

Configuración del portal de invitados autoregistrado de ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topología y flujo](#)

[Configurar](#)

[WLC](#)

[ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Configuración opcional](#)

[Configuración de autorregistro](#)

[Configuración de invitado de inicio](#)

[Configuración de registro de dispositivos](#)

[Configuración de cumplimiento del dispositivo invitado](#)

[Configuración de BYOD](#)

[Cuentas aprobadas por el patrocinador](#)

[Entregar credenciales por SMS](#)

[Registro de dispositivos](#)

[Condición](#)

[BYOD](#)

[Cambio de VLAN](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y resolver problemas de la funcionalidad del Portal de invitados autoregistrado de ISE.

Prerequisites

Requirements

Cisco recomienda que tenga experiencia con la configuración de ISE y conocimientos básicos sobre estos temas:

- Implementaciones de ISE y flujos de invitados
- Configuración de controladores de LAN inalámbrica (WLC)

Componentes Utilizados

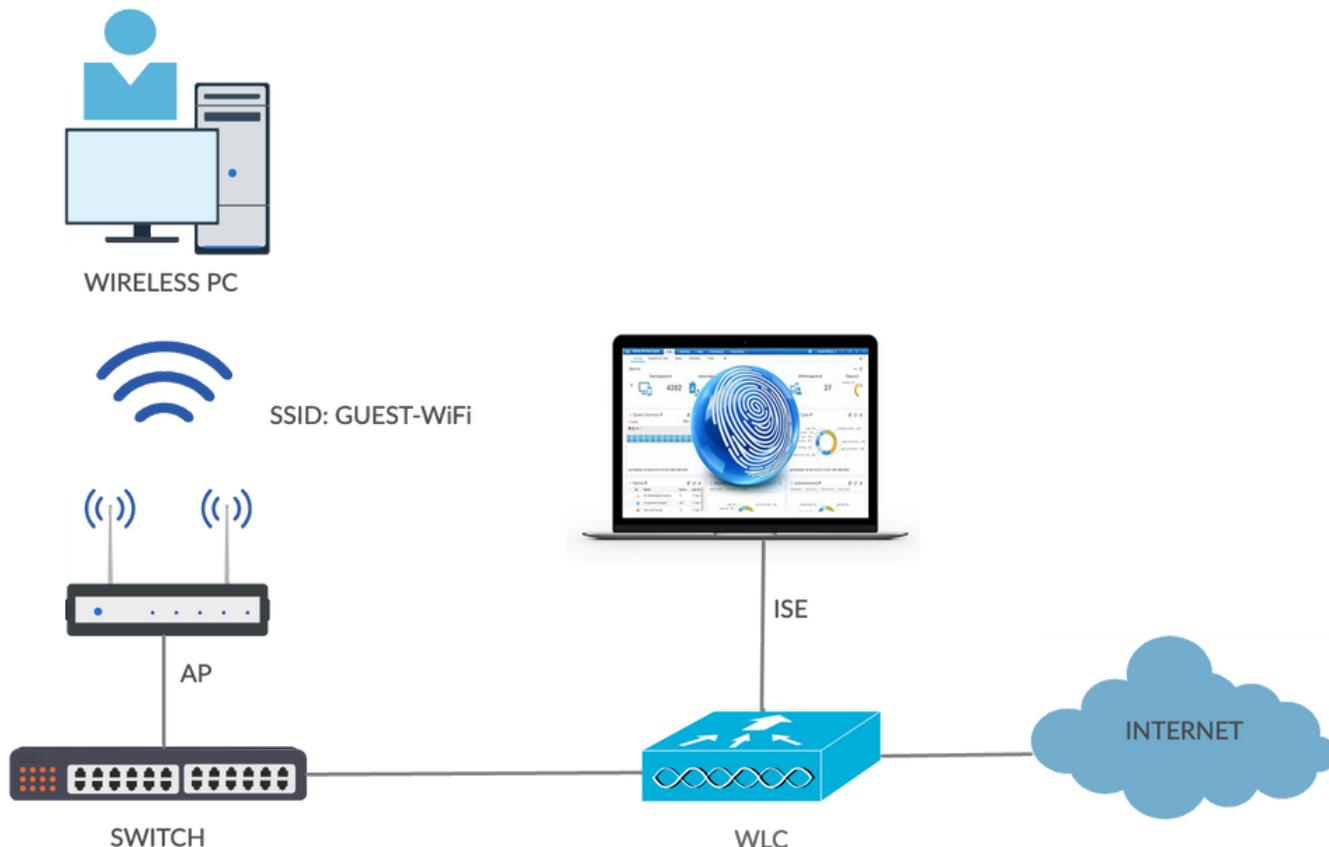
Portal de invitados registrado automáticamente, que permite a los usuarios invitados registrarse ellos mismos junto con los empleados utilizar sus credenciales de AD para obtener acceso a los recursos de la red. Este portal le permite configurar y personalizar varias funciones.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 10 Pro
- Cisco WLC 5508 con versión 8.5.135.0
- Software ISE, versión 3.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología y flujo



Este escenario presenta varias opciones disponibles para los usuarios invitados cuando realizan

el autorregistro.

Este es el flujo general:

Paso 1. El usuario invitado se asocia al identificador del conjunto de servicios (SSID): Guest-WiFi. Se trata de una red abierta con filtrado de MAC e ISE para la autenticación. Esta autenticación coincide con la segunda regla de autorización en ISE y el perfil de autorización se redirige al portal de autoregistro de invitados. ISE devuelve una aceptación de acceso de RADIUS con dos pares cisco-av:

- url-redirect-acl (qué tráfico debe redirigirse y el nombre de la lista de control de acceso (ACL) definida localmente en el WLC)
- url-redirect (dónde redirigir ese tráfico a ISE)

Paso 2. El usuario invitado se redirige a ISE. En lugar de proporcionar credenciales para iniciar sesión, el usuario hace clic en Registrar para acceso de invitado. Se redirige al usuario a una página en la que se puede crear la cuenta. Se puede habilitar un código de registro secreto opcional para limitar el privilegio de autorregistro a las personas que conocen ese valor secreto. Una vez creada la cuenta, se proporcionan al usuario credenciales (nombre de usuario y contraseña) y se inicia sesión con esas credenciales.

Paso 3. ISE envía una reautenticación de cambio de autorización (CoA) RADIUS al WLC. El WLC reautentica al usuario cuando envía la petición de acceso RADIUS con el atributo Authorize-Only. ISE responde con Access-Accept y Airespace ACL definidos localmente en el WLC, que proporciona acceso solo a Internet (el acceso final para el usuario invitado depende de la política de autorización).

 Nota: en las sesiones de protocolo de autenticación ampliable (EAP), ISE debe enviar una terminación de CoA para activar la reautenticación, ya que la sesión de EAP se encuentra entre el solicitante y el ISE. Pero para el MAB (filtrado de MAC), CoA Reauthenticate es suficiente; no hay necesidad de desasociar/desautenticar el cliente inalámbrico.

Paso 4. El usuario invitado ha deseado acceder a la red.

Es posible habilitar varias funciones adicionales, como la postura y la iniciativa "Trae tu propio dispositivo" (BYOD) (que se explicará más adelante).

Configurar

WLC

1. Agregue el nuevo servidor RADIUS para Autenticación y Contabilización. Navegue hasta Seguridad > AAA > Radio > Autenticación para habilitar RADIUS CoA (RFC 3576).

