Configuración del portal de invitados autoregistrado de ISE

Contenido

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

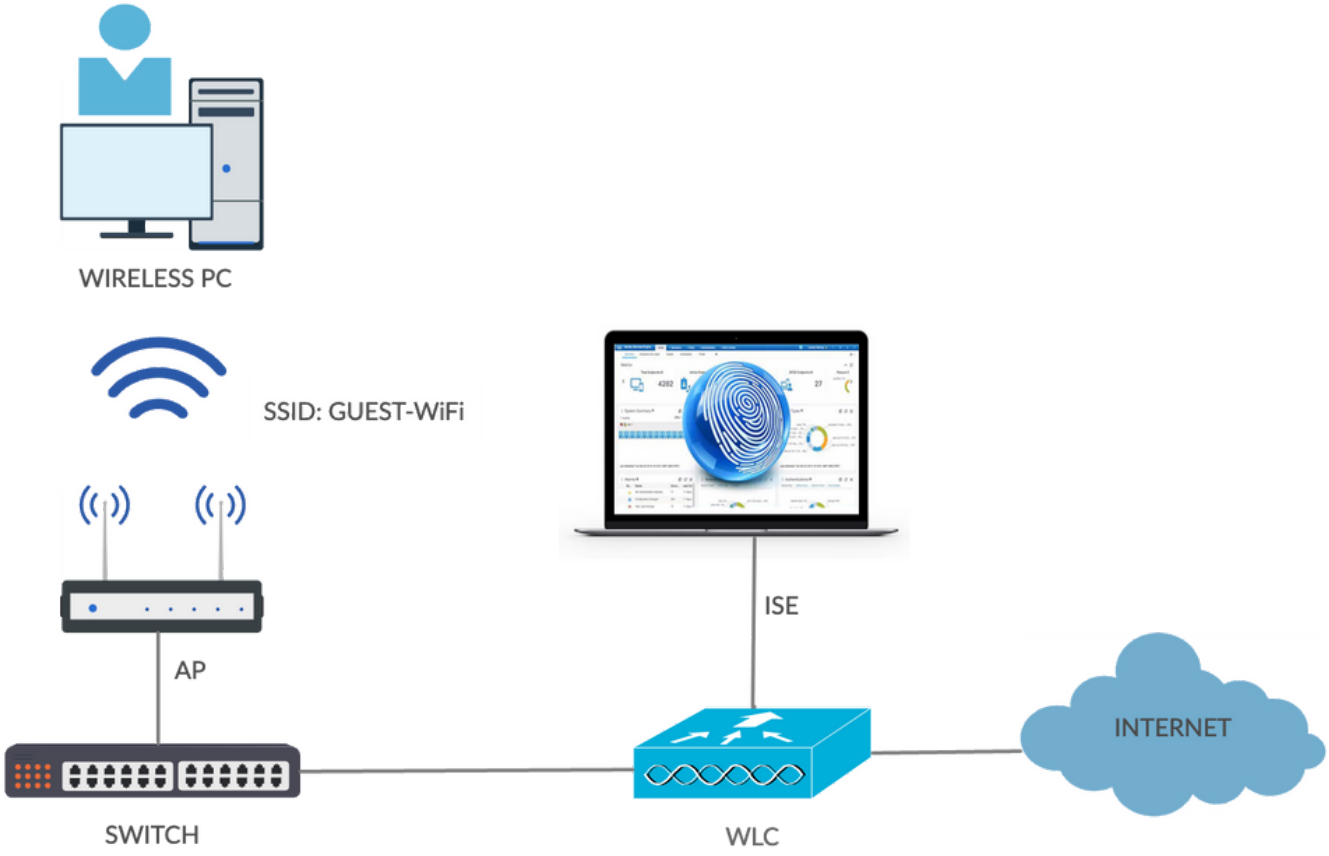
Portal de invitados registrado automáticamente, que permite a los usuarios invitados registrarse ellos mismos junto con los empleados utilizar sus credenciales de AD para obtener acceso a los recursos de la red. Este portal le permite configurar y personalizar varias funciones.

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.

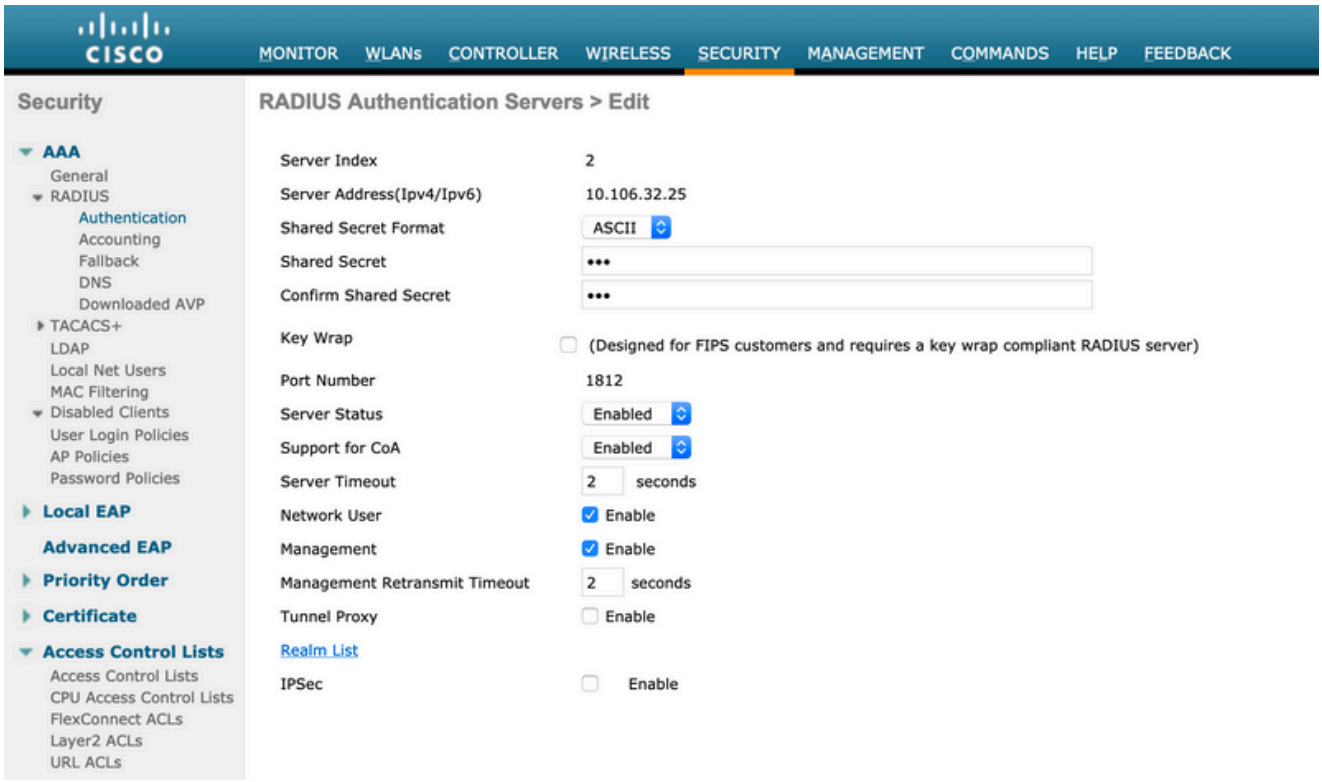
Paso 4. El usuario invitado ha deseado acceder a la red.

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

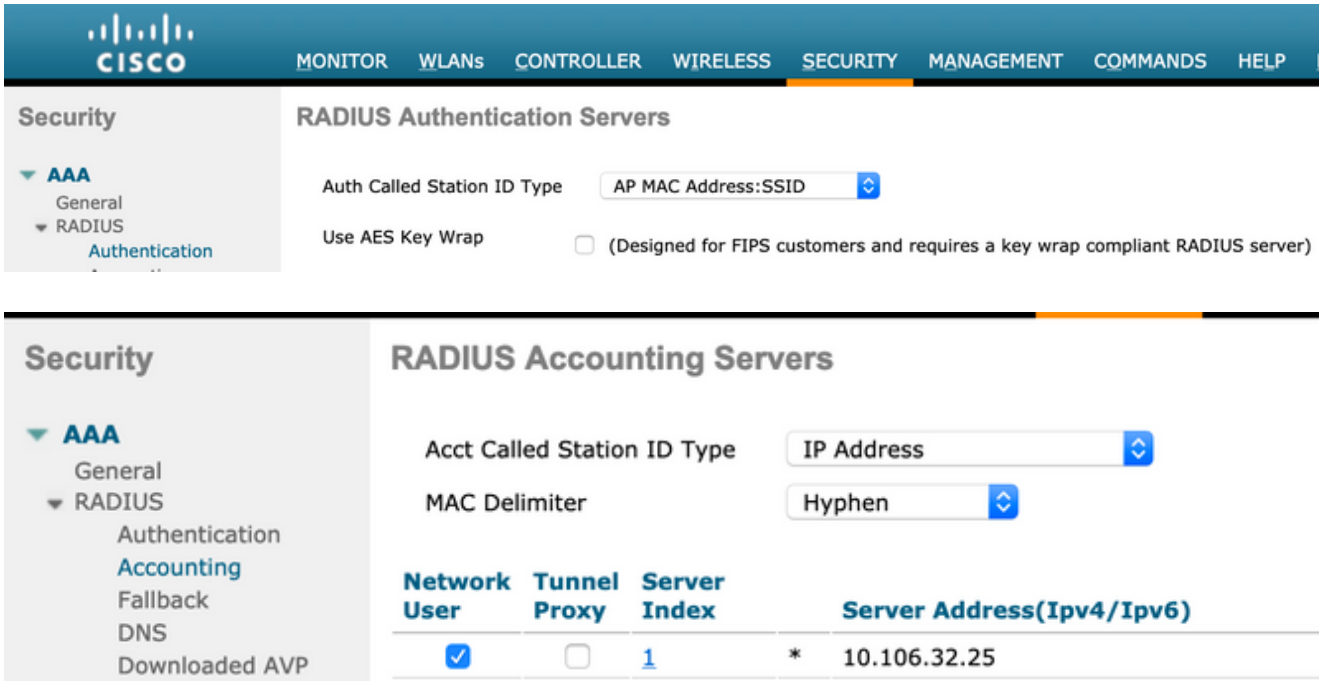
Configurar

WLC

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



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:



2. 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).

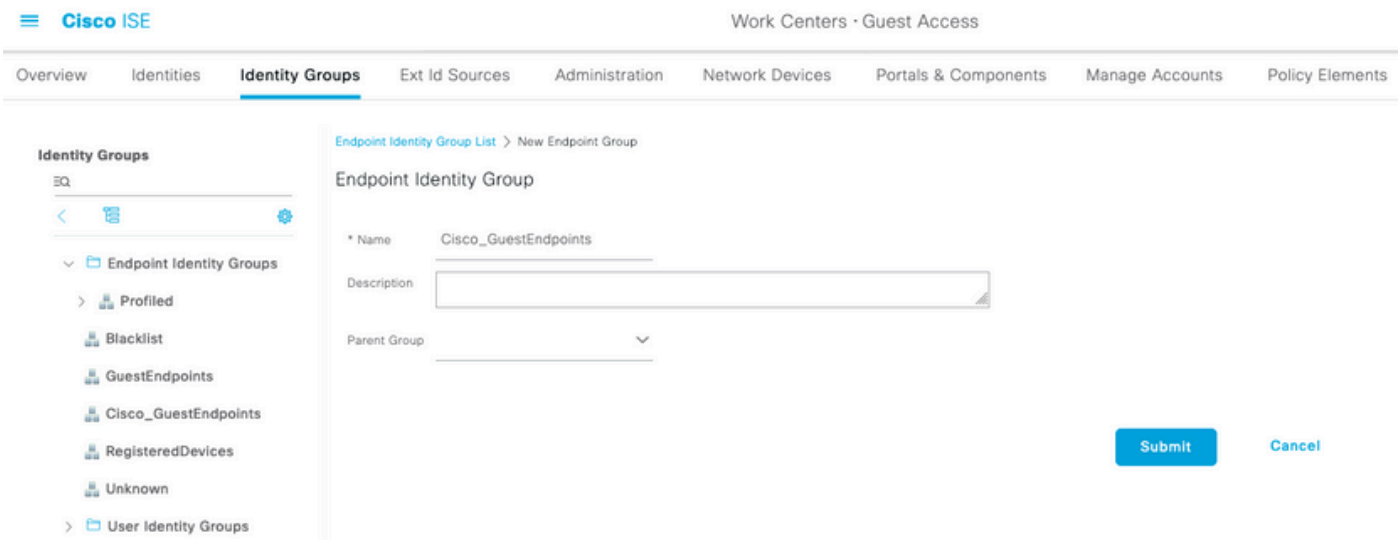
3. Navegue hasta Seguridad > Listas de control de acceso > Listas de control de acceso y cree dos listas de acceso:

    - 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

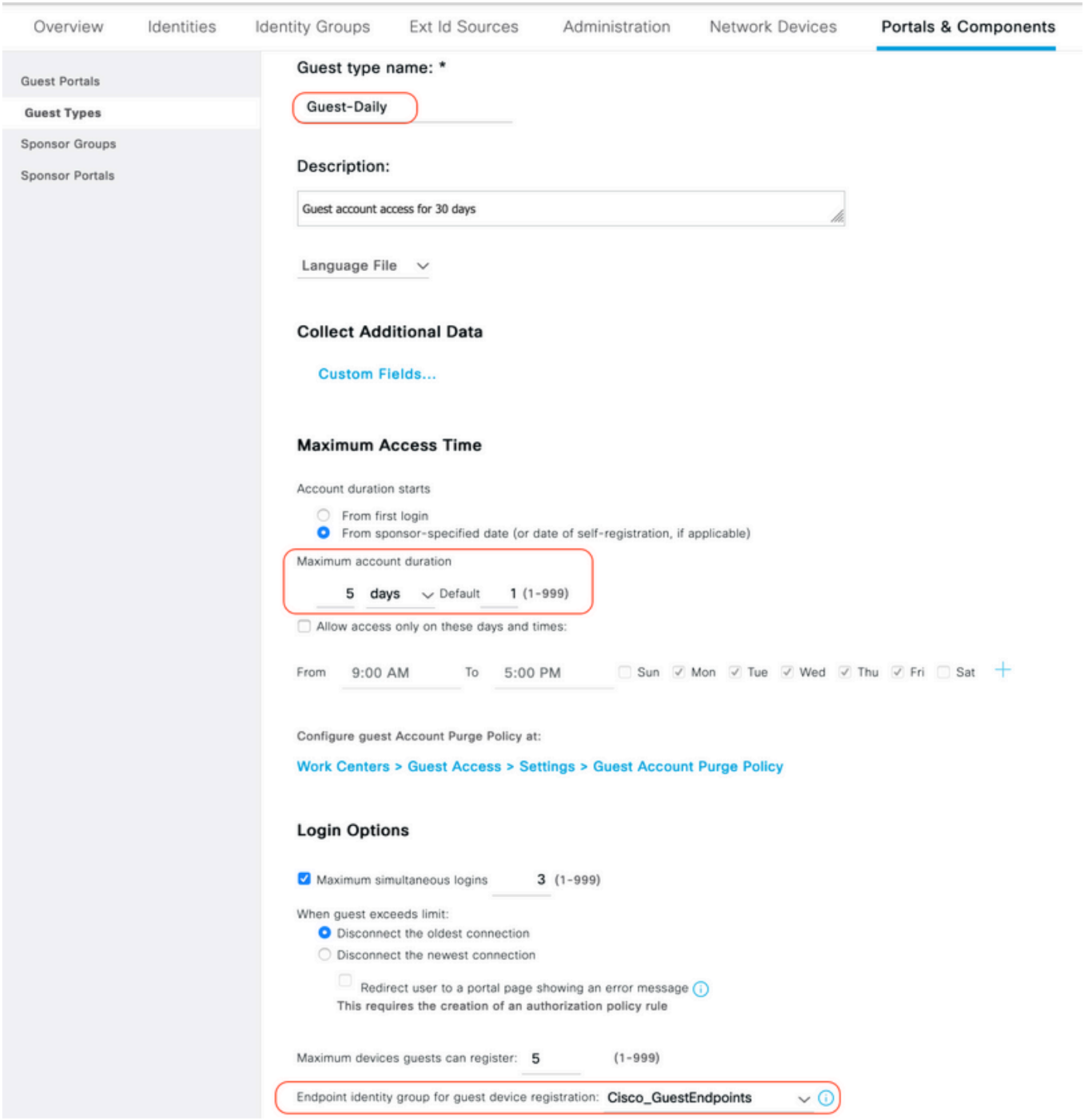
    A continuación se muestra un ejemplo de la lista de control de acceso GuestRedirect (debe excluir el tráfico hacia/desde ISE de la redirección):

ISE

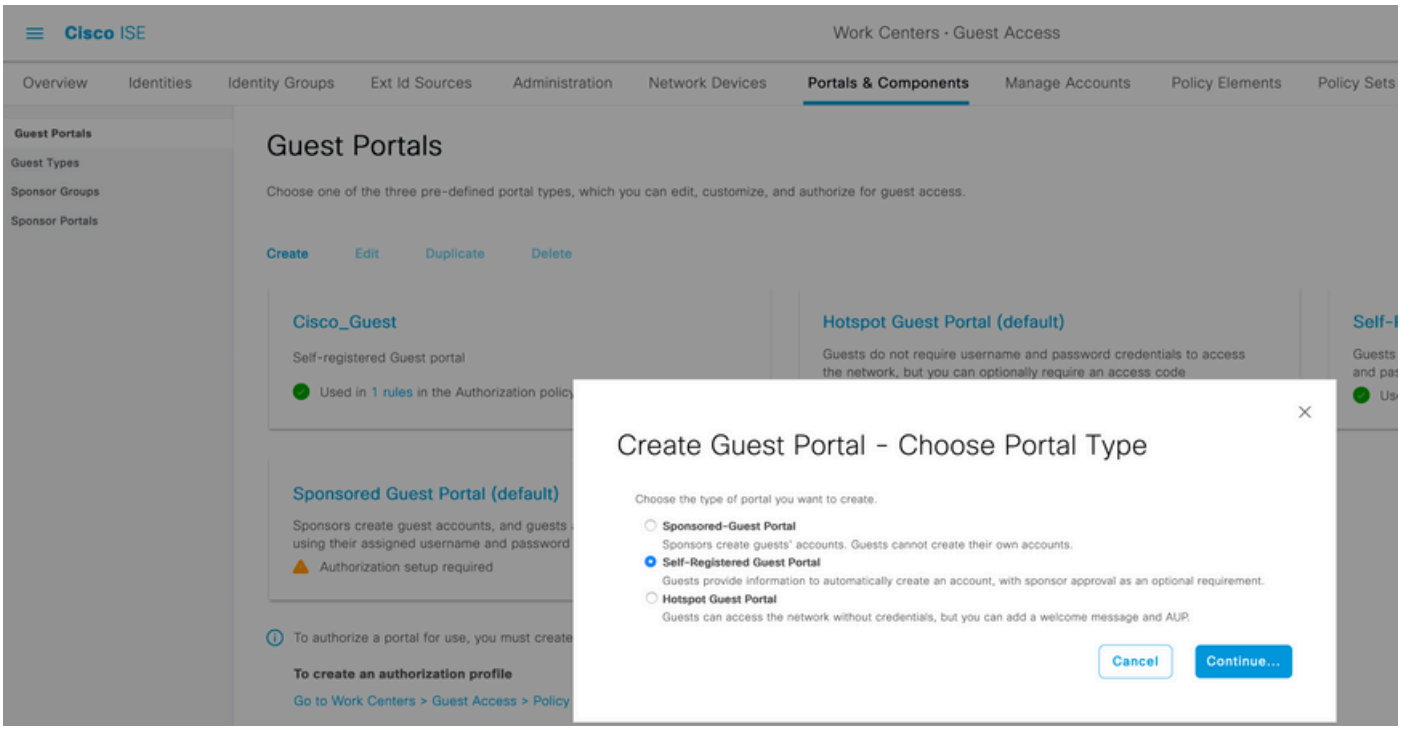
1. Agregue el WLC como un dispositivo de acceso a la red desde Centros de trabajo > Acceso de invitado > Dispositivos de red.
2. Crear grupo de identidades de terminales. Vaya a Centros de trabajo > Acceso de invitado > Grupos de identidad > Grupos de identidad de terminales.



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.



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.

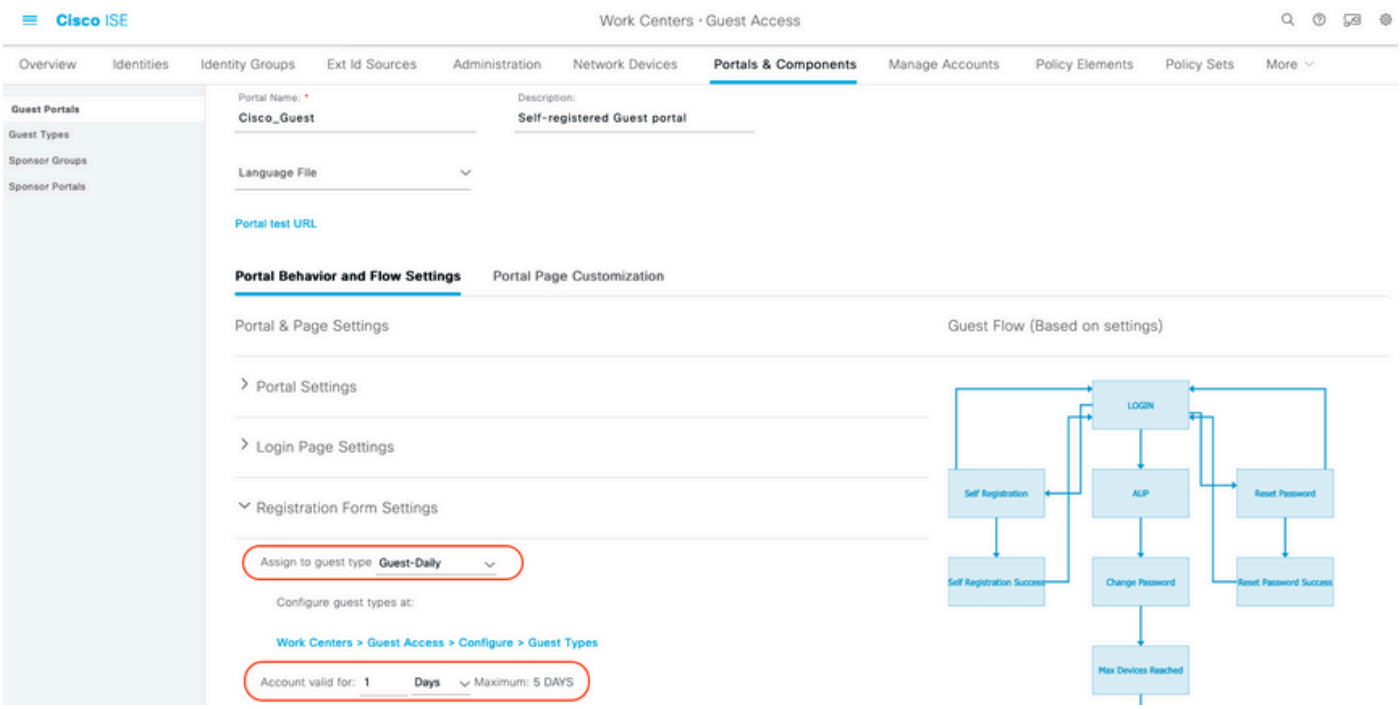


5. Seleccione el nombre del portal, consulte el tipo de invitado creado anteriormente y envíe la configuración de notificación de credenciales en Configuración del formulario de registro para enviar las credenciales por correo electrónico.

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

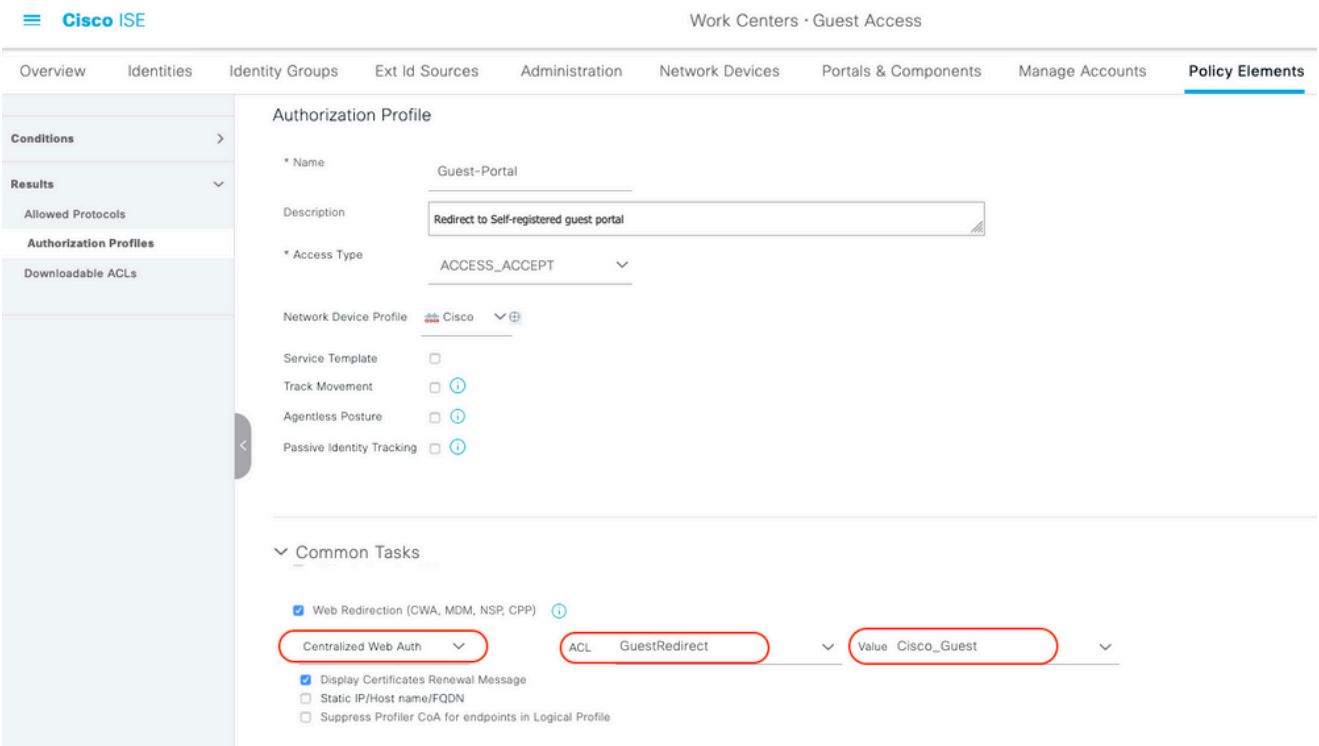
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

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.

