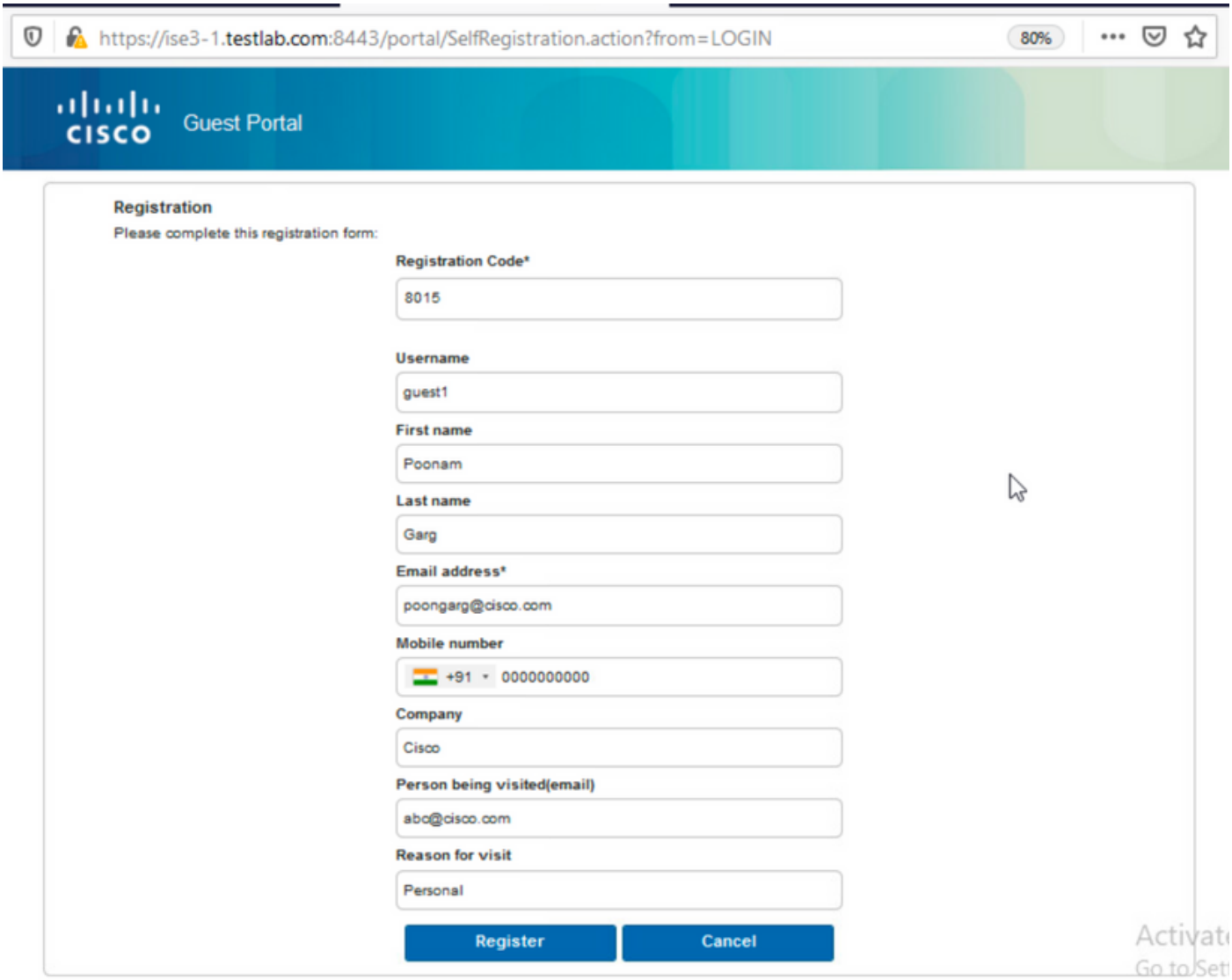
Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Nadat u met de Gast SSID associeert en een URL typt, wordt u doorgestuurd naar de Gast

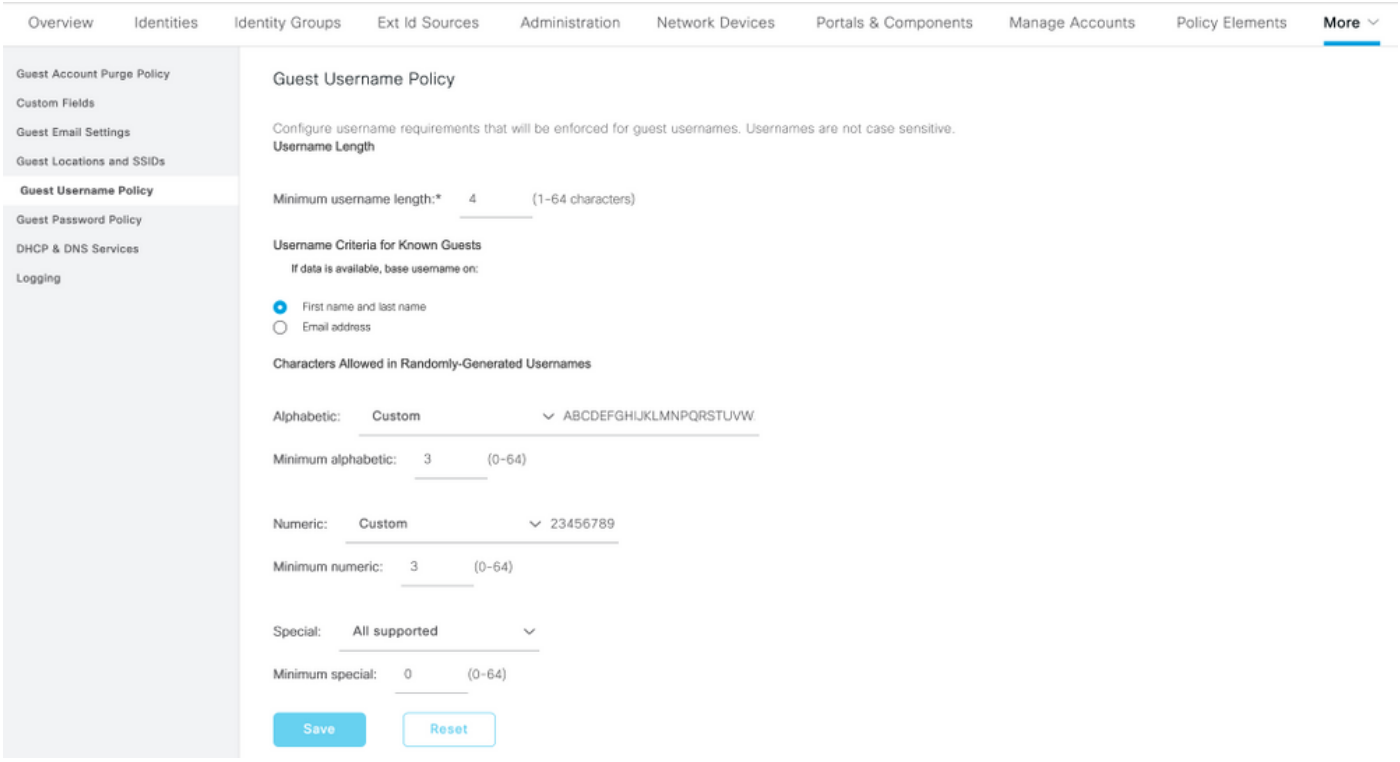
Portal pagina, zoals in de afbeelding.



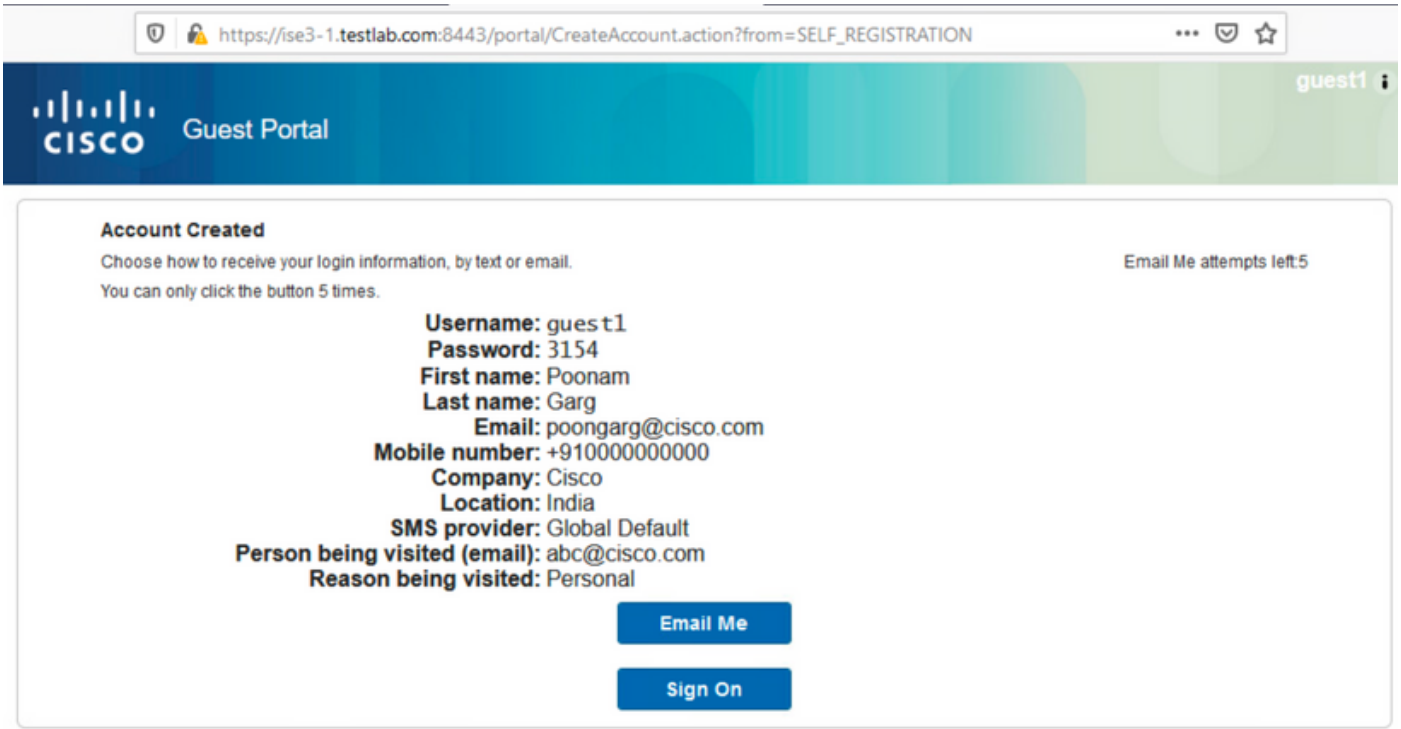
2. Aangezien u nog geen referenties hebt, moet u de optie **Register for Guest access** kiezen. U wordt met het registratieformulier getoond om de account aan te maken. Als de optie Registratiecode is ingeschakeld onder de configuratie van de Guest Portal, dan is die geheime waarde vereist (dit zorgt ervoor dat alleen mensen met de juiste rechten zichzelf mogen registreren).