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu under Security > AAA > RADIUS > Authentication. The main content area is titled "RADIUS Authentication Servers > Edit" and contains the following configuration fields:

- Server Index: 2
- Server Address(Ipv4/Ipv6): 10.106.32.25
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- 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
- IPSec: Enable

Existe una configuración similar para la contabilidad. También se recomienda configurar el WLC para enviar SSID en el atributo Called Station ID, lo que permite que ISE configure reglas flexibles basadas en SSID:

This screenshot shows the configuration for the "Auth Called Station ID Type" field, which is set to "AP MAC Address:SSID". Below this, the "Use AES Key Wrap" checkbox is unchecked, with a note: "(Designed for FIPS customers and requires a key wrap compliant RADIUS server)".

This screenshot shows the configuration for RADIUS Accounting Servers. The "Acct Called Station ID Type" is set to "IP Address" and the "MAC Delimiter" is set to "Hyphen". Below these fields is a table listing the configured servers:

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

- En la ficha WLANs (WLAN), cree la red WLAN (LAN inalámbrica) Guest-WiFi y configure la interfaz correcta. Establezca la seguridad de capa 2 en Ninguno con el filtrado de MAC. En Servidores de seguridad/autenticación, autorización y contabilidad (AAA), seleccione la dirección IP de ISE tanto para Autenticación como para Contabilización. En la ficha Opciones avanzadas, habilite AAA Override y establezca el estado de Network Admission Control (NAC) en ISE NAC (compatibilidad con CoA).

3. Navegue hasta Seguridad > Listas de control de acceso > Listas de control de acceso y cree dos listas de acceso:

- GuestRedirect, que permite el tráfico que no se debe redirigir y redirige el resto del tráfico
- Internet, que se deniega para las redes corporativas y se permite para todas las demás

A continuación se muestra un ejemplo de la lista de control de acceso GuestRedirect (debe excluir el tráfico hacia/desde ISE de la redirección):

The screenshot shows the configuration page for an Access Control List (ACL) named 'GuestRedirect'. The left sidebar contains a navigation menu with categories like AAA, Local EAP, and Access Control Lists. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab. The 'Access List Name' is 'GuestRedirect' and 'Deny Counters' is 0. Below this is a table with columns: Seq, Action, Source IP/Mask, Destination IP/Mask, Protocol, Source Port, Dest Port, DSCP, Direction, and Number of Hits. Two entries are listed:

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. Agregue el WLC como un dispositivo de acceso a la red desde Centros de trabajo > Acceso de invitado > Dispositivos de red.
2. Crear grupo de identidades de terminales. Vaya a Centros de trabajo > Acceso de invitado > Grupos de identidad > Grupos de identidad de terminales.

Identity Groups

EQ



Endpoint Identity Groups

Profiled

Blacklist

GuestEndpoints

Cisco_GuestEndpoints

RegisteredDevices

Unknown

User Identity Groups

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

* Name Cisco_GuestEndpoints

Description

Parent Group

Submit

Cancel

3. Cree un tipo de invitado accediendo a Centros de trabajo > Acceso de invitado > Portal y componentes > Tipos de invitado. Consulte el grupo de identidad de terminales creado anteriormente en este nuevo tipo de invitado y guárdelo.

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

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

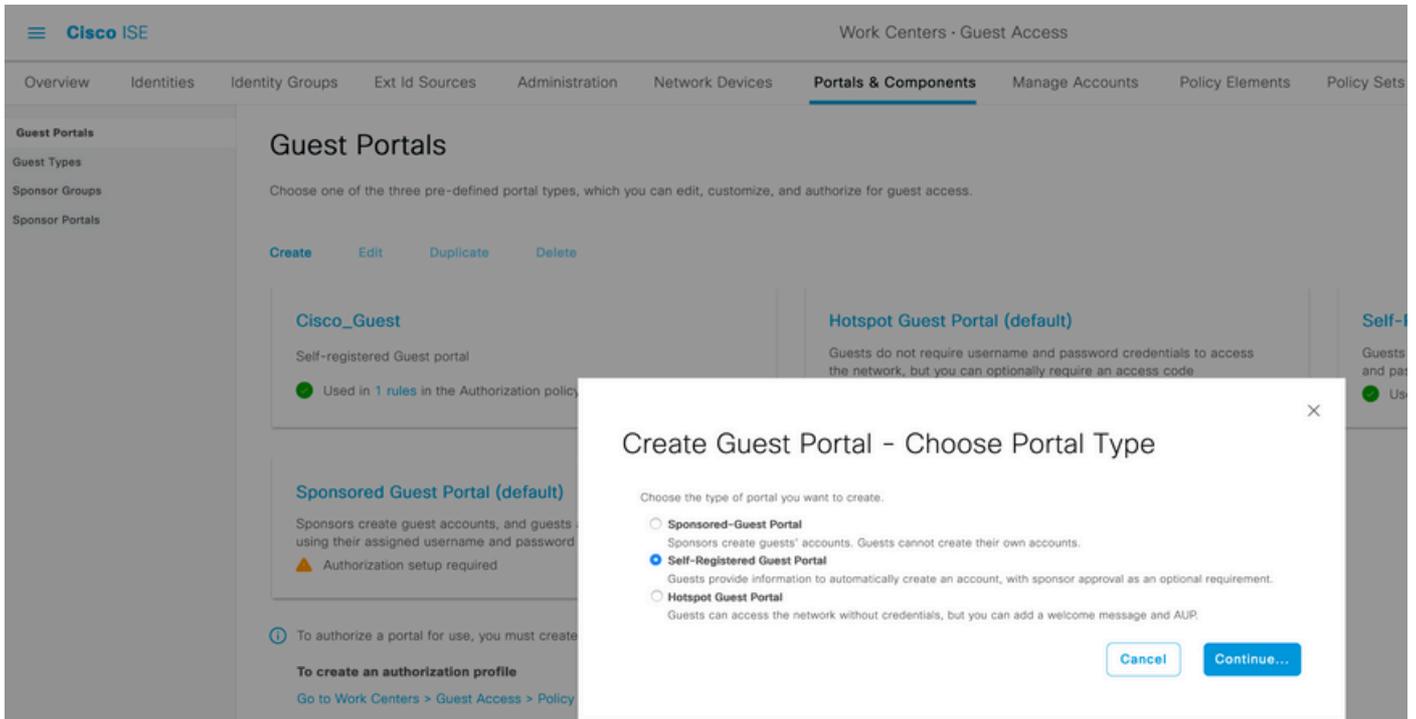
Redirect user to a portal page showing an error message

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. Cree un nuevo tipo de portal de invitados: Portal de invitados registrado automáticamente. Vaya a Centros de trabajo > Acceso de invitado > Portales de invitado.



5. Seleccione el nombre del portal, consulte el tipo de invitado creado anteriormente y envíe la configuración de notificación de credenciales en Configuración del formulario de registro para enviar las credenciales por correo electrónico.

Consulte este documento sobre cómo configurar el servidor SMTP en ISE:

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

Deje el resto de parámetros predeterminados. En Personalización de la página del portal, se pueden personalizar todas las páginas presentadas. De forma predeterminada, la cuenta Invitado es válida para 1 día y se puede ampliar al número de días configurado en el tipo de invitado específico.