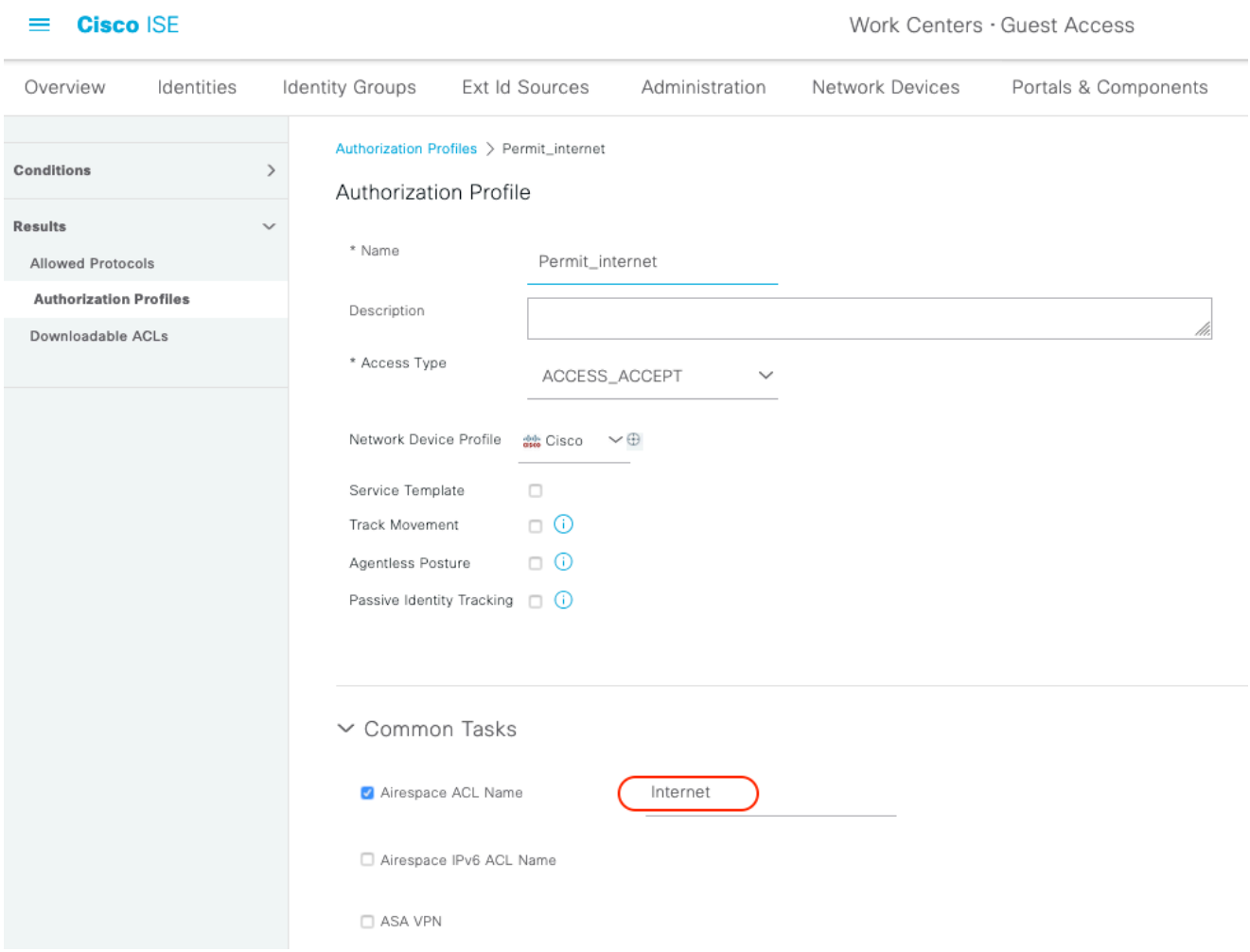


6. Configure estos dos perfiles de autorización navegando hasta Centros de trabajo > Acceso de invitado > Elementos de política > Resultados > Perfiles de autorización.

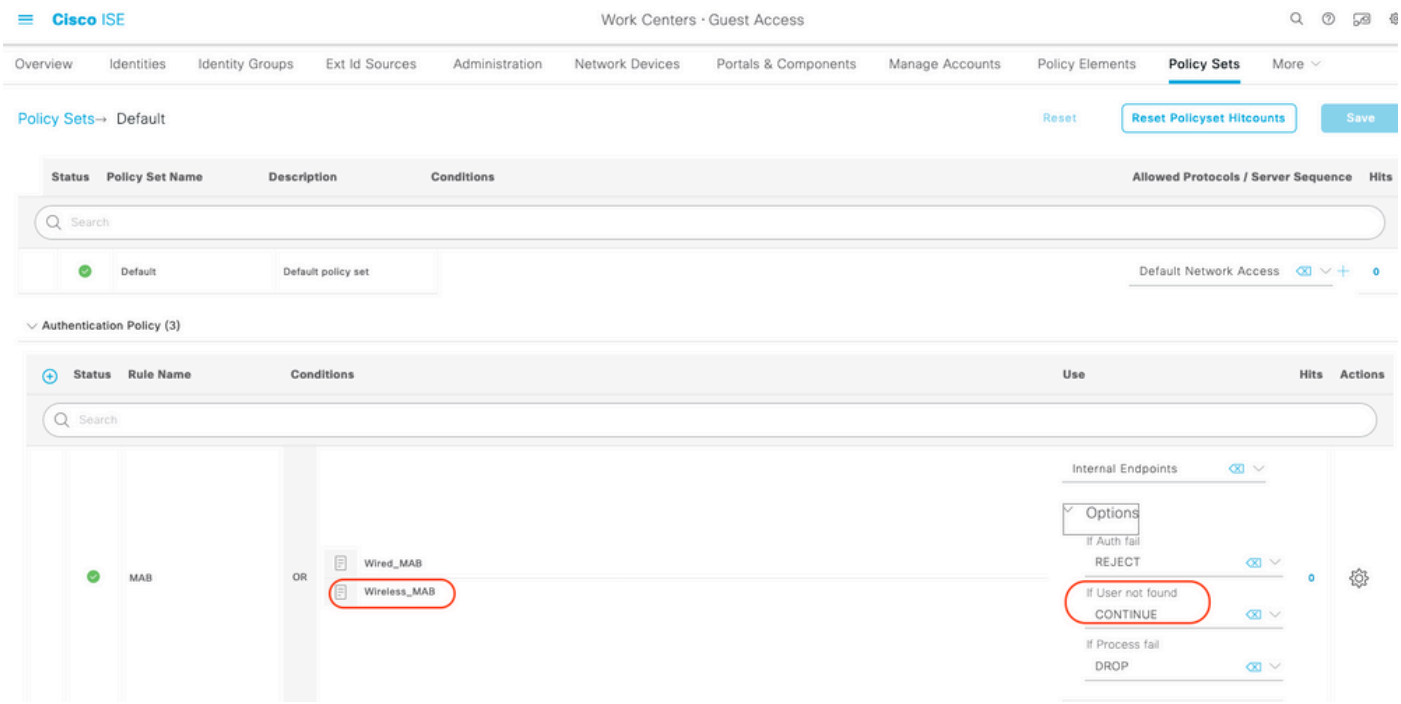
- Guest-Portal (con redirección al portal de invitados Cisco_Guest y una ACL de redirección denominada GuestRedirect). Esta ACL GuestRedirect fue creada anteriormente en el WLC.



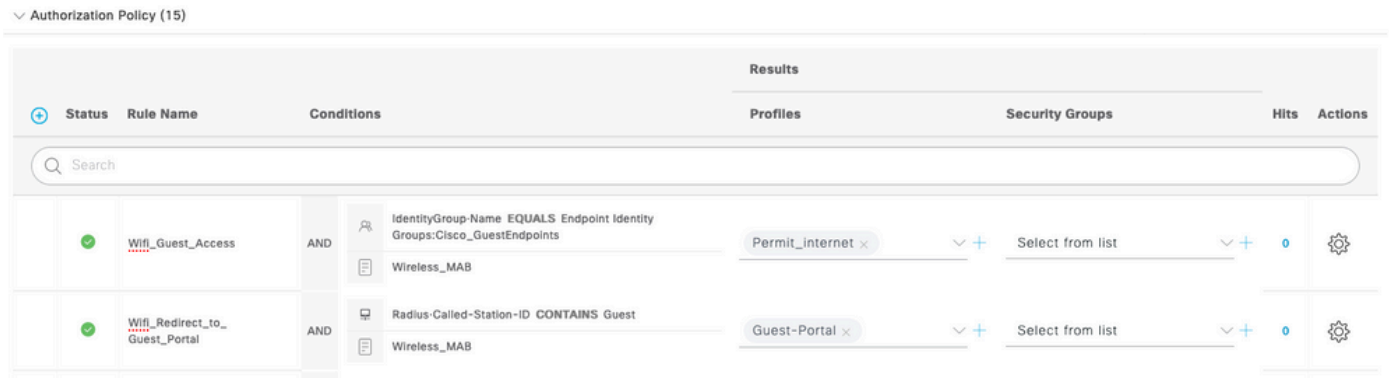
- Permit_Internet (con Airespace ACL igual a Internet)



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.

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

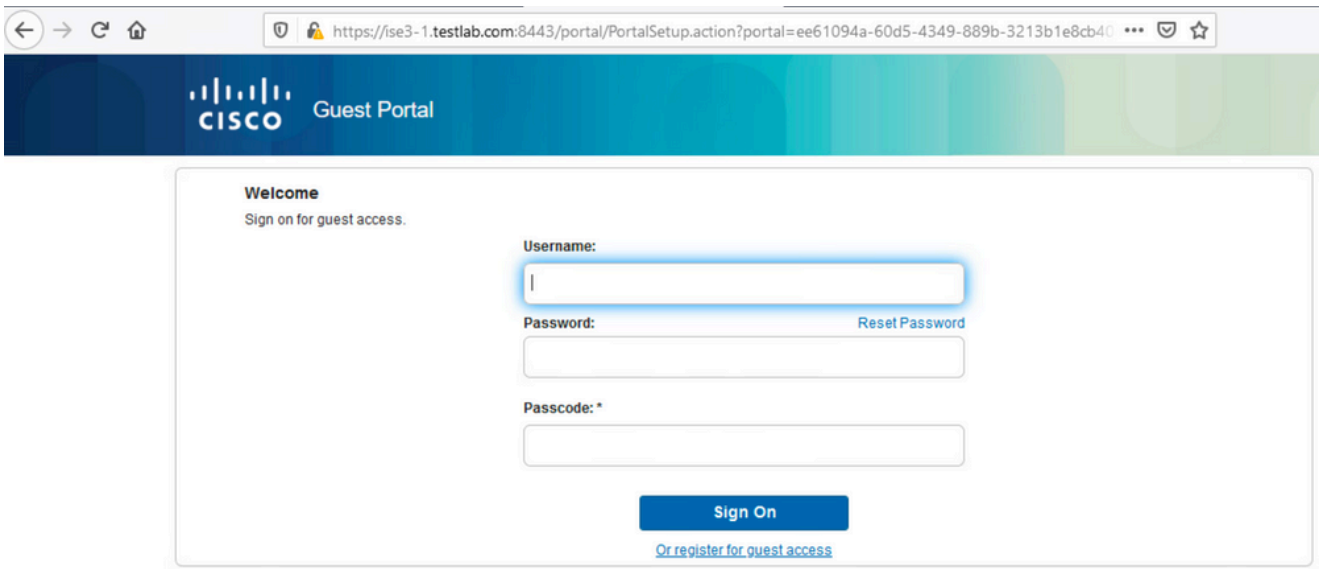
Consulte este documento para obtener información detallada sobre la configuración de acceso temporal y permanente para invitados de ISE.

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

Verificación

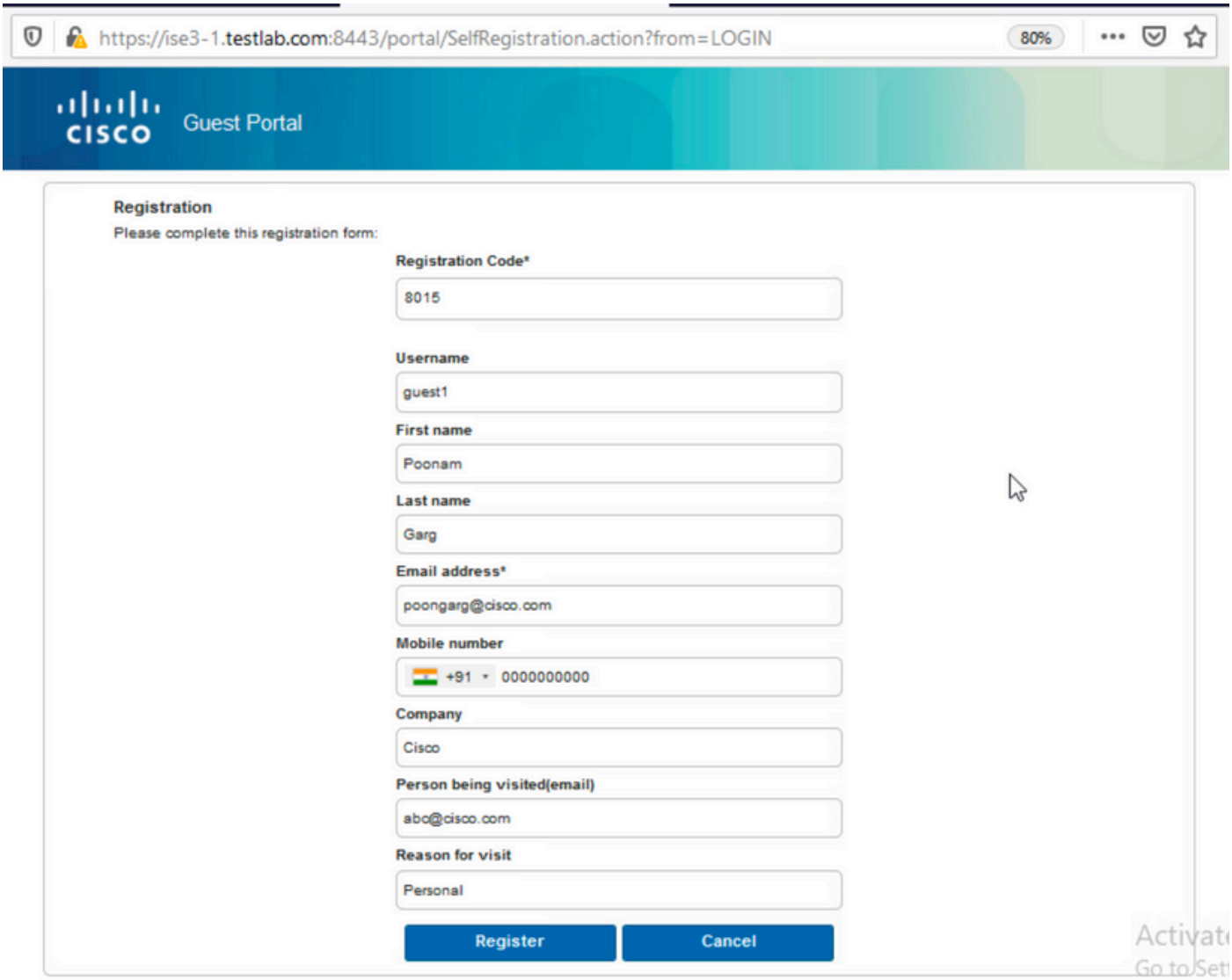
Utilize esta sección para confirmar que su configuración funcione correctamente.

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.

