

Configuratievoorbeeld van ISE versie 1.3, zelfgeregistreerd Guest Portal

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Topologie en stroom](#)
- [Configureren](#)
- [WLC](#)
- [ISE](#)
- [Verifiëren](#)
- [Problemen oplossen](#)
- [Optionele configuratie](#)
- [Instellingen voor zelfregistratie](#)
- [Instellingen inloggen](#)
- [Instellingen apparaatregistratie](#)
- [Instellingen voor apparaatnaleving](#)
- [BYOD-instellingen](#)
- [Door sponsor goedgekeurde rekeningen](#)
- [Credentials leveren via sms](#)
- [Apparaatregistratie](#)
- [postuur](#)
- [BYOD](#)
- [VLAN-wijziging](#)
- [Gerelateerde informatie](#)

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:

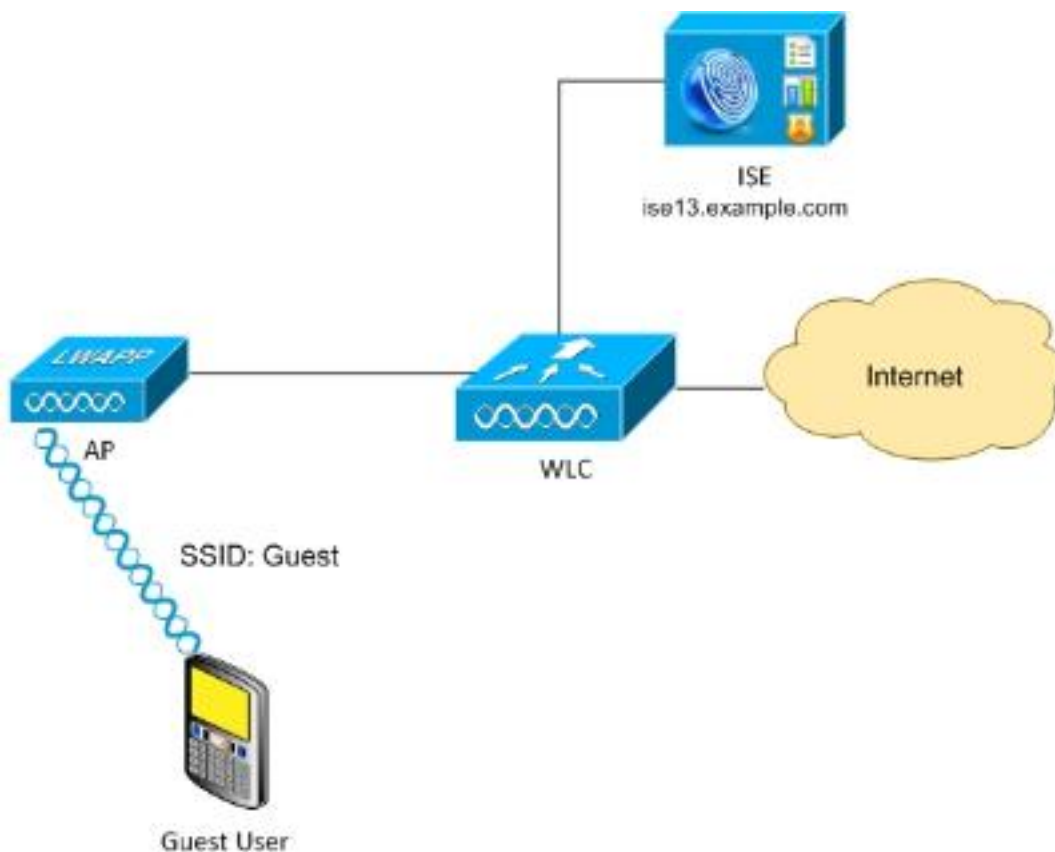
- ISE-implementaties en Guest-stromen
- Configuratie van draadloze LAN-controllers (WLC)

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 Recht 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.

CISCO [MONITOR](#) [WLANs](#) [CONTROLLER](#) [WIRELESS](#) [SECURITY](#)

Security

- ▼ **AAA**
 - General
 - ▼ **RADIUS**
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - ▶ TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- ▶ **Local EAP**
- ▶ **Priority Order**
- ▶ **Certificate**
- ▶ **Access Control Lists**

RADIUS Authentication Servers > Edit

Server Index	2	
Server Address	10.62.97.21	
Shared Secret Format	ASCII ▼	
Shared Secret	●●●	
Confirm Shared Secret	●●●	
Key Wrap	<input type="checkbox"/>	(Designed for FIPS custome
Port Number	1812	
Server Status	Enabled ▼	
Support for RFC 3576	Enabled ▼	
Server Timeout	5	seconds
Network User	<input checked="" type="checkbox"/>	Enable
Management	<input checked="" type="checkbox"/>	Enable
IPSec	<input type="checkbox"/>	Enable