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

Guest Portals

Portal Name: Cisco_Guest Description: Self-registered Guest portal

Language File

Portal test URL

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings Guest Flow (Based on settings)

Portal Settings

Login Page Settings

Registration Form Settings

Assign to guest type: **Guest-Daily**

Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types

Account valid for: **1** Days Maximum: 5 DAYS

6. Configure estos dos perfiles de autorización navegando hasta Centros de trabajo > Acceso de invitado > Elementos de política > Resultados > Perfiles de autorización.

- Guest-Portal (con redirección al portal de invitados Cisco_Guest y una ACL de redirección denominada GuestRedirect). Esta ACL GuestRedirect fue creada anteriormente en el WLC.

Cisco ISE Work Centers - Guest Access

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

Conditions

Results

Allowed Protocols

Authorization Profiles

Downloadable ACLs

Authorization Profile

* 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: ⓘ

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth ⓘ

ACL: GuestRedirect Value: Cisco_Guest

Display Certificates Renewal Message

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

- Permit_Internet (con Airespace ACL igual a 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. Modifique el conjunto de políticas denominado Predeterminado. El conjunto de políticas predeterminado está preconfigurado para el acceso al portal de invitados. Existe una política de autenticación denominada MAB, que permite que la autenticación mediante derivación de autenticación MAC (MAB) continúe (no se rechace) para direcciones MAC desconocidas.

8. Acceda a Política de Autorización en la misma página. Cree estas reglas de autorización, como se muestra en esta imagen.

Los nuevos usuarios cuando se asocian con el SSID de invitado todavía no forman parte de ningún grupo de identidad y, por lo tanto, coinciden con la segunda regla y se les redirige al portal de invitados.

Una vez que el usuario inicia sesión correctamente, ISE envía una CoA RADIUS y el WLC realiza una reautenticación. Esta vez, la primera regla de autorización coincide (ya que el terminal pasa a formar parte del grupo de identidad de terminal definido) y el usuario obtiene el perfil de autorización Permit_internet.

9. También podemos proporcionar acceso temporal a los invitados mediante el uso de la condición de flujo de invitado. Esta condición consiste en comprobar las sesiones activas en ISE y se le atribuye. Si esa sesión tiene el atributo que indica que el usuario invitado anterior se ha autenticado correctamente, la condición coincide. Después de que ISE reciba el mensaje de detención de contabilidad de RADIUS del dispositivo de acceso a la red (NAD), la sesión finaliza y se elimina posteriormente. En ese momento, la condición Network Access:UseCase = Guest Flow ya no se cumple. Como resultado, todas las autenticaciones subsiguientes de ese terminal llegan

a la redirección de reglas genéricas para la autenticación de invitado.

Authorization Policy (15)

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

 Nota: A la vez, puede utilizar el acceso de invitado temporal o el acceso de invitado permanente, pero no ambos.

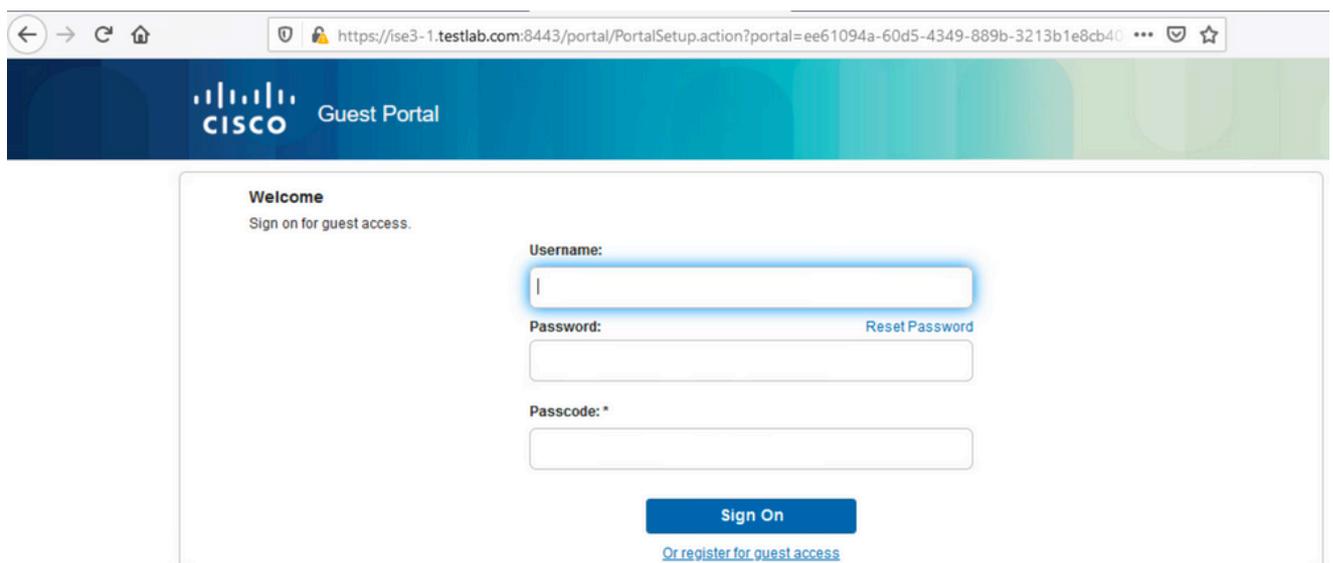
Consulte este documento para obtener información detallada sobre la configuración de acceso temporal y permanente para invitados de ISE.

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

Verificación

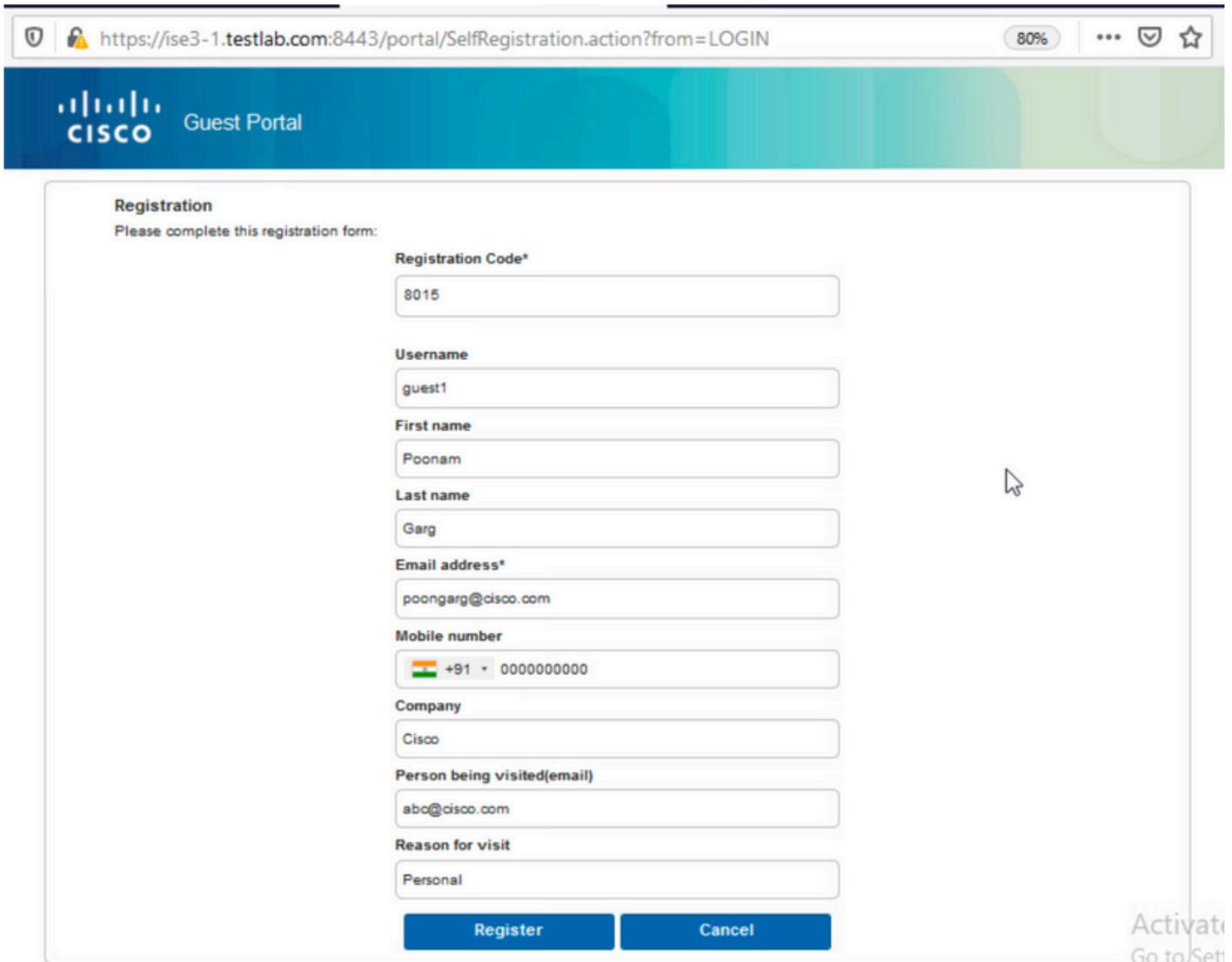
Utilice esta sección para confirmar que su configuración funcione correctamente.