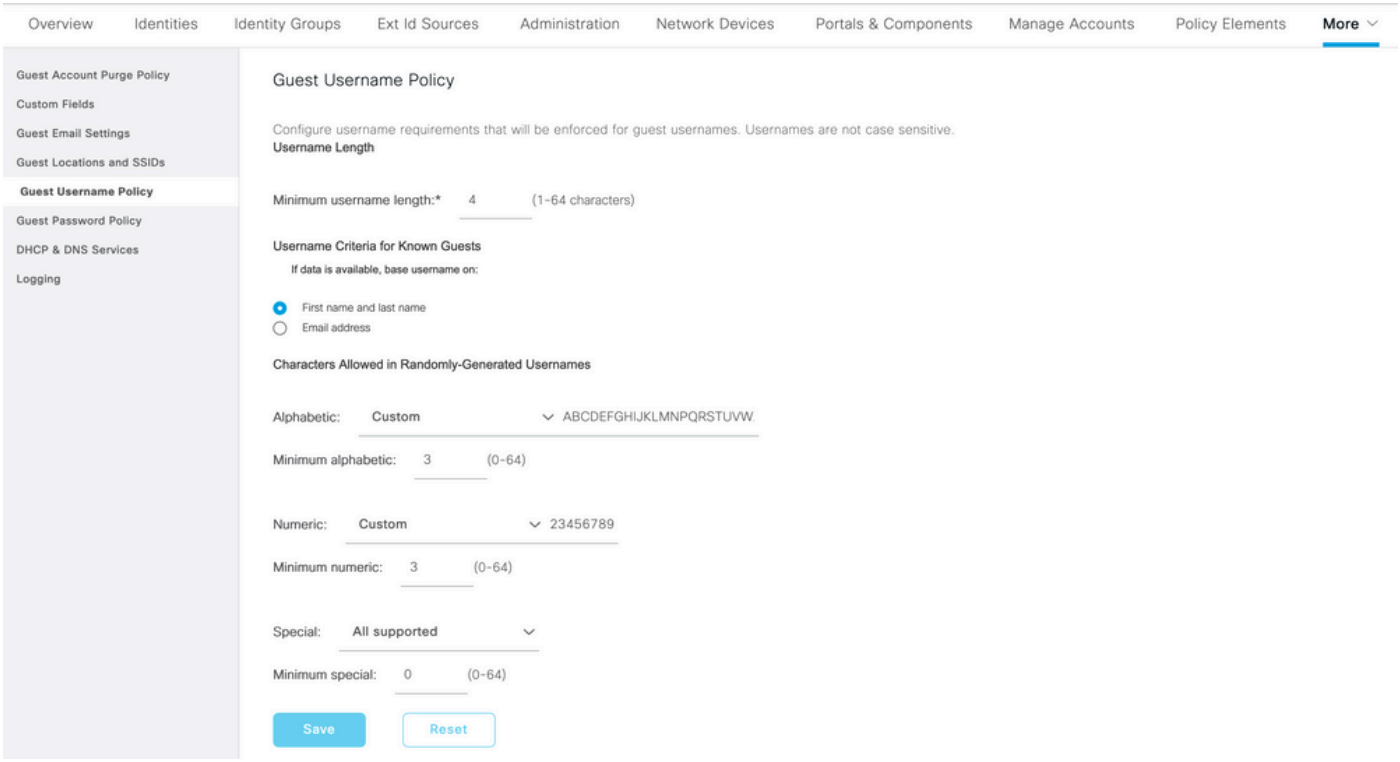


2. Dado que aún no tiene credenciales, debe elegir la opción Register for Guest access (Registrarse para el acceso de invitado). Se le presentará el formulario de registro para crear la cuenta. Si la opción Código de registro estaba habilitada en la configuración del Portal de invitados, ese valor secreto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

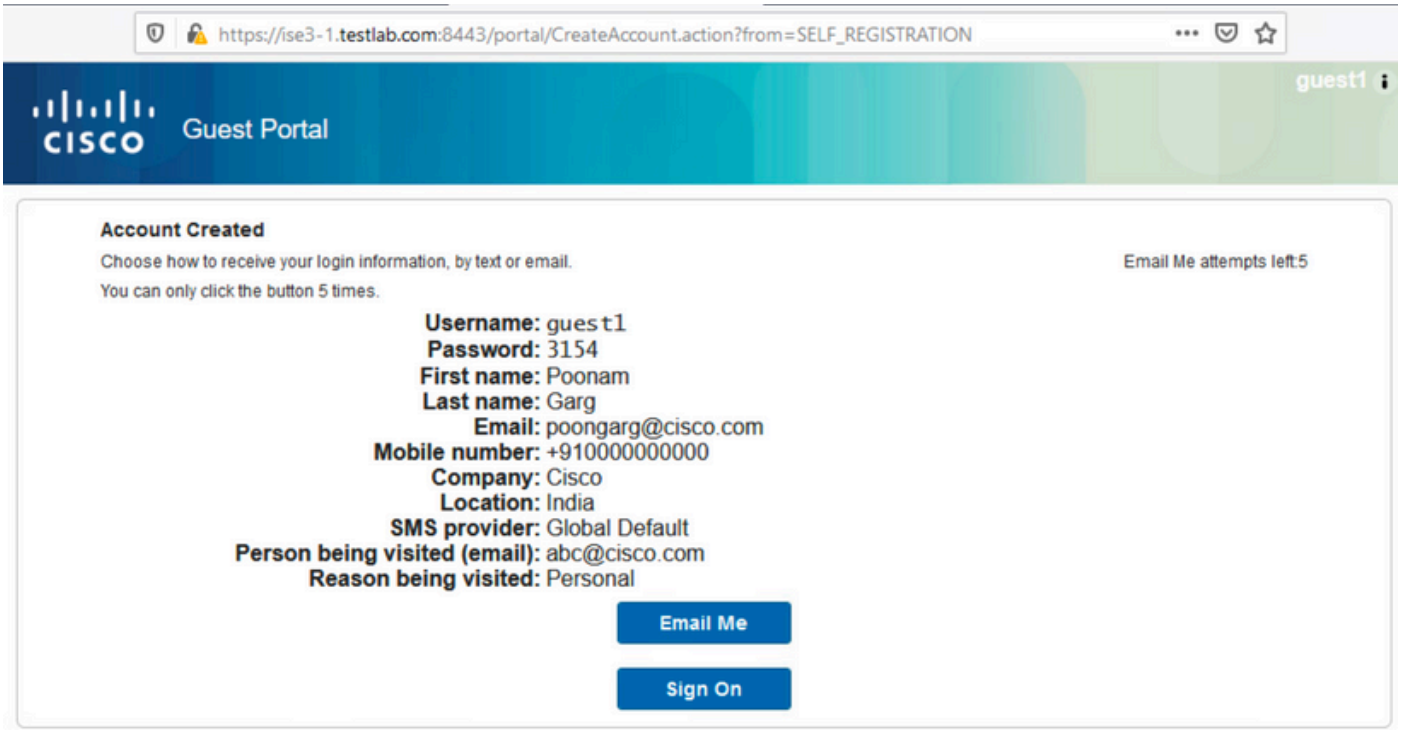
con los permisos correctos puedan registrarse automáticamente).

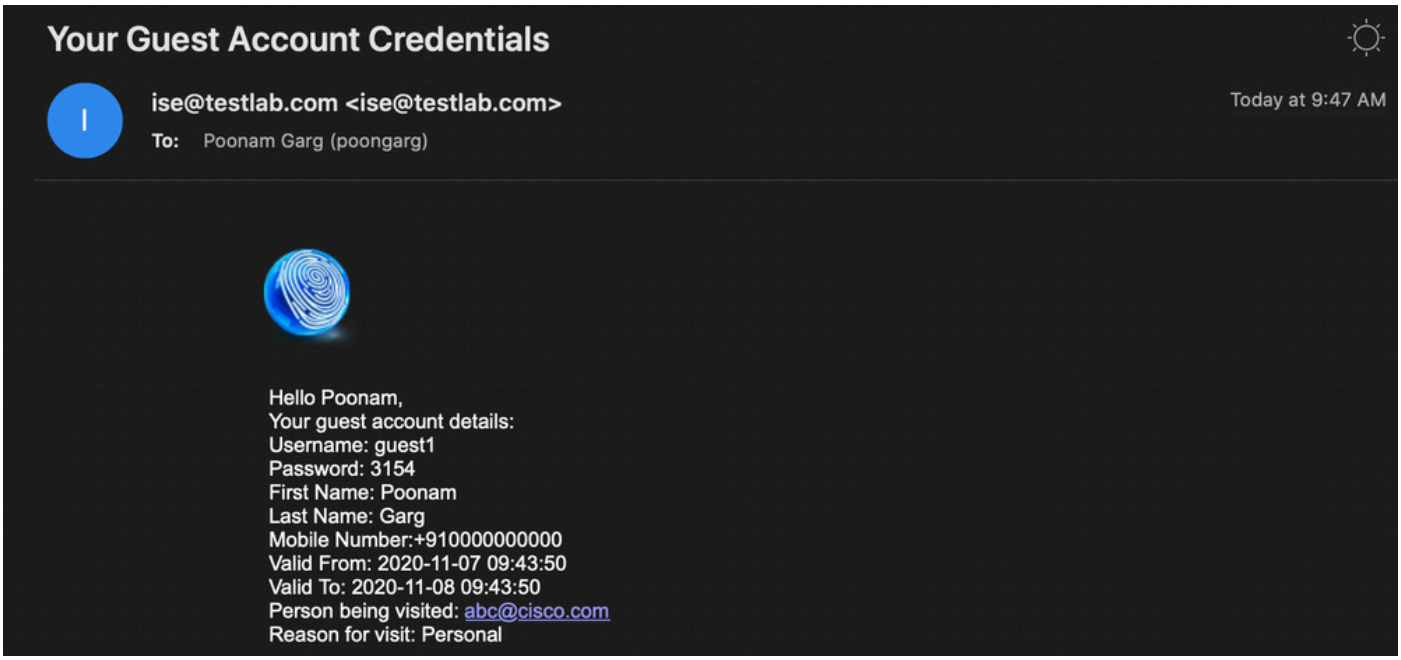


3. Si hay algún problema con la contraseña o la política de usuario, navegue hasta Centros de trabajo > Acceso de invitado > Configuración > Política de nombre de usuario de invitado para cambiar la configuración. Aquí tiene un ejemplo:

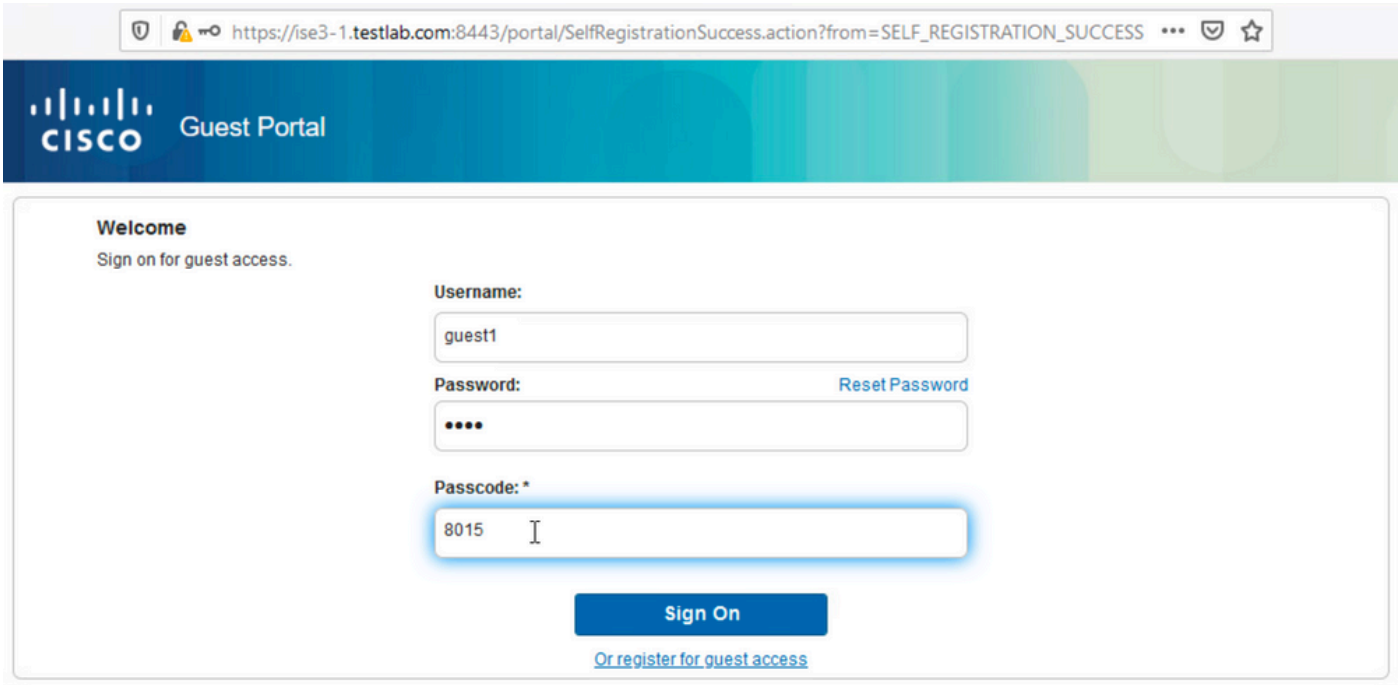


4. Después de la creación de cuenta exitosa, se le presentan credenciales (contraseña generada según las políticas de contraseña de invitado) también el usuario invitado recibe la notificación por correo electrónico si está configurado:

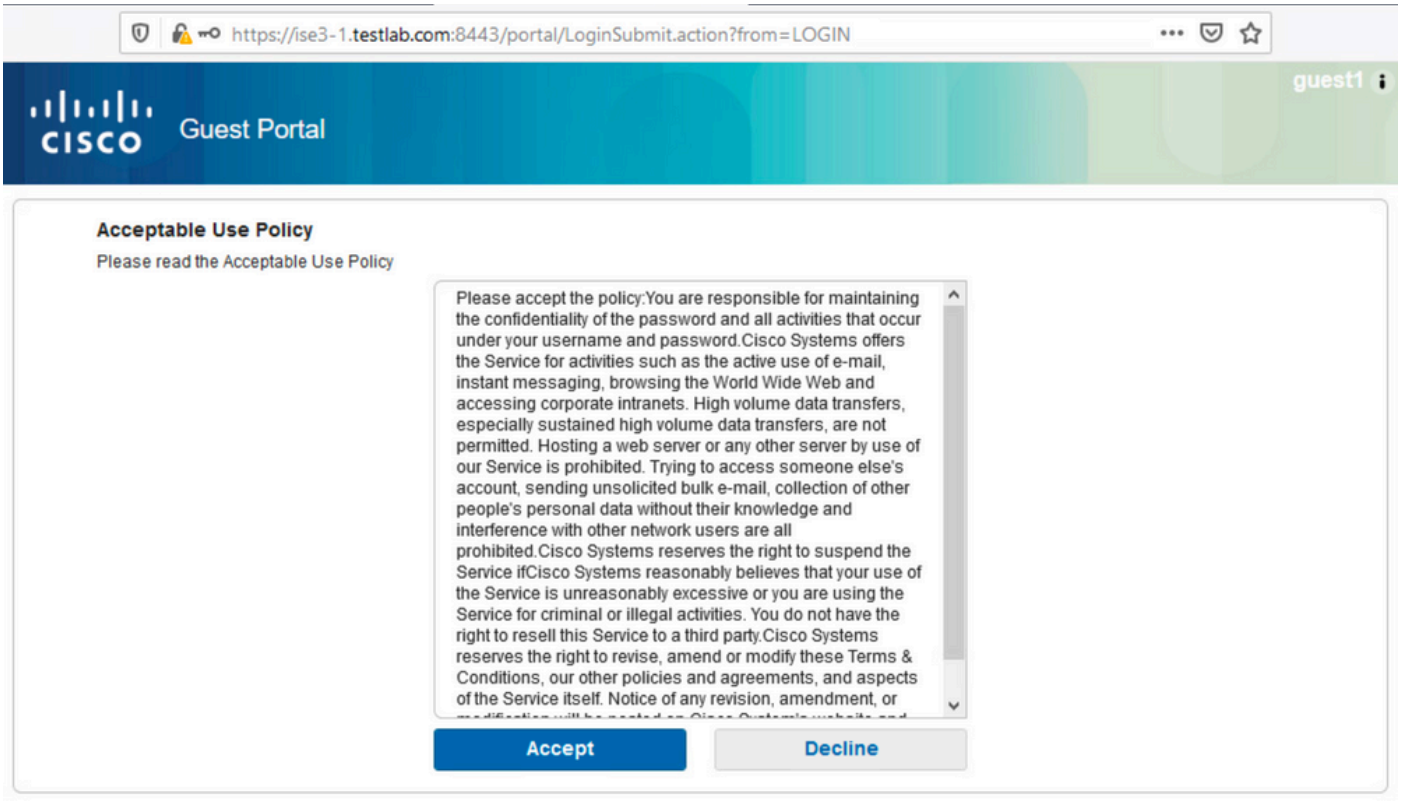


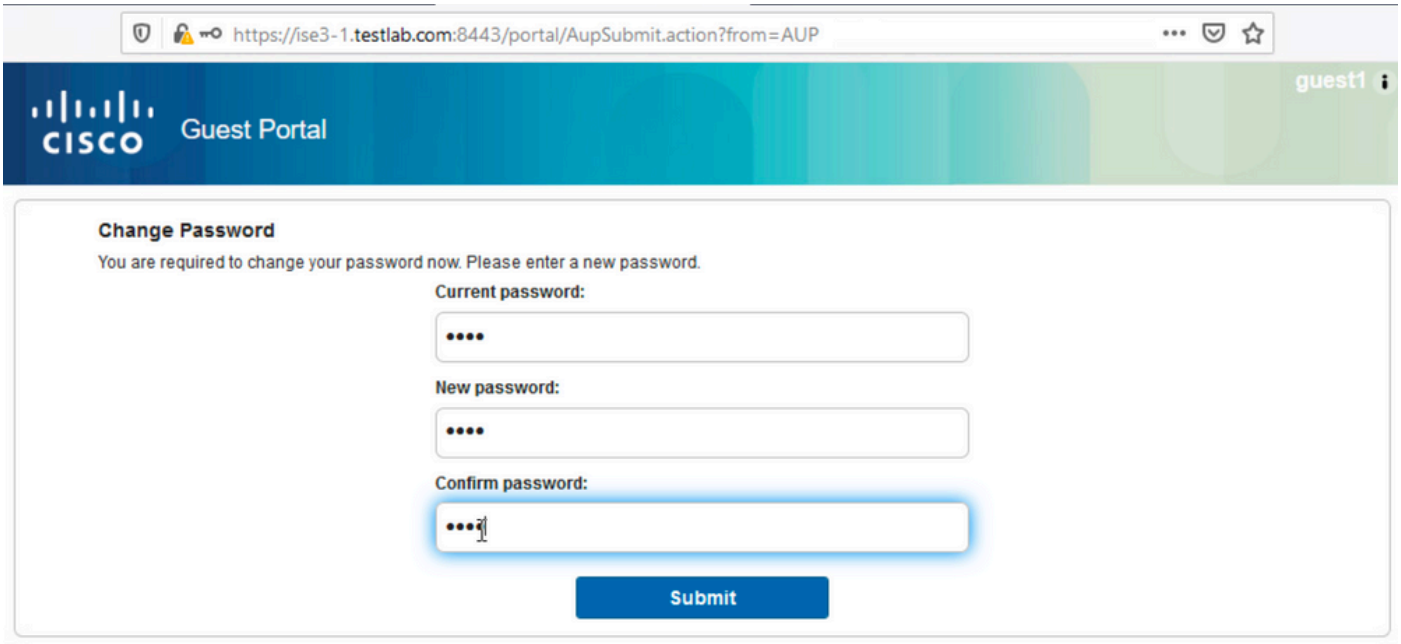


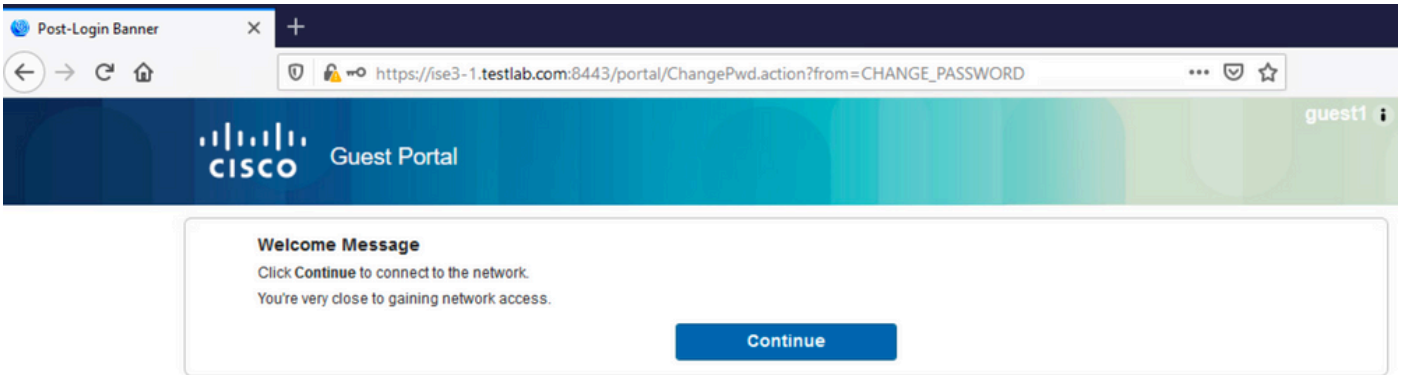
5. Haga clic en Iniciar sesión y proporcione credenciales (se puede requerir una contraseña de acceso adicional si se configura en el portal de invitados; este es otro mecanismo de seguridad que permite iniciar sesión sólo a aquellos que conocen la contraseña).



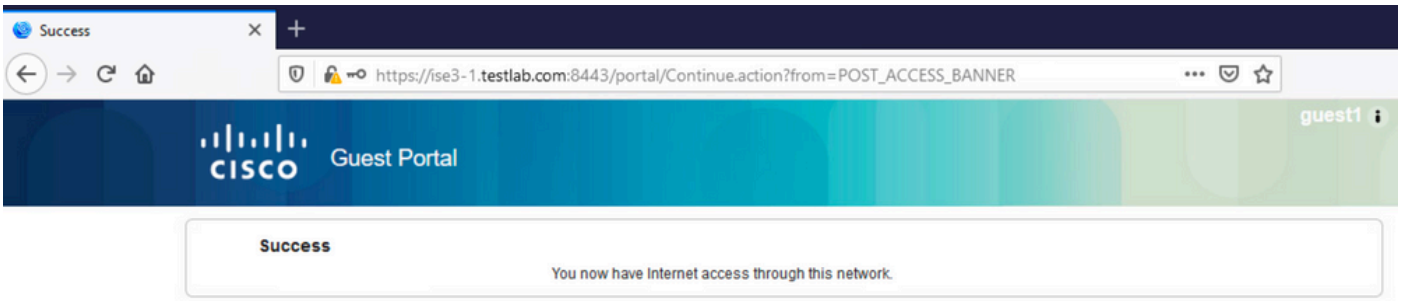
6. Si se realiza correctamente, se puede presentar una política de uso aceptable (AUP) opcional (si está configurada en el portal de invitados). Se muestra al usuario una opción de cambio de contraseña y también se puede mostrar el banner posterior al inicio de sesión (también configurable en el portal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


https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN
guest1
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 ifCisco 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
Accept
Decline


https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP
guest1
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
Guest Portal
Welcome Message
Click Continue to connect to the network.
You're very close to gaining network access.
Continue

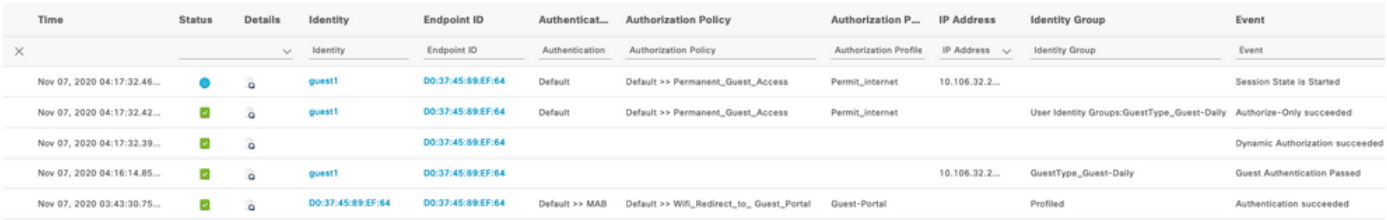
7. La última página (Banner posterior al inicio de sesión) confirma que se ha concedido acceso:



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.



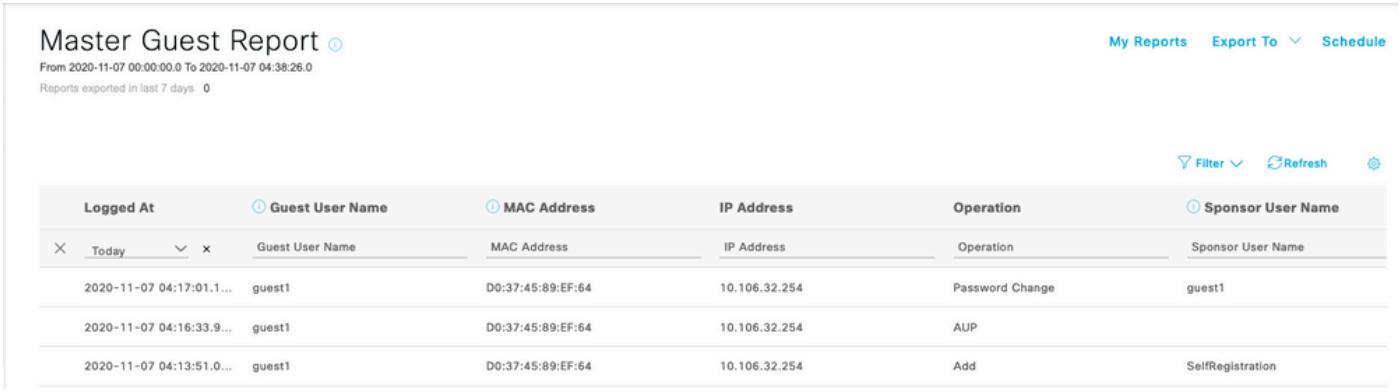
Este es el flujo:

- 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).

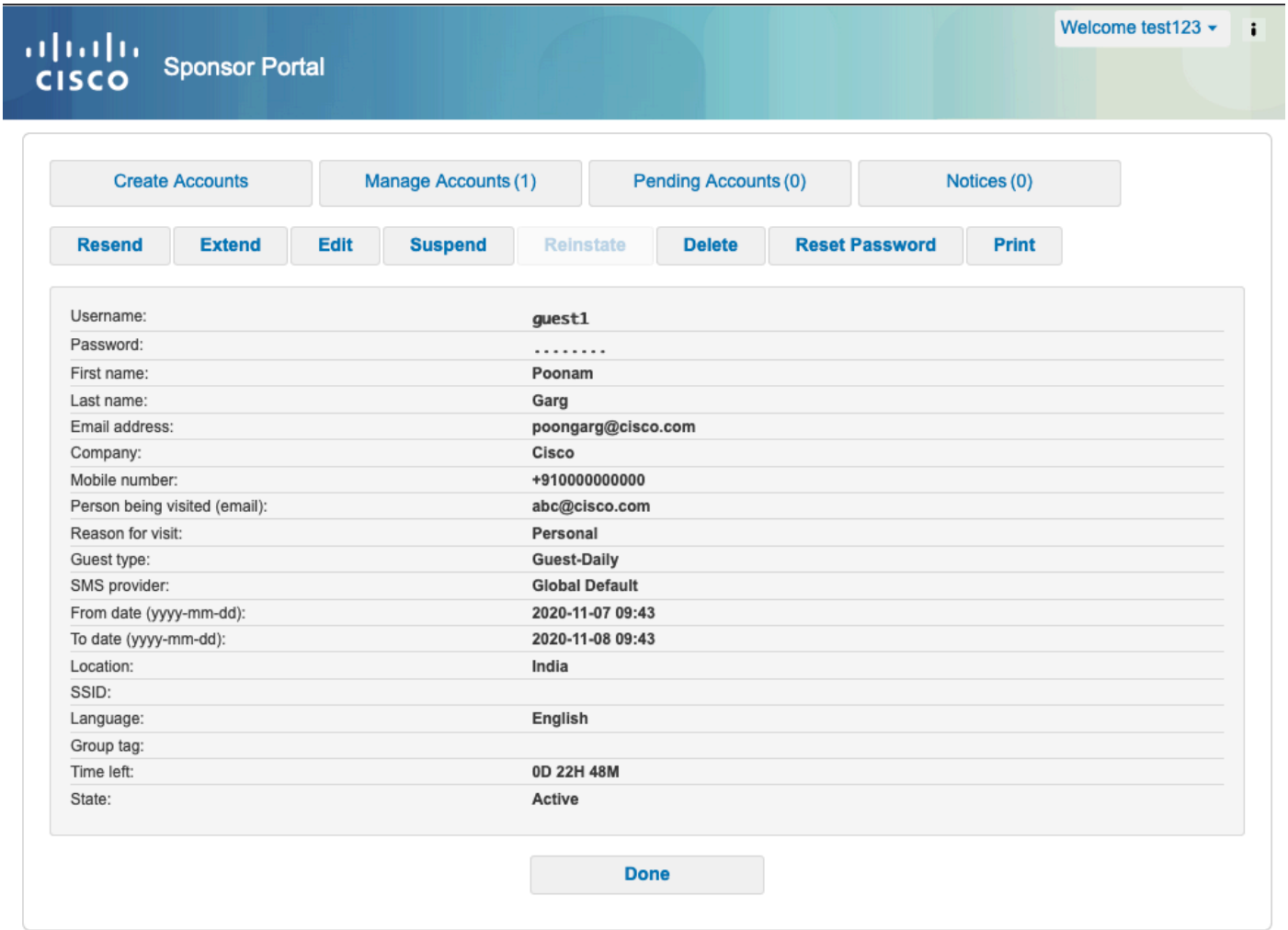
- El WLC realiza la reautenticación con el atributo Authorize-Only y se devuelve el nombre de ACL (Authorize-Only se realiza correctamente). Se proporcionará al invitado el acceso a la red correcto.

