

ISE Self Registered Guest Portal configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie en gegevensstroom](#)

[Configureren](#)

[WLC](#)

[ISE](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Optionele configuratie](#)

[Instellingen voor zelfregistratie](#)

[Aanmelden als gast](#)

[Instellingen voor apparaatregistratie](#)

[Instellingen voor naleving van gastapparaat](#)

[BYOD-instellingen](#)

[Door sponsor goedgekeurde accounts](#)

[Credentials leveren via sms](#)

[Apparaatregistratie](#)

[houding](#)

[BYOD](#)

[VLAN-wijziging](#)

[Gerelateerde informatie](#)

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)

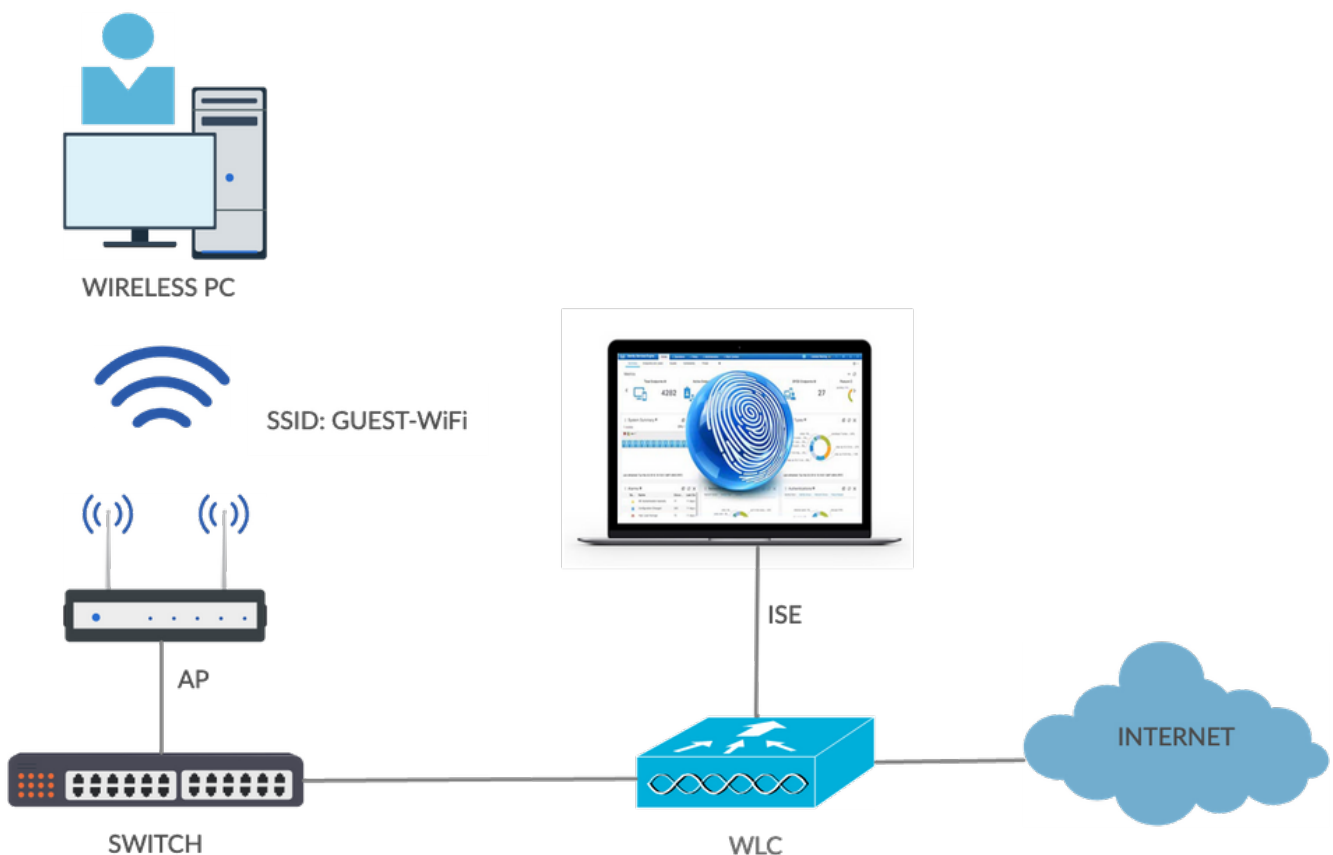
Gebruikte componenten

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 Airspace 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).

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
 - Access Control Lists
 - CPU Access Control Lists
 - FlexConnect ACLs
 - Layer2 ACLs
 - URL ACLs

RADIUS Authentication Servers > Edit

Server Index: 2

Server Address(Ipv4/Ipv6): 10.106.32.25

Shared Secret Format: ASCII

Shared Secret: ***

Confirm Shared Secret: ***

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 2 seconds

Network User: Enable

Management: Enable

Management Retransmit Timeout: 2 seconds

Tunnel Proxy: Enable

[Realm List](#)

IPsec: Enable

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:

Security

- AAA
 - General
 - RADIUS
 - Authentication

RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

RADIUS Accounting Servers

Acct Called Station ID Type: IP Address

MAC Delimiter: Hyphen

Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	* 10.106.32.25

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):

Security

Access Control Lists > Edit

General

Access List Name: GuestRedirect

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.106.32.25 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.106.32.25 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

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**.

Cisco ISE

Work Centers · Guest Access

Overview Identities **Identity Groups** Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements

Identity Groups

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

* Name: Cisco_GuestEndpoints

Description:

Parent Group:

Submit Cancel

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.

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Guest type name: *

Guest-Daily

Description:

Guest account access for 30 days

Language File ▼**Collect Additional Data**[Custom Fields...](#)**Maximum Access Time**

Account duration starts

 From first login From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

5 days ▼ Default 1 (1-999) Allow access only on these days and times:From 9:00 AM To 5:00 PM Sun Mon Tue Wed Thu Fri Sat +

Configure guest Account Purge Policy at:

[Work Centers](#) > [Guest Access](#) > [Settings](#) > [Guest Account Purge Policy](#)**Login Options** Maximum simultaneous logins 3 (1-999)

When guest exceeds limit:

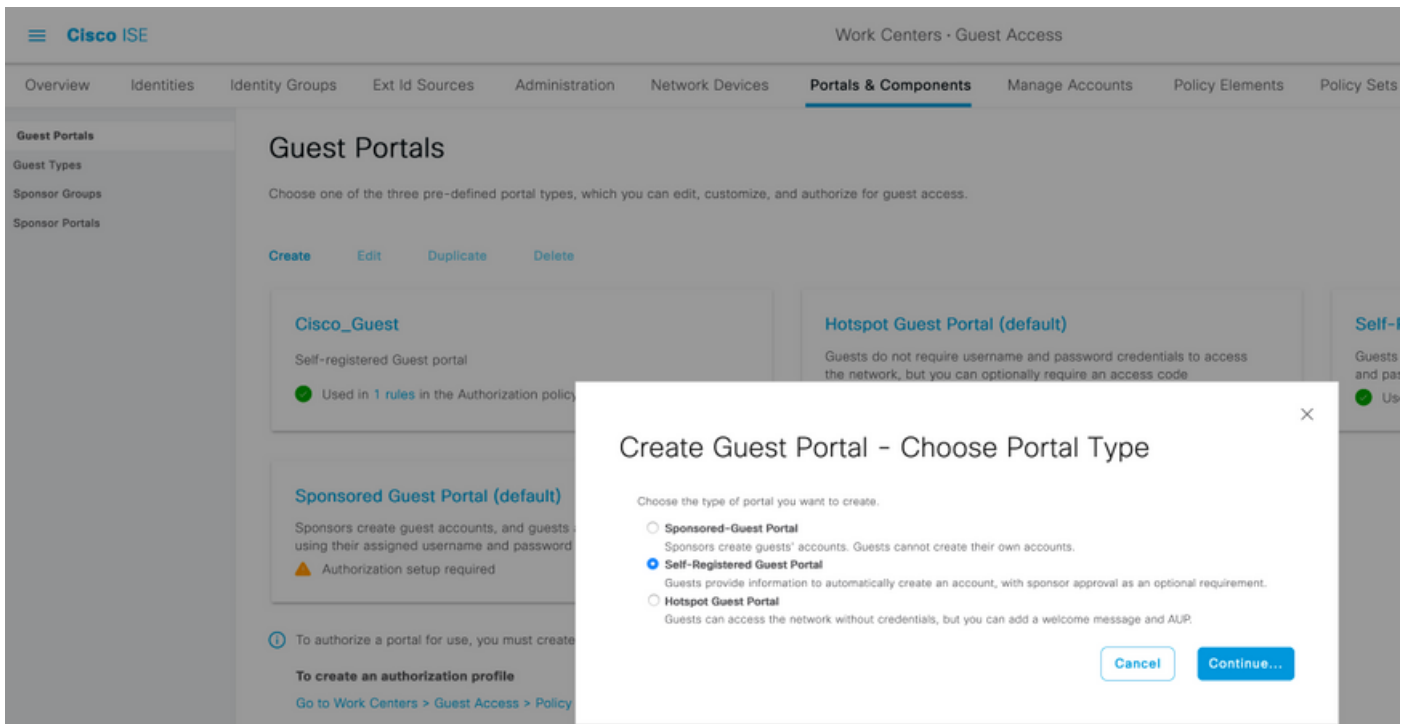
 Disconnect the oldest connection Disconnect the newest connection Redirect user to a portal page showing an error message ⓘ

This requires the creation of an authorization policy rule

Maximum devices guests can register: 5 (1-999)

Endpoint identity group for guest device registration: Cisco_GuestEndpoints ▼ ⓘ

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

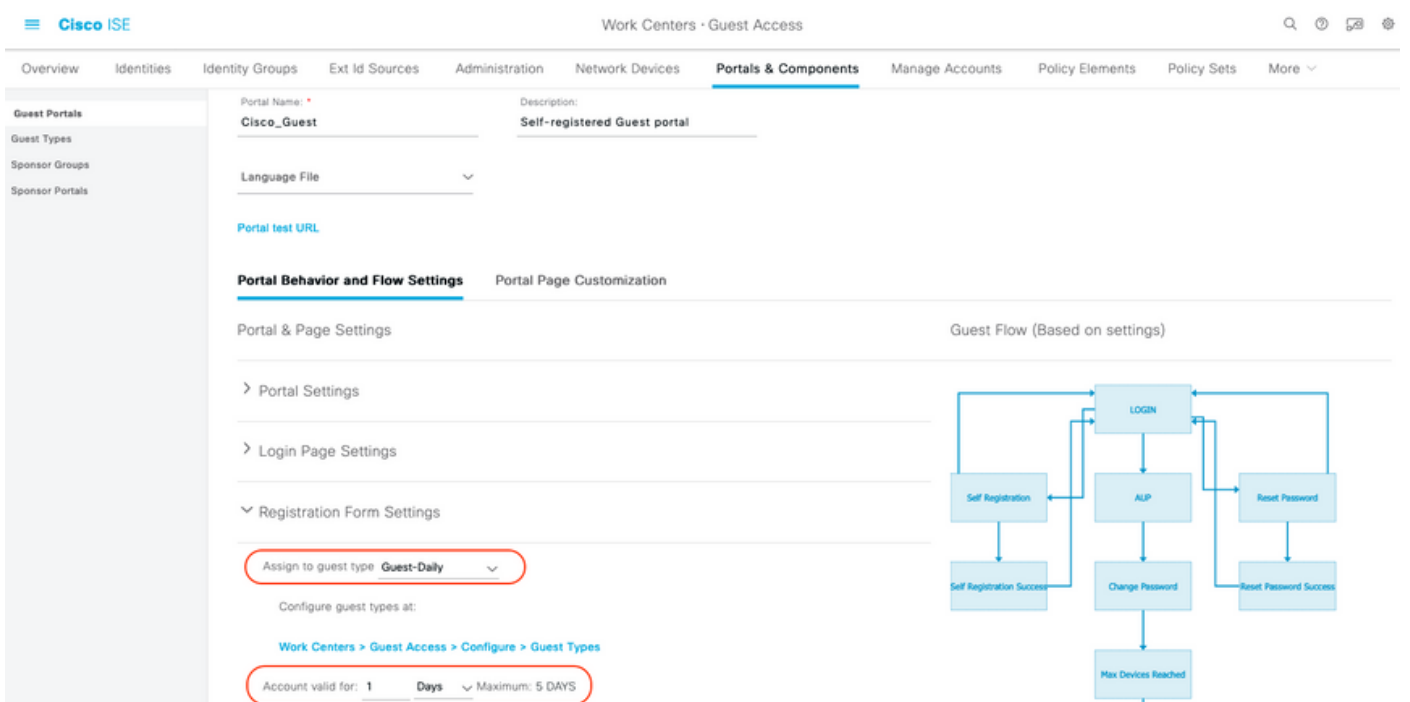


5. Kies de portaalnaam, verwijst naar het Gasttype dat eerder is gemaakt en verstuur de aanmeldingsinstellingen onder Registratieformulier instellingen om de aanmeldingsgegevens via e-mail te versturen.

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.

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb navigation is: Work Centers · Guest Access > Policy Elements. The left sidebar contains navigation options: Overview, Identities, Identity Groups, Ext Id Sources, Administration, Network Devices, Portals & Components, Manage Accounts, and Policy Elements (selected). The main content area is titled 'Authorization Profile' and shows the following configuration:

- Name:** Guest-Portal
- Description:** Redirect to Self-registered guest portal
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:** ⓘ
- Agentless Posture:** ⓘ
- Passive Identity Tracking:** ⓘ

Under the 'Common Tasks' section, the following options are visible:

- Web Redirection (CWA, MDM, NSP, CPP) ⓘ
- Centralized Web Auth (dropdown menu)
- Display Certificates Renewal Message
- Static IP/Host name/FQDN
- Suppress Profiler CoA for endpoints in Logical Profile

In the 'Web Redirection' configuration, the 'ACL' is set to 'GuestRedirect' and the 'Value' is set to 'Cisco_Guest'. These two fields are circled in red in the original image.

- Permit_Internet (met Airespace ACL gelijk internet)

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Authorization Profiles > Permit_internet

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Airespace ACL Name

Airespace IPv6 ACL Name

ASA VPN

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).

Cisco ISE Work Centers · Guest Access

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **Policy Sets** More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	Wired_MAB Wireless_MAB	Internal Endpoints Options If Auth fail REJECT If User not found CONTINUE If Process fail DROP	0	

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

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Wifi_Guest_Access	AND IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB	Permit_internet x	Select from list	0
●	Wifi_Redirect_to_Guest_Portal	AND Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	Select from list	0

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 authenticaties van dat eindpunt generische regel die voor gastauthenticatie opnieuw richt.

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Temporary_Guest_Access	AND Network Access-UseCase EQUALS Guest Flow Wireless_MAB	Permit_internet x	Select from list	1
○	Permanent_Guest_Access	AND IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB	Permit_internet x	Select from list	2
●	Wifi_Redirect_to_Guest_Portal	AND Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	Select from list	3

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.

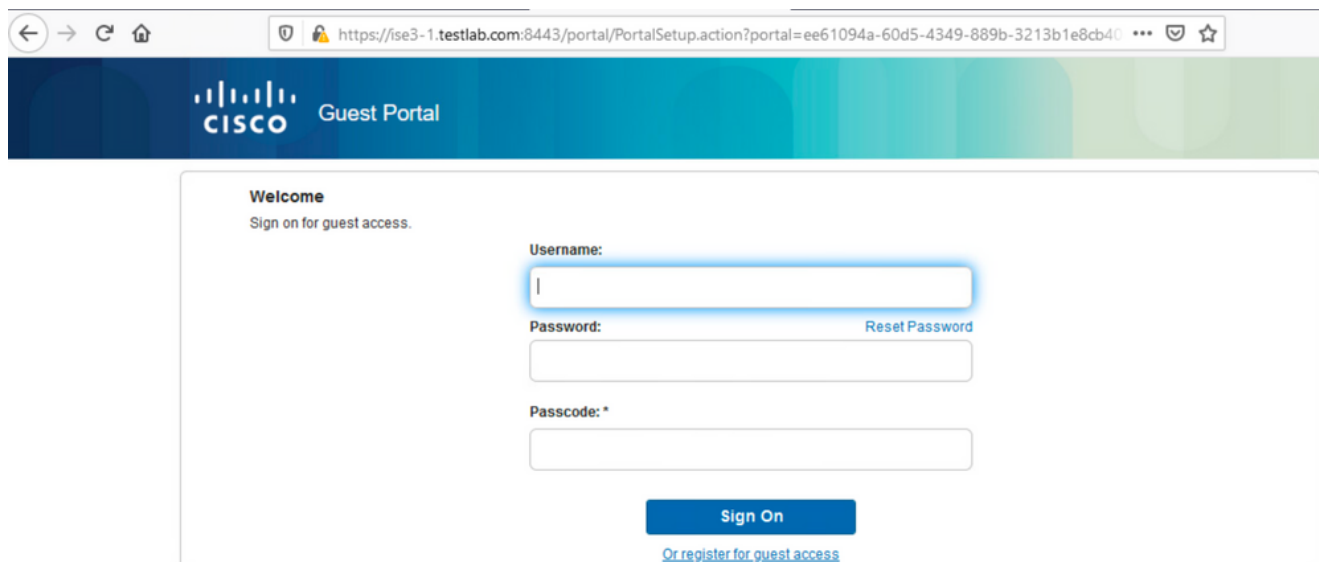
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html>

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.



← → ↻ 🏠

🔒 <https://ise3-1.testlab.com:8443/portal/PortalSetup.action?portal=ee61094a-60d5-4349-889b-3213b1e8cb40> ... 📄 ☆

CISCO Guest Portal

Welcome
Sign on for guest access.

Username:

Password: [Reset Password](#)

Passcode: *

[Sign On](#)

[Or register for guest access](#)

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).

https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN 80%

CISCO Guest Portal

Registration
Please complete this registration form:

Registration Code*
8015

Username
guest1

First name
Poonam

Last name
Garg

Email address*
poongarg@cisco.com

Mobile number
+91 0000000000

Company
Cisco

Person being visited(email)
abc@cisco.com

Reason for visit
Personal

Register **Cancel**

Activati
Go.to.Set

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:

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **More** ▾

Guest Account Purge Policy
Custom Fields
Guest Email Settings
Guest Locations and SSIDs
Guest Username Policy
Guest Password Policy
DHCP & DNS Services
Logging

Guest Username Policy

Configure username requirements that will be enforced for guest usernames. Usernames are not case sensitive.

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: ▾ ABCDEFGHIJKLMNOPQRSTUVWXYZ

Minimum alphabetic: (0-64)

Numeric: ▾ 23456789

Minimum numeric: (0-64)

Special: ▾

Minimum special: (0-64)

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:

https://fise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION

CISCO Guest Portal guest1 ⓘ

Account Created

Choose how to receive your login information, by text or email. Email Me attempts left:5

You can only click the button 5 times.

Username: guest1
Password: 3154
First name: Poonam
Last name: Garg
Email: poongarg@cisco.com
Mobile number: +910000000000
Company: Cisco
Location: India
SMS provider: Global Default
Person being visited (email): abc@cisco.com
Reason being visited: Personal

Your Guest Account Credentials



ise@testlab.com <ise@testlab.com>

Today at 9:47 AM

To: Poonam Garg (poongarg)



Hello Poonam,
Your guest account details:
Username: guest1
Password: 3154
First Name: Poonam
Last Name: Garg
Mobile Number:+910000000000
Valid From: 2020-11-07 09:43:50
Valid To: 2020-11-08 09:43:50
Person being visited: abc@cisco.com
Reason for visit: Personal

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).

The screenshot shows a web browser window with the URL https://ise3-1.testlab.com:8443/portal/SelfRegistrationSuccess.action?from=SELF_REGISTRATION_SUCCESS. The page header features the Cisco logo and the text "Guest Portal". The main content area is titled "Welcome" and "Sign on for guest access." It contains three input fields: "Username:" with the value "guest1", "Password:" with masked characters "****" and a "Reset Password" link, and "Passcode: *" with the value "8015". A blue "Sign On" button is positioned below the fields, with a link "[Or register for guest access](#)" underneath it.

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.

https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN

guest1

CISCO Guest Portal

Acceptable Use Policy
Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco Systems website.

Accept **Decline**

https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP

guest1

CISCO Guest Portal

Change Password
You are required to change your password now. Please enter a new password.

Current password:
.....

New password:
.....

Confirm password:
.....

Submit

Post-Login Banner

https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD

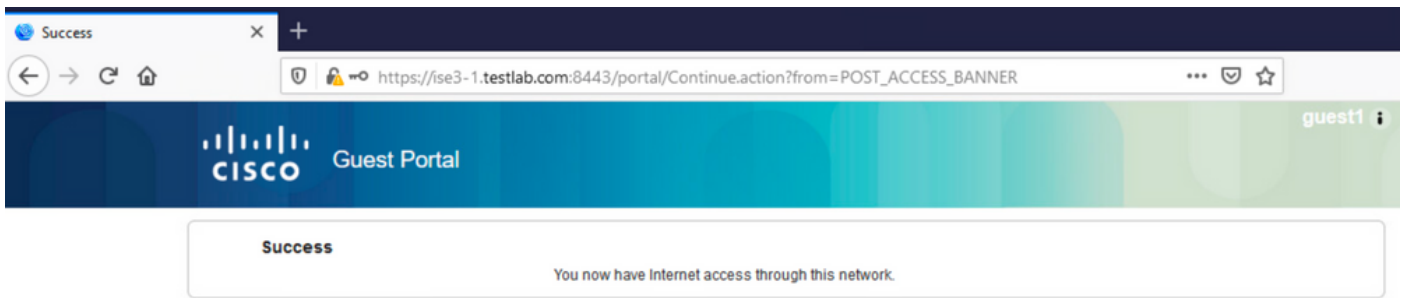
guest1

CISCO Guest Portal

Welcome Message
Click **Continue** to connect to the network.
You're very close to gaining network access.

Continue

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.

Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address	Identity Group	Event
Nov 07, 2020 04:17:32.46...	●	🔍	guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_Internet	10.106.32.2...		Session State is Started
Nov 07, 2020 04:17:32.42...	■	🔍	guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_Internet		User Identity Groups:GuestType_Guest-Daily	Authorize-Only succeeded
Nov 07, 2020 04:17:32.39...	■	🔍		D0:37:45:89:EF:64						Dynamic Authorization succeeded
Nov 07, 2020 04:16:14.85...	■	🔍	guest1	D0:37:45:89:EF:64				10.106.32.2...	GuestType_Guest-Daily	Guest Authentication Passed
Nov 07, 2020 03:43:30.75...	■	🔍	D0:37:45:89:EF:64	D0:37:45:89:EF:64	Default >> MAB	Default >> Wifi_Redirect_to_Guest_Portal	Guest-Portal		Profiled	Authentication succeeded

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:

Logged At	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
2020-11-07 04:17:01.1...	guest1	D0:37:45:89:EF:64	10.106.32.254	Password Change	guest1
2020-11-07 04:16:33.9...	guest1	D0:37:45:89:EF:64	10.106.32.254	AUP	
2020-11-07 04:13:51.0...	guest1	D0:37:45:89:EF:64	10.106.32.254	Add	SelfRegistration

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:

The screenshot shows the Cisco Sponsor Portal interface. At the top, there is a header with the Cisco logo and the text 'Sponsor Portal'. On the right side of the header, there is a user greeting 'Welcome test123' and a user icon. Below the header, there are several buttons for account management: 'Create Accounts', 'Manage Accounts (1)', 'Pending Accounts (0)', and 'Notices (0)'. Below these are more action buttons: 'Resend', 'Extend', 'Edit', 'Suspend', 'Reinstate', 'Delete', 'Reset Password', and 'Print'. The main content area displays a user profile for 'guest1' with the following details:

Username:	guest1
Password:
First name:	Poonam
Last name:	Garg
Email address:	poongarg@cisco.com
Company:	Cisco
Mobile number:	+910000000000
Person being visited (email):	abc@cisco.com
Reason for visit:	Personal
Guest type:	Guest-Daily
SMS provider:	Global Default
From date (yyyy-mm-dd):	2020-11-07 09:43
To date (yyyy-mm-dd):	2020-11-08 09:43
Location:	India
SSID:	
Language:	English
Group tag:	
Time left:	0D 22H 48M
State:	Active

At the bottom of the profile section, there is a 'Done' button.

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.

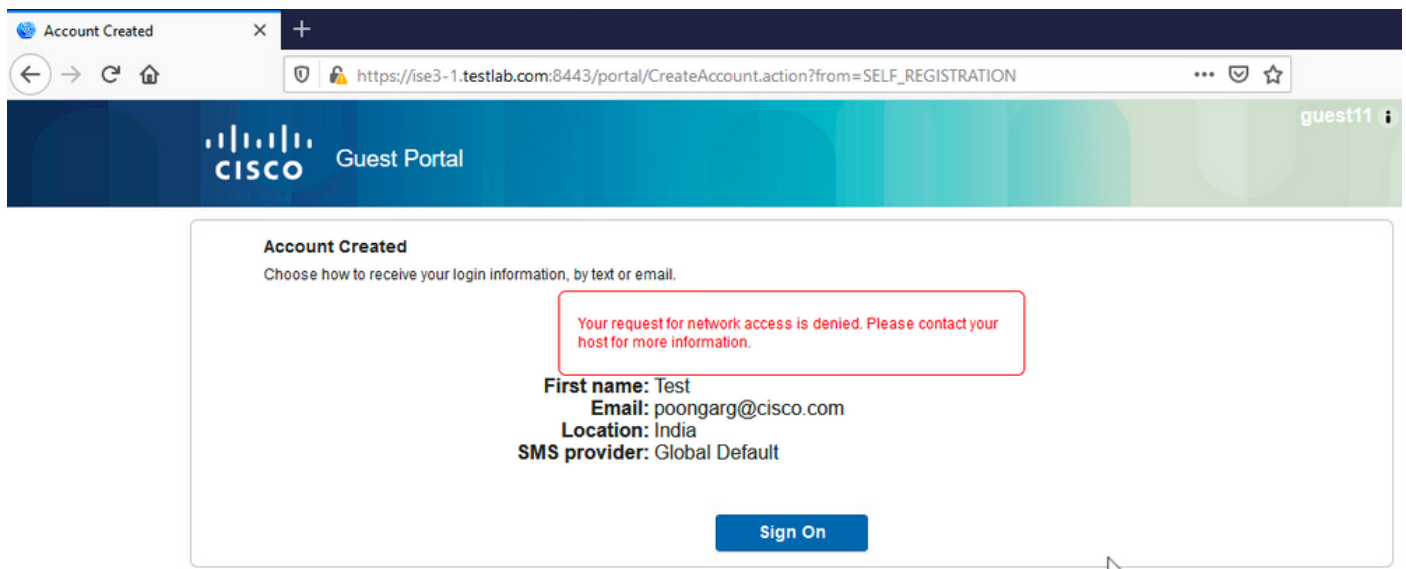
BYOD-instellingen

- 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:

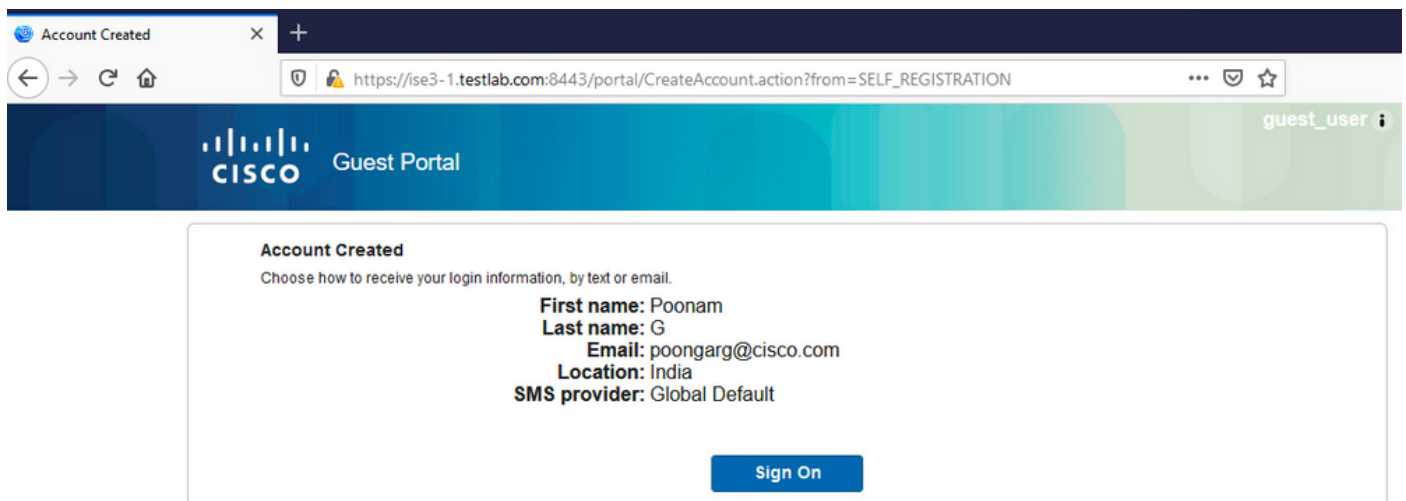
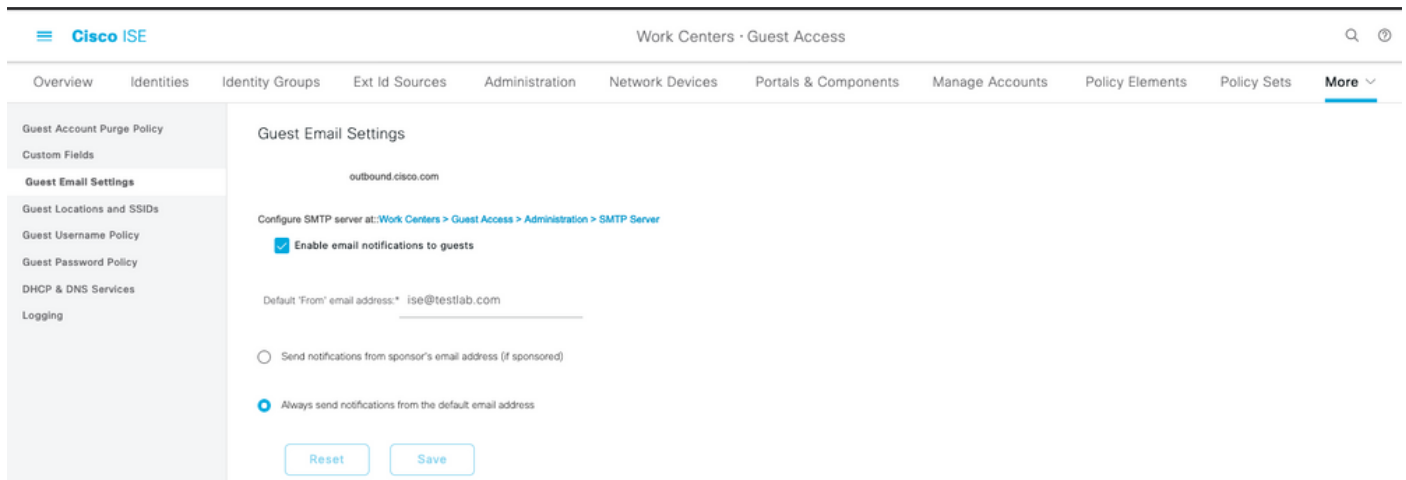


Het logbestand van guest.log bevestigt dat er een probleem is met het verzenden van een goedkeuringsbericht naar de sponsor e-mail omdat de SMTP-server verkeerd is geconfigureerd:

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD] []
cpm.guestaccess.apiservices.util.SmtplibMsgRetryThreadUtil -:::- An exception occurred while sending
email :
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cisco.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:

Guest Approval Request



ise@testlab.com <ise@testlab.com>

Today at 1:07 PM

To: Poonam Garg (poongarg)



Please approve (or deny) this self-registering guest. The guest provided the following information:

Username: guest_user

First Name: Poonam

Last Name: G

[Approve](#)

[Deny](#)

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



Guest (guest_user) has been approved.

[Help](#)

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:

SMS Service Provider

Guests can choose from these SMS providers:

- Global Default
- T-Mobile
- ATT
- Verizon
- ClickatellViaSMTP
- Orange
- Inmobile
- TheRingRingCompany
- Sprint
- NaaS

Guest see providers list only if multiple are selected

Configure SMS providers at:

[Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

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

Send credential notification upon approval using:

- Email
- SMS

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

Registration

Please complete this registration form:

Registration Code*

8015

Username

Guest13

First name

Poonam

Last name

Email address*

poongarg@cisco.com

Mobile number*

+91 9999999999

Company

SMS provider*

NaaS

ATT

Global Default

NaaS

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

https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION

guest13

CISCO Guest Portal

Account Created
Choose how to receive your login information, by text or email.

First name: Poonam
Email: poongarg@cisco.com
Mobile number: +919999999999
Location: India
SMS provider: NaaS

Sign On

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:

Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers](#) > [Guest Access](#) > [Configure](#) > [Guest Types](#)

Device Registration

You can add a maximum of 5 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 *

D0:37:45:89:EF:64

Device Description *

Add Save, Continue

Cancel, Continue

Manage Devices (1)

D0:37:45:89:EF:64	Delete
-------------------	--------

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:

✓ Guest_Complaint	AND	IdentityGroup-Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints Wireless_MAB Radius-Called-Station-ID CONTAINS Guest Session-PostureStatus EQUALS Compliant	PermitAccess x	+
✓ Permanent_Guest_Access	AND	IdentityGroup-Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints Wireless_MAB Radius-Called-Station-ID CONTAINS Guest	Limited_Access x	+
✓ Wifi_Redirect_to_Guest_Portal	AND	Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	+

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 netwerkoctie** 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:

▼ Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding is not configured on a PSN, use: ⓘ	If bonding is configured on a PSN, use: ⓘ
<input checked="" type="checkbox"/> Gigabit Ethernet 0 <input type="checkbox"/> Gigabit Ethernet 1 <input type="checkbox"/> Gigabit Ethernet 2 <input type="checkbox"/> Gigabit Ethernet 3 <input type="checkbox"/> Gigabit Ethernet 4 <input type="checkbox"/> Gigabit Ethernet 5	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet 0 as primary , 1 as backup . <input type="checkbox"/> Bond 1 Uses Gigabit Ethernet 2 as primary , 3 as backup . <input type="checkbox"/> Bond 2 Uses Gigabit Ethernet 4 as primary , 5 as backup .

Certificate group tag: * Default Portal Certificate Group ▼

Configure certificates at:

[Work Centers > Guest Access > Administration > System Certificates](#)

Authentication method: * Guest_Portal_Sequence ▼ ⓘ

Configure authentication methods at:

[Work Centers > Guest Access > Identities > Identity Source Sequences](#)

Dit is de interne opslagopvolging 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 authenticatie kan worden betreden, kan een Werknemer met interne geloofsbrieven of geloofsbrieven van de Kaart aan het portaal inloggen.

Overview **Identities** Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Endpoints
Network Access Users
Identity Source Sequences

Identity Source Sequence

* Name: Guest_Portal_Sequence

Description: A built-in Identity Sequence for the Guest Portal

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
	Guest Users
	All_AD_Join_Points

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:

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.

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

Start

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

- [Opdrachtsservices 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.html Cisco 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.