Configuratievoorbeeld van ISE versie 1.3, zelfgeregistreerd Guest Portal

Inhoud

Inleiding

Cisco Identity Services Engine (ISE) versie 1.3 heeft een nieuw type Guest Portal, het Self Registered Guest Portal, dat gastgebruikers in staat stelt zichzelf te registreren wanneer ze toegang tot netwerkbronnen krijgen. Met dit portal kunt u meerdere functies configureren en aanpassen. Dit document beschrijft hoe u deze functionaliteit kunt configureren en oplossen.

Voorwaarden

Vereisten

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

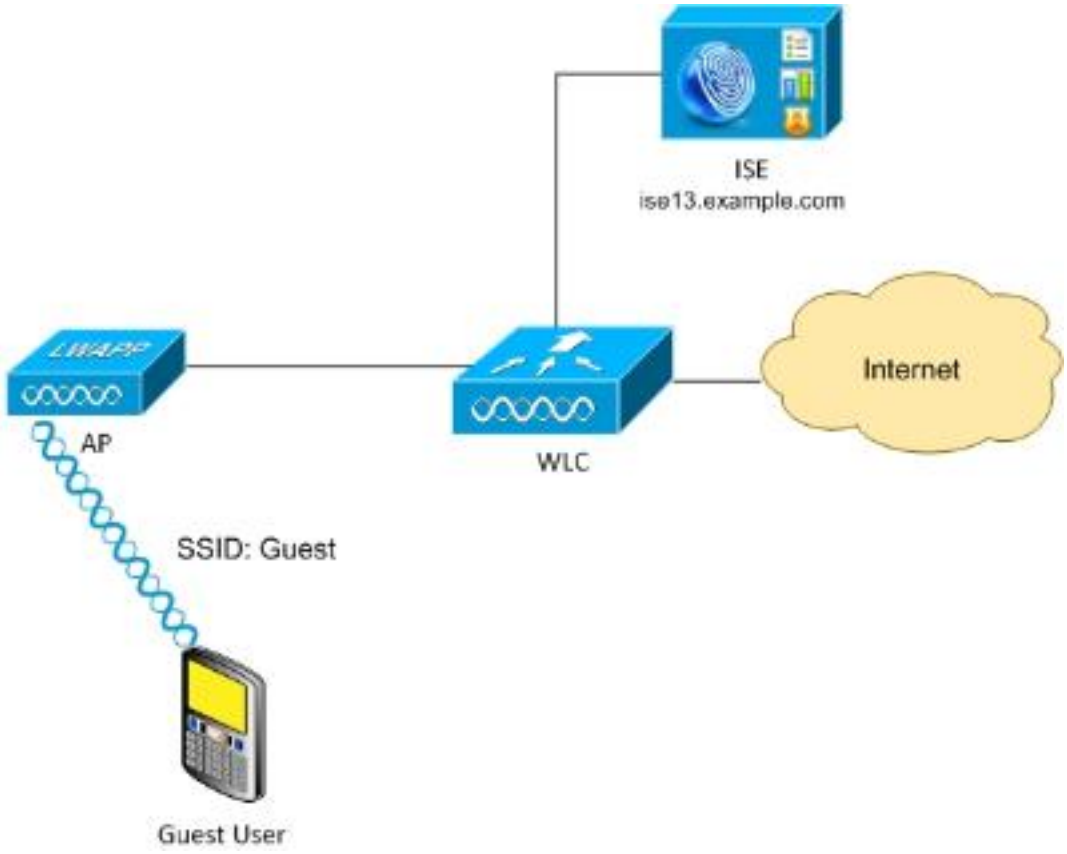
- ISE-implementaties en Guest-stromen
- Configuratie van draadloze LAN-controllers (WLC)

Gebruikte componenten

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

- Microsoft Windows 7
- Cisco WLC versie 7.6 en hoger
- ISE-software, versie 3.1 en hoger

Topologie en stroom



Dit scenario presenteert meerdere opties beschikbaar voor gastgebruikers wanneer ze zichzelf registreren.

Hier is de algemene stroom:

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

- url-redirect-acl (welk verkeer moet worden omgeleid, en de naam van toegangscontrolelijst (ACL) lokaal gedefinieerd op de WLC)

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

Stap 2. De gastgebruiker wordt opnieuw naar ISE gericht. In plaats van aanmeldingsgegevens te verstrekken om in te loggen, klikt de gebruiker op "Geen account". De gebruiker wordt naar een pagina terugverwezen waar die account kan worden gemaakt. Een optionele geheime registratiecode zou in staat kunnen zijn om het zelfregistratieprecht te beperken tot mensen die die geheime waarde kennen. Nadat de account is aangemaakt, krijgt de gebruiker aanmeldingsgegevens (gebruikersnaam en wachtwoord) en logt hij in met die aanmeldingsgegevens.

Stap 3. ISE verstuurt een RADIUS-wijziging van autorisatie (CoA), opnieuw gewaarmerkt naar de WLC. WLC verklaart opnieuw de gebruiker wanneer het de RADIUS access-aanvraag met de Authorize-Only eigenschap verstuurt. ISE reageert met ACL-toegangscontrole (toegangscontrole) en Airespace die lokaal wordt gedefinieerd op de WLC, die alleen toegang tot internet biedt (de definitieve toegang voor gastgebruiker is afhankelijk van het vergunningsbeleid).

Merk op dat ISE voor Extensible Authentication Protocol (EAP) sessies een CoA Terminate moet verzenden om opnieuw authenticatie te starten omdat de EAP sessie tussen de aanvrager en de ISE loopt. Maar voor MAB (MAC-filtering) is CoA Reecht genoeg; er is geen noodzaak om de draadloze client los te koppelen van de associatie/de authenticatie ervan uit te schakelen.

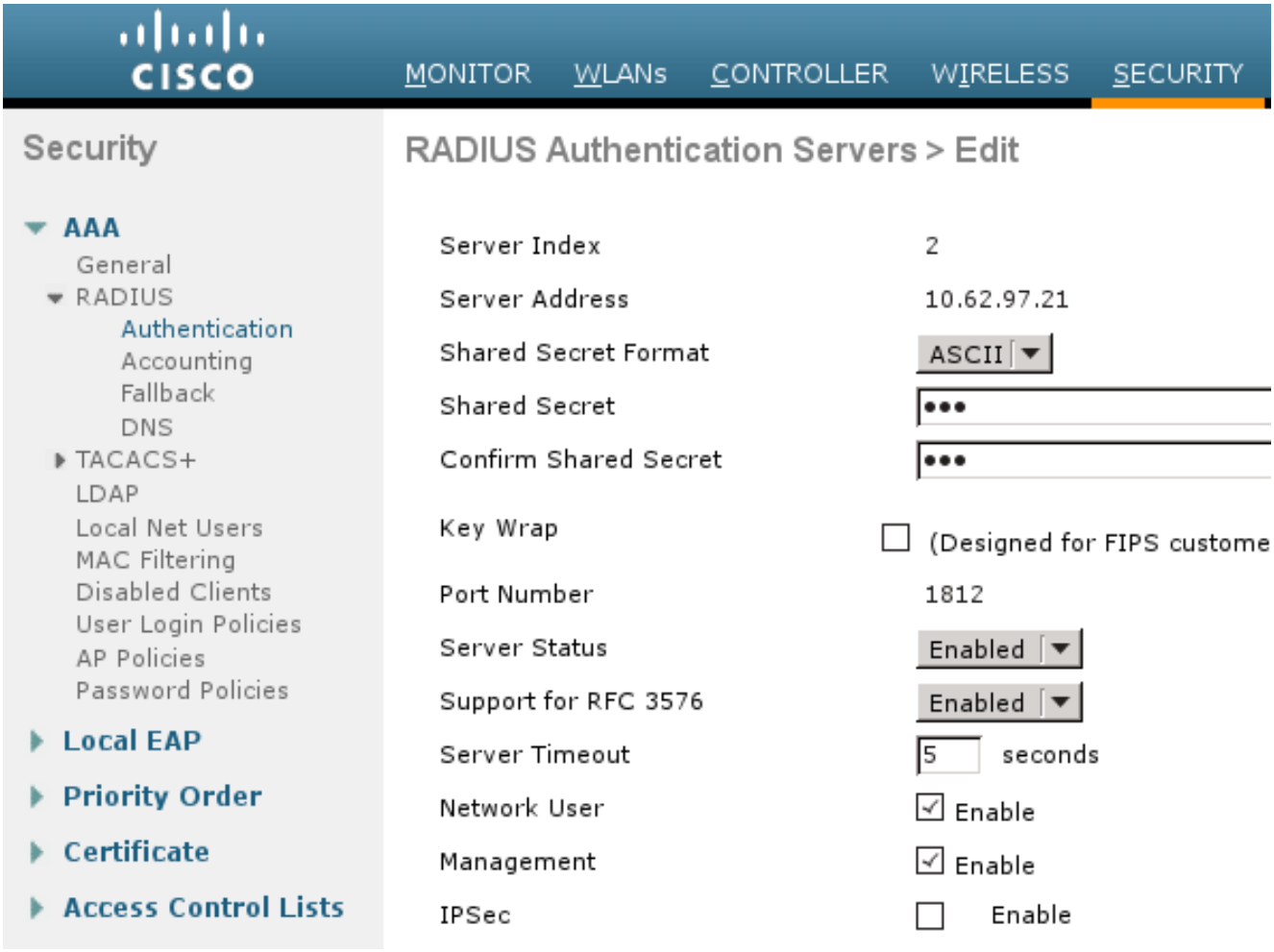
Stap 4 . De gastgebruiker heeft gewenste toegang tot het netwerk.

Meervoudige extra functies zoals houding en het Behalen van Uw Eigen Apparaat (BYOD) kunnen worden geactiveerd (later besproken).

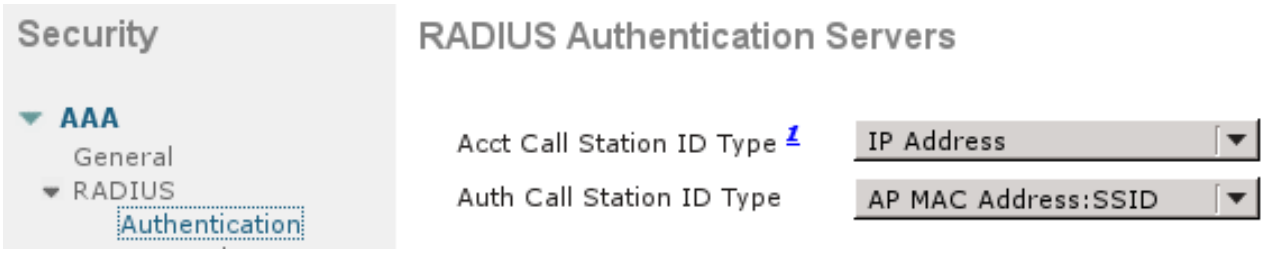
Configureren

WLC

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



Er is een vergelijkbare configuratie voor accounting. Het wordt ook geadviseerd om de WLC te vormen om SSID in de eigenschap van het geroepen Station ID te verzenden, die ISE toestaat om flexibele regels te vormen op SSID:

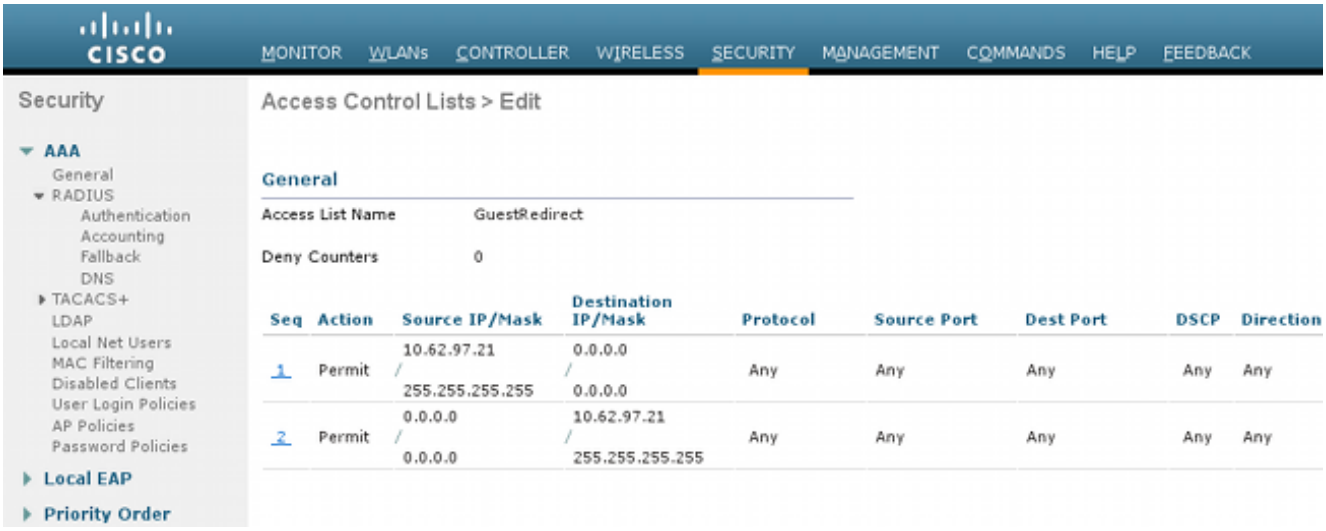


2. Onder het tabblad WLAN's kunt u de draadloze LAN-gast (WLAN) maken en de juiste interface configureren. Stel Layer 2 security in op **niets** met MAC-filtering. In Security/Verificatie, autorisatie en accounting (AAA) servers selecteert u het ISE IP-adres voor zowel verificatie als accounting. Selecteer in het tabblad Advanced de optie **AAA-override** en stel de status Network Admission Control (NAC) in op RADIUS NAC (CoA-ondersteuning).