1. Después de asociarse con el SSID de invitado y escribir una URL, se le redirigirá a la página Portal de invitados, como se muestra en la imagen.



2. Dado que aún no tiene credenciales, debe elegir la opción Register for Guest access (Registrarse para el acceso de invitado). Se le presentará el formulario de registro para crear la cuenta. Si la opción Código de registro estaba habilitada en la configuración del Portal de invitados, ese valor secreto es obligatorio (esto garantiza que sólo las personas

con los permisos correctos puedan registrarse automáticamente).



The image shows a web browser window displaying a Cisco Guest Portal registration form. The browser's address bar shows the URL: <https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN>. The page has a blue header with the Cisco logo and the text "Guest Portal". The main content area is titled "Registration" and contains the instruction "Please complete this registration form:". The form includes the following fields:

- 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

At the bottom of the form are two buttons: "Register" and "Cancel".

3. Si hay algún problema con la contraseña o la política de usuario, navegue hasta Centros de trabajo > Acceso de invitado > Configuración > Política de nombre de usuario de invitado para cambiar la configuración. Aquí tiene un ejemplo:

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. Después de la creación de cuenta exitosa, se le presentan credenciales (contraseña generada según las políticas de contraseña de invitado) también el usuario invitado recibe la notificación por correo electrónico si está configurado:

https://ise3-1.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. Haga clic en Iniciar sesión y proporcione credenciales (se puede requerir una contraseña de acceso adicional si se configura en el portal de invitados; este es otro mecanismo de seguridad que permite iniciar sesión sólo a aquellos que conocen la contraseña).

https://ise3-1.testlab.com:8443/portal/SelfRegistrationSuccess.action?from=SELF_REGISTRATION_SUCCESS

CISCO Guest Portal

Welcome
Sign on for guest access.

Username:
guest1

Password: [Reset Password](#)
.....

Passcode: *
8015

Sign On

[Or register for guest access](#)

6. Si se realiza correctamente, se puede presentar una política de uso aceptable (AUP) opcional (si está configurada en el portal de invitados). Se muestra al usuario una opción de cambio de contraseña y también se puede mostrar el banner posterior al inicio de sesión (también configurable en el portal de invitados).



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 and

Accept

Decline



Change Password

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

Current password:

New password:

Confirm password:

Submit

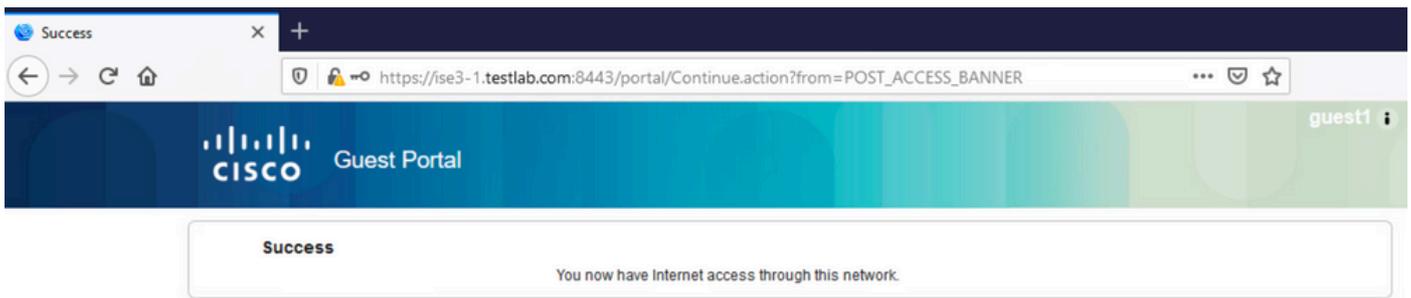


Welcome Message

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

Continue

7. La última página (Banner posterior al inicio de sesión) confirma que se ha concedido acceso:



Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

En esta etapa, ISE presenta estos registros en Operaciones > RADIUS > Registros activos, como se muestra en la imagen.

Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address	Identity Group	Event
Nov 07, 2020 04:17:32.46...	●	Q	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...	■	Q	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...	■	Q		D0:37:45:89:EF:64						Dynamic Authorization succeeded
Nov 07, 2020 04:16:14.85...	■	Q	guest1	D0:37:45:89:EF:64				10.106.32.2...	GuestType_Guest-Daily	Guest Authentication Passed
Nov 07, 2020 03:43:30.75...	■	Q	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

Este es el flujo:

- El usuario invitado encuentra la segunda regla de autorización (Wifi_Redirect_to_Guest_Portal) y es redirigido a Guest-Portal (Autenticación correcta).
- Se redirige al invitado para que se registre automáticamente. Después de iniciar sesión correctamente (con la cuenta recién creada), ISE envía la CoA Reauthenticate, que confirma el WLC (autorización dinámica correcta).
- El WLC realiza la reautenticación con el atributo Authorize-Only y se devuelve el nombre de ACL (Authorize-Only se realiza correctamente). Se proporcionará al invitado el acceso a la red correcto.

Informes (Operaciones > Informes > Invitado > Informe maestro de invitado) también confirma que:

Master Guest Report

From 2020-11-07 00:00:00.0 To 2020-11-07 04:38:26.0

Reports exported in last 7 days 0

My Reports Export To Schedule

Filter Refresh

Logged At	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
Today	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

Un usuario patrocinador (con los privilegios correctos) puede verificar el estado actual de un usuario invitado.