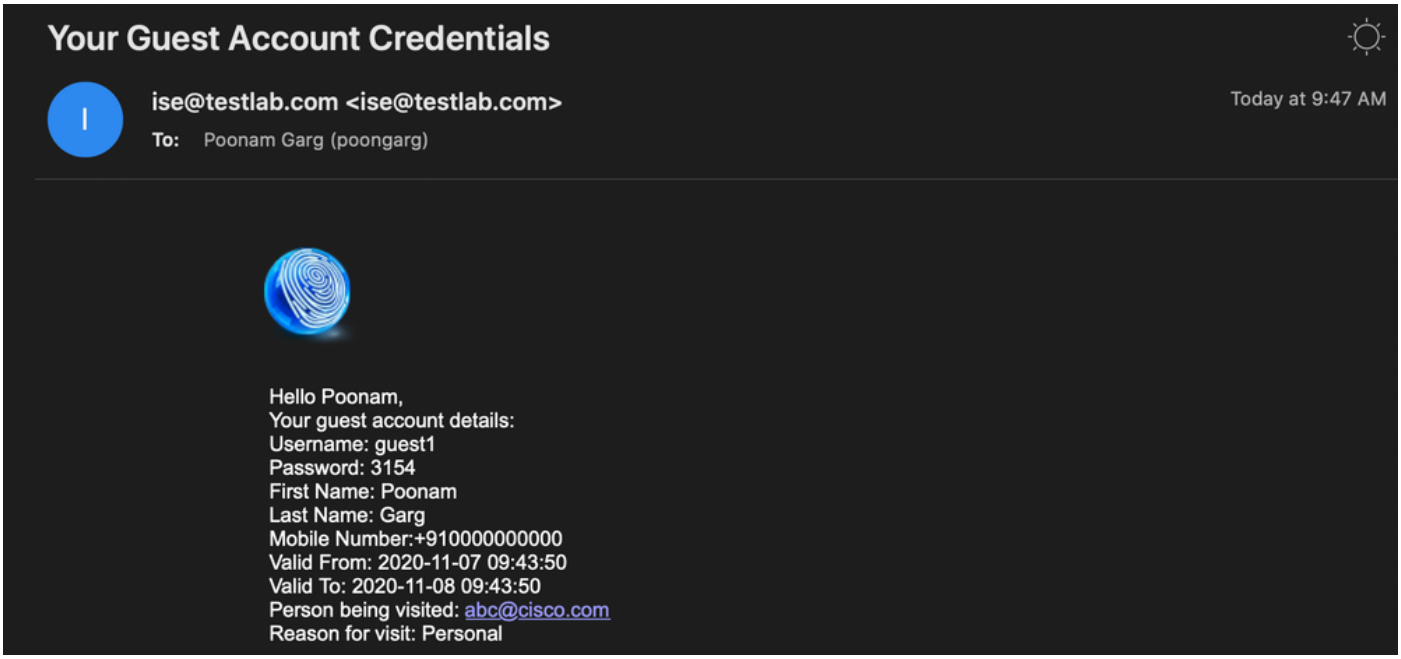


3. Als er problemen zijn met het wachtwoord of het gebruikersbeleid, navigeer dan naar **Workcentres > Guest Access > Instellingen > Gebruikersbeleid voor het gast** om de instellingen te wijzigen. Hierna volgt een voorbeeld:

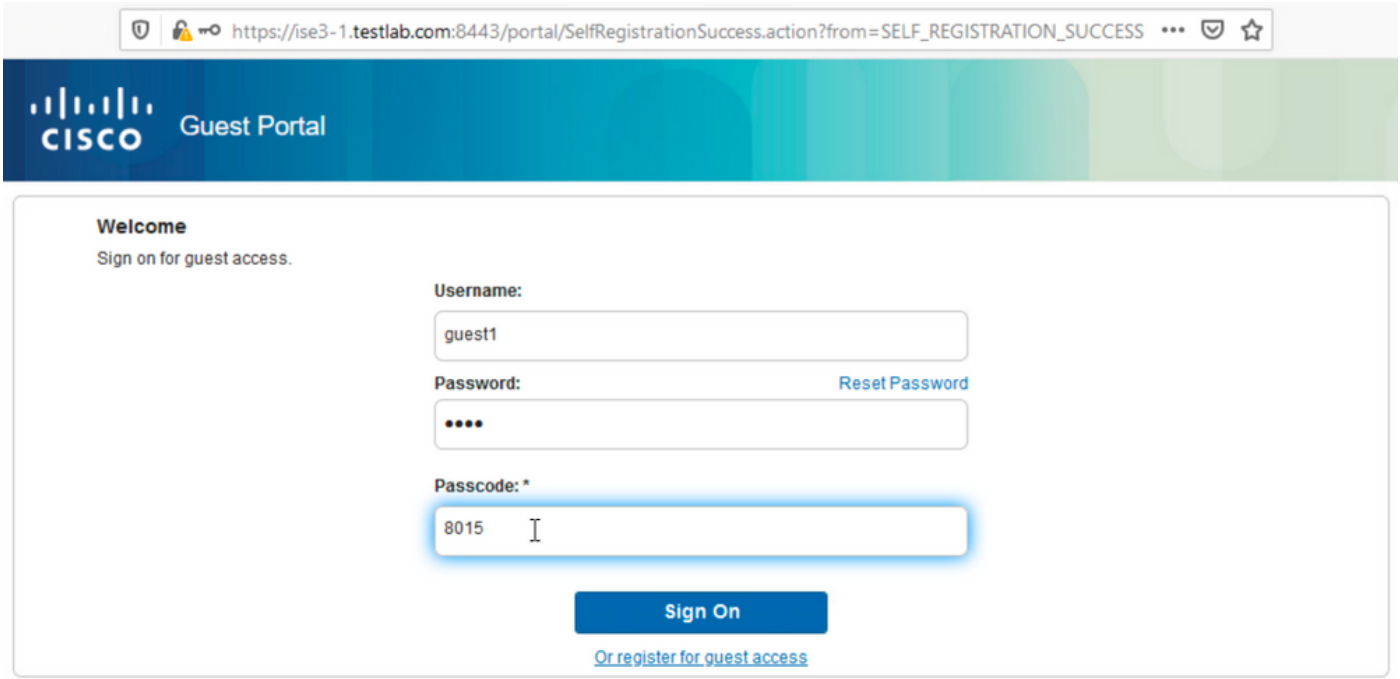


4. Na een succesvolle account aanmaken, krijgt u aanmeldingsgegevens (wachtwoord gegenereerd volgens het beleid van het gastwachtwoord). Ook de gastgebruiker krijgt het e-mailbericht als het is geconfigureerd:

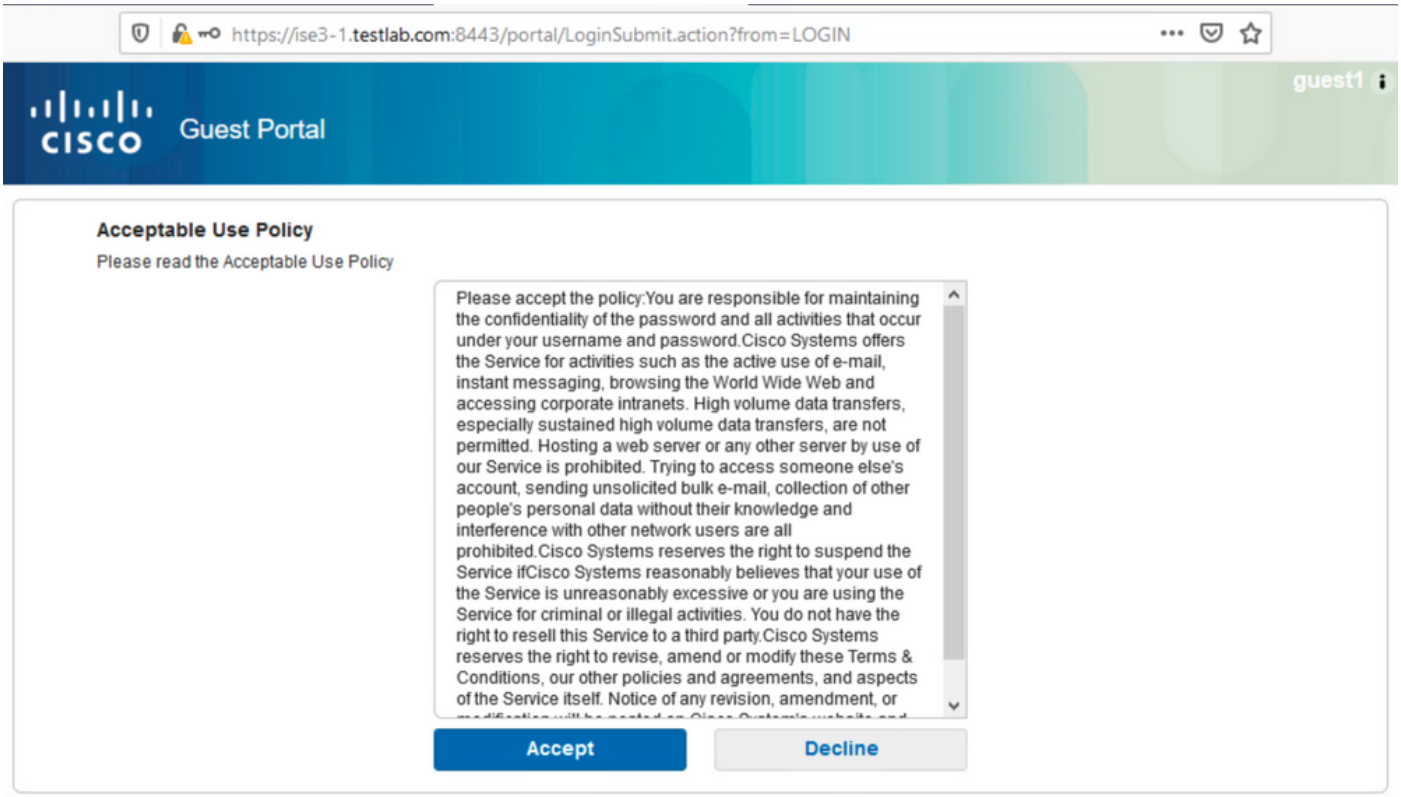


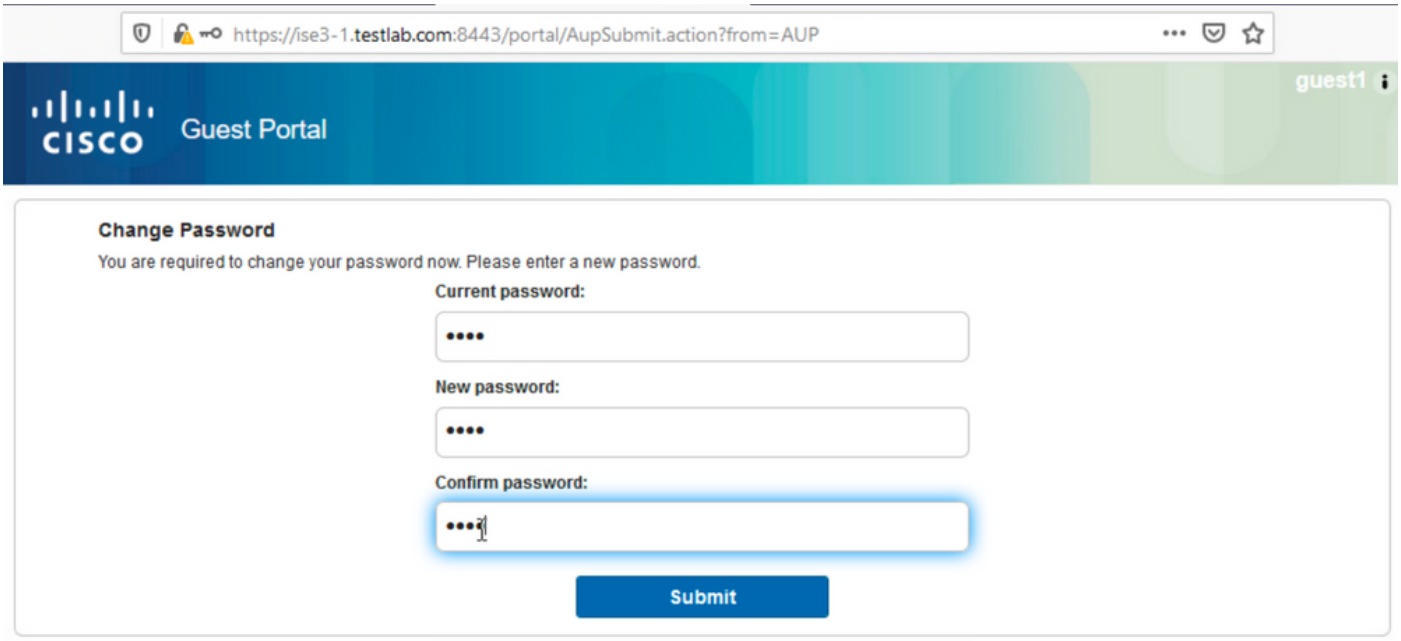


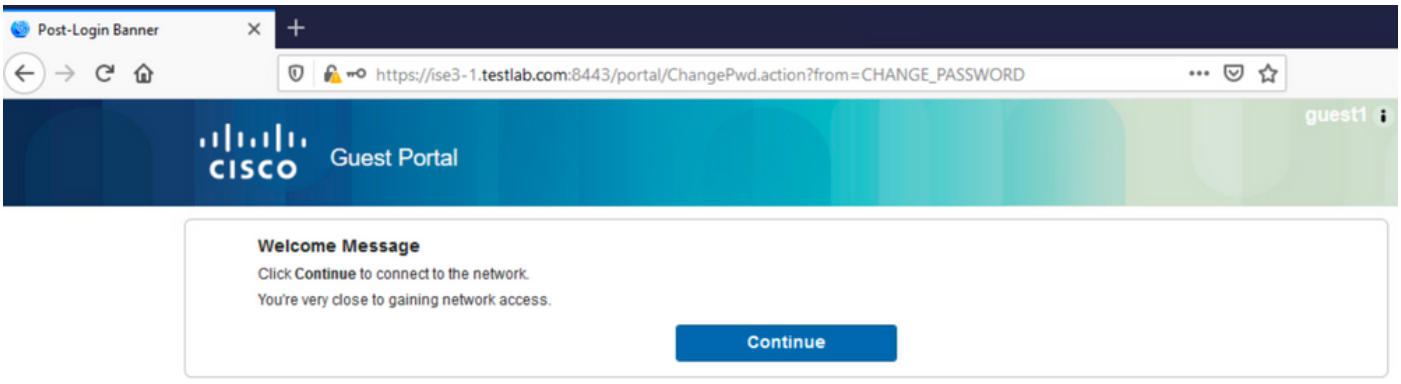
5. Klik op **Sign On** en geef aanmeldingsgegevens op (extra toegangscode kan worden vereist indien geconfigureerd onder het Gastenportaal; dit is een ander beveiligingsmechanisme dat alleen degenen die het wachtwoord kennen in staat stelt in te loggen).



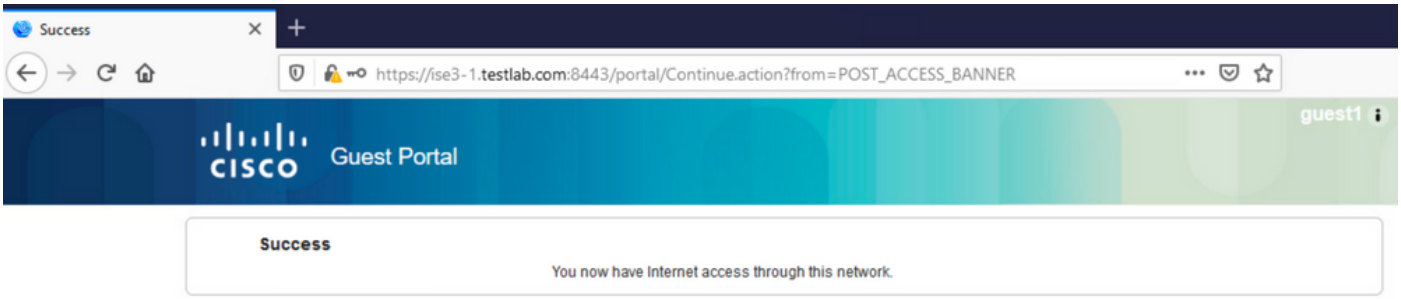
6. Indien geslaagd, kan een optioneel beleid voor acceptabel gebruik (AUP) worden gepresenteerd (indien geconfigureerd onder het gastportaal). De gebruiker wordt voorgesteld met een optie van het veranderingswachtwoord en de Post-Login Banner (ook configureerbaar onder het Portaal van de Gast) kan ook tonen.







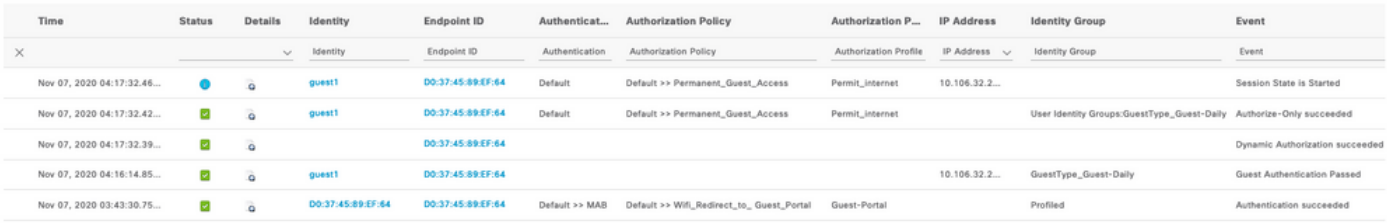
7. Op de laatste pagina (Post-Login Banner) wordt bevestigd dat toegang is verleend:



Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

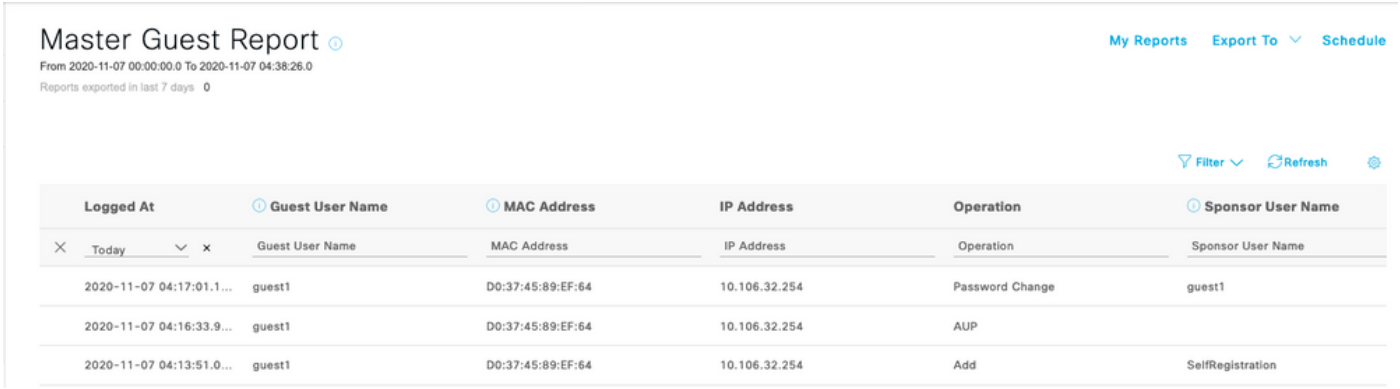
In deze fase presenteert ISE deze logboeken onder **Operations > RADIUS > Live Logs**, zoals in de afbeelding.