3. Navigeren in **Security > Access Control Lists > Access Control Lists** en maken twee toegangslijsten:

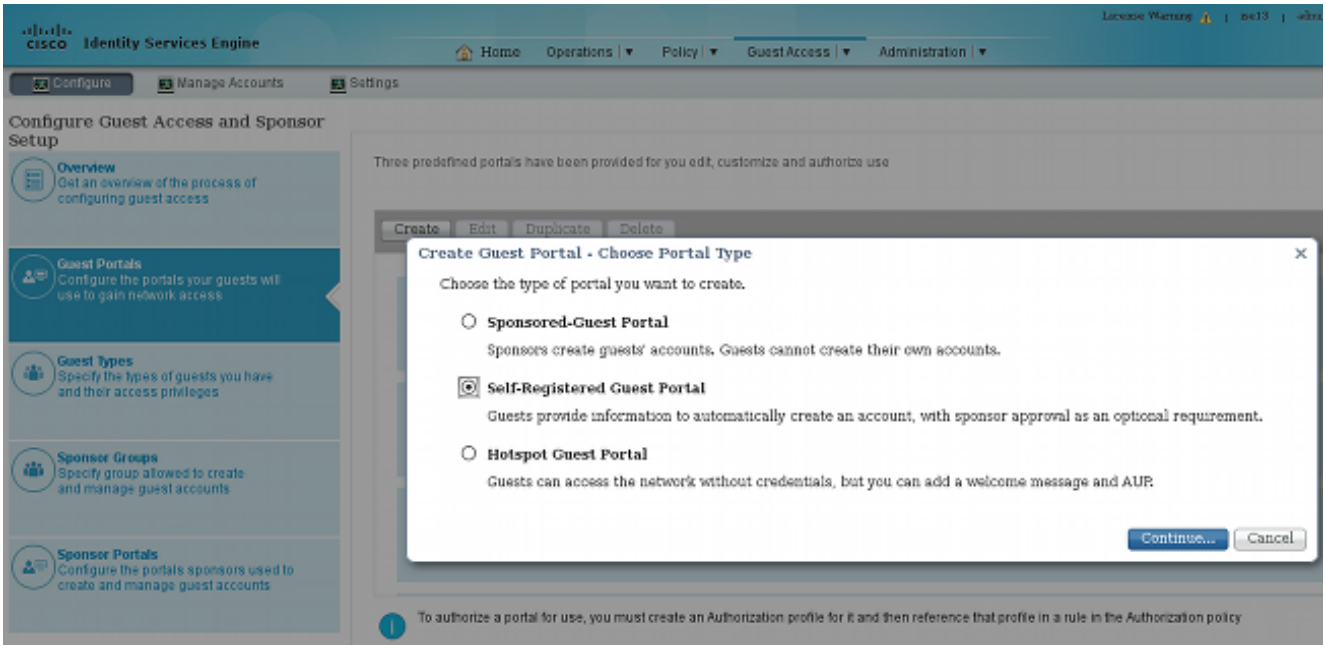
   GuestRedirect, dat verkeer toestaat dat niet opnieuw zou moeten worden gericht en al ander verkeer omwijstHet internet wordt ontzegd voor bedrijfsnetwerken en voor alle anderen toegestaan

Hier is een voorbeeld voor GuestRedirect ACL (moet verkeer naar/van ISE van redirectie uitsluiten):



ISE

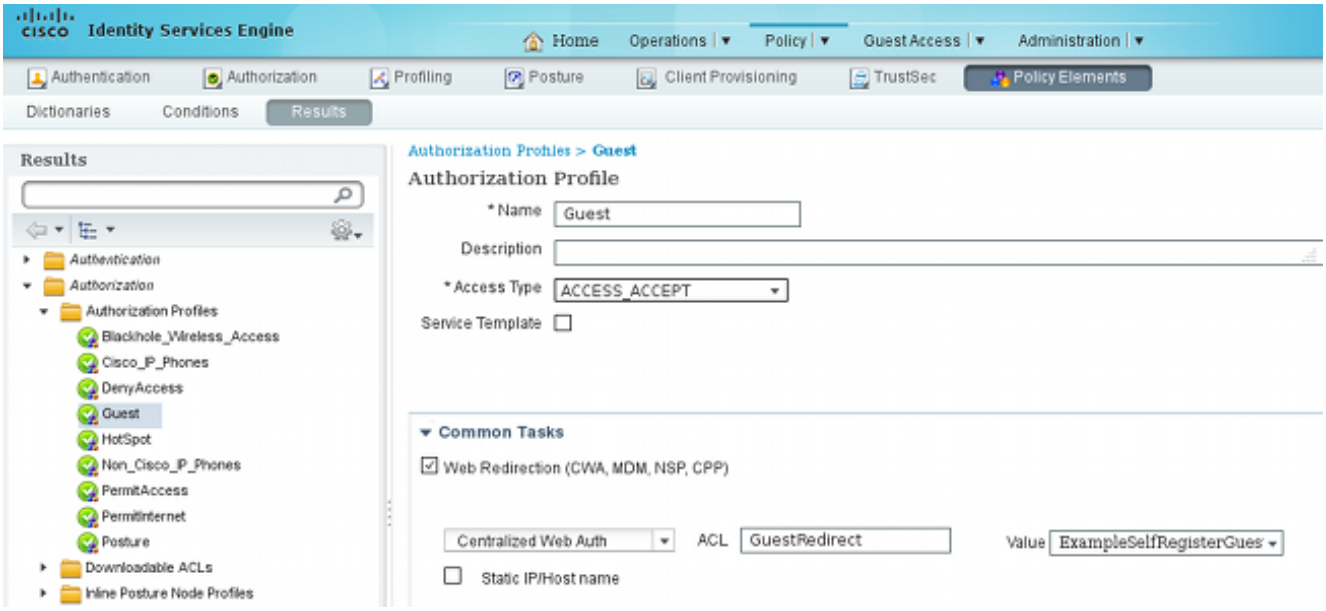
1. navigeren om **toegang te gisten > Portals van de Gast te configureren** en een nieuw type portaal te maken, zelfgeregistreerd Guest Portal:



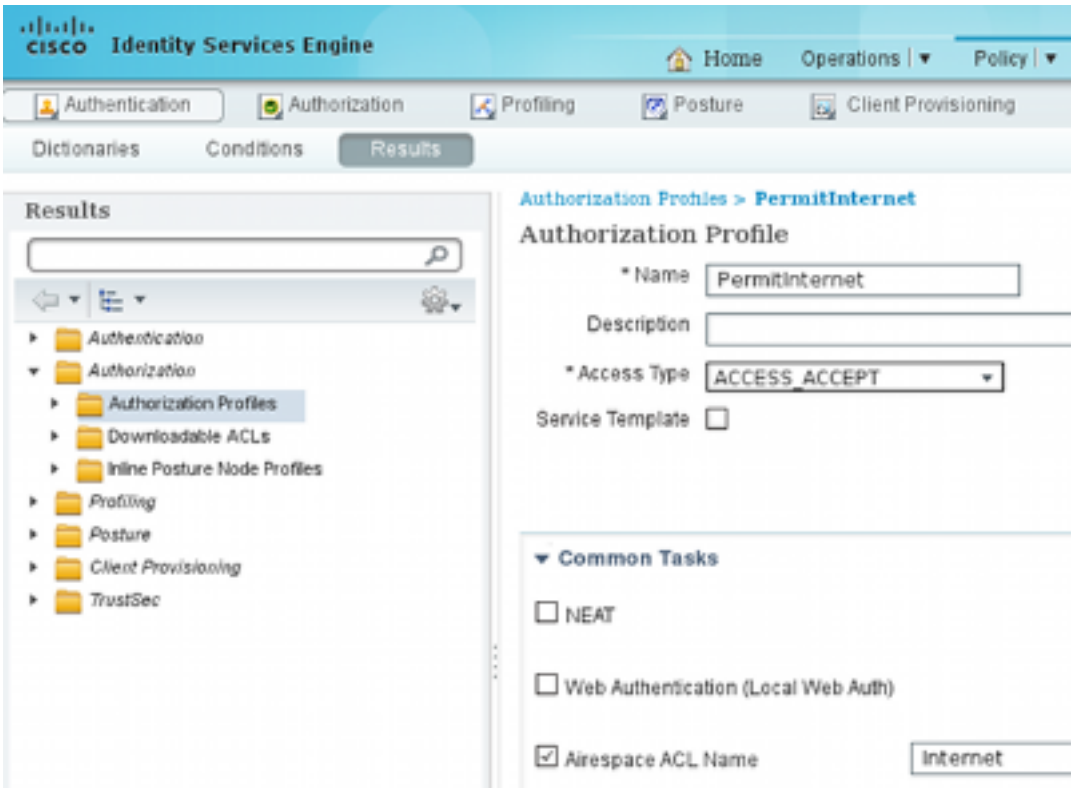
2. Kies de naam van het portal die verwezen zal worden in het vergunningsprofiel. Standaard alle andere instellingen instellen. Onder Portal Pagina-aanpassing kunnen alle pagina's die worden gepresenteerd, worden aangepast.

3. Bewerkingen autorisatie configureren:

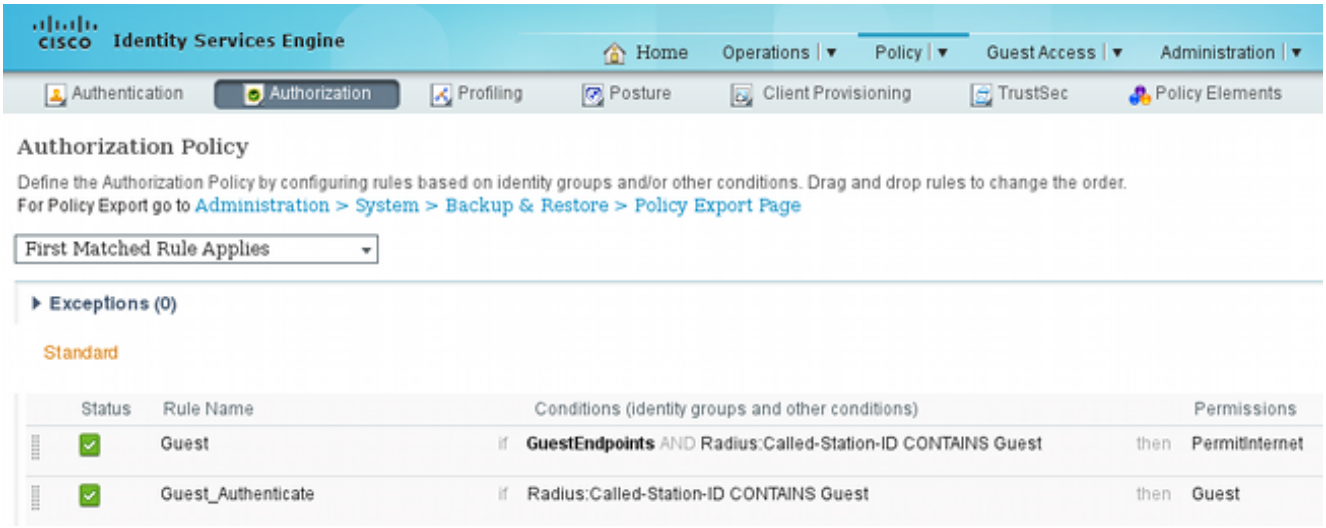
   Guest (met omleiding naar de naam van het Guest-portaal en ACL-richting)



Internet (met Airespace ACL gelijk internet)



4. Om de vergunningsregels te controleren, dient u te navigeren naar **Beleidsbeleid > Toestemming**. In ISE versie 1.3 wordt standaard voor mislukte MAC-verificatie-bypass (MAB)-toegang (MAC-adres niet gevonden) opnieuw ingesteld (niet verworpen). Dit is zeer nuttig voor Guest Portals omdat er geen noodzaak is om iets te veranderen in standaard authenticatieregels.