Este ejemplo confirma que se ha creado la cuenta y que el usuario ha iniciado sesión en el portal:

Welcome test123

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

Resend Extend Edit Suspend Reinstate Delete Reset Password Print

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**

Done

Configuración opcional

Para cada etapa de este flujo, se pueden configurar diferentes opciones. Todo esto se configura según el Portal de invitados en Centros de trabajo > Acceso de invitados > Portales y componentes > Portales de invitados > Nombre del portal > Editar > Comportamiento del portal y configuración de flujo. Entre las opciones más importantes se incluyen:

Configuración de autorregistro

- Tipo de invitado: describe el tiempo que la cuenta está activa, las opciones de caducidad de la contraseña, las horas de inicio de sesión y las opciones (esta es una mezcla de perfil de tiempo y función de invitado)
- Código de registro: si está habilitado, solo los usuarios que conocen el código secreto pueden registrarse ellos mismos (deben proporcionar la contraseña cuando se cree la cuenta)
- AUP: aceptación de la política de uso durante el autorregistro
- El requisito para que el patrocinador apruebe/active la cuenta de invitado.

Configuración de invitado de inicio

- Código de acceso: si está habilitado, solo los usuarios invitados que conocen el código secreto pueden iniciar sesión.
- AUP: acepte la política de uso durante el autorregistro.
- Opción de cambio de contraseña.

Configuración de registro de dispositivos

- De forma predeterminada, el dispositivo se registra automáticamente.

Configuración de cumplimiento del dispositivo invitado

- Permite una postura dentro del flujo.

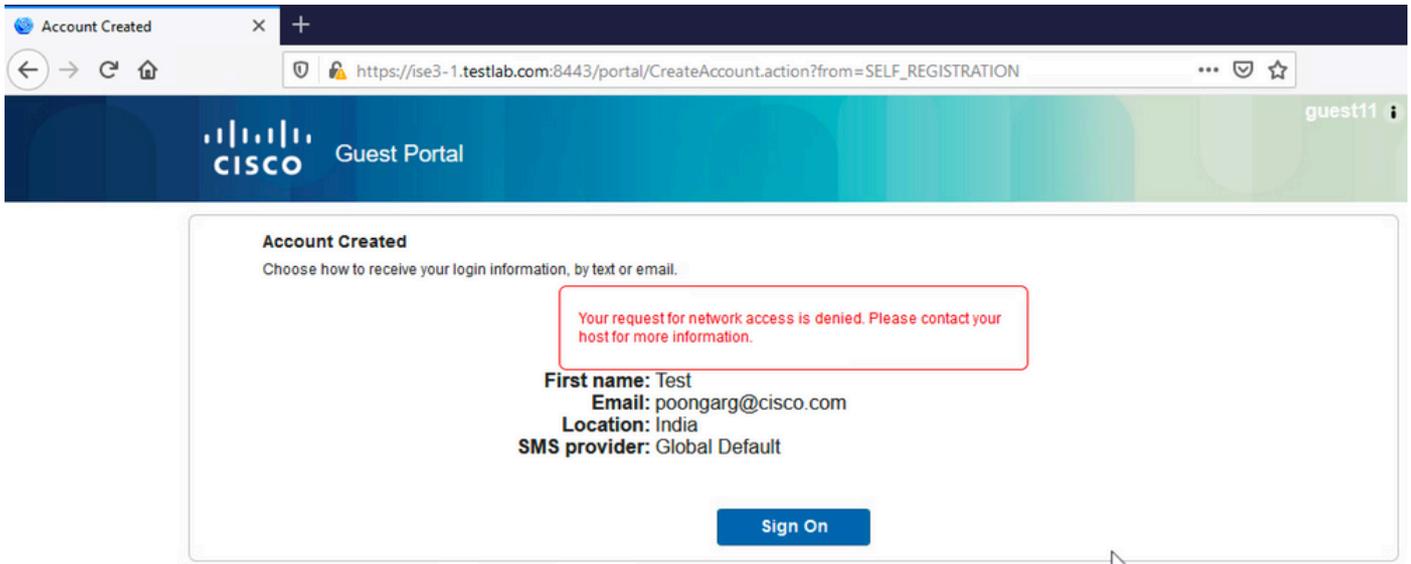
Configuración de BYOD

- Permite a los usuarios corporativos que utilizan el portal como invitados registrar sus dispositivos personales.

Cuentas aprobadas por el patrocinador

Si la opción Requerir que los invitados sean aprobados se selecciona en Configuración del formulario de registro, la cuenta creada por el invitado debe ser aprobada por un patrocinador. Esta función puede utilizar el correo electrónico para enviar una notificación al patrocinador (para la aprobación de la cuenta de invitado):

Si el servidor de Protocolo simple de transferencia de correo (SMTP) está mal configurado, la cuenta no se crea:



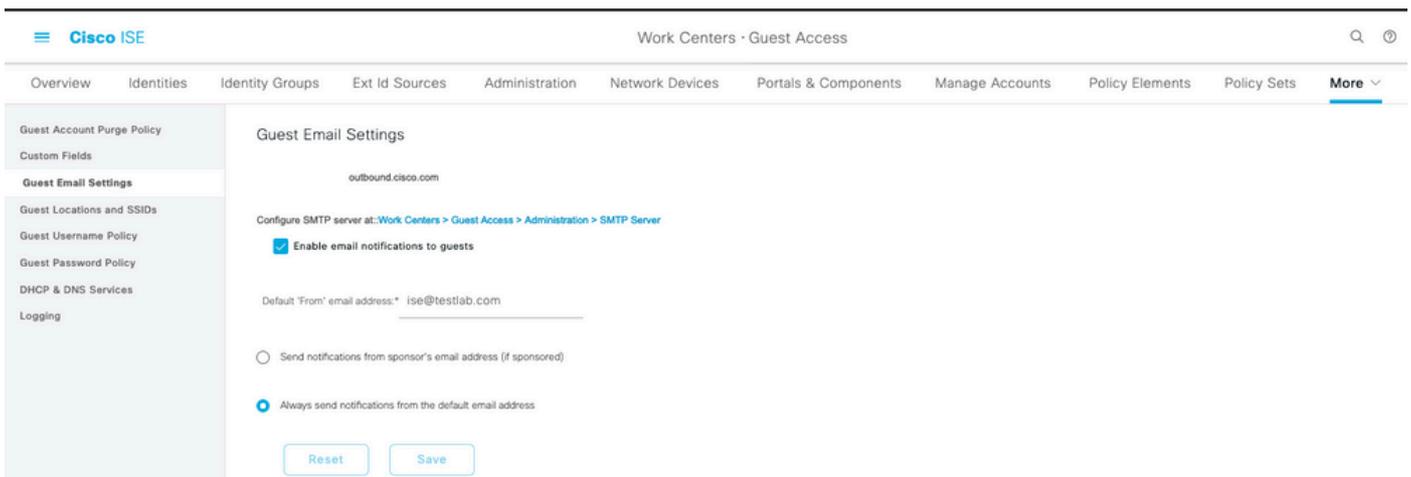
El registro de guest.log confirma que hay un problema con el envío de notificaciones de aprobación al correo electrónico del patrocinador, ya que el servidor SMTP está mal configurado:

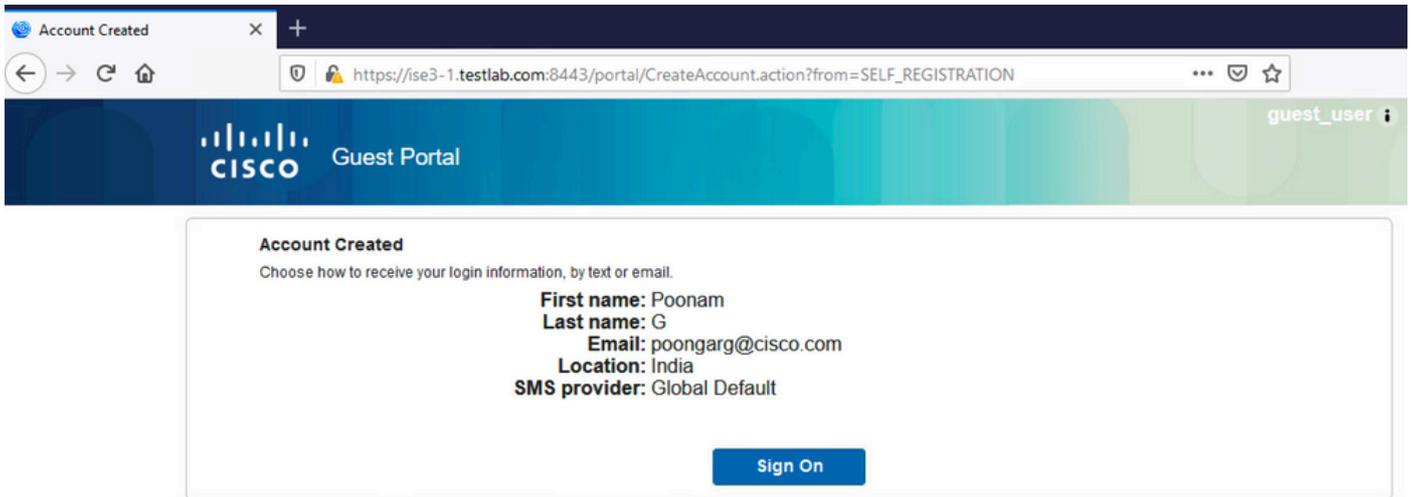
<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][ ] cpm.guestaccess.apiservices.util.SmtptM  
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25, response: 4
```

```
2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][ ] cpm.guestaccess.apiservices.no  
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

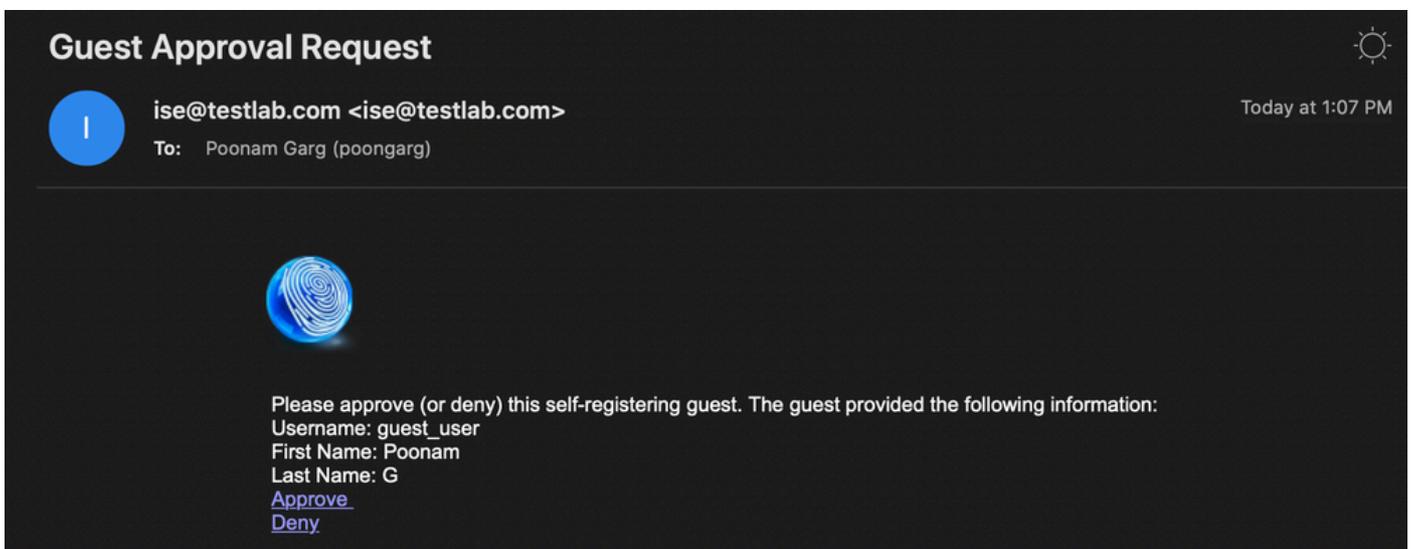
Cuando tenga la configuración de correo electrónico y servidor SMTP adecuada, se creará la cuenta:



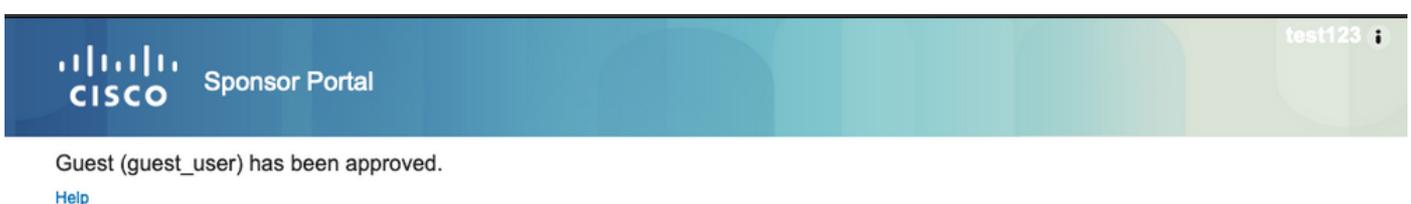


Después de habilitar la opción Requerir que los invitados sean aprobados, los campos de nombre de usuario y contraseña se eliminan automáticamente de la sección Incluir esta información en la página de autorregistro correcto. Por este motivo, cuando se necesita la aprobación del patrocinador, las credenciales de los usuarios invitados no se muestran de forma predeterminada en la página web que presenta información para mostrar que se ha creado la cuenta. En su lugar, deben ser entregados por SMS o correo electrónico. Esta opción debe estar habilitada en la sección Enviar notificación de credencial tras aprobación mediante (marcar correo electrónico/SMS).

Se envía un correo electrónico de notificación al patrocinador:



El patrocinador hace clic en el enlace Aprobación e inicia sesión en el portal del patrocinador y se aprueba la cuenta:



A partir de este momento, el usuario invitado puede iniciar sesión (con las credenciales recibidas por correo electrónico o SMS).

En resumen, en este flujo se utilizan tres direcciones de correo electrónico:

- Dirección "De" de notificación. Se define de forma estática o se toma de la cuenta del patrocinador y se utiliza como dirección de origen tanto para la notificación al patrocinador (para su aprobación) como para los detalles de credenciales al invitado. Se configura en Centros de trabajo > Acceso de invitado > Configuración > Configuración de correo electrónico de invitado.
- Dirección "Para" de notificación. Se utiliza para notificar al patrocinador que ha recibido una cuenta para su aprobación. Esto se configura en el Portal de invitados en Centros de trabajo > Acceso de invitados > Portales de invitados > Portales y componentes > Nombre del portal > Configuración del formulario de registro > Requerir que los invitados sean aprobados > Solicitud de aprobación por correo electrónico a.
- Dirección "Para" del invitado. El usuario invitado se lo proporcionará durante el registro. Si se selecciona Enviar notificación de credenciales tras aprobación mediante Correo electrónico, se entrega al invitado el correo electrónico con los detalles de credenciales (nombre de usuario y contraseña).