Hier is de flow:

- De gastgebruiker komt de tweede autorisatieregel tegen (Wifi_Redirect_to_Guest_Portal) en wordt doorgestuurd naar Guest-Portal (**Auhentication succeeded**).
- De gast wordt omgeleid voor zelfregistratie. Na succesvolle aanmelding (met de nieuwe account) stuurt ISE de CoA Reauthenticate, die wordt bevestigd door de WLC (**Dynamic Authorisation succeeded**).
- De WLC voert herverificatie uit met het kenmerk Alleen autoriseren en de ACL-naam wordt geretourneerd (**alleen autoriseren geslaagd**). De gast krijgt de juiste netwerktoegang.

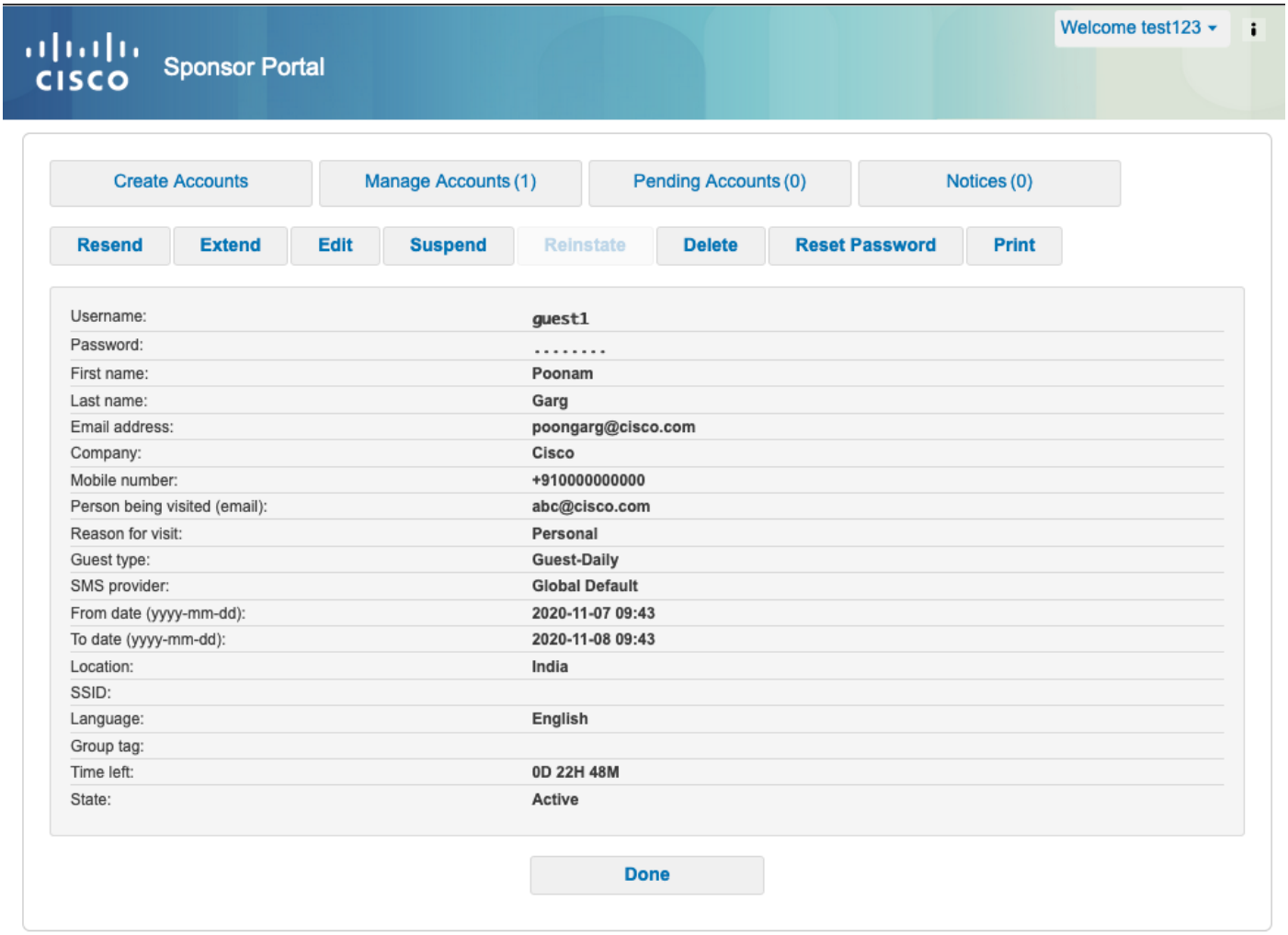
Rapporten (**Operations > Reports > Guest > Master Guest Report**) bevestigt ook dat:



Een sponsor-gebruiker (met de juiste rechten) kan de huidige status van een gastgebruiker verifiëren.

Dit voorbeeld bevestigt dat de account is aangemaakt en dat de gebruiker is aangemeld bij het

portal:



Optionele configuratie

Voor elke fase van deze stroom kunnen verschillende opties worden geconfigureerd. Dit alles is ingesteld volgens de Guest Portal op **Work Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settings**. Belangrijkste instellingen zijn:

Instellingen voor zelfregistratie

- Gasttype - Beschrijft hoe lang de account actief is, opties voor het verlopen van wachtwoorden, aanmeldingstijden en opties (dit is een combinatie van tijdprofiel en gastenrol)
- Registratiecode - Indien ingeschakeld, mogen alleen gebruikers die de geheime code kennen zich zelf registreren (moet het wachtwoord opgeven wanneer de account wordt aangemaakt)
- AUP - Beleid voor gebruik tijdens zelfregistratie accepteren
- De verplichting voor de sponsor om het gastaccount goed te keuren/te activeren.

Aanmelden als gast

- Toegangscode - Indien ingeschakeld, mogen alleen gastgebruikers die de geheime code kennen, inloggen.
- AUP - Accepteer het gebruiksbeleid tijdens de zelfregistratie.

- Wachtwoordwijziging.

Instellingen voor apparaatregistratie

- Het apparaat wordt standaard automatisch geregistreerd.

Instellingen voor naleving van gastapparaat

- Laat een houding binnen de stroom toe.

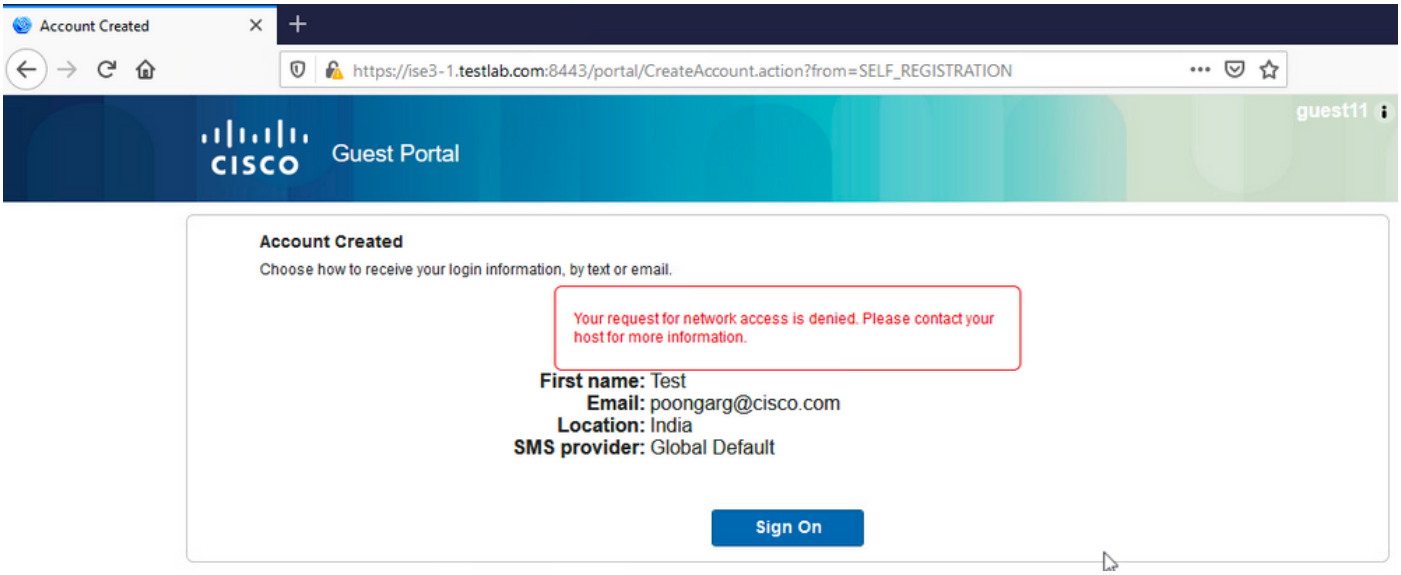
BYOD-instellingen

- Hiermee kunnen zakelijke gebruikers die de portal gebruiken als gasten hun persoonlijke apparaten registreren.