Nieuwe gebruikers die de Guest SSID associëren, maken nog geen deel uit van een identiteitsgroep. Dit is de reden dat ze overeenkomen met de tweede regel, die het machtigingsprofiel van de Gast gebruikt om hen naar het juiste portaal van de Gast te leiden.

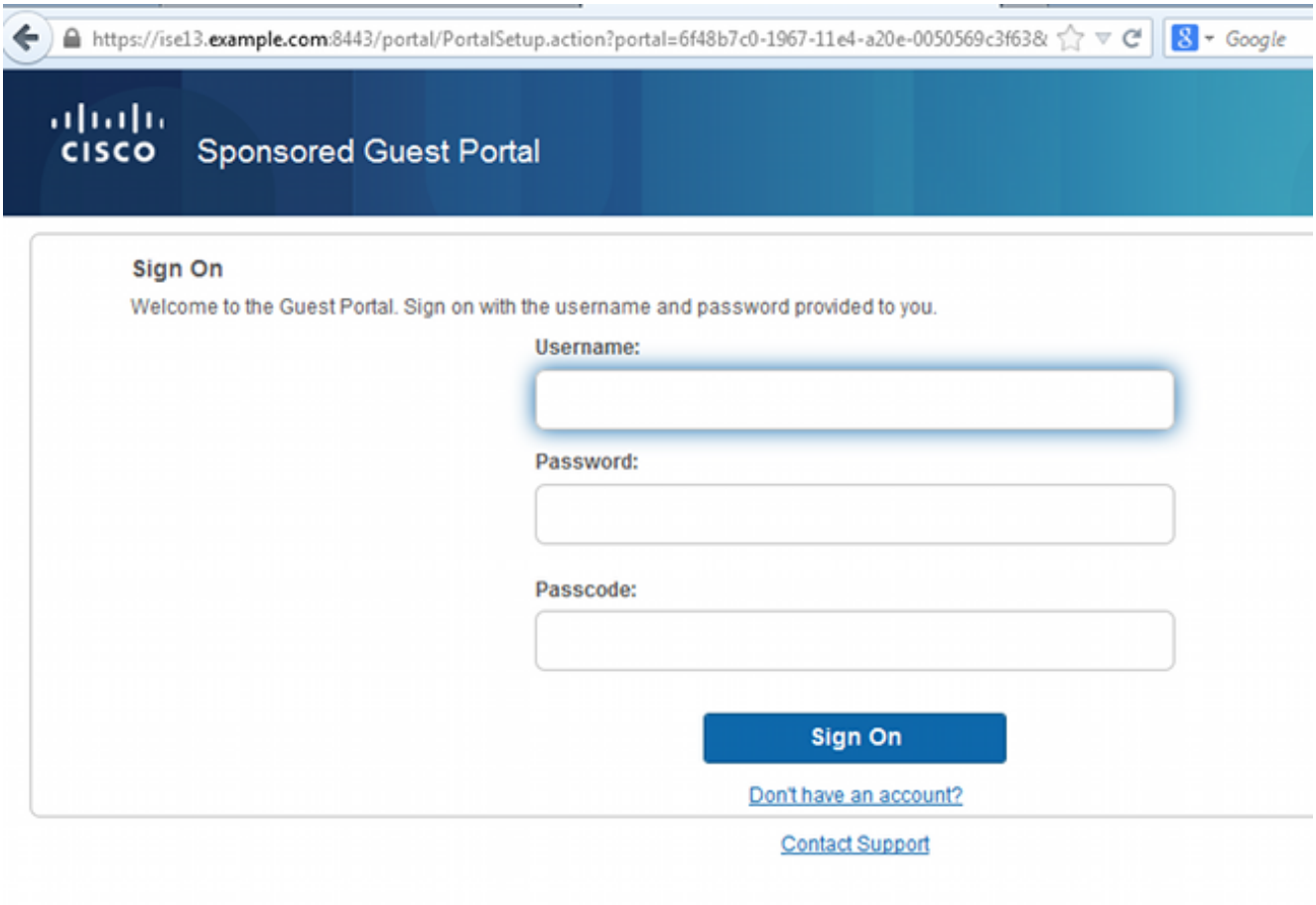
Nadat een gebruiker een account maakt en zich met succes inlogt, stuurt ISE een RADIUS-CoA en voert de WLC opnieuw verificatie uit. Deze keer, wordt de eerste regel gecombineerd met autorisatieprofiel PermitInternet en keert de ACL naam terug die op WLC wordt toegepast.

5. Voeg de WLC toe als een Netwerktoegangsapparaat van **Beheer > Netwerkbronnen > Netwerkapparaten**.

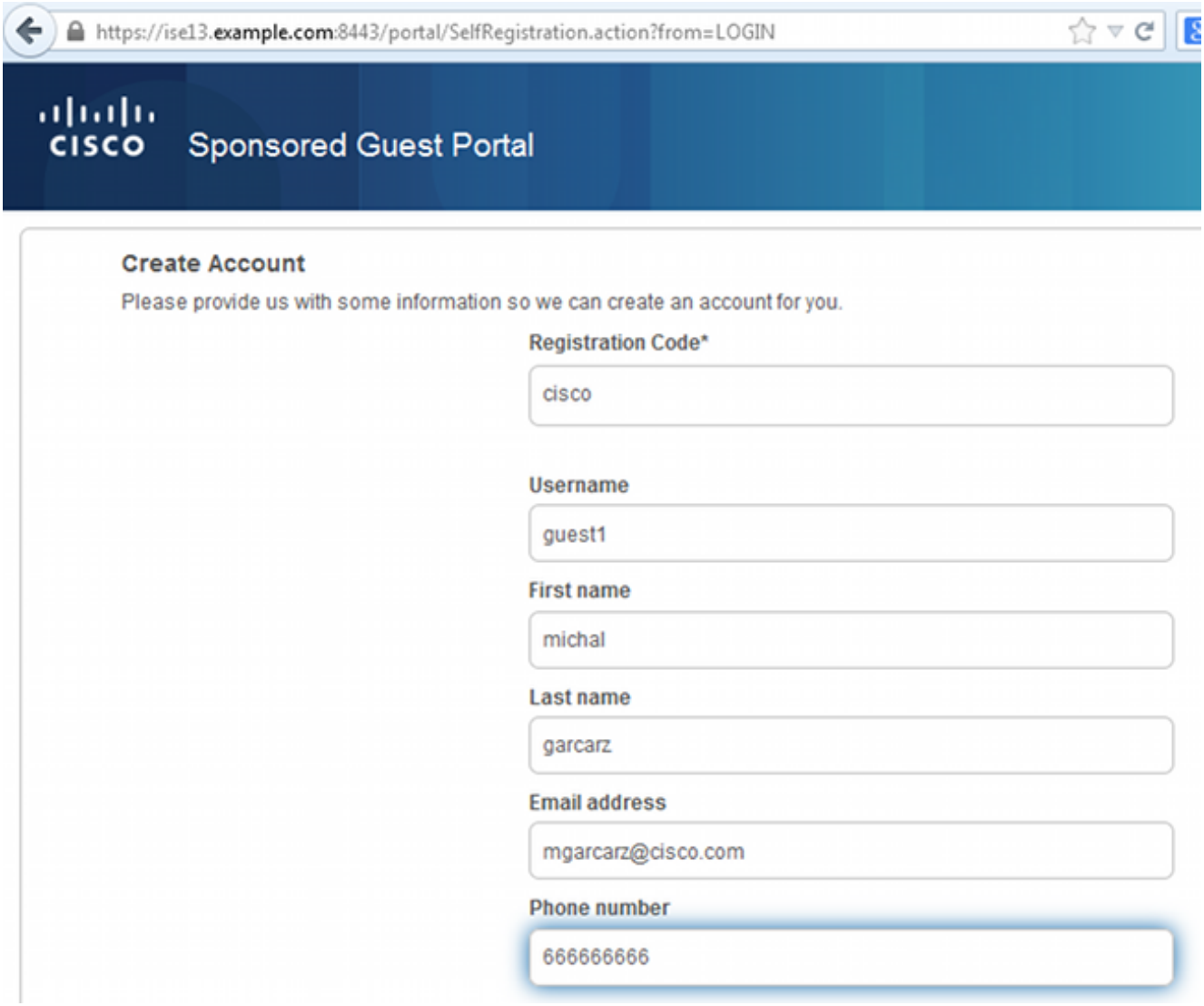
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

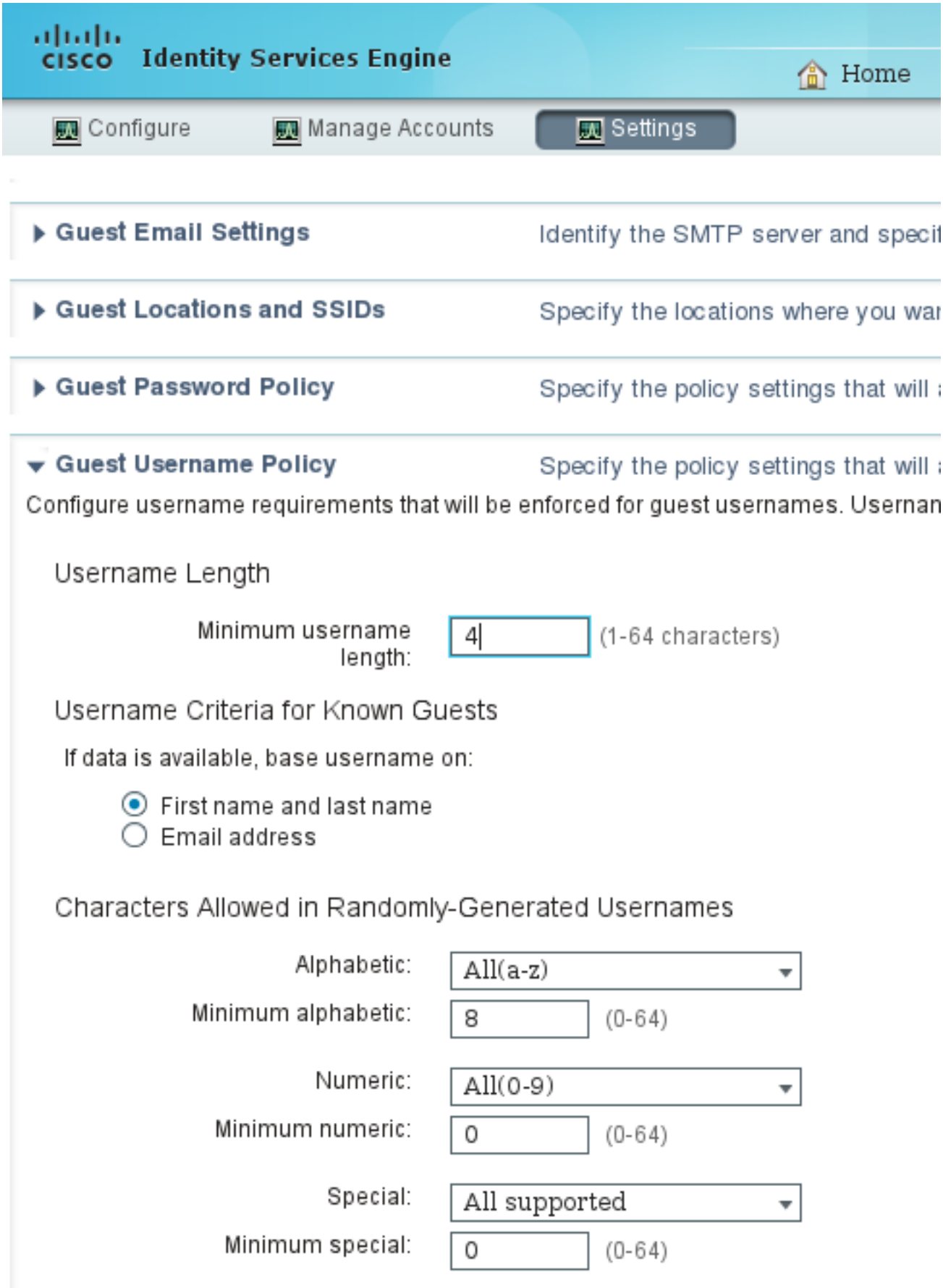
1. Nadat u met SSID van de Kast hebt geassocieerd en een URL typt, wordt u opnieuw gericht naar de loginpagina:



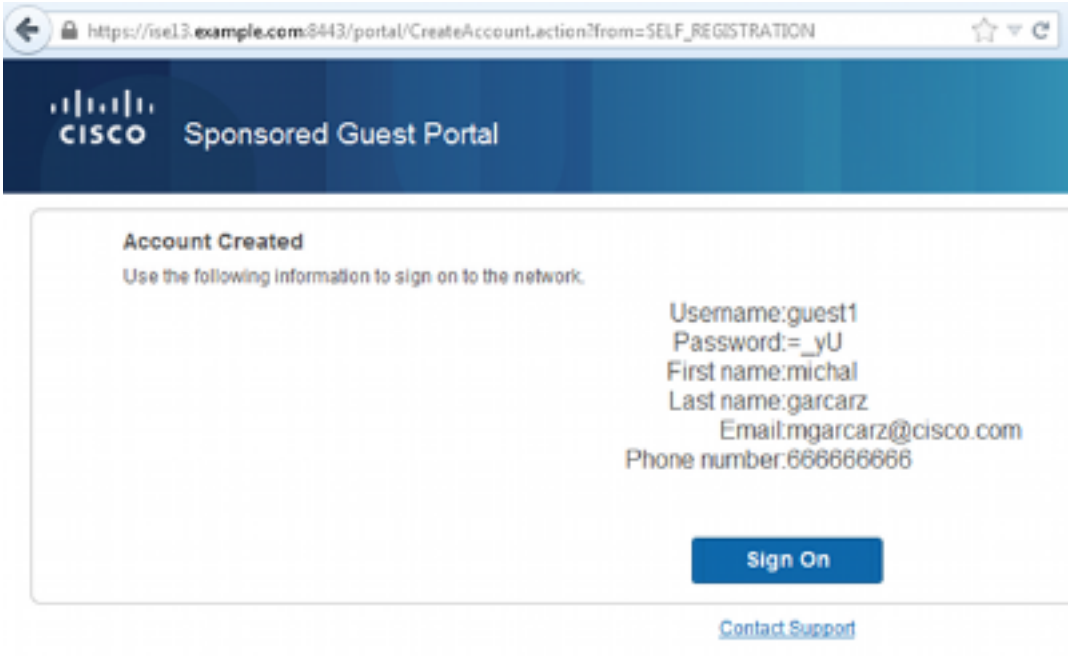
2. Omdat je nog geen geloofsbrieven hebt, moet je kiezen **geen account heeft?** optie. Een nieuwe pagina die account aanmaakt, wordt weergegeven. Als de optie Registratiecode is ingeschakeld onder de configuratie van Guest Portal, dan is die geheime waarde vereist (dit garandeert dat alleen mensen met de juiste rechten zichzelf mogen registreren).



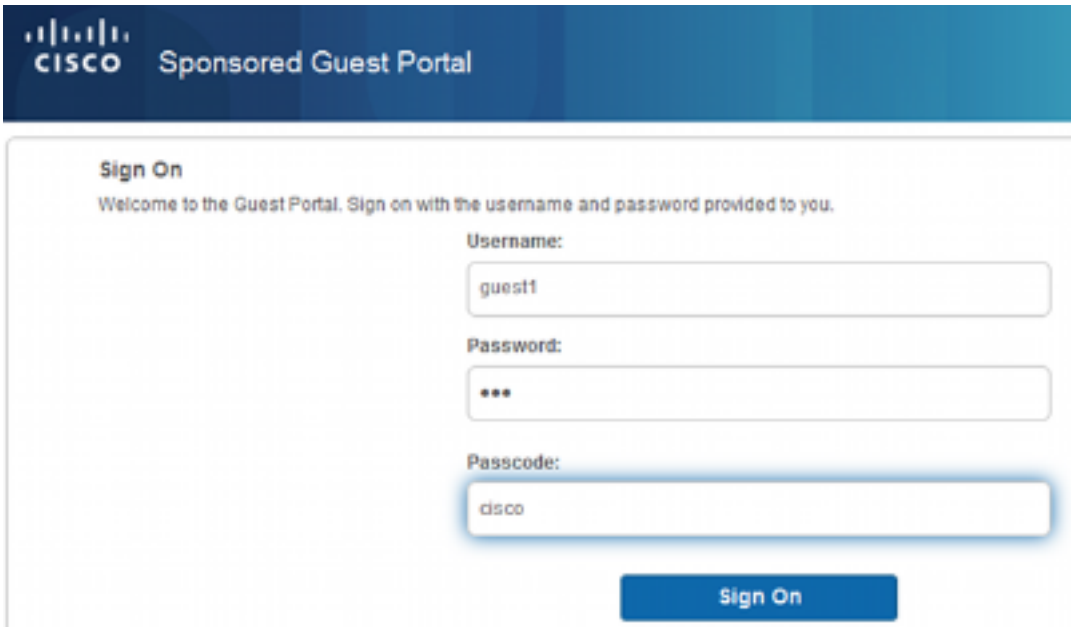
3. Als er problemen zijn met het wachtwoord of het gebruikersbeleid, navigeer dan naar **Guest Access > Instellingen > Wachtwoordbeleid voor Guest of Guest Access > Instellingen > Gebruikersnaam voor Guest** om instellingen te wijzigen. Hierna volgt een voorbeeld:



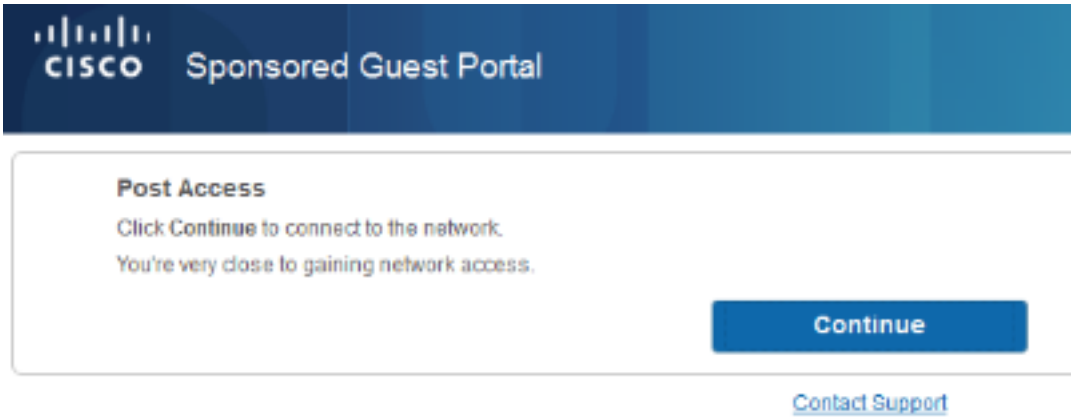
4. Na het maken van succesvolle account wordt u aangeleverd met aanmeldingsgegevens (wachtwoord dat gegenereerd wordt als per beleid van een gastwachtwoord):



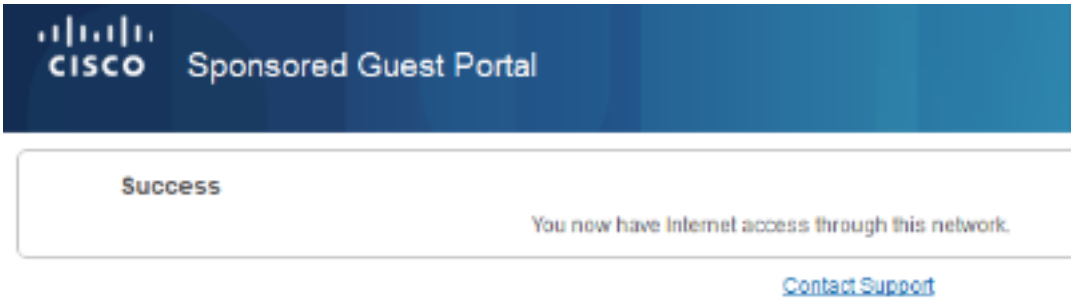
5. Klik op **Aanmelden** en geef referenties (er kan een aanvullende toegangswachtcode nodig zijn als deze is ingesteld onder het Guest Portal; dit is een ander beveiligingsmechanisme dat alleen personen die het wachtwoord kennen , de mogelijkheid biedt in te loggen .



6. Indien geslaagd, kan een optioneel Acceptable Use Policy (AUP) worden aangeboden (indien geconfigureerd onder het Guest Portal). De pagina Post Access (ook configureerbaar onder Guest Portal) kan ook worden weergegeven.



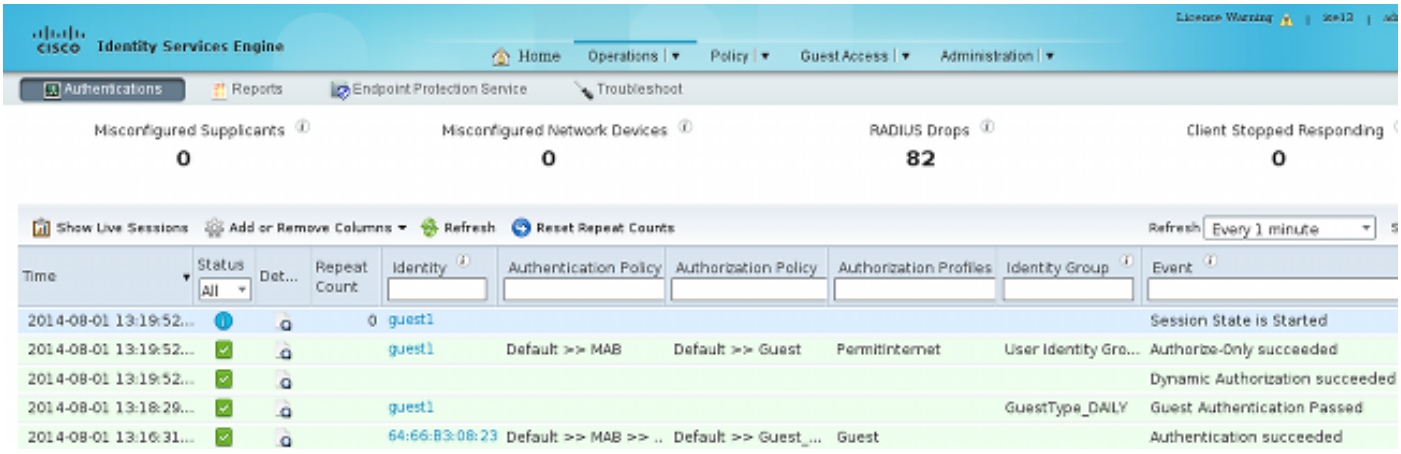
Op de laatste pagina wordt bevestigd dat toegang is verleend:



Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

In deze fase presenteert ISE de volgende blogs:



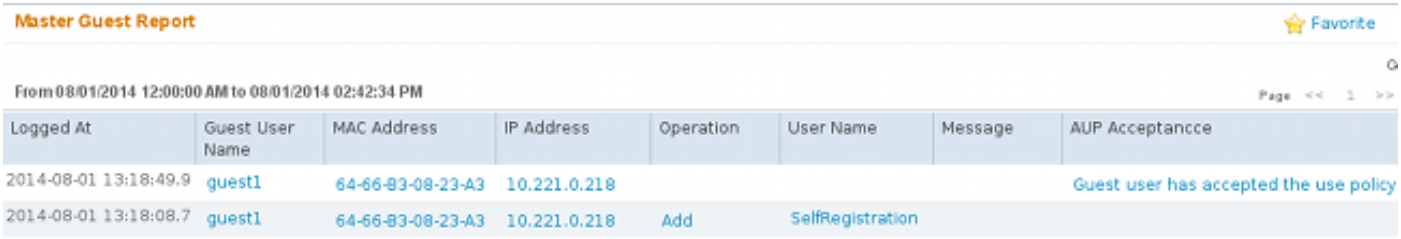
Hier is de stroom:

- De gastgebruiker ontmoet de tweede autorisatieregel (Guest_Authenticate) en wordt omgeleid naar Guest ("Auhentication connected").