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



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:



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.

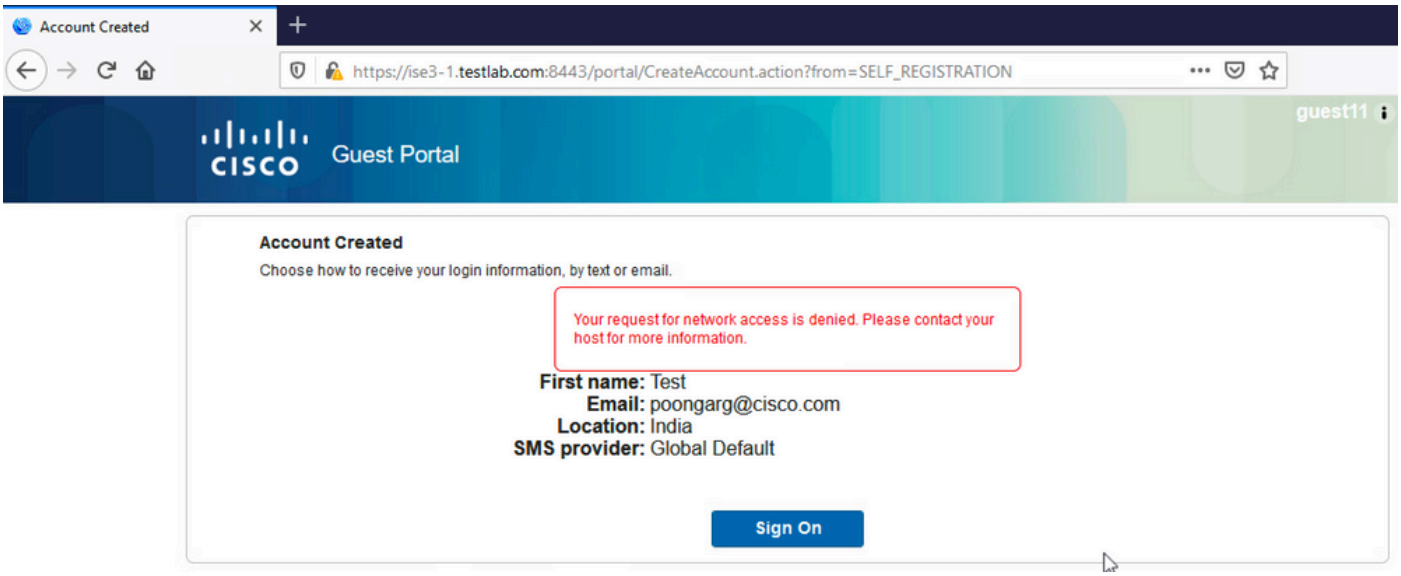
Configuración de BYOD

- 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:



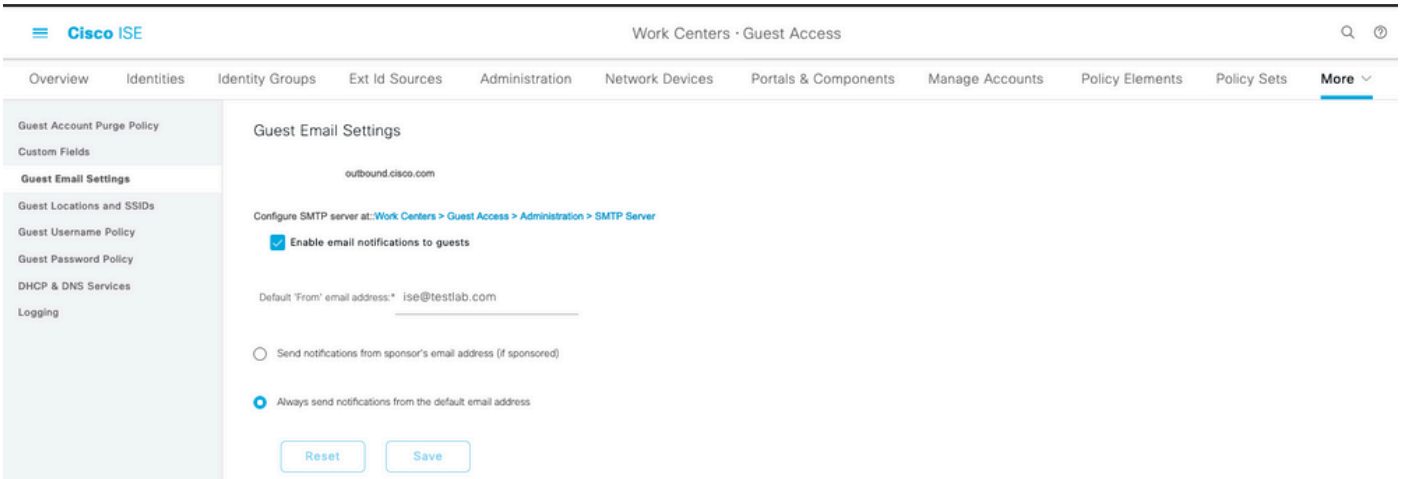
El registro de guest.log confirma que hay un problema con el envío de notificaciones de aprobación al correo electrónico del patrocinador, ya que el servidor SMTP está mal configurado:

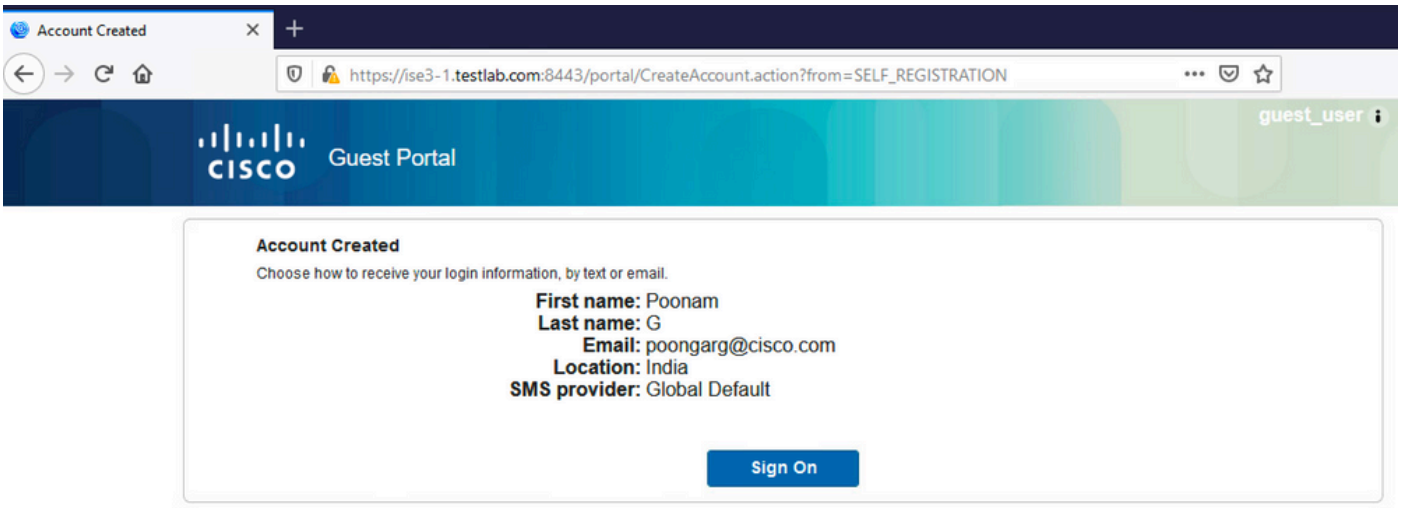
<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][] cpm.guestaccess.apiservices.util.SmtpMs
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
```

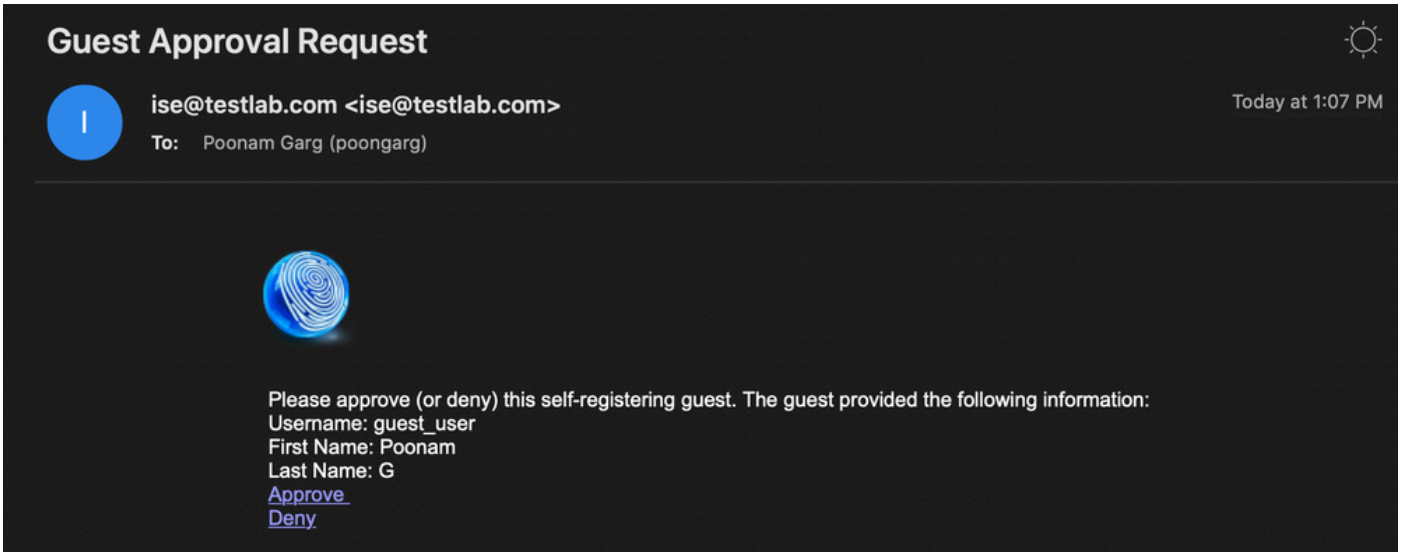
Cuando tenga la configuración de correo electrónico y servidor SMTP adecuada, se creará la cuenta:





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.

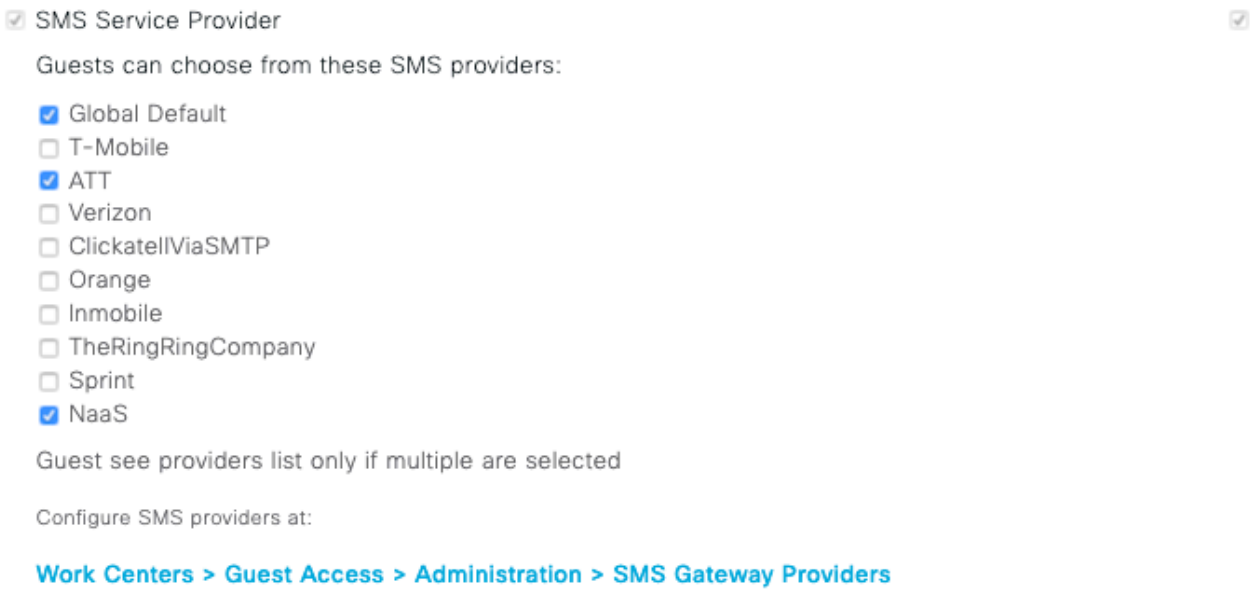
- Dirección "Para" de notificación. Se utiliza para notificar al patrocinador que ha recibido una cuenta para su aprobación. Esto se configura en el Portal de invitados en Centros de trabajo > Acceso de invitados > Portales de invitados > Portales y componentes > Nombre del portal > Configuración del 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

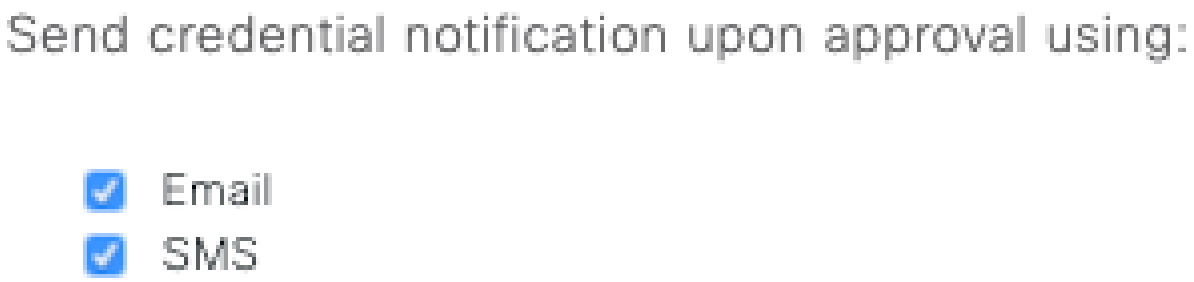
Las credenciales de invitado también se pueden entregar por SMS. Se deben configurar estas opciones:

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

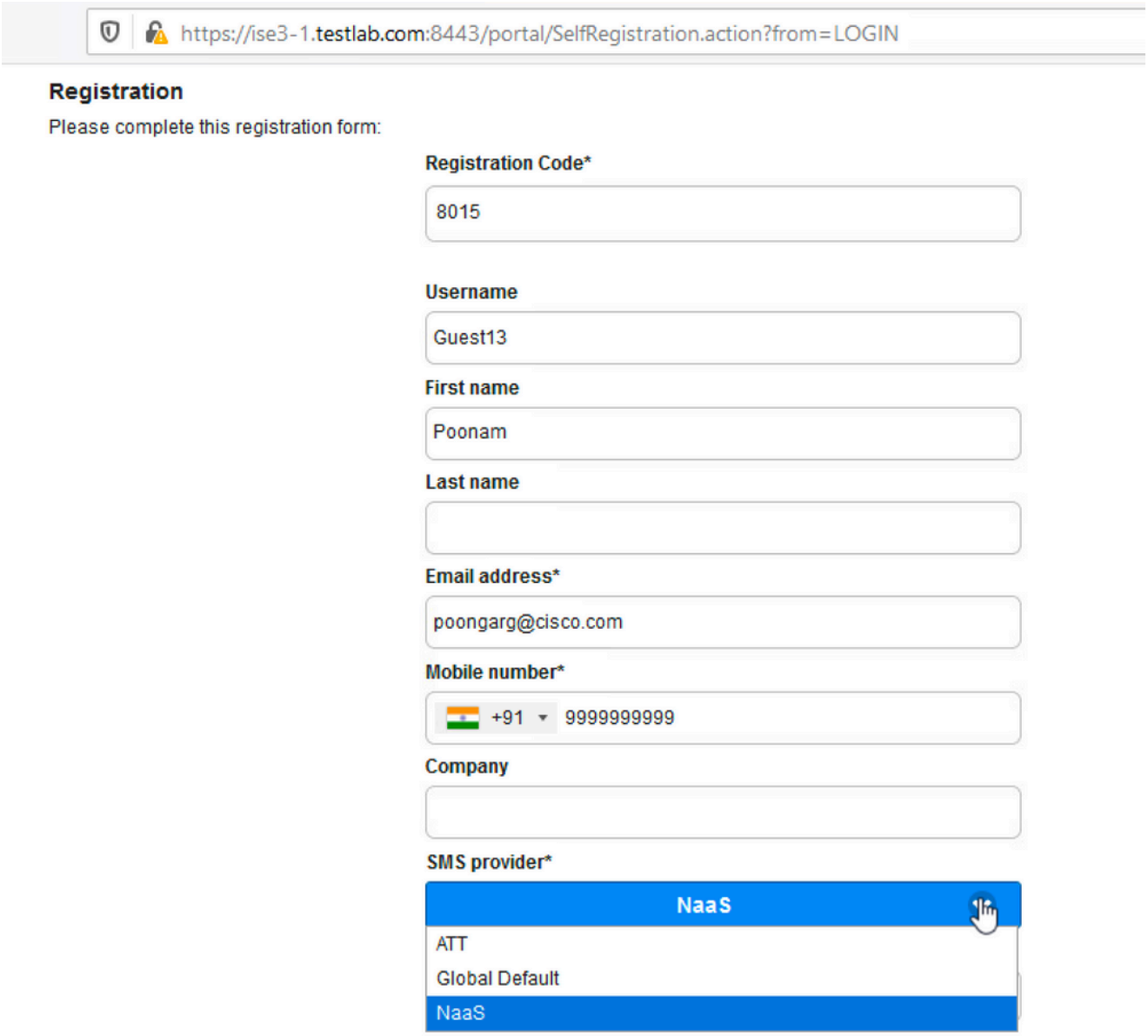


2. Marque la casilla de verificación Enviar notificación de credenciales tras la aprobación

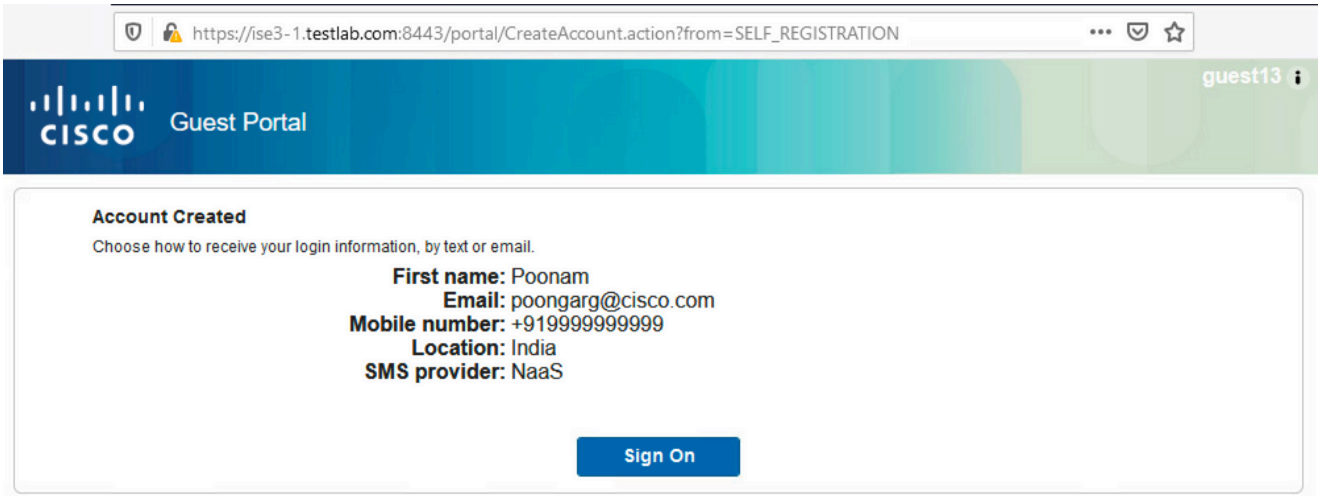
mediante: SMS.



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



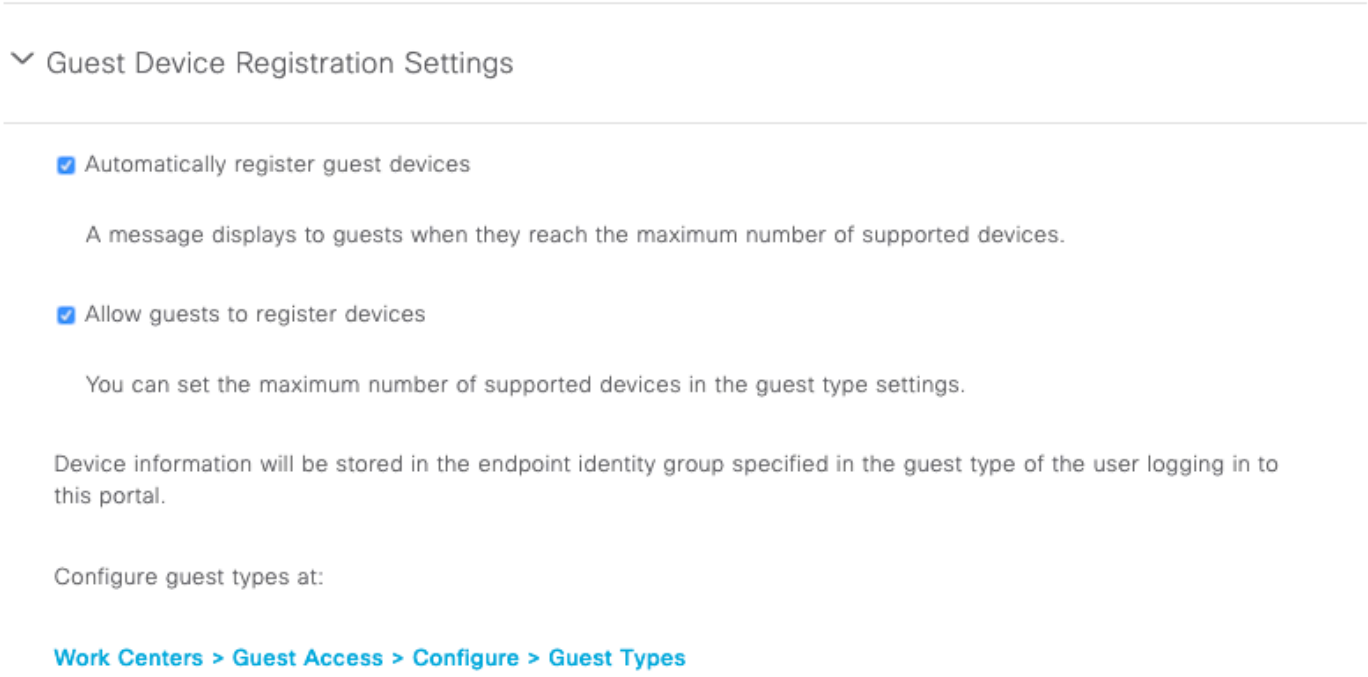
4. Se envía un SMS con el proveedor y el número de teléfono elegidos:

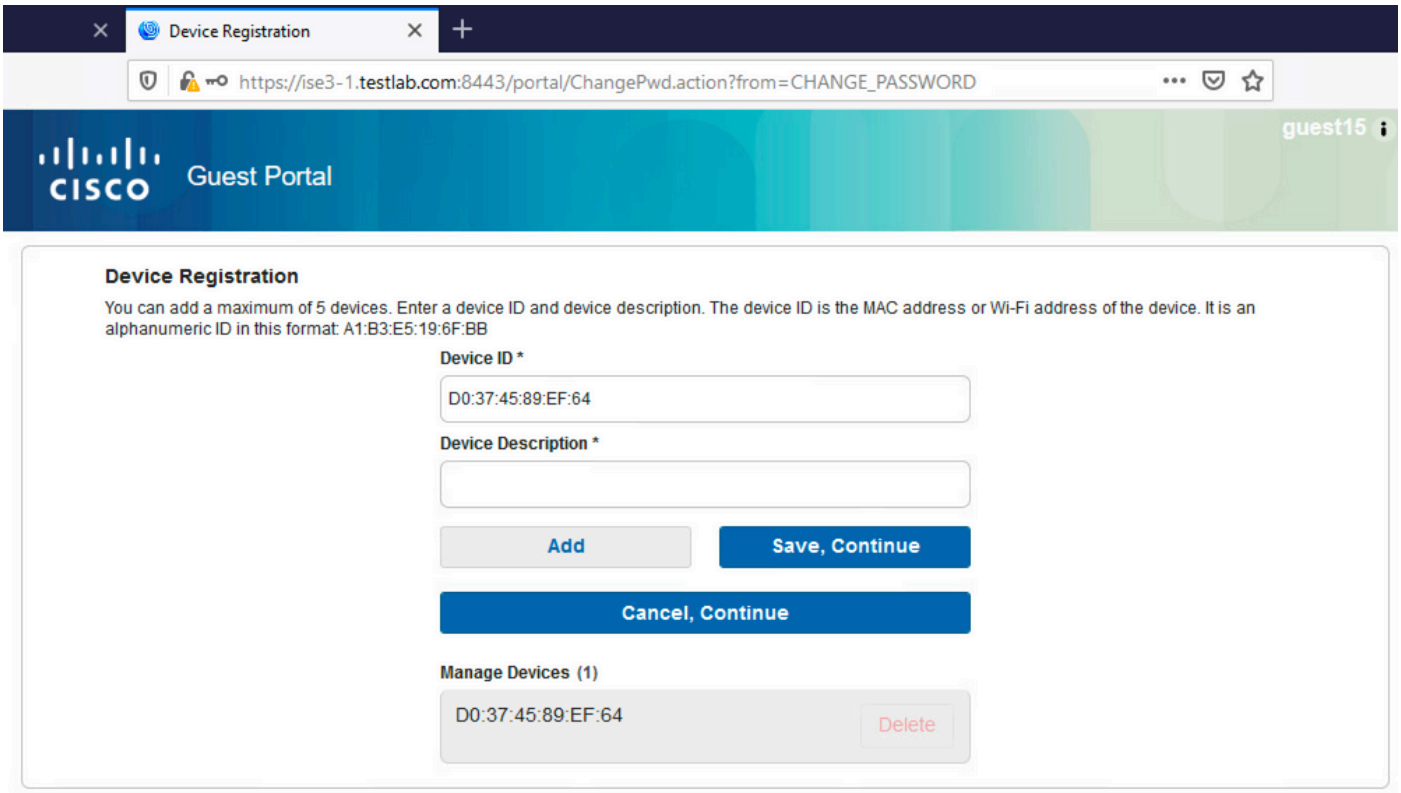


5. Puede configurar los proveedores de SMS en Administration > System > Settings > SMS Gateway.

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:



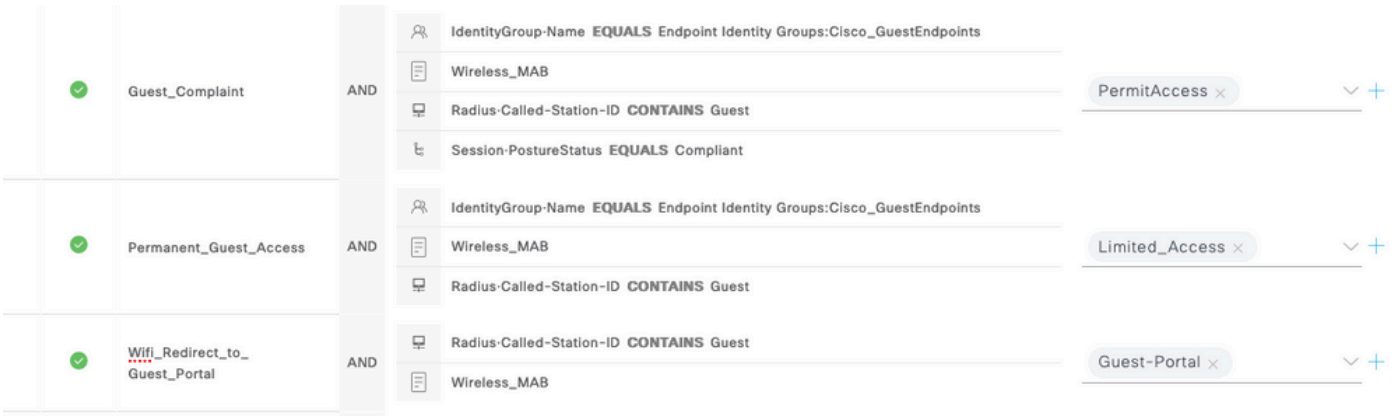


Observe que el dispositivo ya se ha agregado automáticamente (está en la lista Administrar dispositivos). Esto se debe a que se seleccionaron Registración automática de dispositivos invitados.

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.

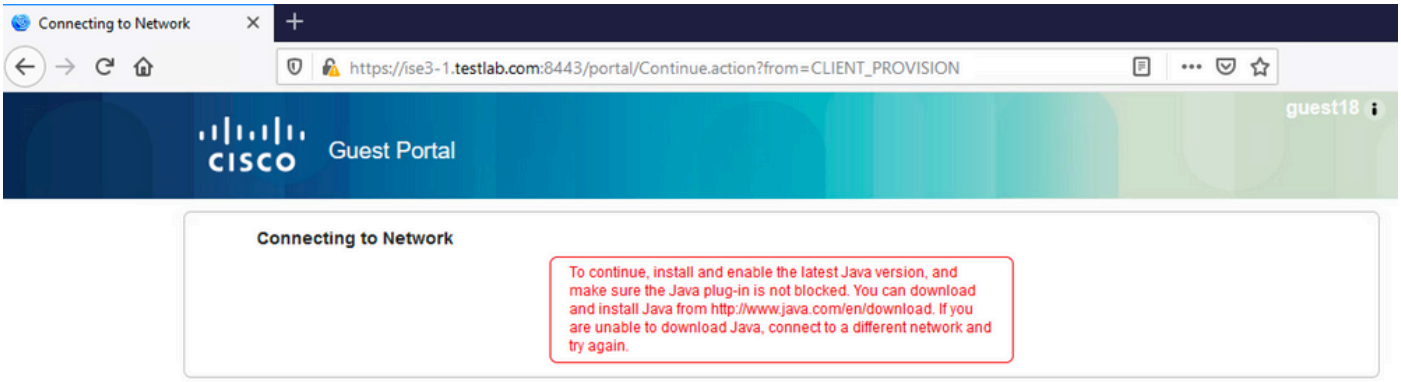
Las posibles reglas de autorización pueden tener un aspecto similar al siguiente:



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>

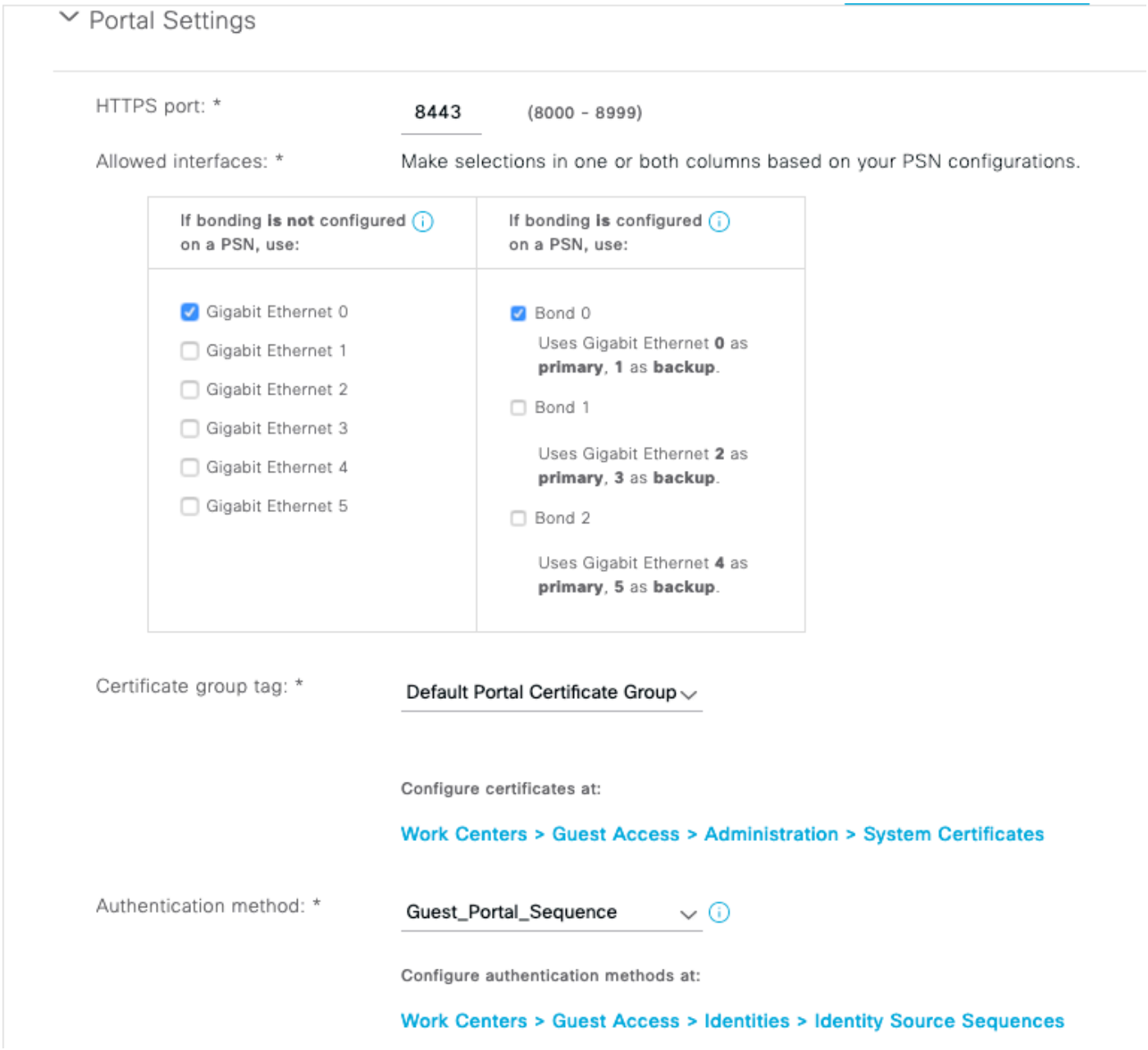
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

BYOD

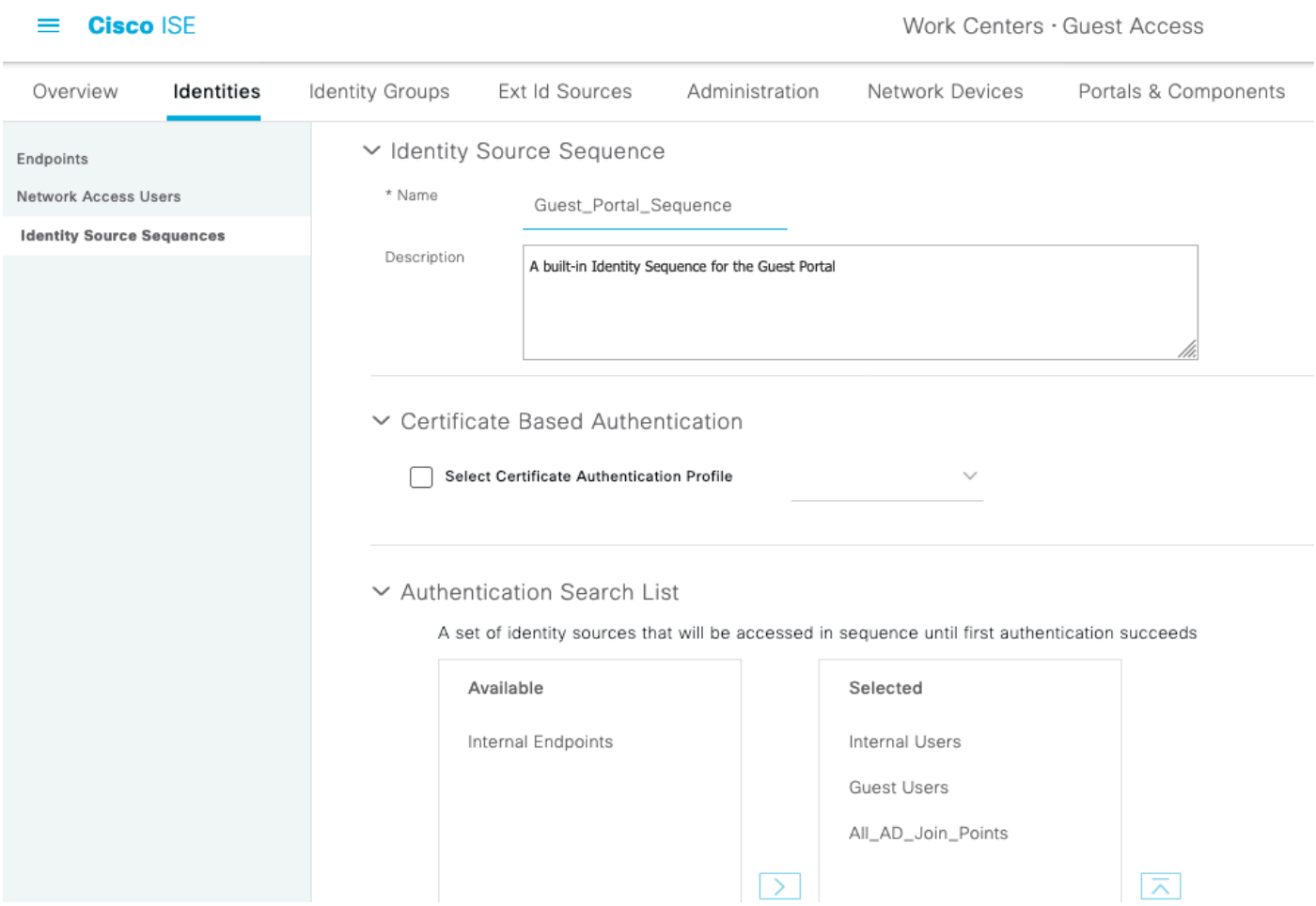
Si la opción Permitir a los empleados utilizar dispositivos personales en la red está seleccionada, los usuarios corporativos que utilicen este portal podrán pasar por el flujo de BYOD y registrar los dispositivos personales. Para los usuarios invitados, esta configuración no cambia nada.

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

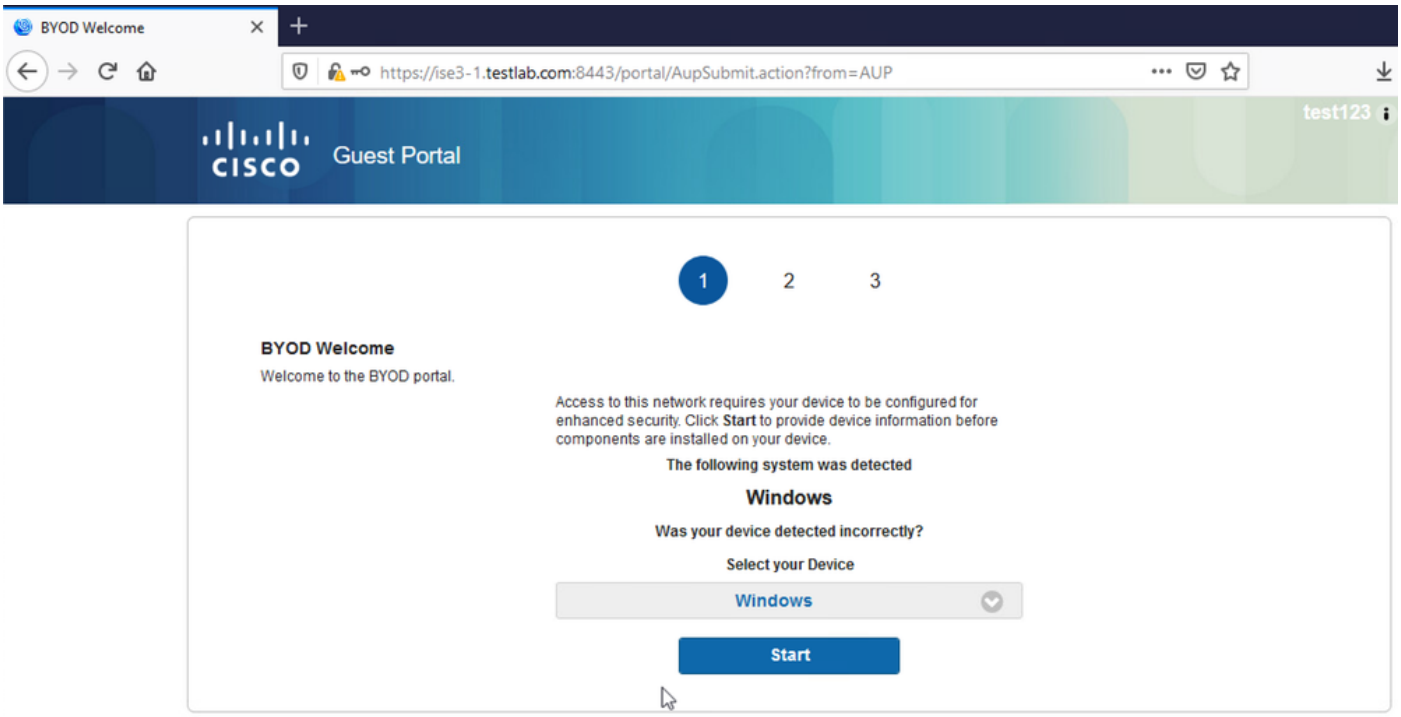
De forma predeterminada, los portales de invitados se configuran con el almacén de identidad Guest_Portal_Sequence:



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.



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:



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).