Door sponsor goedgekeurde accounts

Als de optie **Vergen dat gasten worden goedgekeurd** is geselecteerd onder **Instellingen voor registratieformulier**, dan moet de account die door de gast is aangemaakt worden goedgekeurd door een sponsor. Deze functie kan e-mail gebruiken om een melding aan de sponsor te sturen (voor een gastaccount goedkeuring):

Als de Simple Mail Transfer Protocol (SMTP)-server verkeerd is geconfigureerd, dan wordt de account niet aangemaakt:

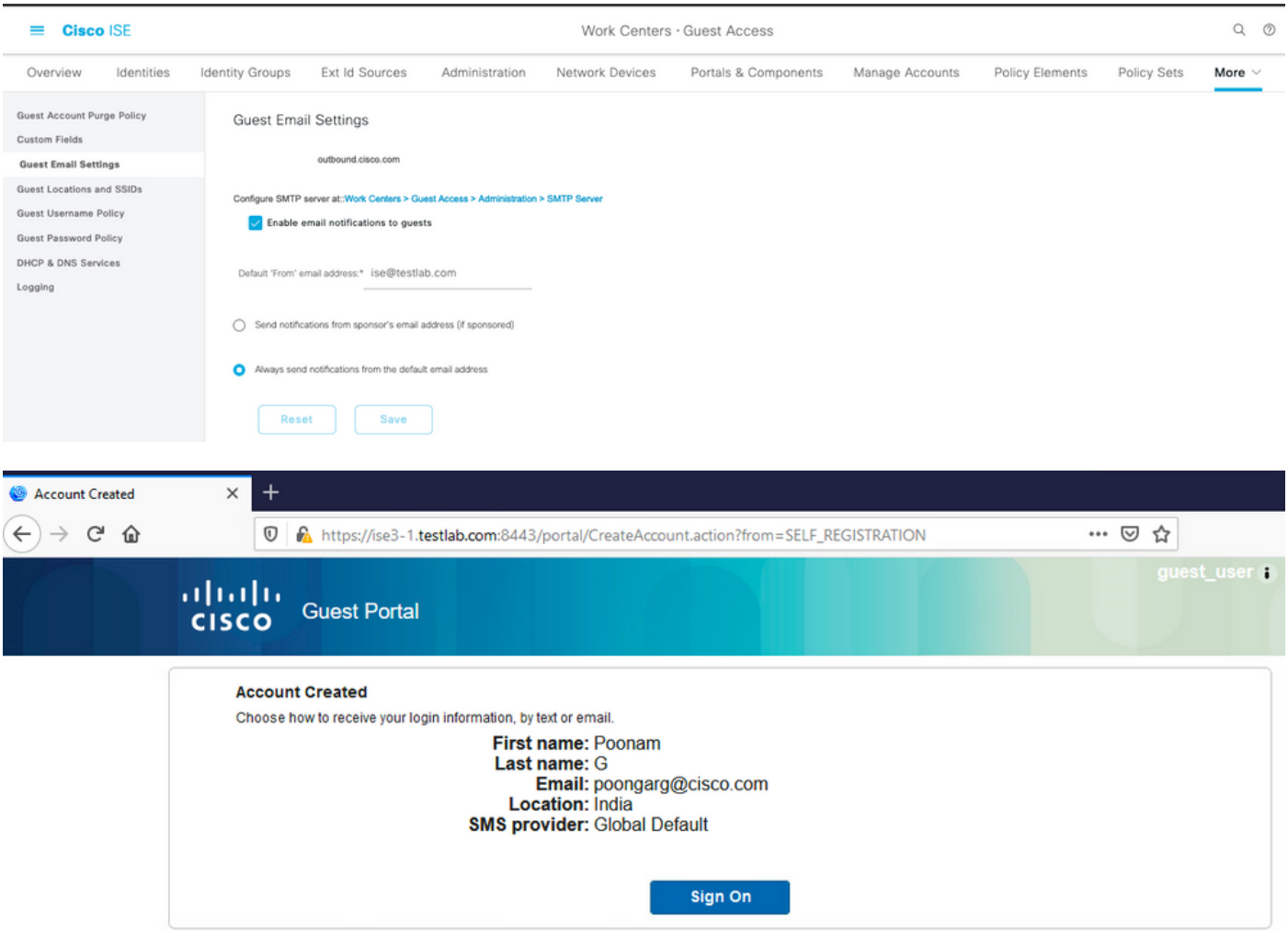


Het logbestand van guest.log bevestigt dat er een probleem is met het verzenden van een goedkeuringsbericht naar de sponsor e-mail omdat de SMTP-server verkeerd is geconfigureerd:

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][]
cpm.guestaccess.apiservices.util.SmtpMsgRetryThreadUtil -::- An exception occurred while sending
email :
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25,
response: 421
```

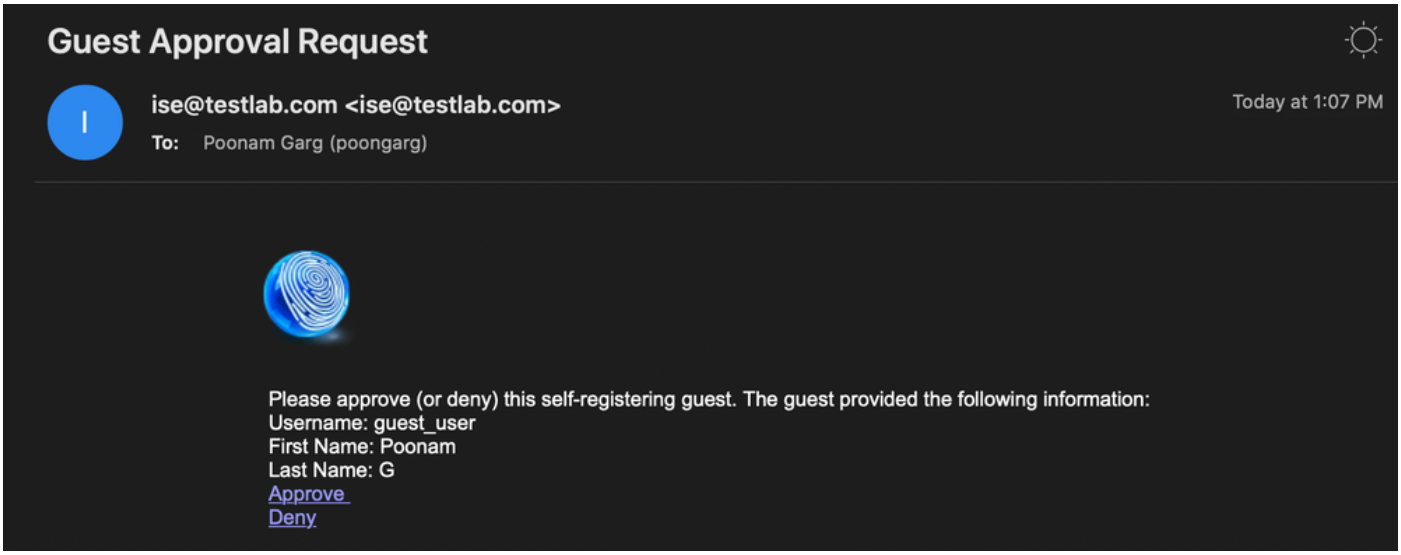
```
2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][]
cpm.guestaccess.apiservices.notification.NotificationService -::- sendApprovalNotification
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException:
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: Unable to send mail. Failure
occured
```

Wanneer u de juiste e-mail- en SMTP-serverconfiguratie hebt, wordt de account aangemaakt:



Nadat u de optie **Vereist dat gasten worden goedgekeurd**, worden de velden voor gebruikersnaam en wachtwoord automatisch verwijderd uit de sectie **Deze informatie opnemen op de** pagina **voor** zelfregistratie. Dit is waarom, wanneer de goedkeuring van de sponsor wordt vereist, de geloofsbrieven voor gastgebruikers niet door gebrek op de Web-pagina worden getoond die informatie voorstelt om aan te tonen dat de rekening is gemaakt. In plaats daarvan moeten ze worden geleverd via Short Message Services (SMS) of per e-mail. Deze optie moet worden ingeschakeld in het **aanmeldingsformulier Verzenden na goedkeuring via** sectie (e-mail/sms markeren).

Aan de sponsor wordt een e-mail met de melding gestuurd:



De sponsor klikt op de Goedkeuringslink en logt in op het Sponsor-portal en de account is goedgekeurd:

Vanaf dit punt mag de gastgebruiker inloggen (met de aanmeldingsgegevens die per e-mail of sms worden ontvangen).

Samengevat, zijn er drie e-mailadressen die in deze stroom worden gebruikt:

- Bericht "Van" adres. Dit wordt statisch gedefinieerd of uit de sponsor-account gehaald en gebruikt als het Van-adres voor zowel: kennisgeving aan de sponsor (ter goedkeuring) en de geloofsbrieven aan de gast. Dit wordt ingesteld onder **Work Centers > Guest Access > Settings > Guest Email Settings**.

- Bericht "Aan" adres. Dit wordt gebruikt om de sponsor ervan in kennis te stellen dat hij een rekening voor goedkeuring heeft ontvangen. Dit is ingesteld in de Guest Portal onder **Work Centers > Guest Access > Guest Portals > Portals en Componenten > Portal Name > Registerformulier Settings > Vereist dat gasten worden goedgekeurd > E-mail goedkeuring aanvraag aan**.

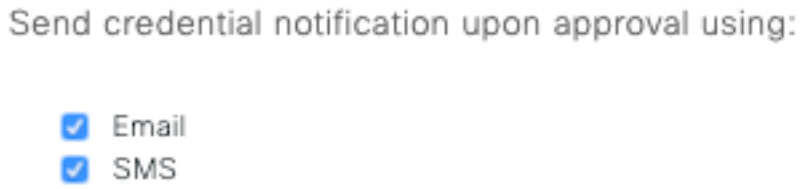
- Gast "Aan" adres. Dit wordt door de gastgebruiker tijdens de registratie verstrekt. Als **Credentials melding verzenden bij goedkeuring via E-mail** is geselecteerd, wordt de e-mail met credentiële details (gebruikersnaam en wachtwoord) aan de gast geleverd.

Credentials leveren via sms

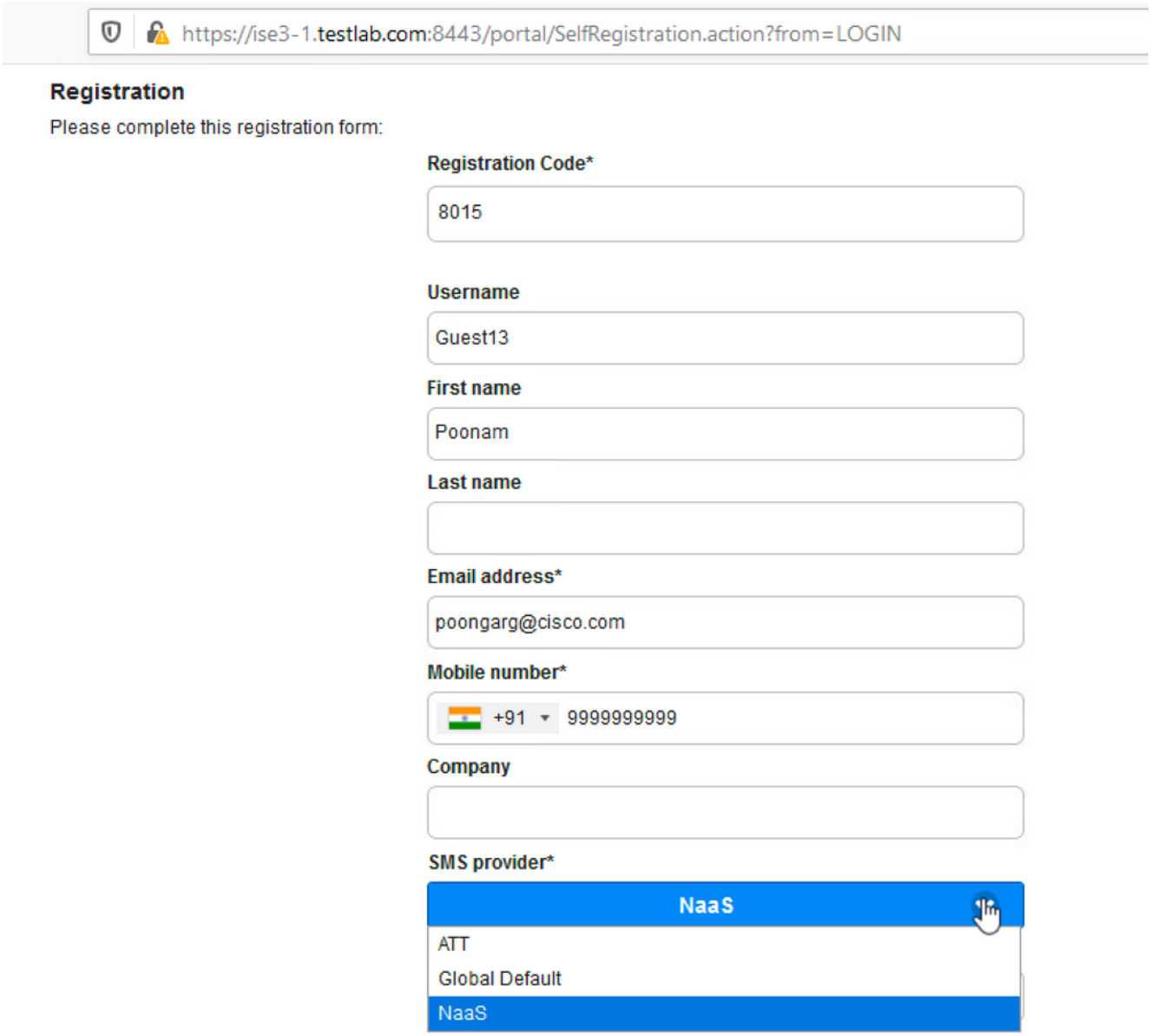
Gastreferenties kunnen ook worden geleverd via SMS. Deze opties moeten worden geconfigureerd:

1. Kies de SMS-serviceprovider onder Instellingen registratieformulier:

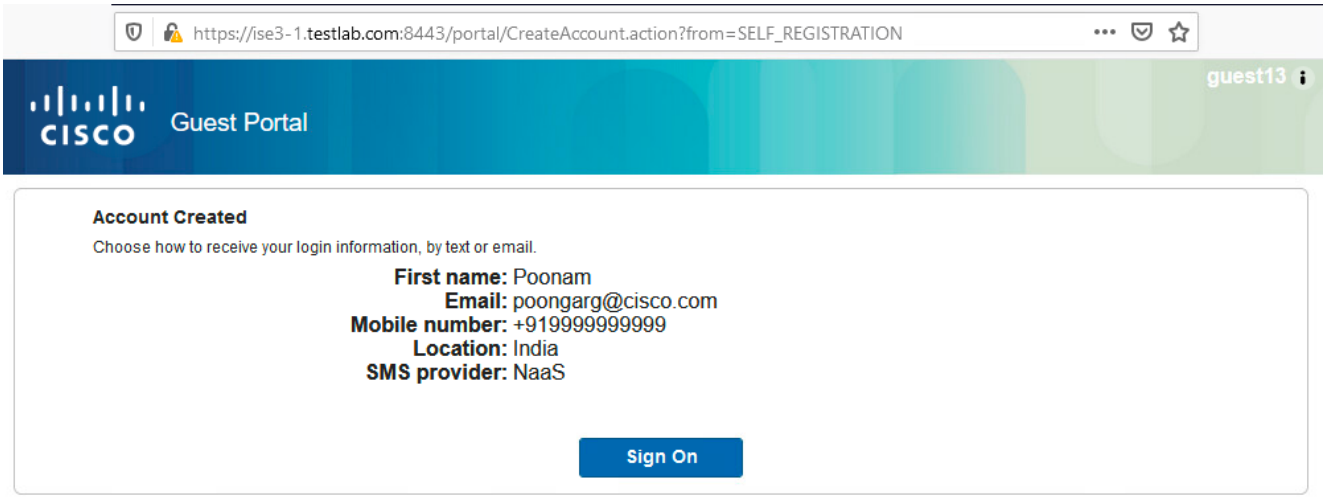
2. Controleer het **aanmeldingsformulier Verzenden bij goedkeuring met: SMS** aanvinkvakje.



3. Vervolgens wordt de gastgebruiker gevraagd om de beschikbare provider te kiezen wanneer hij een account aanmaakt:



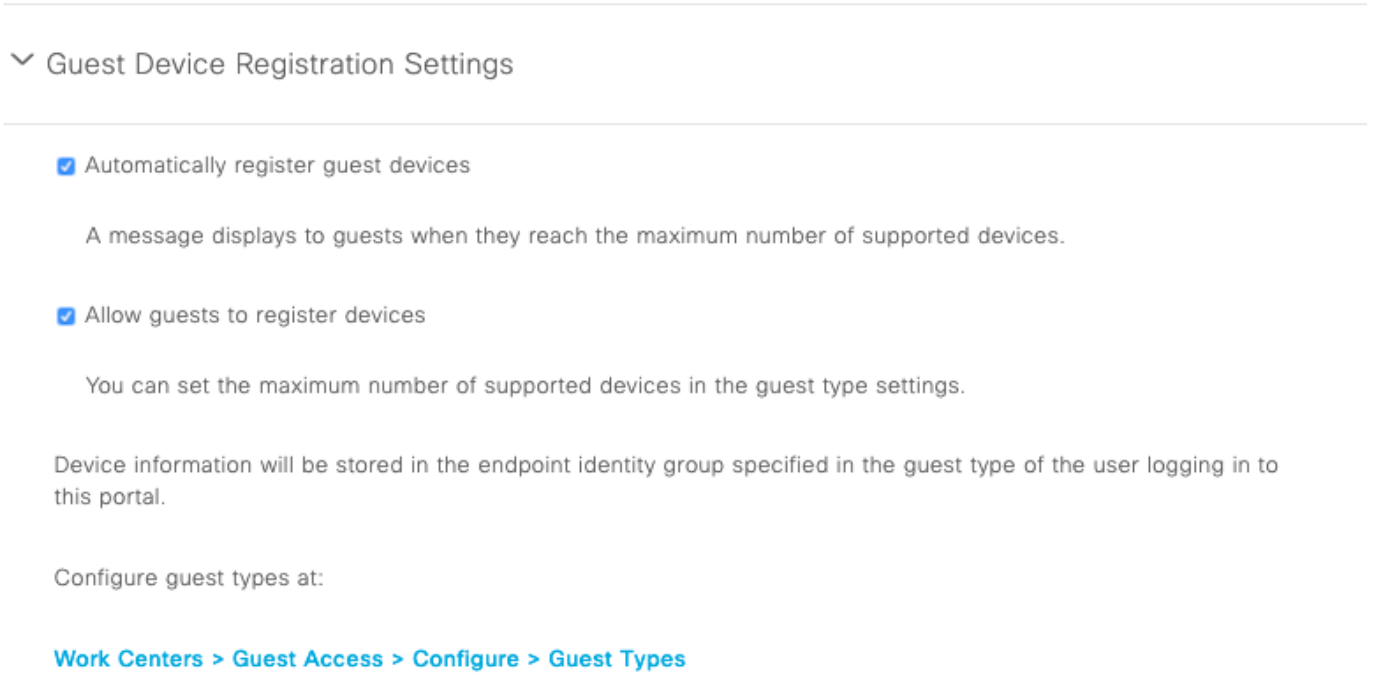
4. Een SMS wordt geleverd met de gekozen provider en telefoonnummer:

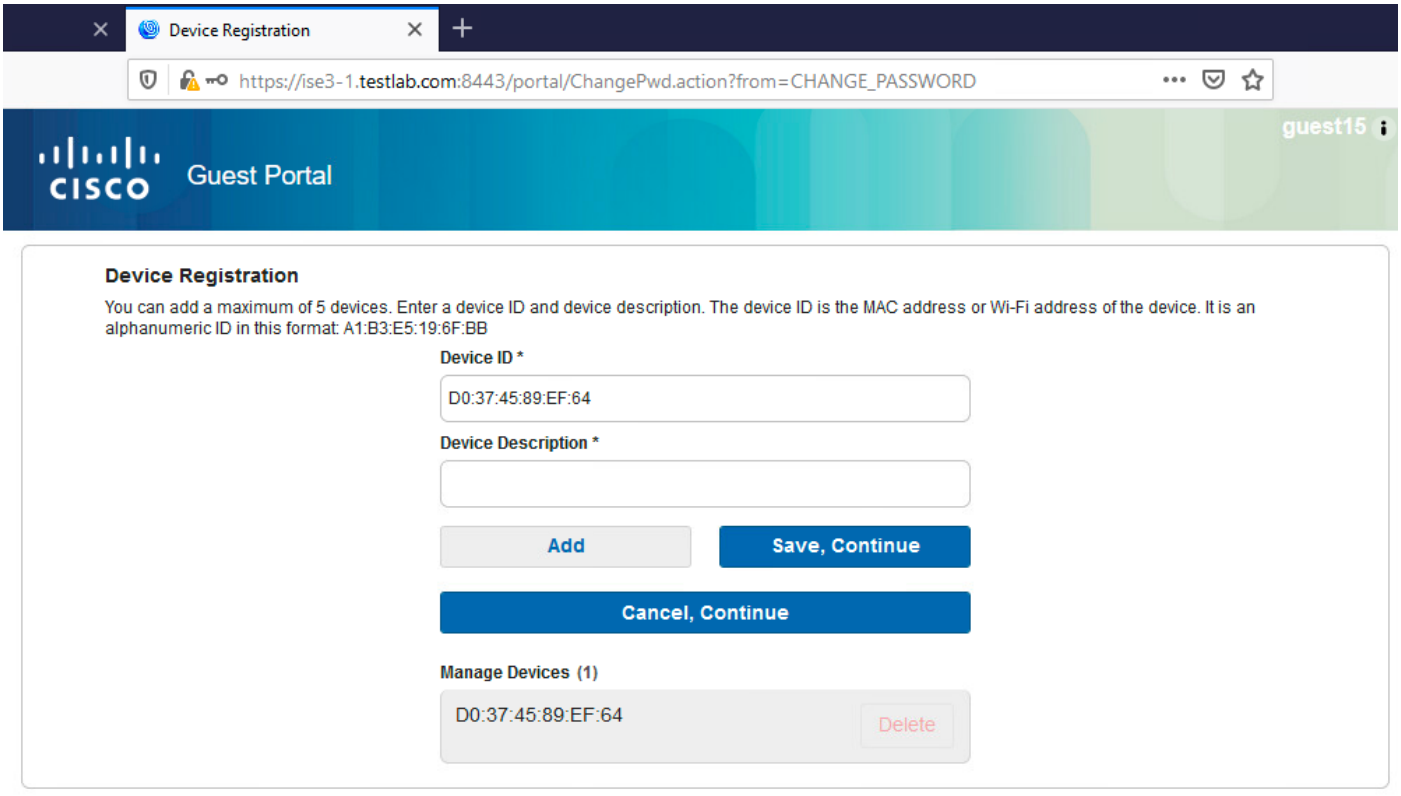


5. U kunt SMS-providers configureren onder **Beheer > Systeem > Instellingen > SMS Gateway**.

Apparaatregistratie

Als de optie **Toestaan gasten om apparaten te registreren** is geselecteerd nadat een gastgebruiker inlogt en de AUP accepteert, kunt u apparaten registreren:





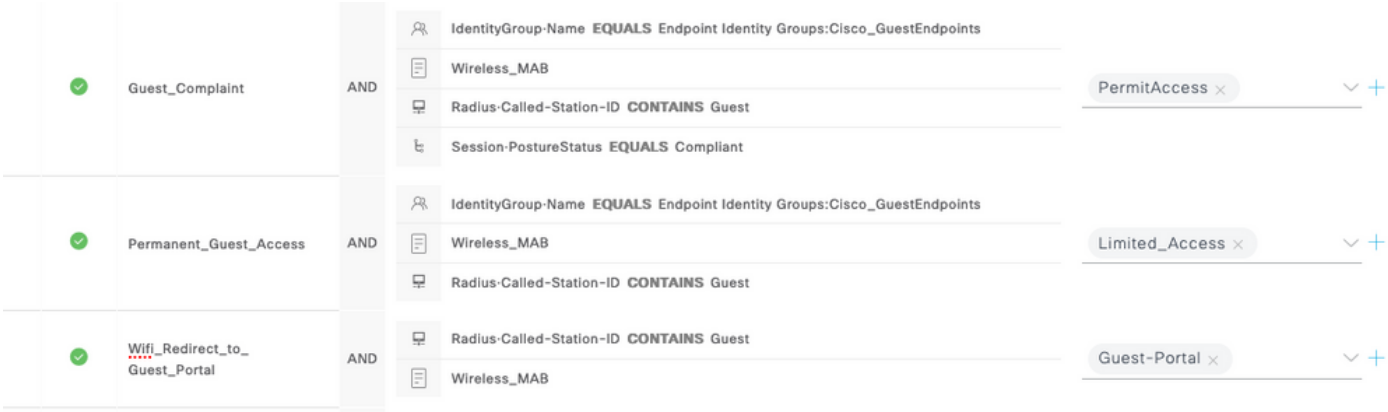
Bericht dat het apparaat al automatisch is toegevoegd (het staat in de lijst Apparaten beheren). Dit komt doordat **gastapparaten automatisch registreren** is geselecteerd.

houding

Als de optie **Naleving van gastapparaat vereisen** is geselecteerd, dan zijn gastgebruikers voorzien van een Agent die de houding (NAC/Web Agent) uitvoert nadat zij inloggen en de AUP accepteren (en naar keuze apparaatregistratie uitvoeren). ISE verwerkt regels voor clientprovisioning om te

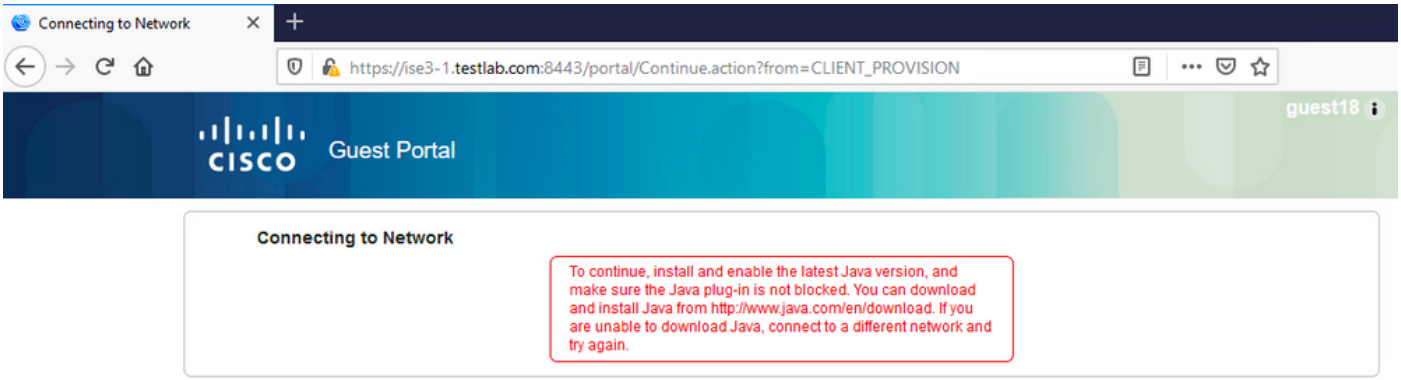
beslissen welke agent moet worden provisioneerd. Dan voert de Agent die op het station loopt de postuur uit (volgens Posture regels) en stuurt resultaten naar de ISE, die de CoA reauthenticate om de autorisatiestatus te veranderen indien nodig.

Mogelijke vergunningsregels kunnen er ongeveer zo uitzien:



De eerste nieuwe gebruikers die te maken krijgen met de regel Guest_Authenticate gaan terug naar de Self Register Guest portal. Nadat de gebruiker zich heeft aangemeld en inlogt, verandert CoA de autorisatiestatus en krijgt de gebruiker beperkte toegang om de houding en de remediëring uit te voeren. Pas nadat de NAC Agent is voorzien en het station voldoet aan de eisen verandert CoA autorisatiestatus nogmaals om toegang tot het internet te bieden.

De typische problemen met houding omvatten gebrek aan correcte regels van de Clientprovisioning:



Dit kan ook worden bevestigd als u het bestand **guest.log** onderzoekt:

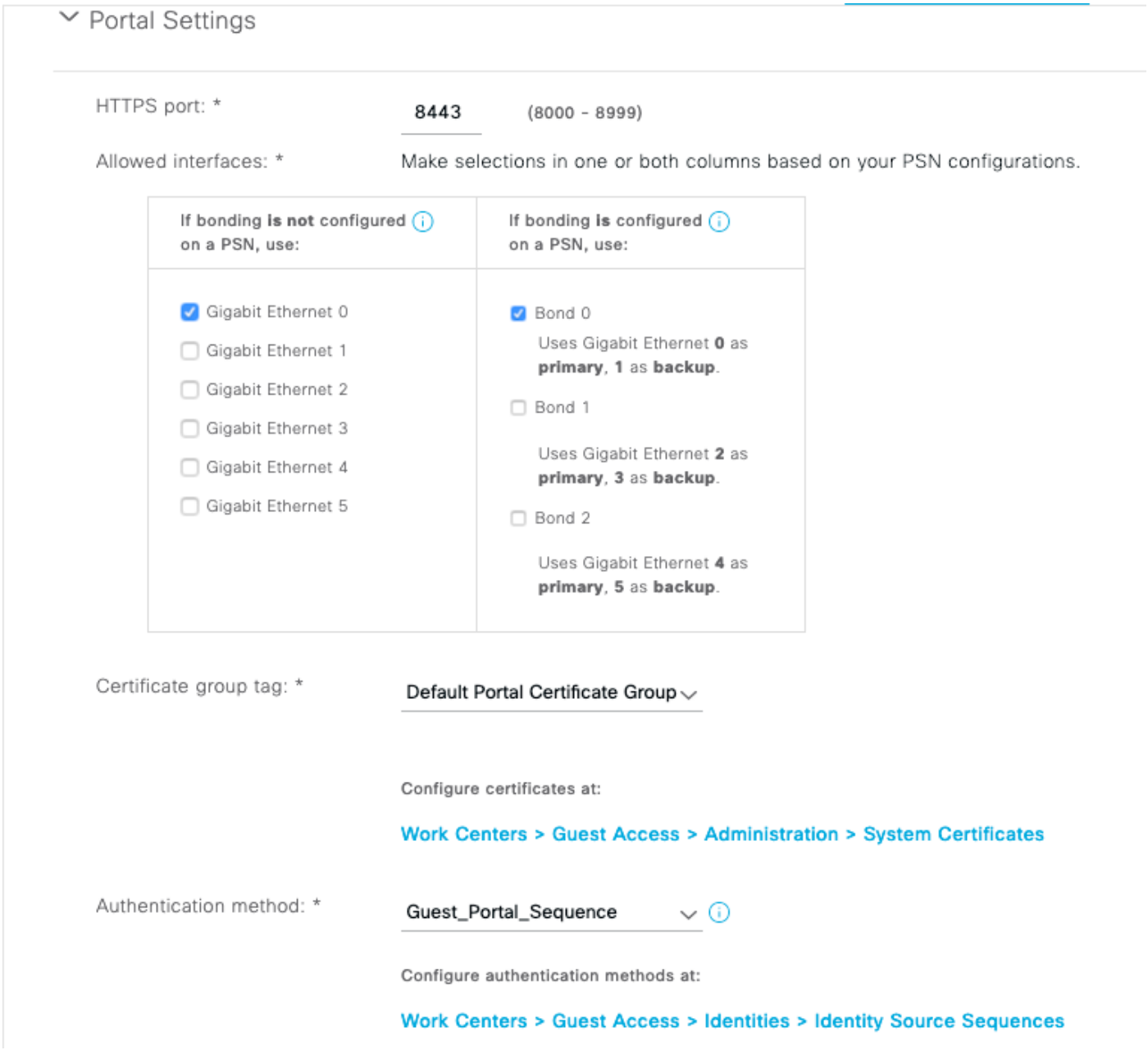
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:guest18:- CP Response is not
successful, status=NO_POLICY
```

BYOD

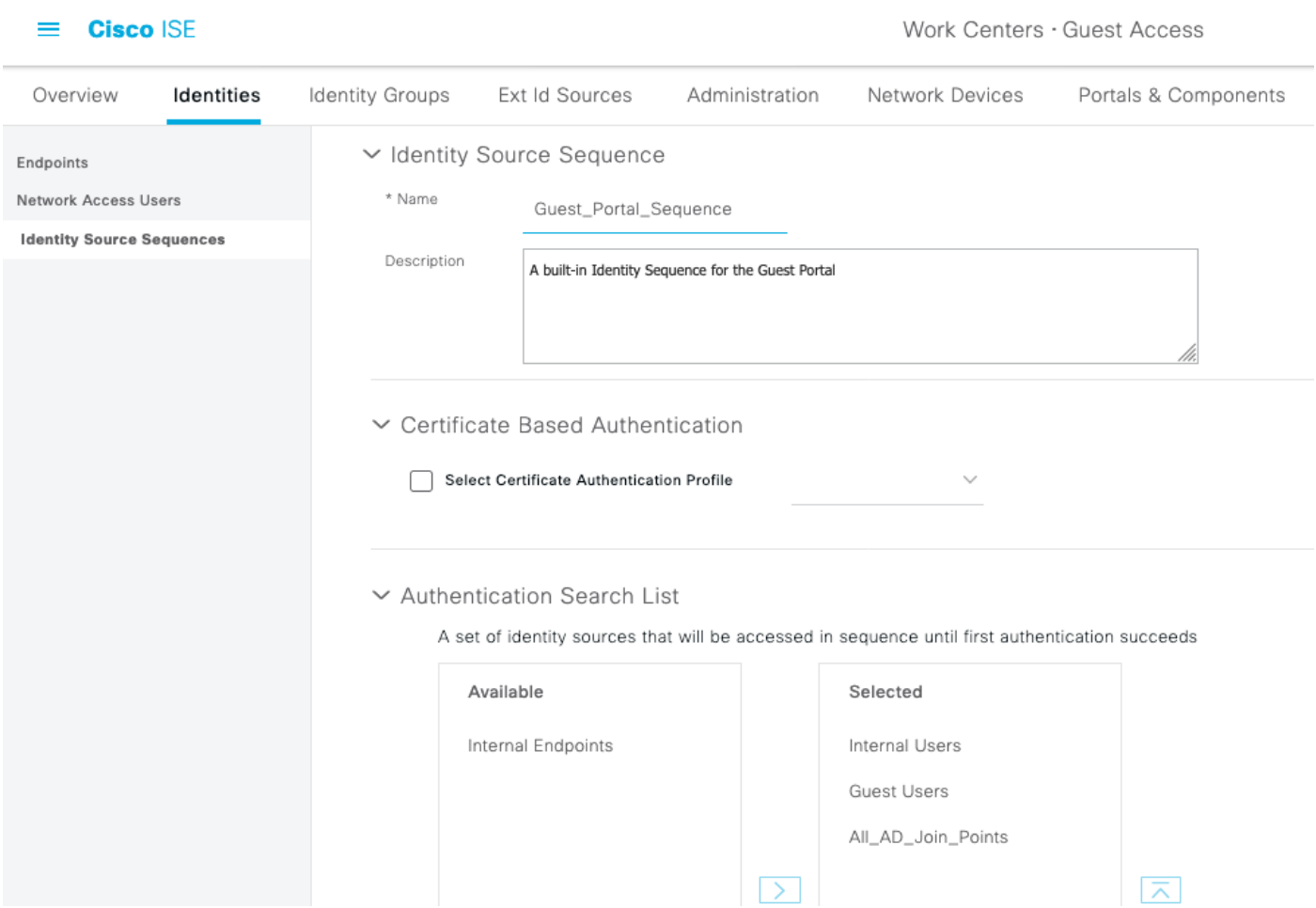
Als **Werknemers toestaan om persoonlijke apparaten te gebruiken op de** netwerkoptie is geselecteerd, dan kunnen zakelijke gebruikers die deze portal gebruiken door BYOD flow gaan en persoonlijke apparaten registreren. Voor gastgebruikers verandert die instelling niets.

Wat betekent "werknemers die portal gebruiken als gast"?

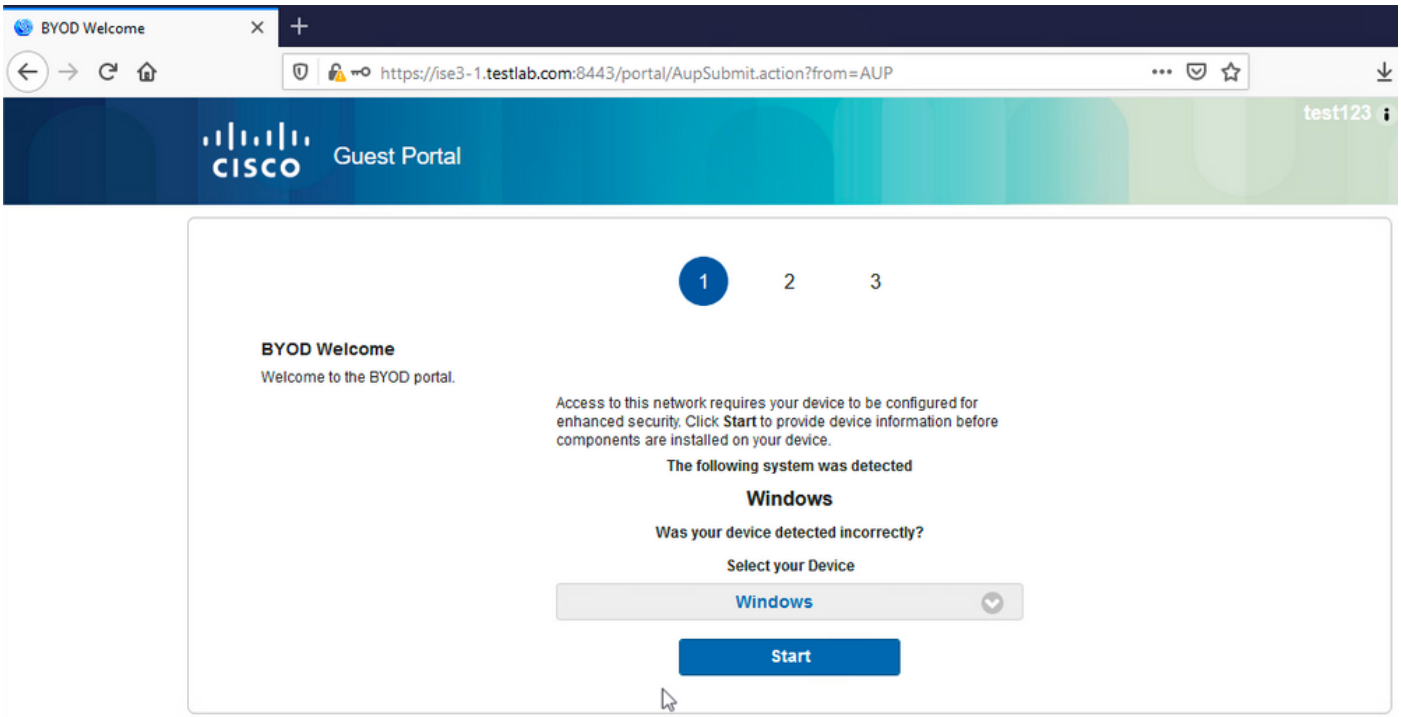
Gastportals zijn standaard geconfigureerd met het **Guest_Portal_Sequence** identiteitsarchief:



Dit is de interne opslagopeenvolging die eerst de Interne Gebruikers (vóór Gastgebruikers) en dan de geloofsbrieven van de Post probeert, Aangezien de Geavanceerde instellingen aan de volgende opslag in de opeenvolging moeten te werk gaan wanneer een geselecteerde identiteitsopslag niet voor authentificatie kan worden betreden, kan een Werknemer met interne geloofsbrieven of geloofsbrieven van de Kaart aan het portaal inloggen.



In deze fase op het guest portal, de gebruiker geeft referenties die zijn gedefinieerd in de Interne Gebruikers Store of Active Directory en de BYOD-omleiding komt voor:



Op deze manier kunnen zakelijke gebruikers BYOD uitvoeren voor persoonlijke apparaten.

Wanneer in plaats van de inloggegevens voor interne gebruikers/advertenties de inloggegevens voor gastgebruikers worden verstrekt, wordt de normale stroom voortgezet (geen BYOD).

VLAN-wijziging

Hiermee kunt u activeX of een Java-applet uitvoeren, waardoor DHCP wordt geactiveerd om uit te geven en te vernieuwen. Dit is nodig wanneer CoA de verandering van VLAN voor het eindpunt teweegbrengt. Wanneer MAB wordt gebruikt, is het eindpunt zich niet bewust van een verandering van VLAN. Een mogelijke oplossing is VLAN (DHCP-release/verlenging) te wijzigen met de NAC Agent. Een andere optie is om een nieuw IP-adres aan te vragen via het applet dat terugkomt op de webpagina. Er kan een vertraging tussen release/CoA/renew worden geconfigureerd. Deze optie wordt niet ondersteund voor mobiele apparaten.

Gerelateerde informatie

- Opdrachtservices op de Cisco ISE-configuratiehandleiding
- https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_overview.htmlCisco ISE 1.3 Beheerdershandleiding
- Draadloze BYOD met Identity Services Engine
- ISE SCEP-ondersteuning voor BYOD Configuration Voorbeeld
- Configuratievoorbeeld van centrale webverificatie op WLC en ISE
- Centrale webverificatie met FlexConnect-AP's op een WLC met ISE-configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems

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.