- De gast wordt opnieuw gericht op zelfregistratie. Na inloggen (met de nieuw gemaakte account) stuurt ISE de CoA-reauthentiek, wat door de WLC is bevestigd ("Dynamische autorisatie gelukt").

- De WLC voert opnieuw authenticatie uit met het attribuut Authorize-Only en de ACL naam wordt geretourneerd ("Enkel autorisatie"). De gast krijgt de juiste netwerktoegang.

Rapporten (**transacties > Meldingen > ISE-rapporten > Guest Access Reports > Master Guest Report**) bevestigen ook dat:



Master Guest Report

Favorite

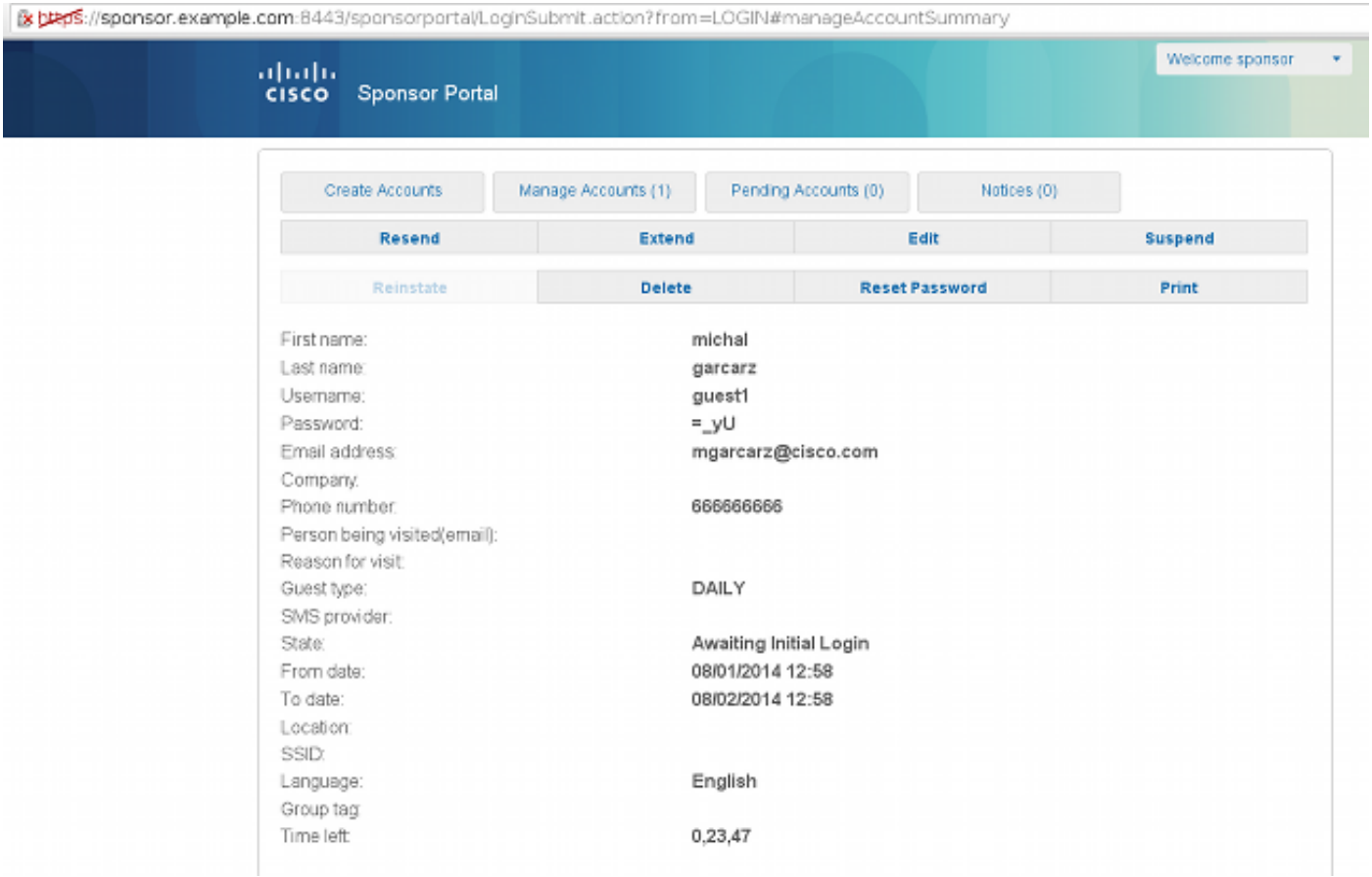
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM

Page << 1 >>

Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptancce
2014-08-01 13:18:49.9	guest1	64-66-B3-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	guest1	64-66-B3-08-23-A3	10.221.0.218	Add	SelfRegistration		

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

Dit voorbeeld bevestigt dat de account aangemaakt is maar de gebruiker heeft nooit aangemeld ("wacht eerste aanmelding"):



Optionele configuratie

Voor elke fase van deze stroom kunnen verschillende opties worden ingesteld. Dit alles is ingesteld per Guest Portal bij **Guest Access > Portals instellen > Guest > PortalName > PortalName > Portal** Gedragdheid **en stroominstellingen**. Belangrijker instellingen zijn:

Instellingen voor zelfregistratie

- Guest Type - beschrijft hoe lang de account actief is, de opties voor wachtwoorden, de openingstijden en de opties voor aanmelding (dit is een combinatie van Tijdprofiel en rol voor zoekresultaten van ISE, versie 1.2)
- Registratiecode - Als deze optie ingeschakeld is, mogen alleen gebruikers die de geheime code kennen zich zelf registreren (moet het wachtwoord invoeren wanneer er een account wordt aangemaakt)
- AUP - Gebruiksbeleid tijdens zelfregistratie accepteren
- Voorschrift voor sponsor om de gastaccount goed te keuren/in werking te stellen

Instellingen inloggen

- Toegangscode - Indien ingeschakeld, zijn alleen gastgebruikers die de geheime code kennen, toegestaan om in te loggen
- AUP - Gebruiksbeleid tijdens zelfregistratie accepteren
- Wachtwoordwijziging

Instellingen apparaatregistratie

- Het apparaat wordt standaard automatisch geregistreerd

Instellingen voor apparaatnaleving

- Hiermee kan een houding in de stroom worden toegestaan

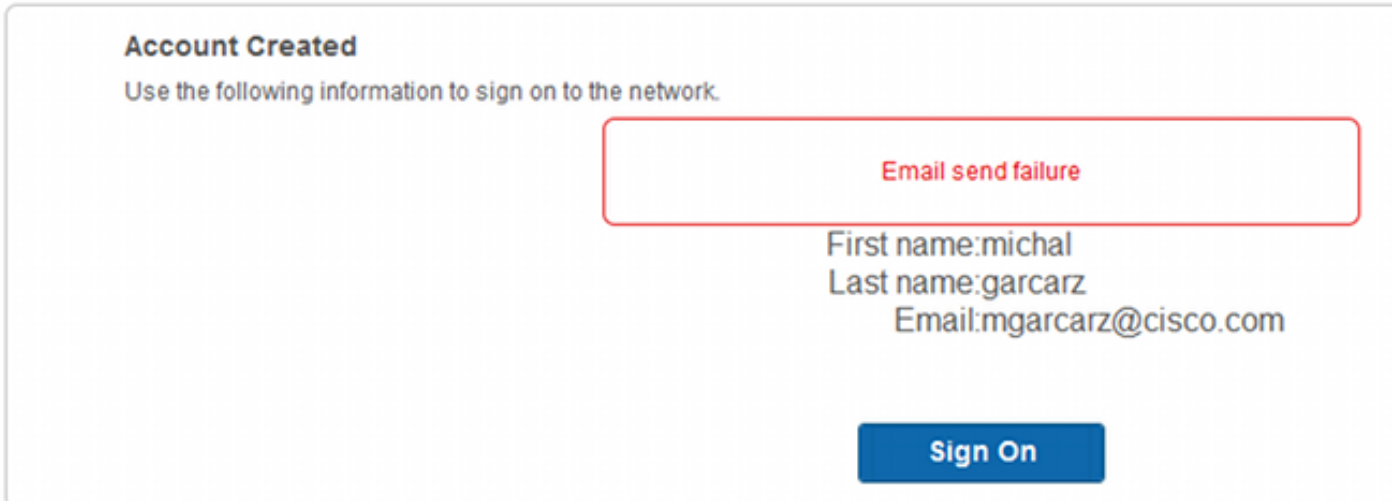
BYOD-instellingen

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

Door sponsor goedgekeurde rekeningen

Als de optie **Laat** de **zelf geregistreerde gasten** goedkeuren is geselecteerd, moet de account die door de gast is aangemaakt, door een sponsor worden goedgekeurd. Deze functie kan e-mail gebruiken om de opdrachtgever op de hoogte te stellen (voor toestemming van de gastaccount):

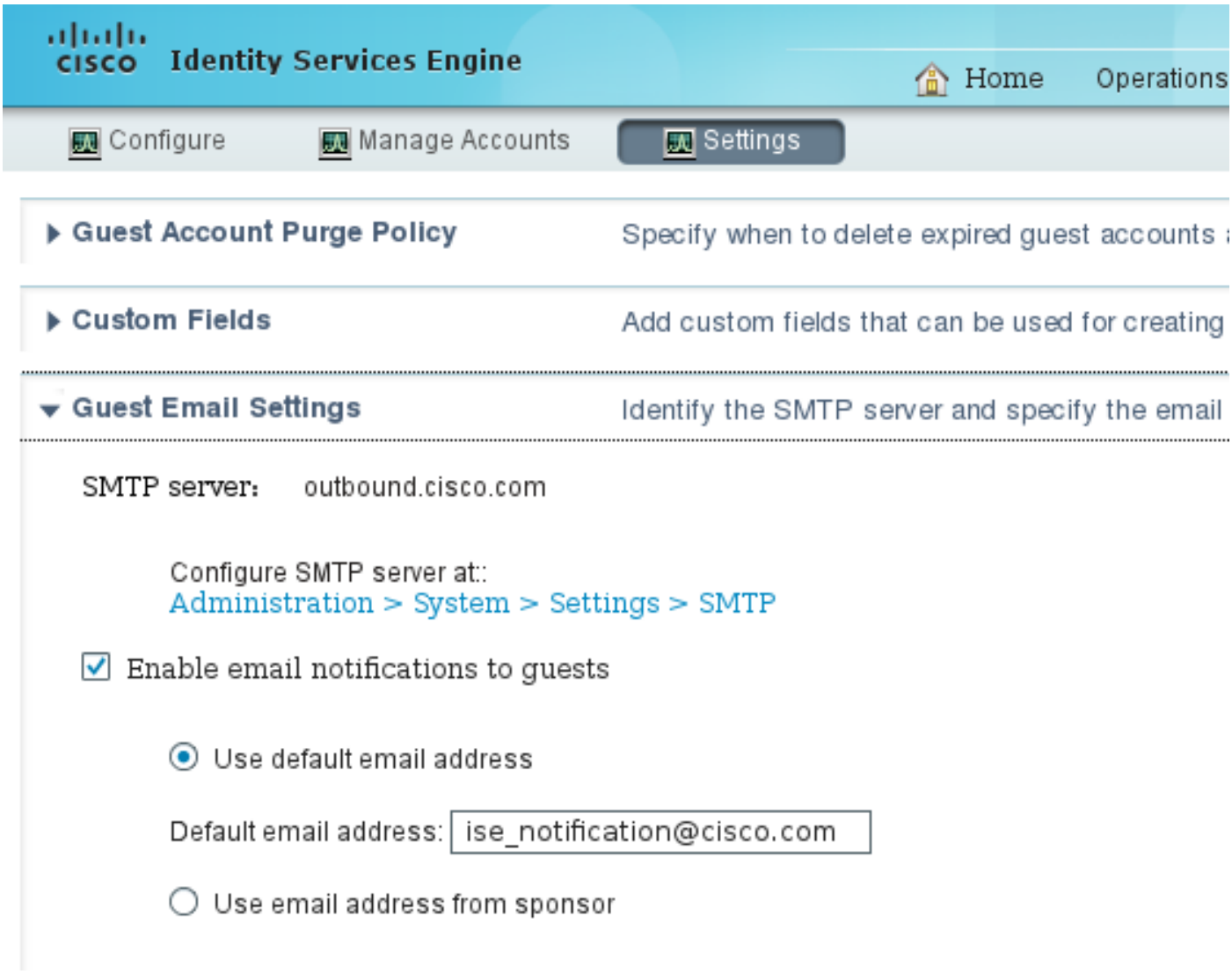
Als de Simple Mail Transfer Protocol (MTP) server of standaard vanaf e-mail niet is ingesteld wordt de account niet aangemaakt:

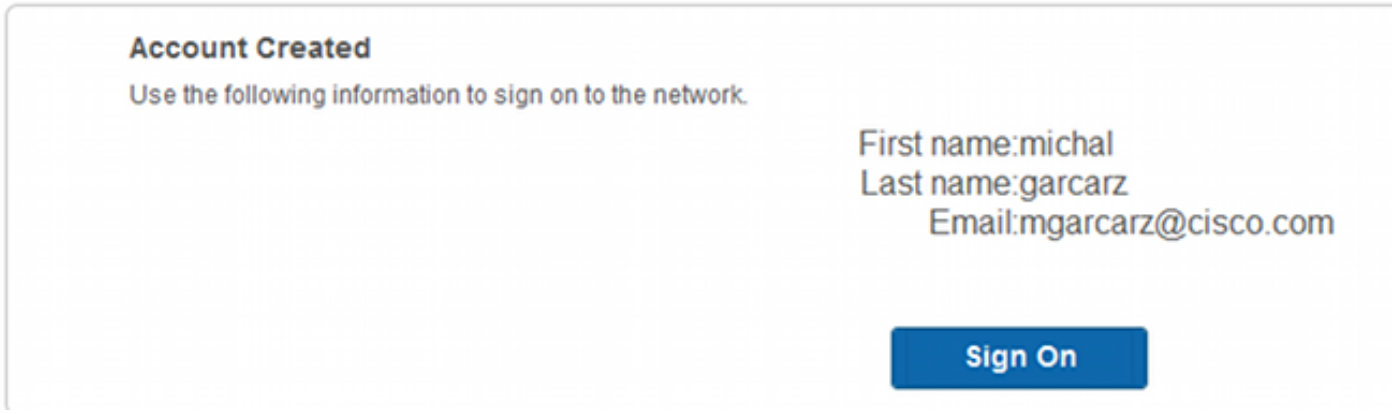


Het logbestand van gastarts.log bevestigt dat het globale adres dat gebruikt wordt voor kennisgeving ontbreekt:

```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

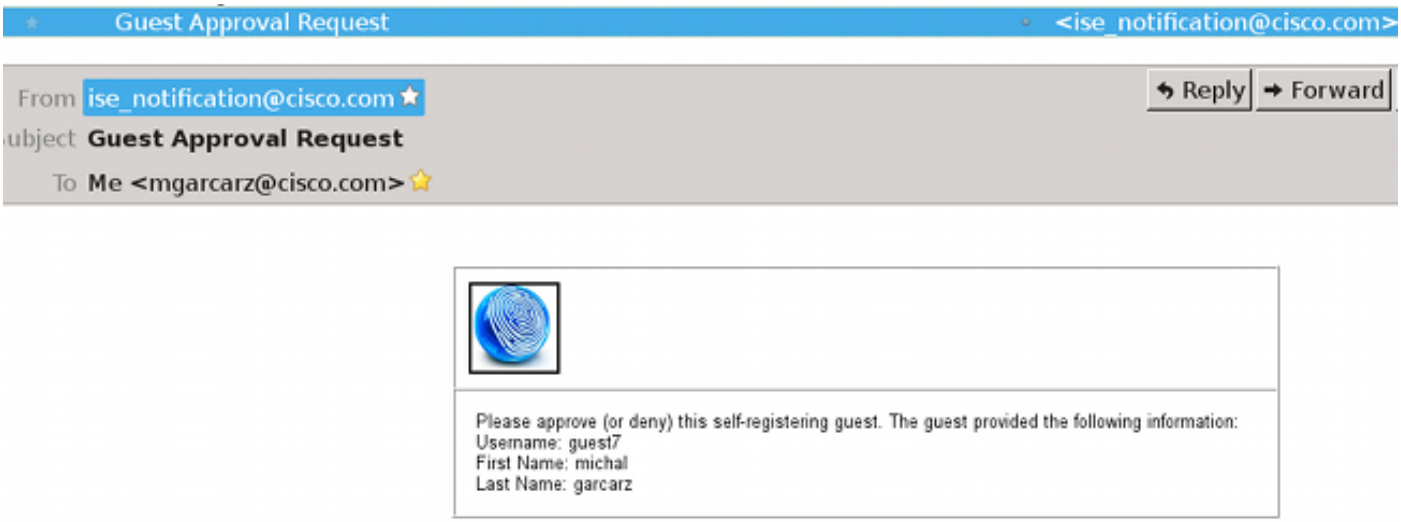
Wanneer u de juiste e-mailconfiguratie hebt, wordt de account aangemaakt:



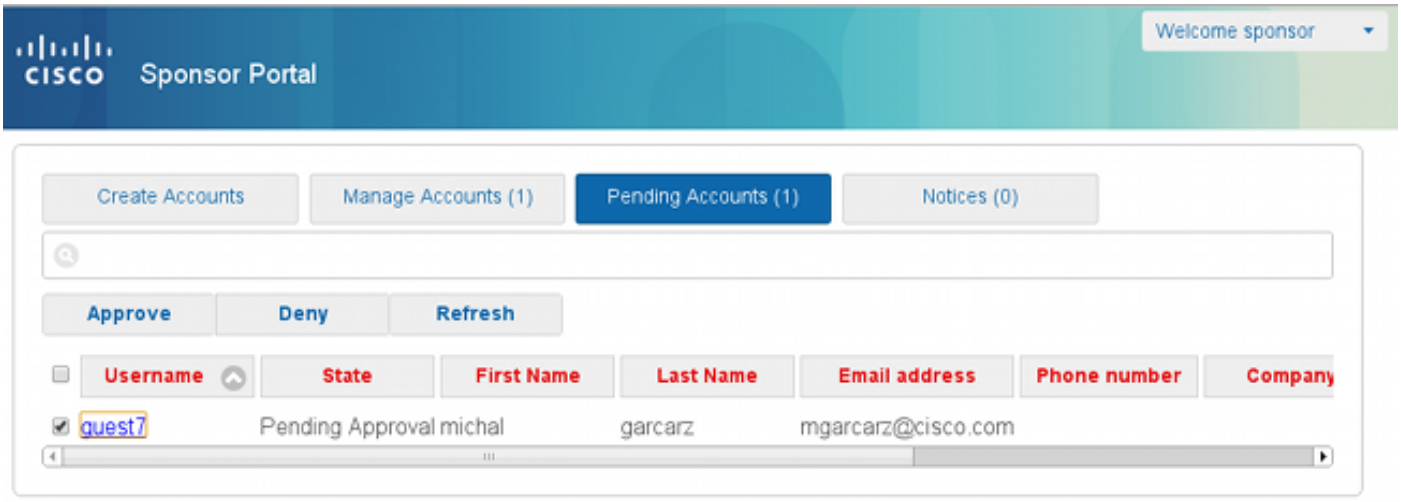


Nadat u de **optie Vereiste dat zelf geregistreerde gasten worden goedgekeurd** , worden **de** gebruikersnaam en het wachtwoord automatisch verwijderd uit de **sectie Deze informatie in het** gedeelte **Zelfregistratie Success pagina** verwijderen. Dit is de reden dat als goedkeuring van sponsor nodig is, de geloofsbrieven voor gastgebruikers standaard niet worden weergegeven op de website die informatie toont om aan te tonen dat de rekening is gemaakt. In plaats daarvan moeten ze worden afgeleverd via een sms of e-mail. Deze optie moet zijn ingeschakeld in de **Send Credentiential notification when approval using** Section (mark e-mail/sms).

Aan de opdrachtgever wordt een e-mail verzonden:



De sponsor logt in op het Sponsor-portal en keurt de account goed:



Vanaf dit punt is het de gastgebruiker toegestaan om in te loggen (met de aanmeldingsgegevens

die per e-mail of sms ontvangen worden).

Samengevat worden er drie e-mailadressen gebruikt in deze flow:

- Bericht "van" adres. Dit wordt statistisch gedefinieerd of is afgeleid van de sponsor rekening en wordt gebruikt als het Van adres voor beide: kennisgeving aan de opdrachtgever (ter goedkeuring) en aan de gast door middel van creditdetails . Dit wordt ingesteld onder **Gast Access > Instellingen > Instellingen > E-mailinstellingen controleren**.

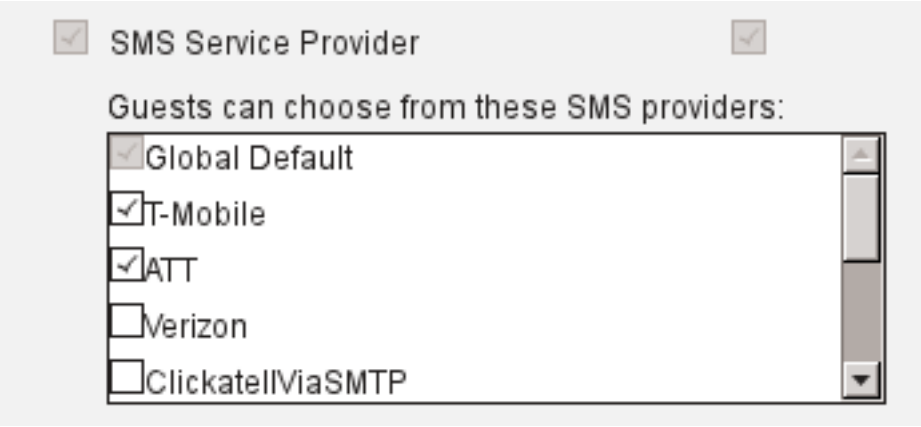
- Bericht "aan" adres. Dit wordt gebruikt om de opdrachtgever ervan in kennis te stellen dat hij een rekening ter goedkeuring heeft ontvangen. Dit is ingesteld in het Guest Portal onder **Guest Access > Configureren > Guest Portals > Portal Name > Portal Name > vereisen dat zelf-geregistreerde gasten worden goedgekeurd > E-mail goedkeuringsaanvraag om**.

- Guest 'To'-adres. Dit wordt door de gastgebruiker tijdens de registratie geboden. Als u **een** melding **per e-mail** wilt **verzenden nadat deze** is **verzonden**, wordt de e-mail met de wachtwoordgegevens (gebruikersnaam en wachtwoord) aan de gast geleverd.

Credentials leveren via sms