Entregar credenciales por SMS

Las credenciales de invitado también se pueden entregar por SMS. Se deben configurar estas opciones:

1. Seleccione el proveedor de servicios SMS en Configuración del formulario de registro:

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](#)

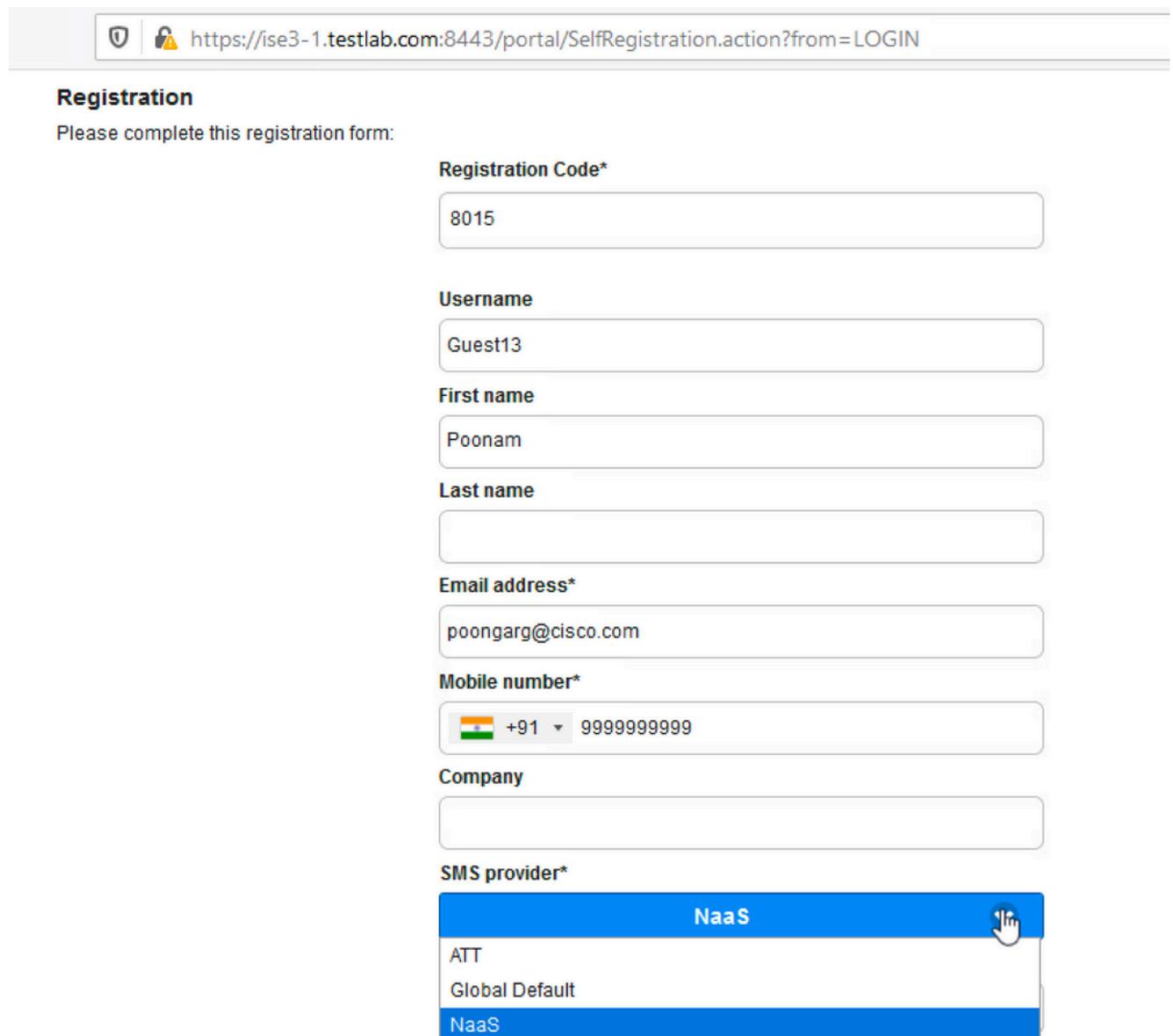
2. Marque la casilla de verificación Enviar notificación de credenciales tras la aprobación

mediante: SMS.

Send credential notification upon approval using:

- Email
- SMS

3. A continuación, se le solicita al usuario invitado que elija el proveedor disponible cuando cree una cuenta:



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

Registration
Please complete this registration form:

Registration Code*
8015

Username
Guest13

First name
Poonam

Last name

Email address*
poongarg@cisco.com

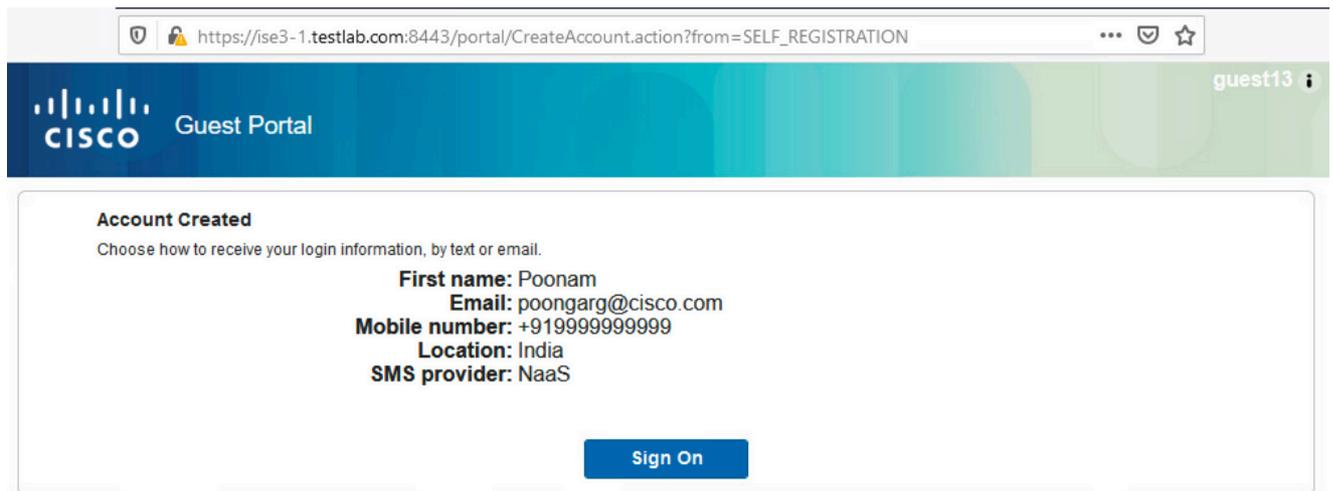
Mobile number*
+91 9999999999

Company

SMS provider*

NaaS
ATT
Global Default
NaaS

4. Se envía un SMS con el proveedor y el número de teléfono elegidos:



5. Puede configurar los proveedores de SMS en Administration > System > Settings > SMS Gateway.

Registro de dispositivos

Si se selecciona la opción Permitir a los invitados registrar dispositivos después de que un usuario invitado inicie sesión y acepte la PUA, puede registrar los dispositivos:

Guest Device Registration Settings

- Automatically register guest devices

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

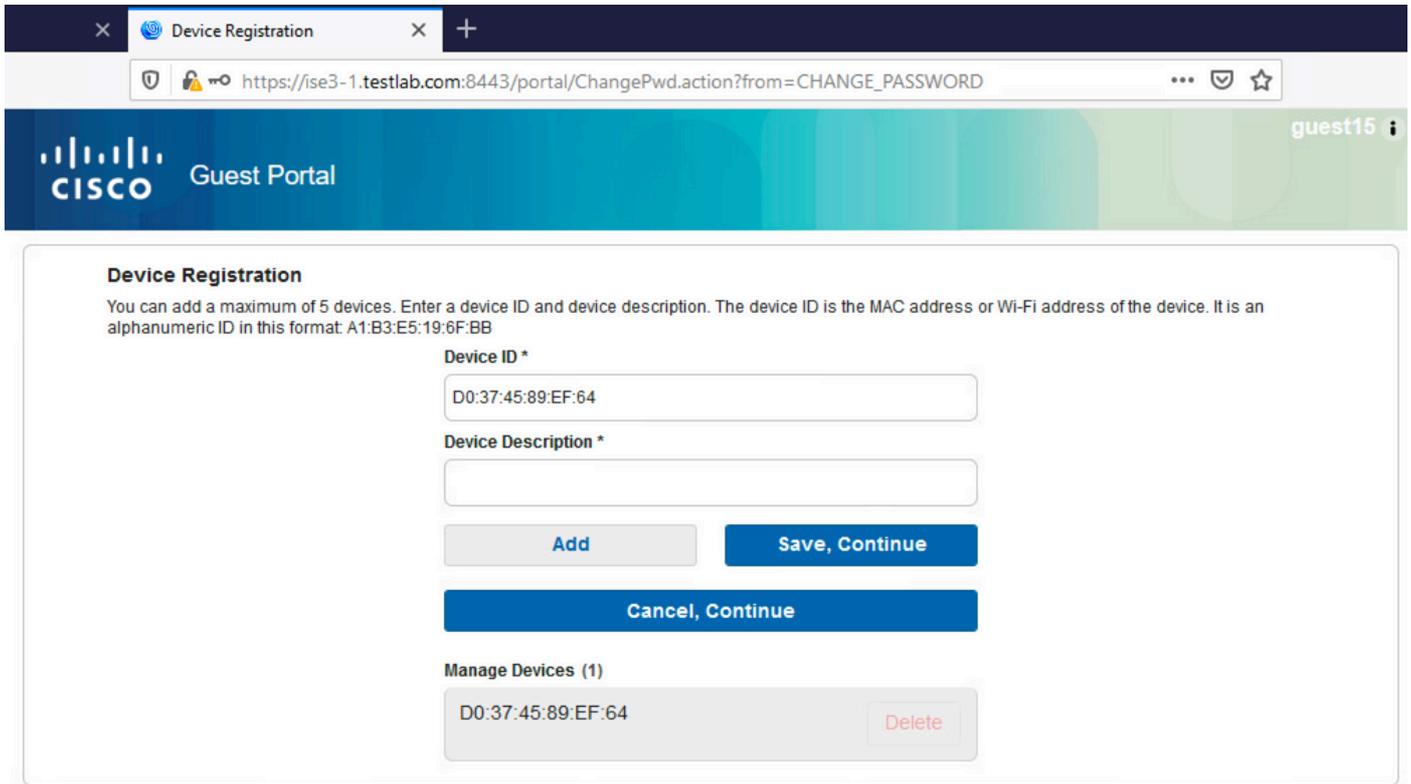
- Allow guests to register devices

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](#)



Observe que el dispositivo ya se ha agregado automáticamente (está en la lista Administrar dispositivos). Esto se debe a que se seleccionaron Registración automática de dispositivos invitados.

Condición

Si se selecciona la opción Require guest device compliance, los usuarios invitados reciben un agente que realiza el estado (NAC/Web Agent) después de conectarse y aceptar la PUA (y, opcionalmente, realizar el registro del dispositivo). ISE procesa las reglas de aprovisionamiento de clientes para decidir qué agente se debe aprovisionar. A continuación, el agente que se ejecuta en la estación realiza la postura (según las reglas de postura) y envía los resultados al ISE, que envía la CoA reautenticada para cambiar el estado de autorización si es necesario.

Las posibles reglas de autorización pueden tener un aspecto similar al siguiente:

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

Los primeros usuarios nuevos que encuentran la regla Guest_Authenticate se redirigen al portal

Self Register Guest. Después de que el usuario se autorregistra e inicia sesión, el CoA cambia el estado de autorización y se proporciona al usuario un acceso limitado para realizar tareas de estado y remediación. Solo después de aprovisionar el agente NAC y de que la estación cumpla con los requisitos, el CoA cambia el estado de autorización una vez más para proporcionar acceso a Internet.

Entre los problemas típicos con el estado se incluyen la falta de reglas correctas de aprovisionamiento de clientes:



Esto también se puede confirmar si examina el archivo guest.log:

```
<#root>
```

```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

BYOD

Si la opción Permitir a los empleados utilizar dispositivos personales en la red está seleccionada, los usuarios corporativos que utilicen este portal podrán pasar por el flujo de BYOD y registrar los dispositivos personales. Para los usuarios invitados, esta configuración no cambia nada.

¿Qué significa "empleados que utilizan el portal como invitados"?

De forma predeterminada, los portales de invitados se configuran con el almacén de identidad Guest_Portal_Sequence:

▼ 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](#)

Esta es la secuencia de almacenamiento interno que intenta primero los usuarios internos (antes que los usuarios invitados) y, a continuación, las credenciales de AD. Dado que la configuración avanzada es continuar con el siguiente almacén de la secuencia cuando no se puede acceder a un almacén de identidades seleccionado para la autenticación, un empleado con credenciales internas o credenciales de AD puede iniciar sesión en el portal.

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

Endpoints
Network Access Users
Identity Source Sequences

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
	Guest Users
	All_AD_Join_Points

En esta etapa del portal de invitados, el usuario proporciona credenciales definidas en el almacén de usuarios internos o Active Directory y se produce la redirección de BYOD:

BYOD Welcome

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

test123

CISCO Guest Portal

1 2 3

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

Start

De esta forma, los usuarios corporativos pueden usar sus dispositivos personales para la adopción de BYOD.

Cuando se proporcionan credenciales de usuarios internos/AD en lugar de usuarios invitados, continúa el flujo normal (sin BYOD).

Cambio de VLAN

Le permite ejecutar activeX o un applet Java, lo que activa DHCP para liberar y renovar. Esto es necesario cuando CoA activa el cambio de VLAN para el terminal. Cuando se utiliza MAB, el terminal no detecta un cambio de VLAN. Una posible solución es cambiar la VLAN (liberación/renovación de DHCP) con el agente NAC. Otra opción es solicitar una nueva dirección IP a través del applet devuelto en la página web. Se puede configurar un retraso entre la liberación/CoA/renovación. Esta opción no es compatible con dispositivos móviles.

Información Relacionada

- [Guía de configuración de Posture Services en Cisco ISE](#)
- [BYOD inalámbrico con Identity Services Engine](#)
- [Ejemplo de configuración de ISE SCEP para BYOD](#)
- [Ejemplo de configuración de autenticación web central en WLC e ISE](#)
- [Ejemplo de Configuración de Autenticación Web Central con AP FlexConnect en un WLC con ISE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).