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:

Security

- ▼ **AAA**
 - General
 - ▼ **RADIUS**
 - Authentication

RADIUS Authentication Servers

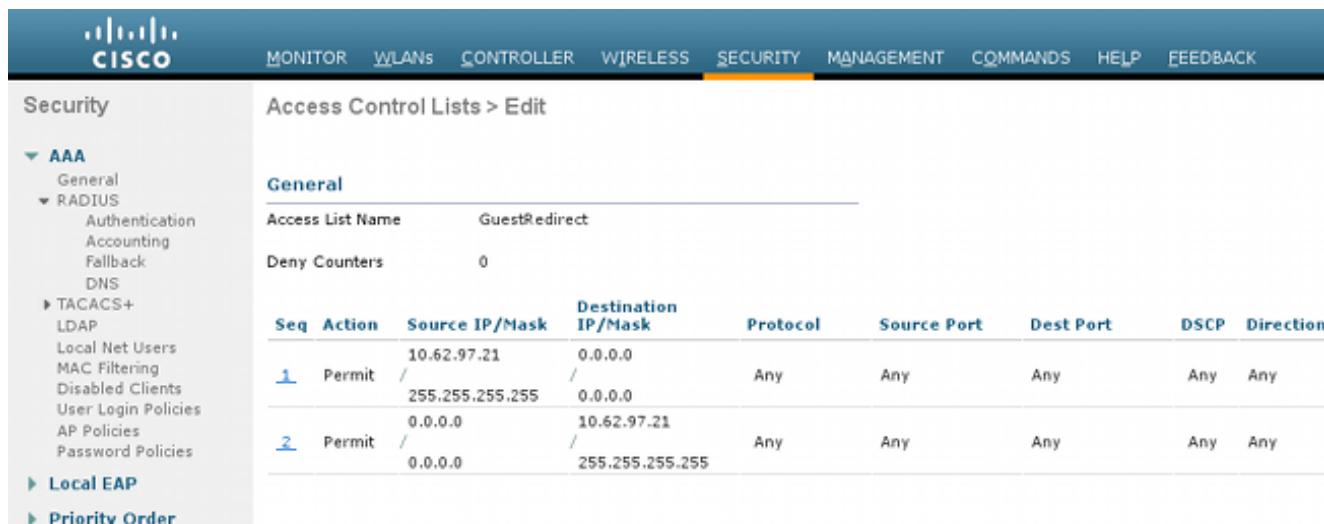
Acct Call Station ID Type ?	IP Address ▼	
Auth Call Station ID Type	AP MAC Address:SSID ▼	

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

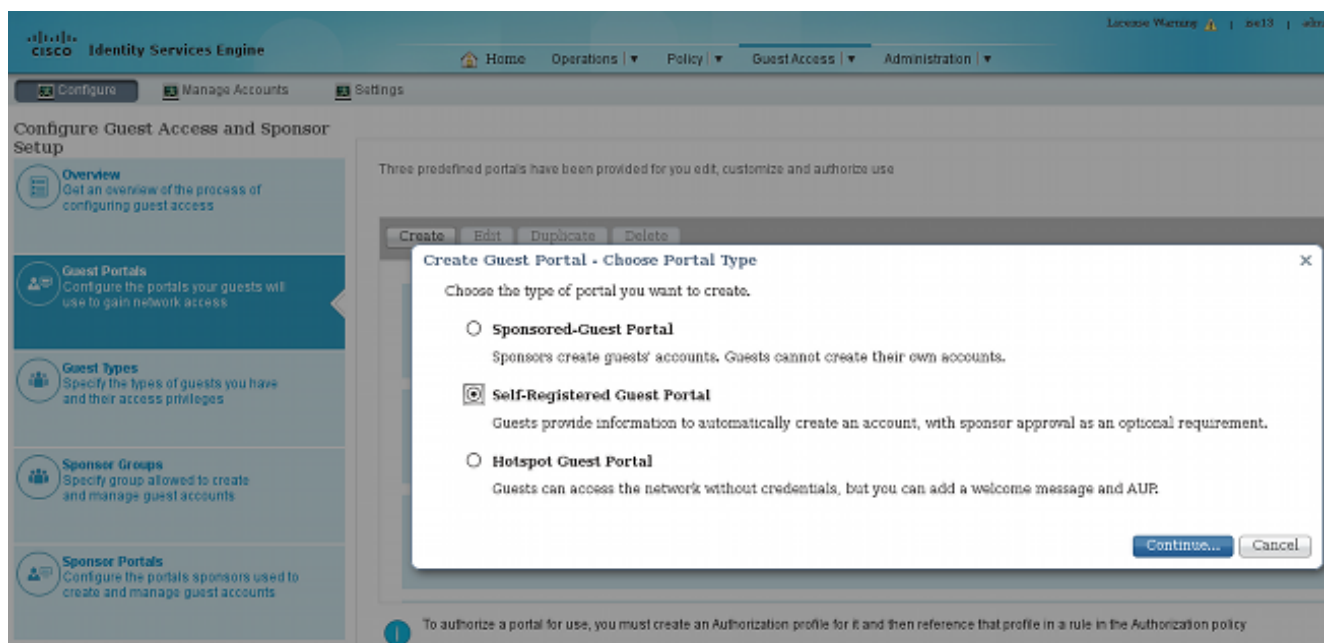
Hier is een voorbeeld voor GuestRedirect ACL (moet verkeer naar/van ISE van redirectie uitsluiten):



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	10.62.97.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	10.62.97.21 / 255.255.255.255	Any	Any	Any	Any	Any

ISE

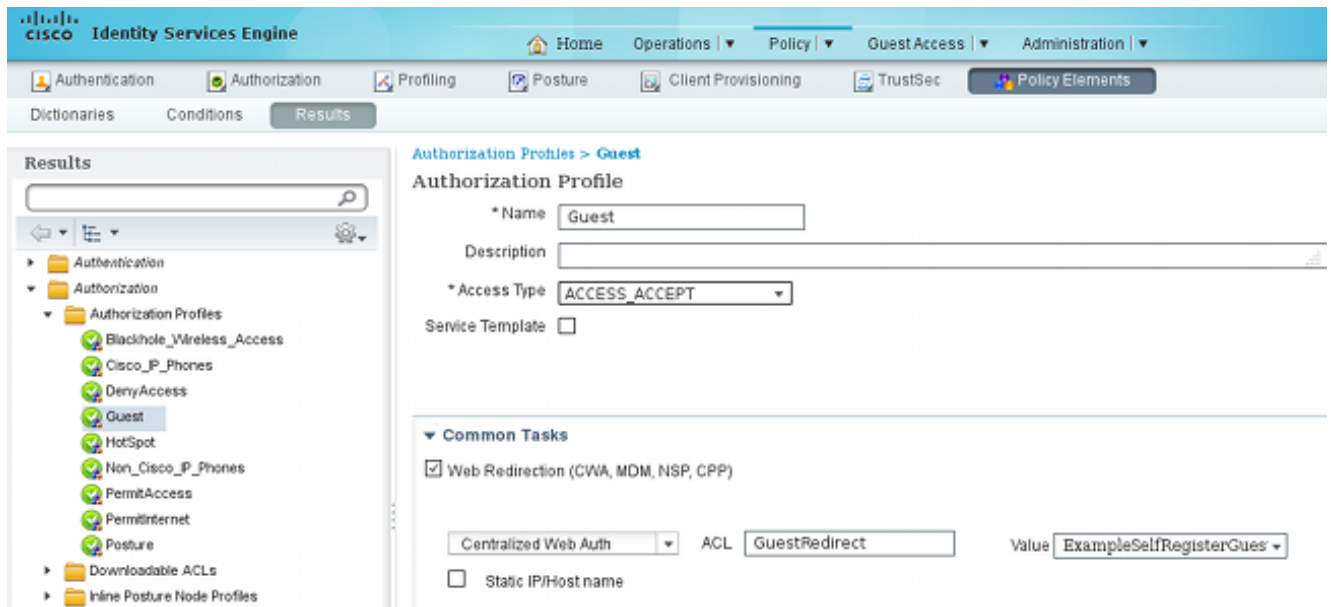
1. navigeren om **toegang te gisten > Portals van de Gast te configureren** en een nieuw type portaal te maken, zelfgeregistreerd Guest Portal:



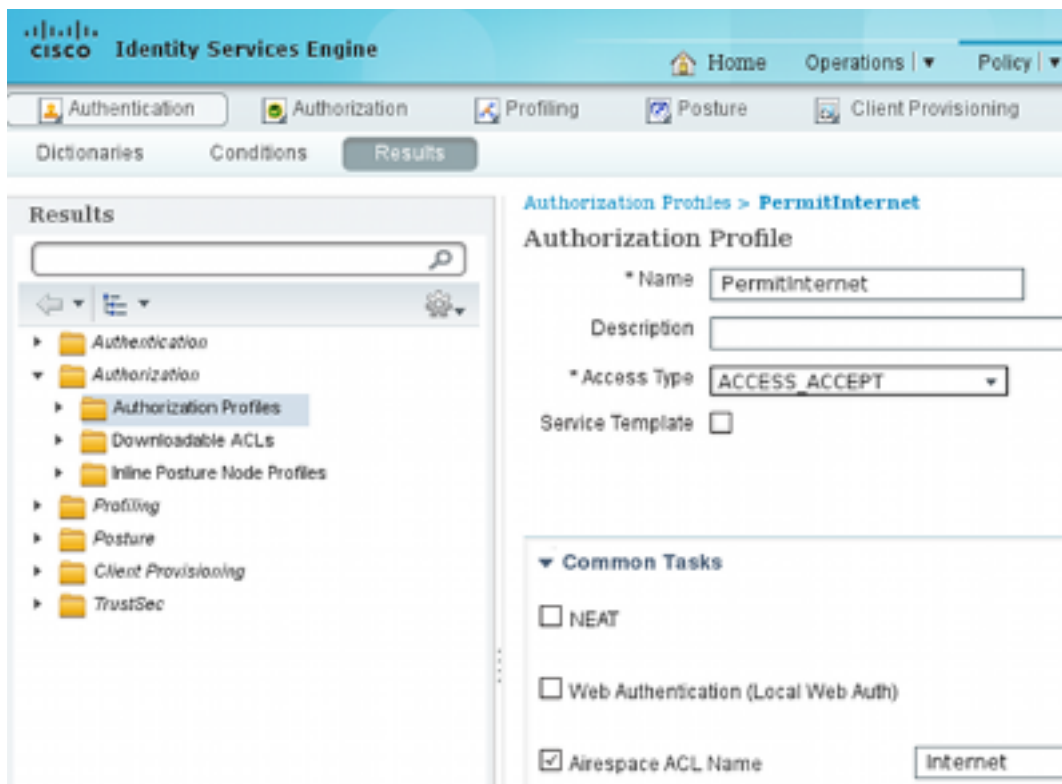
2. Kies de naam van het portaal die verwezen zal worden in het vergunningsprofiel. Standaard alle andere instellingen instellen. Onder Portal Pagina-aanpassing kunnen alle pagina's die worden gepresenteerd, worden aangepast.

3. Bewerkingen autorisatie configureren:

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



Internet (met Airespace ACL gelijk internet)



- 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.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then PermitInternet
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

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 Netwerktogangsapparaat 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:

https://ise13.example.com:8443/portal/PortalSetup.action?portal=6f48b7c0-1967-11e4-a20e-0050569c3f63& ☆ Google

CISCO Sponsored Guest Portal

Sign On
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

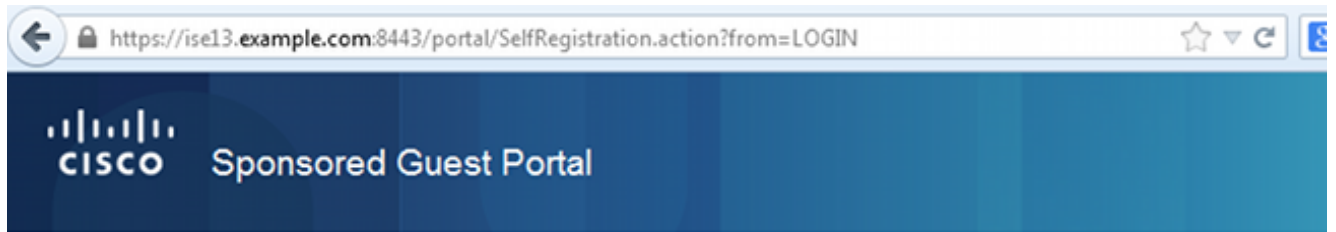
Passcode:

Sign On

[Don't have an account?](#)

[Contact Support](#)

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).



Create Account

Please provide us with some information so we can create an account for you.

Registration Code*

cisco

Username

guest1

First name

Michal

Last name

garcarz

Email address

mgarcarz@cisco.com

Phone number

666666666

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:

▶ **Guest Email Settings**

Identify the SMTP server and specify

▶ **Guest Locations and SSIDs**

Specify the locations where you want

▶ **Guest Password Policy**

Specify the policy settings that will

▼ **Guest Username Policy**

Specify the policy settings that will

Configure username requirements that will be enforced for guest usernames. Usernames

Username Length

Minimum username length: (1-64 characters)

Username Criteria for Known Guests

If data is available, base username on:

- First name and last name
- Email address

Characters Allowed in Randomly-Generated Usernames

Alphabetic:

Minimum alphabetic: (0-64)

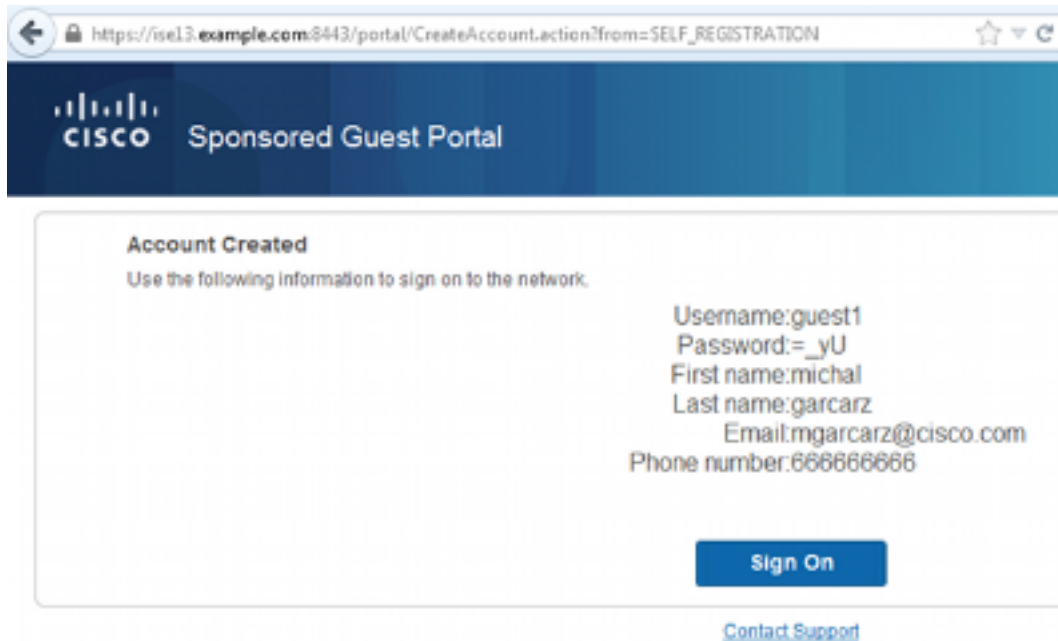
Numeric:

Minimum numeric: (0-64)

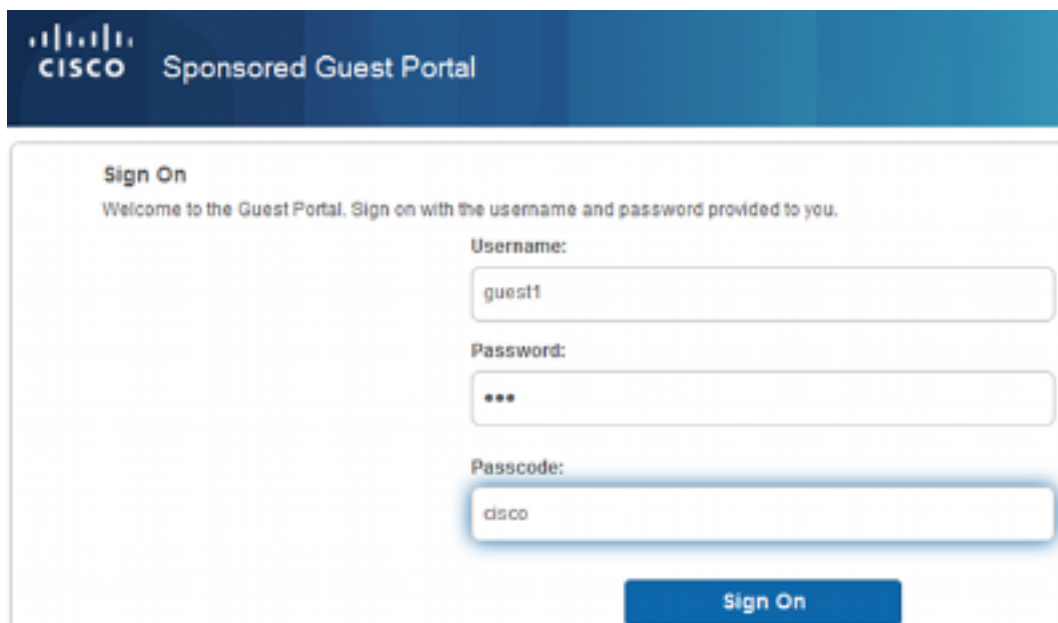
Special:

Minimum special: (0-64)

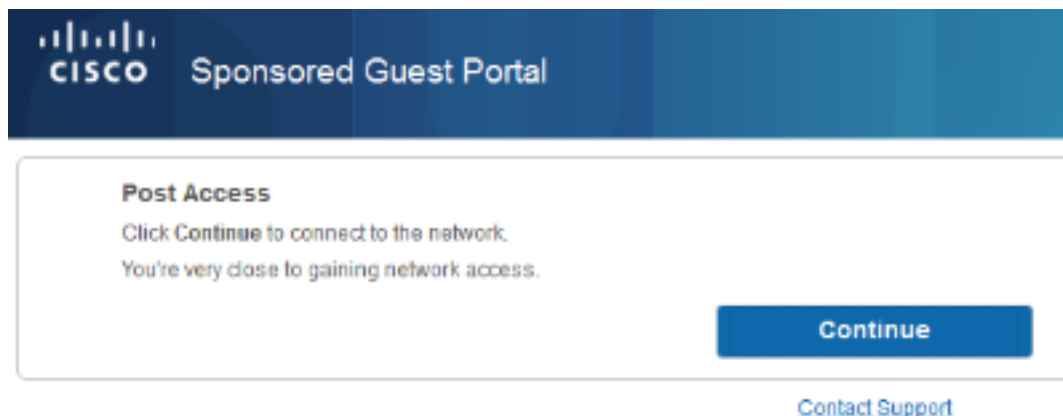
4. Na het maken van succesvolle account wordt u aangeleverd met aanmeldingsgegevens (wachtwoord dat gegenereerd wordt als per beleid van een gastwachtwoord):



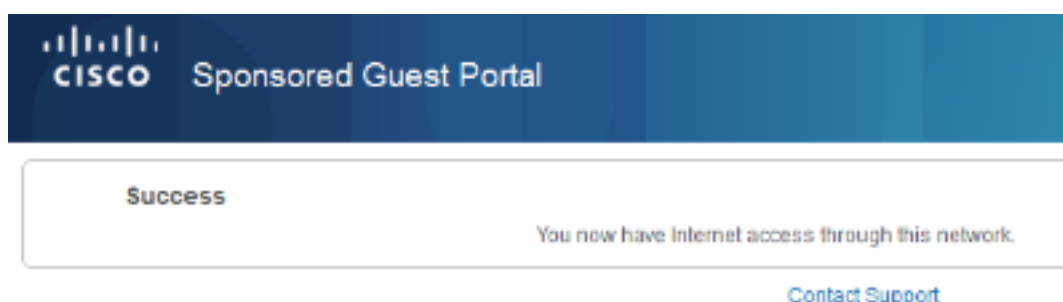
5. Klik op **Aanmelden** en geef referenties (er kan een aanvullende toegangswachtcode nodig zijn als deze is ingesteld onder het Guest Portal; dit is een ander beveiligingsmechanisme dat alleen personen die het wachtwoord kennen , de mogelijkheid biedt in te loggen .



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:

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	🔴		0	guest1					Session State is Started
2014-08-01 13:19:52...	🟢			guest1	Default >> MAB	Default >> Guest	PermitInternet	User Identity Gro...	Authorize-Only succeeded
2014-08-01 13:19:52...	🟢								Dynamic Authorization succeeded
2014-08-01 13:18:29...	🟢			guest1				GuestType_DAILY	Guest Authentication Passed
2014-08-01 13:16:31...	🟢			64:66:B3:08:23	Default >> MAB >> ..	Default >> Guest_...	Guest		Authentication succeeded

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-reauthenticiek, 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 Acceptance	
2014-08-01 13:18:49.9	quest1	64-66-83-08-23-A3	10.221.0.218				Guest user has accepted the use policy	
2014-08-01 13:18:08.7	quest1	64-66-83-08-23-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"):

The screenshot shows the Cisco Sponsor Portal interface. At the top, there is a navigation bar with the Cisco logo and 'Sponsor Portal' text. Below the navigation bar, there are several tabs: 'Create Accounts', 'Manage Accounts (1)', 'Pending Accounts (0)', and 'Notices (0)'. Underneath these tabs, there are buttons for 'Resend', 'Extend', 'Edit', 'Suspend', 'Reinstate', 'Delete', 'Reset Password', and 'Print'. The main content area displays the following account details:

First name:	michal
Last name:	garcarz
Username:	quest1
Password:	=_yU
Email address:	mgarcarz@cisco.com
Company:	
Phone number:	666666666
Person being visited(email):	
Reason for visit:	
Guest type:	DAILY
SMS provider:	
State:	Awaiting Initial Login
From date:	08/01/2014 12:58
To date:	08/02/2014 12:58
Location:	
SSID:	
Language:	English
Group tag:	
Time left:	0,23,47

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:

Account Created

Use the following information to sign on to the network.

Email send failure

First name:michal

Last name:garcarz

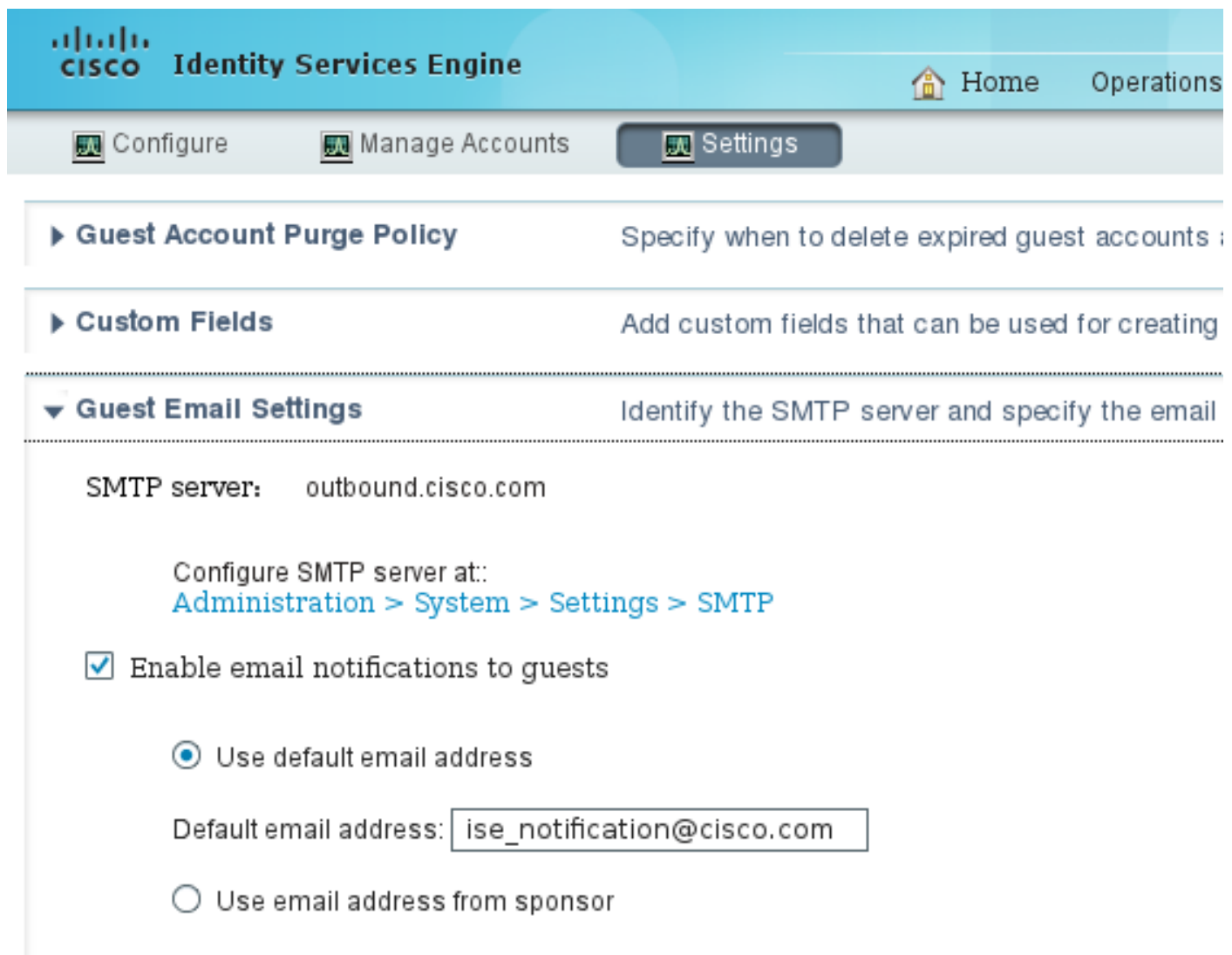
Email:mgarcarz@cisco.com

Sign On

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:



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". On the right side of the navigation bar, there are links for "Home" and "Operations". Below the navigation bar, there are three main tabs: "Configure", "Manage Accounts", and "Settings". The "Settings" tab is currently selected. Under the "Settings" tab, there are three main sections: "Guest Account Purge Policy", "Custom Fields", and "Guest Email Settings". The "Guest Email Settings" section is expanded, showing the following configuration options:

- SMTP server: outbound.cisco.com
- Configure SMTP server at:
[Administration](#) > [System](#) > [Settings](#) > [SMTP](#)
- Enable email notifications to guests
 - Use default email address
 - Default email address:
 - Use email address from sponsor

Account Created

Use the following information to sign on to the network.

First name:michal
Last name:garcarz
Email:mgarcarz@cisco.com

Sign On


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** verwijderd. 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 Credential notification when approval using Section** (mark e-mail/sms).

Aan de opdrachtgever wordt een e-mail verzonden:

Guest Approval Request <ise_notification@cisco.com>

From: ise_notification@cisco.com
Subject: Guest Approval Request
To: Me <mgarcarz@cisco.com>

Reply Forward



Please approve (or deny) this self-registering guest. The guest provided the following information:
Username: guest7
First Name: michal
Last Name: garcarz

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

CISCO Sponsor Portal Welcome sponsor

Create Accounts Manage Accounts (1) Pending Accounts (1) Notices (0)

Approve Deny Refresh

<input type="checkbox"/>	Username	State	First Name	Last Name	Email address	Phone number	Company
<input checked="" type="checkbox"/>	guest7	Pending Approval	michal	garcarz	mgarcarz@cisco.com		

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

die per e-mail of sms ontvangen worden).

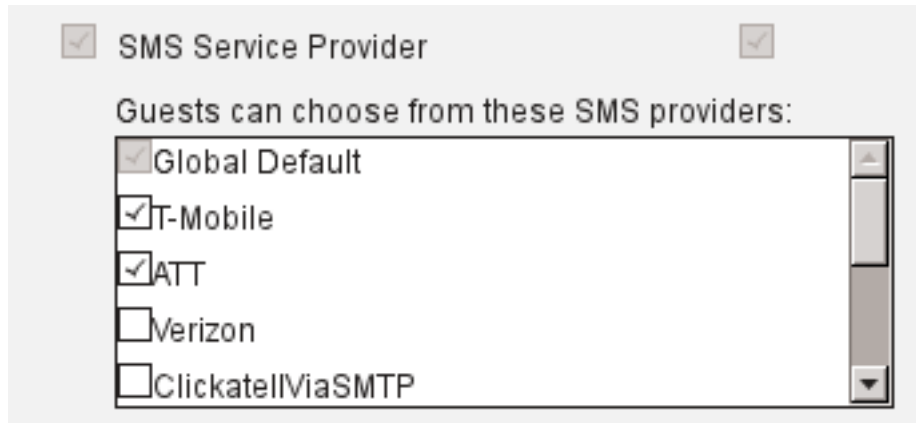
Samengevat worden er drie e-mailadressen gebruikt in deze flow:

- 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:



The screenshot shows a configuration window for SMS Service Providers. At the top, there is a checkbox labeled "SMS Service Provider" which is checked. Below this, the text "Guests can choose from these SMS providers:" is displayed. A list box contains five items, each with a checkbox: "Global Default" (checked), "T-Mobile" (checked), "ATT" (checked), "Verizon" (unchecked), and "ClickatellViaSMTP" (unchecked). The list box has a vertical scrollbar on the right side.

2. Controleer de **Send Credential notification when approval** met behulp van: **Sms** aanvinkvakje.
3. Vervolgens wordt de gastgebruiker gevraagd de beschikbare provider te kiezen wanneer hij een account aanmaakt:

← https://ise13.example.com:8443/portal/SelfRegistration.action?from=LOGIN ☆ ▾ ↻

Phone number*

666666666

Company

SMS provider*

T-Mobile

T-Mobile
ATT
Global Default

Reason for visit

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

Account Created

Use the following information to sign on to the network.

First name:michal
Last name:garcarz
Email:mgarcarz@cisco.com
Phone number:666666666
SMS Provider:Global Default

Sign On

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:

Device Registration

You can add a maximum of \$guest.device_limit\$ devices. Enter a device ID and device description. The device ID is the MAC address or Wi-Fi address of the device. It is an alphanumeric ID in this format: A1:B3:E5:19:6F:BB

Device ID

Device Description

Manage Devices (1)

64:66:B3:08:23:A3	<input type="button" value="Delete"/>
-------------------	---------------------------------------

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 postureringen (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:

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest_Compliant	if GuestEndpoints AND (Radius:Called-Station-ID CONTAINS Guest AND Session:PostureStatus EQUALS Compliant)	then PermitInternet
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then LimitedAccess
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

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 bevoorrad 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:

Device Security Check

ISE is not able to apply an access policy to your log-in session at this time. Please close this browser, wait approximately one minute, and try to connect again. If you are still not able to log-in, please contact your network administrator.

[Contact Support](#)

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**:

▼ Portal Settings

HTTPS port: * (8000 - 8999)

Allowed interfaces: * Gigabit Ethernet 0
 Gigabit Ethernet 1
 Gigabit Ethernet 2
 Gigabit Ethernet 3

Certificate Group Tag: *

Configure certificates at:
[Administration > System > Certificates > System Certificates](#)

Identity source sequence: *

Configure identity source sequence at:
[Administration > Identity Management > Identity Source Sequences](#)

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

CISCO Identity Services Engine Home Operations | Policy |

System Identity Management Network Resources Device Portal Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

[Identity Source Sequences List > Guest_Portal_Sequence](#)

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
AD1	Guest Users
	All_AD_Instances

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:

1

2

3

4

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Start

I want guest access only

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](#)