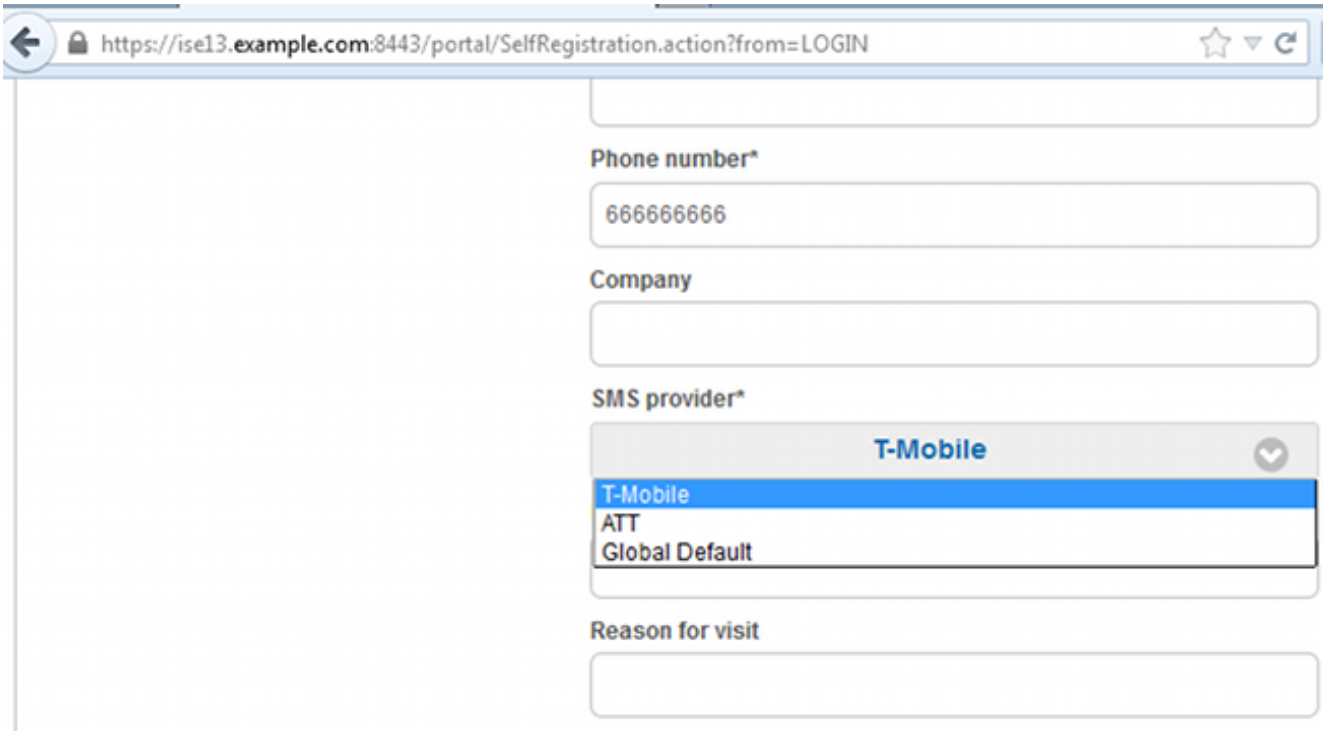
Kiezerreferenties kunnen ook door sms worden geleverd. Deze opties moeten worden ingesteld:

1. Kies de sms-dienstverlener:

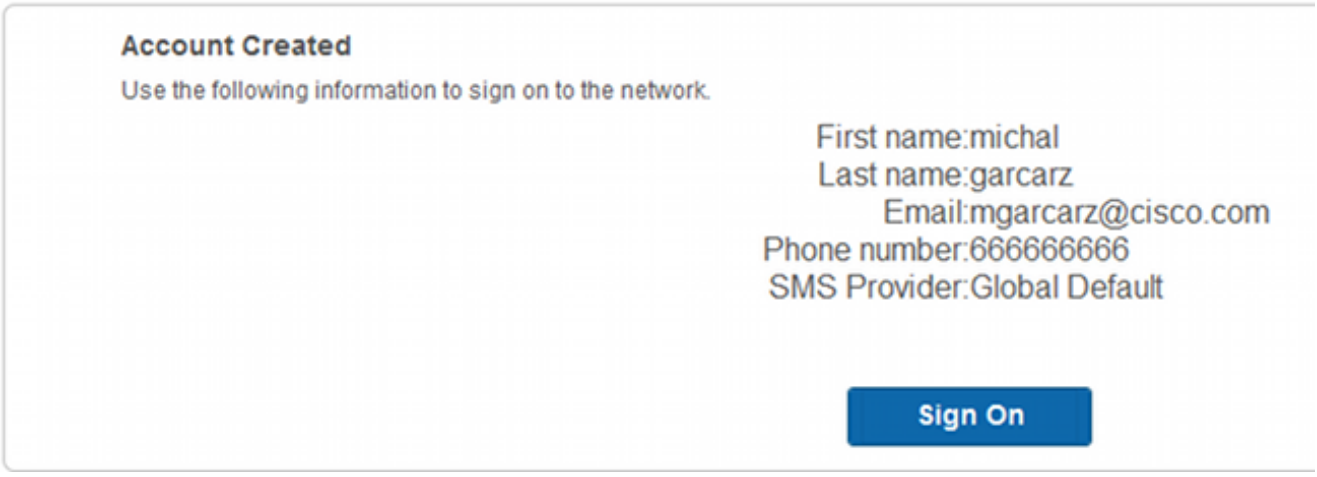


2. Controleer de **Send Credentiential notification when approval met behulp van: Sms** aanvinkvakje.

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



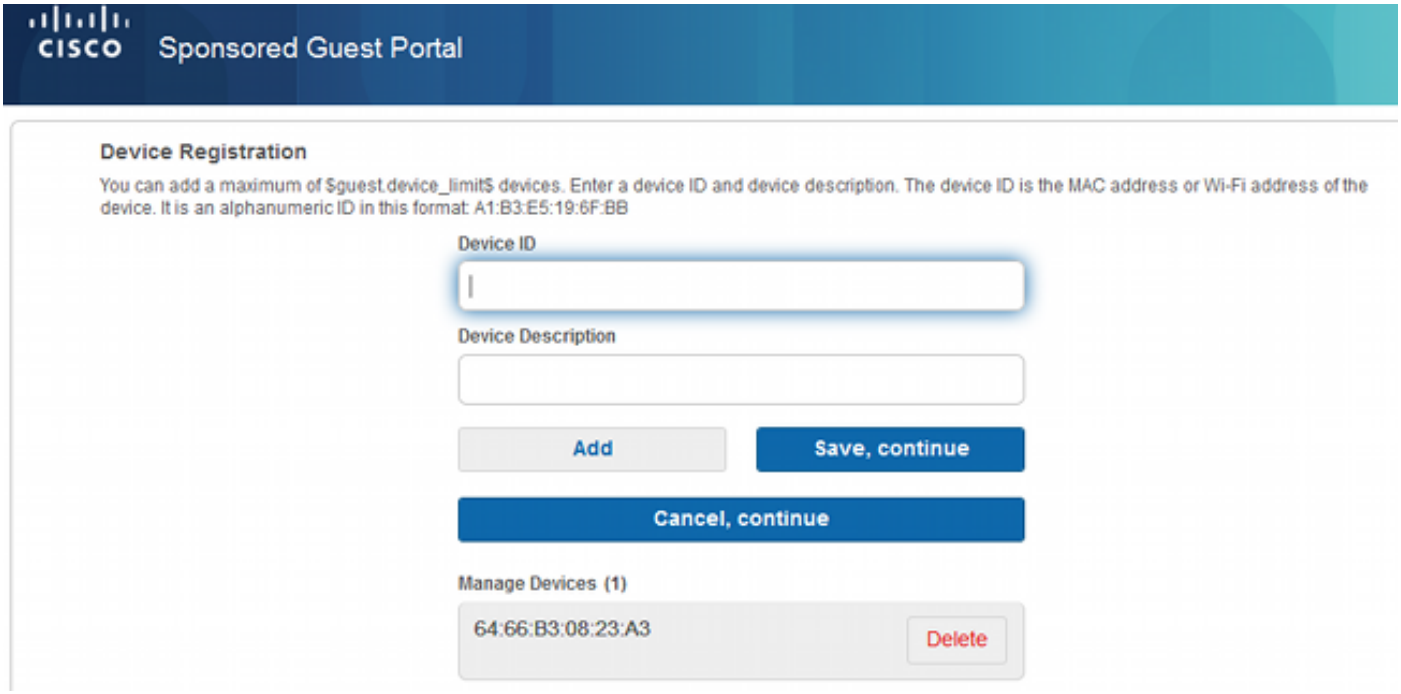
4. Een sms wordt bij de gekozen provider afgeleverd en het telefoonnummer:



5. U kunt sms Providers configureren onder **Beheer > Systeem > Instellingen > Sms Gateway**.

Apparaatregistratie

Als de optie **Demonstranten toestaan om apparaten te registreren** is geselecteerd na het inloggen van een gastgebruiker en het erkennen van de AUP, kunt u apparaten registreren:

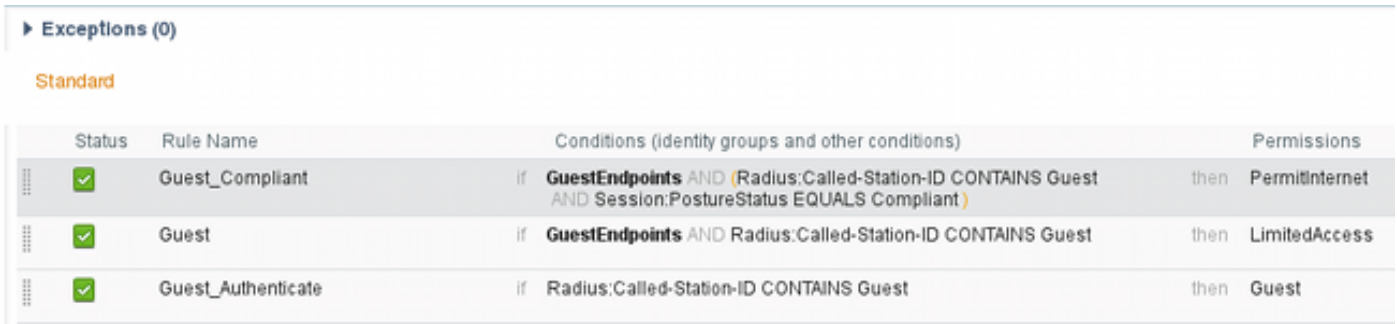


Merk op dat het apparaat al automatisch is toegevoegd (dit staat in de lijst Apparaten beheren). Dit komt doordat **gastenapparaten automatisch registreren** is geselecteerd.

postuur

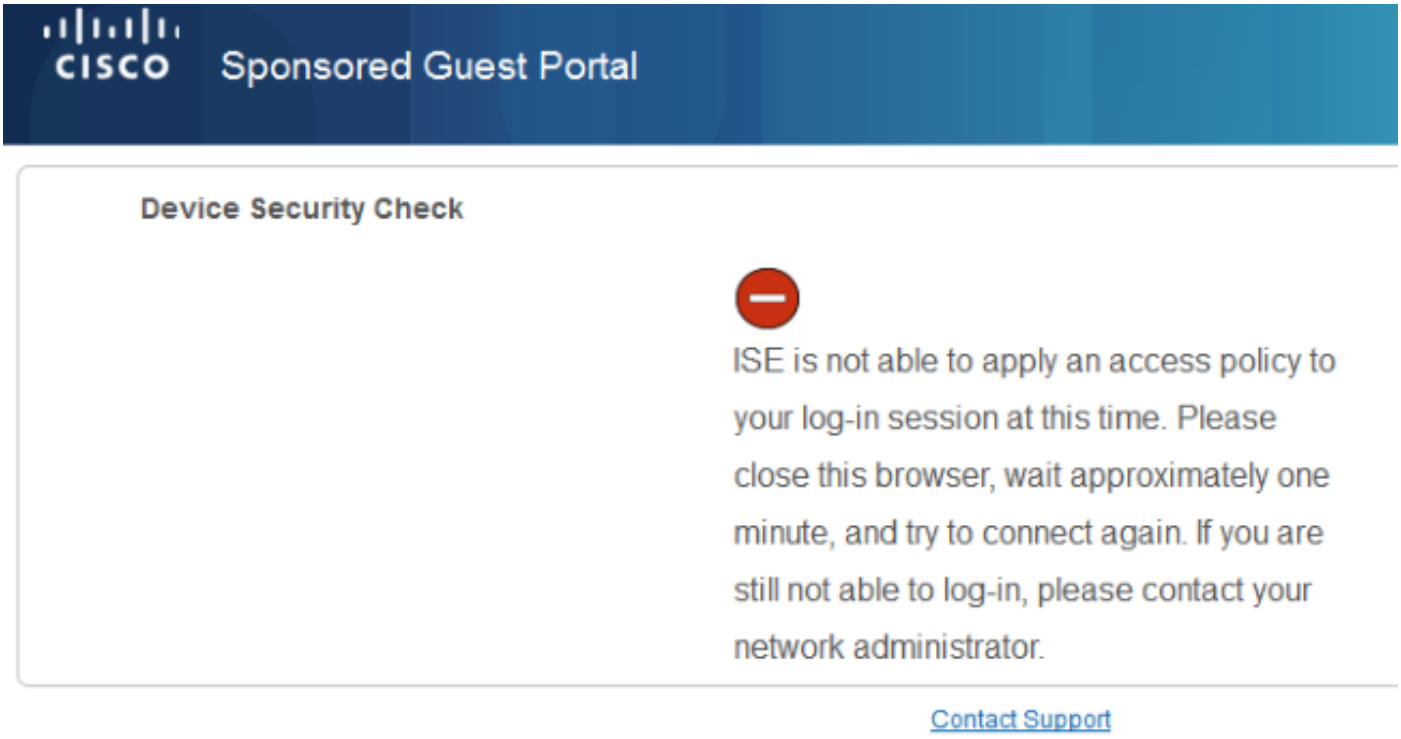
Als de optie **Eisen dat het** gastenapparaat voldoet wordt geselecteerd, dan worden de gastgebruikers van voorziening voorzien van een Agent die de houding (NAC/Web Agent) uitvoert na zij inloggen en de AUP (en naar keuze apparatenregistratie uitvoeren) accepteert. ISE verwerkt regels voor clientprovisioning om te beslissen welke agent moet worden voorzien. Vervolgens verricht de agent die op het station draait de posterijen (volgens de Postregels) en stuurt de resultaten naar de ISE, die de CoA opnieuw bevestigt om indien nodig de vergunningsstatus te wijzigen.

Mogelijke vergunningsregels lijken hierop:



De eerste nieuwe gebruikers die Guest_Authenticate regel tegenkomen richten zich terug naar het portaal van de Gast in het Register. Nadat de gebruiker zichzelf heeft geregistreerd en inlogt, verandert CoA de vergunningsstatus en krijgt de gebruiker beperkte toegang tot het uitvoeren van postuur en herstel. Alleen nadat de NAC Agent is bevoorraad en het station is compatibel, verandert CoA de vergunningsstatus opnieuw om toegang tot het internet te verlenen.

Typische problemen met houding zijn onder meer het ontbreken van correcte regels voor clientprovisioning:



Dit kan ook worden bevestigd als u gast.log bestand (nieuw in ISE versie 1.3) onderzoekt:

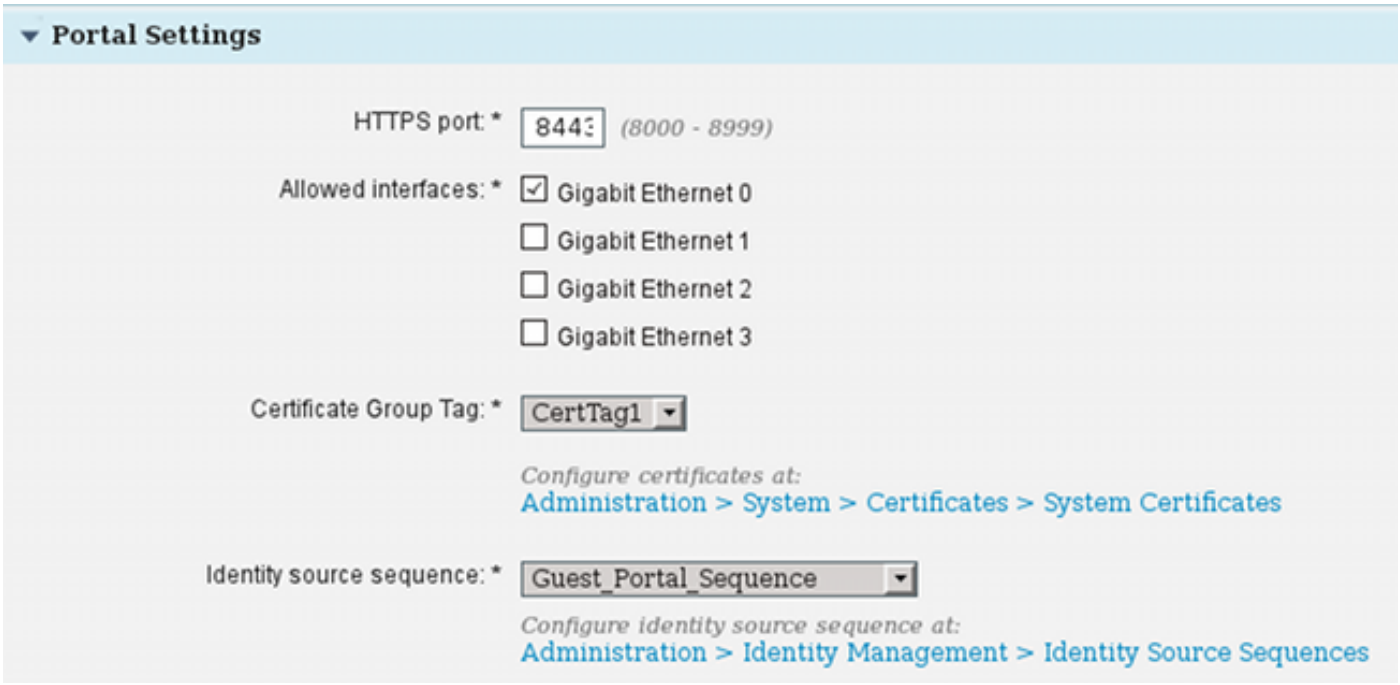
```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

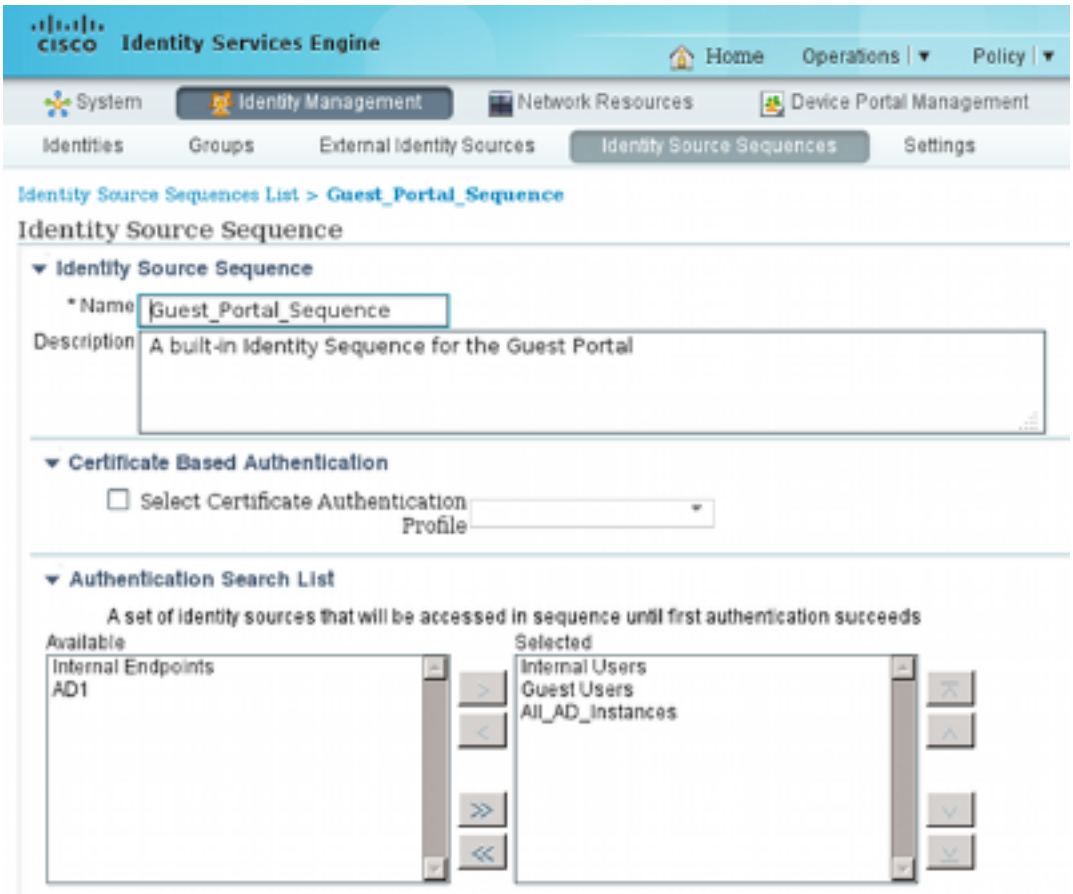
Als de optie **Laat werknemers persoonlijke apparaten op de netwerk** optie **gebruiken** wordt geselecteerd, kunnen de gebruikers van bedrijven die dit portaal gebruiken door BYOD stromen en persoonlijke apparaten registreren. Voor gastgebruikers verandert deze instelling niets.

Wat betekent "werknemers die portaal als gast gebruiken"?

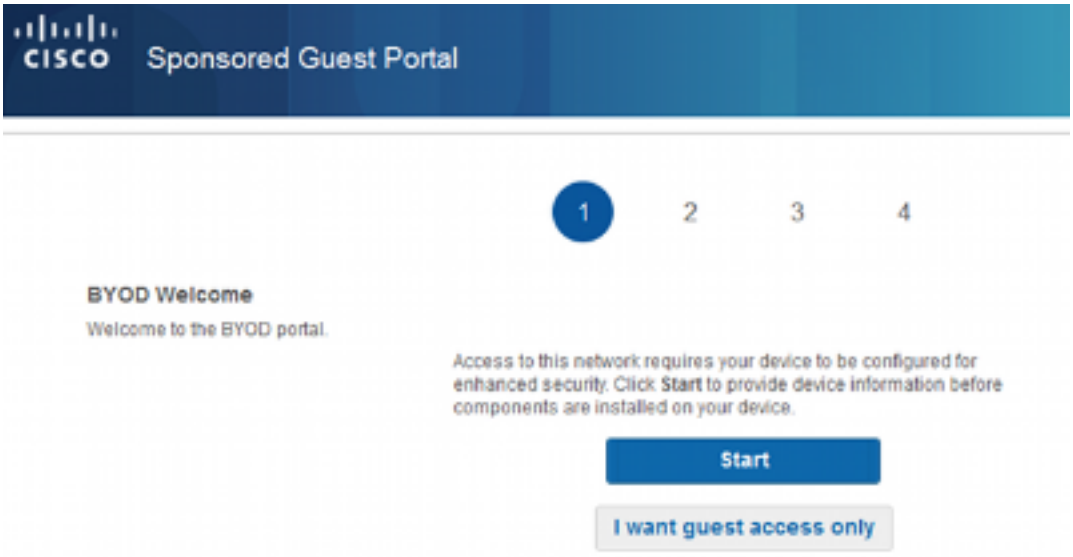
In de standaardinstelling worden gastportals geconfigureerd met de **Guest_Portal_Sequence** Identity Store:



Dit is de interne opslagvolgorde die eerst de interne gebruikers probeert (voor gebruikers van de gast):



Wanneer in deze fase in het gastenportal de gebruiker inzendingen verstrekt die in de winkel Interne gebruikers zijn gedefinieerd en er gebeurt de BYOD-omleiding:



Op deze manier kunnen bedrijven BYOD uitvoeren voor persoonlijke apparaten.

Wanneer in plaats van interne gebruikers aanmeldingsgegevens worden verstrekt, worden de gebruikers van de Gast voorzien, wordt de normale stroom voortgezet (geen BYOD).

VLAN-wijziging

Dit is een zelfde optie als de verandering van VLAN die voor het portaal van de Gast in ISE versie 1.2 wordt gevormd. Het staat u toe om activeX of een Java applet te lopen, die DHCP om te ontgrendelen en te vernieuwen in werking stelt. Dit is nodig als CoA de verandering van VLAN voor het eindpunt in werking stelt. Wanneer MAB wordt gebruikt, is het eindpunt niet op de hoogte van een verandering van VLAN. Een mogelijke oplossing is om VLAN (DHCP-release/vernieuwing) met de NAC Agent te wijzigen. Een andere optie is om een nieuw IP-adres aan te vragen via de applicatie die op de webpagina wordt teruggestuurd. Een vertraging tussen release/CoA/rew kan worden ingesteld. Deze optie wordt niet ondersteund voor mobiele apparaten.

Gerelateerde informatie

- Postservices op Cisco ISE Configuration Guide
- Draadloze BYOD met Identity Services Engine
- ISE SCEP-ondersteuning voor BYOD-configuratievoorbeeld
- Cisco ISE 1.3 beheerdershandleiding
- Central-webverificatie in het configuratievoorbeeld van WLC en ISE
- Central-webverificatie met FlexConnect APs op een WLC met ISE-configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems