

Ejemplo de configuración registrado uno mismo del portal del invitado de la versión 1.3 ISE

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topología y flujo](#)

[Configurar](#)

[WLC](#)

[ISE](#)

[Verificación](#)

[Troubleshooting](#)

[Configuración optativa](#)

[Configuraciones del Uno mismo-registro](#)

[Configuraciones del invitado del login](#)

[Configuraciones del registro del dispositivo](#)

[Configuraciones de la conformidad del dispositivo del invitado](#)

[Configuraciones BYOD](#)

[Cuentas Patrocinador-aprobadas](#)

[Entregue las credenciales vía SMS](#)

[Registro del dispositivo](#)

[Postura](#)

[BYOD](#)

[Cambio de VLAN](#)

[Información Relacionada](#)

Introducción

La versión 1.3 del Cisco Identity Services Engine (ISE) tiene un tipo nuevo de portal del invitado llamado el portal registrado uno mismo del invitado, que permite el uno mismo-registro de los Usuarios invitados cuando él accede a los recursos de red. Este portal permite que usted configure y que personalice las características múltiples. Este documento describe cómo configurar y resolver problemas estas funciones.

Prerequisites

Requisitos

Cisco recomienda que usted tiene experiencia con la configuración ISE y el conocimiento básico de estos temas:

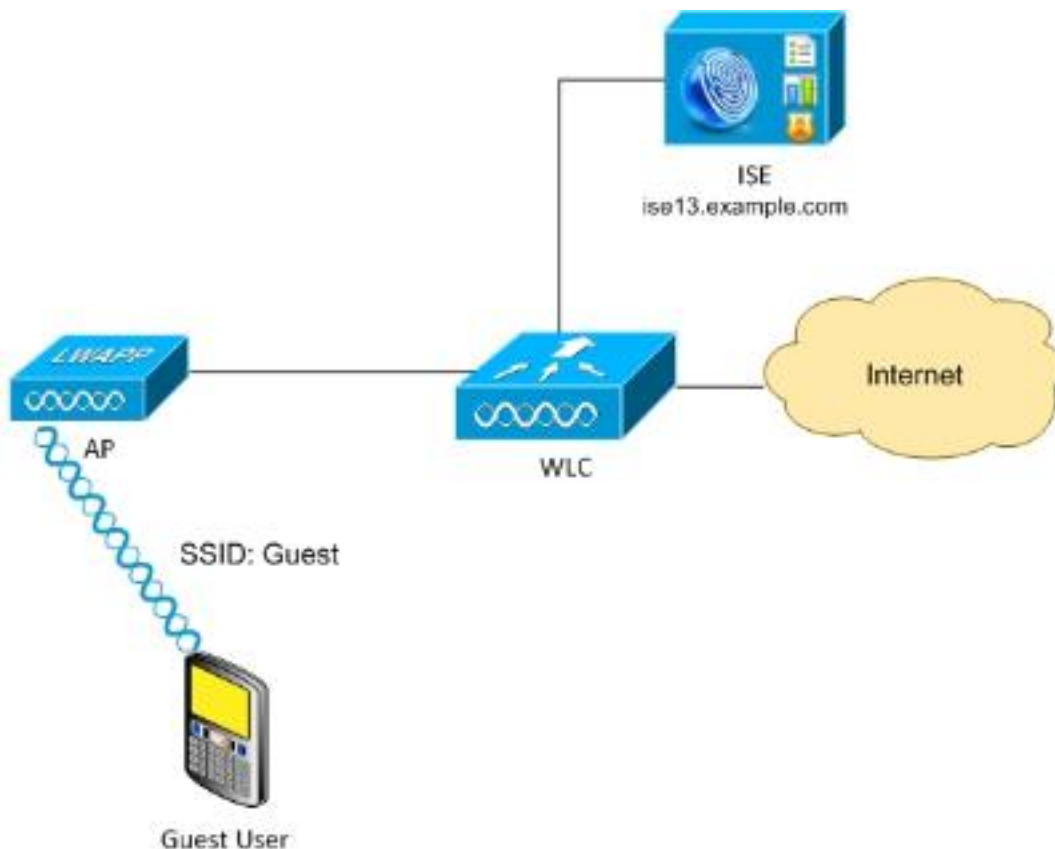
- Implementaciones ISE y flujos del invitado
- Configuración de los reguladores del Wireless LAN (WLC)

Componentes Utilizados

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

- Microsoft Windows 7
- Versión 7.6 y posterior del WLC de Cisco
- Software ISE, versión 3.1 y posterior

Topología y flujo



Este escenario presenta las opciones múltiples disponibles para los Usuarios invitados cuando realizan el uno mismo-registro.

Aquí está el flujo general:

Paso 1. Socios del Usuario invitado al Service Set Identifier (SSID): Invitado. Esto es una red abierta con el MAC que filtra con el ISE para la autenticación. Esta autenticación hace juego la segunda regla de la autorización en el ISE y el perfil de la autorización reorienta al portal registrado uno mismo del invitado. El ISE vuelve un access-accept RADIUS con dos cisco av-pair:

- URL-reorientar-ACL (que el tráfico debe ser reorientado, y el nombre de la lista de control de acceso (ACL) definido localmente en el WLC)
- URL-reorientar (donde reorientar ese tráfico al ISE)

Paso 2. Reorientan al Usuario invitado al ISE. Bastante que las credenciales para iniciar sesión, el usuario que los tecleos “no tienen una cuenta”. Reorientan al usuario a una página donde esa cuenta puede ser creada. Un código secreto opcional del registro se pudo habilitar para limitar el privilegio del uno mismo-registro a la gente que conoce ese valor secreto. Después de que se cree la cuenta, el usuario es credenciales proporcionadas (nombre de usuario y contraseña) y abre una sesión con esas credenciales.

Paso 3. El ISE envía un cambio RADIUS de la autorización (CoA) Reauthenticate al WLC. El WLC reautentifica al usuario cuando envía el pedido de acceso del RADIO con el atributo del autorizar-Solamente. El ISE responde con el access-accept y el Airespace ACL definidos localmente en el WLC, que proporciona el acceso a Internet solamente (el acceso final para el Usuario invitado depende de la directiva de la autorización).

Observe que para las sesiones del Protocolo de Autenticación Extensible (EAP), el ISE debe enviar un CoA termina para accionar la reautenticación porque la sesión EAP está entre el supplicant y el ISE. Pero para MAB (MAC que filtra), el CoA Reauthenticate es bastante; no hay necesidad de-associate/de-authenticate el cliente de red inalámbrica.

Paso 4. El Usuario invitado ha deseado el acceso a la red.

Las características adicionales múltiples como la postura y Bring Your Own Device (BYOD) pueden ser habilitadas (discutido más adelante).

Configurar

WLC

1. Agregue al nuevo servidor de RADIUS para la autenticación y las estadísticas. Navegue a la **Seguridad >AAA > radio > autenticación** para habilitar CoA RADIUS (RFC 3576).

Security

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

RADIUS Authentication Servers > Edit

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

Hay una configuración similar para considerar. También se aconseja configurar el WLC para enviar el SSID en estación que recibe la llamada el atributo ID, que permite que el ISE configure las reglas flexibles basadas en el SSID:

Security

- AAA
 - General
 - RADIUS
 - Authentication

RADIUS Authentication Servers

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

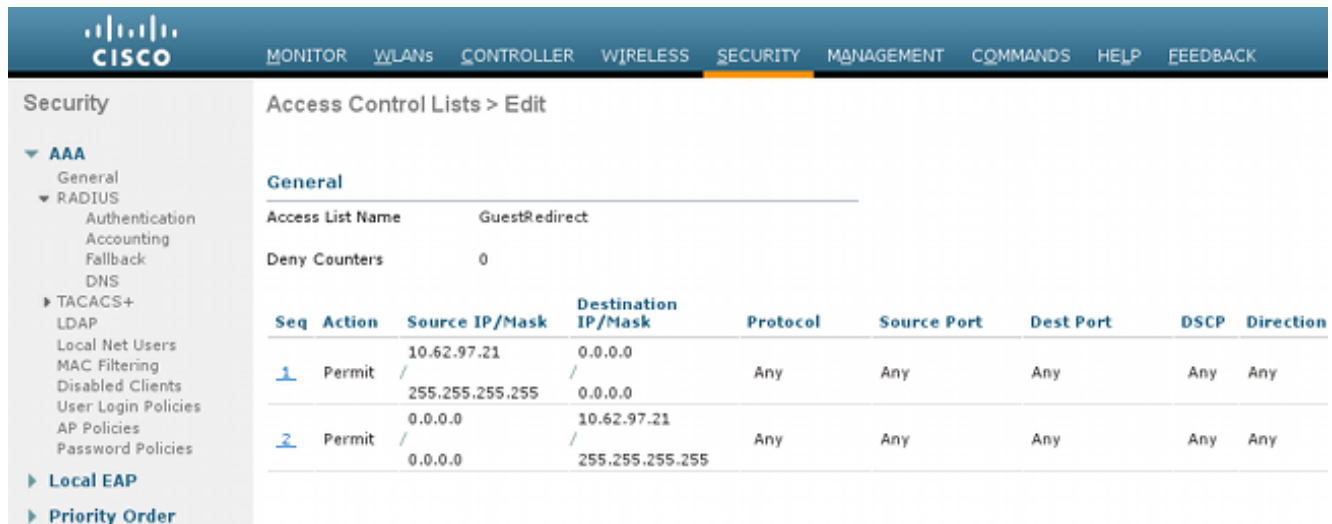
2. Bajo los WLAN tabule, cree al invitado del Wireless LAN (red inalámbrica (WLAN)) y configure la interfaz correcta. Fije la Seguridad Layer2 a **ningunos** con la filtración MAC. En los servidores de la Seguridad/del Authentication, Authorization, and Accounting (AAA), seleccione la dirección IP ISE para la autenticación y las estadísticas. En la ficha Avanzadas, habilite la **invalidación AAA** y fije el estado del Network Admission Control (NAC) al NAC RADIUS (soporte CoA).

3. Navegue a la **Seguridad > a las listas de control de acceso > a las listas de control de acceso** y cree dos Listas de acceso:

GuestRedirect, que permite el tráfico que no debe ser reorientado y reorienta el resto del tráfico Internet, que se niega para las redes corporativas y se permite para todos los demás

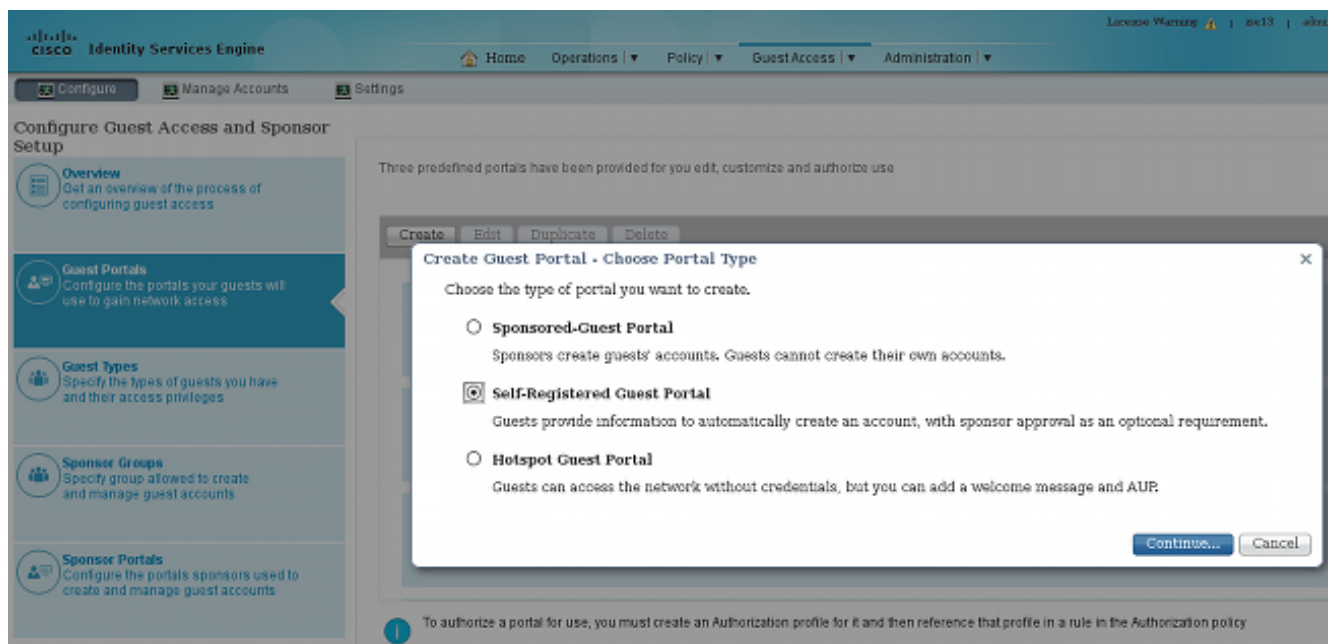
Aquí está un ejemplo para GuestRedirect ACL (necesidad de excluir el tráfico a/desde el ISE

del cambio de dirección):



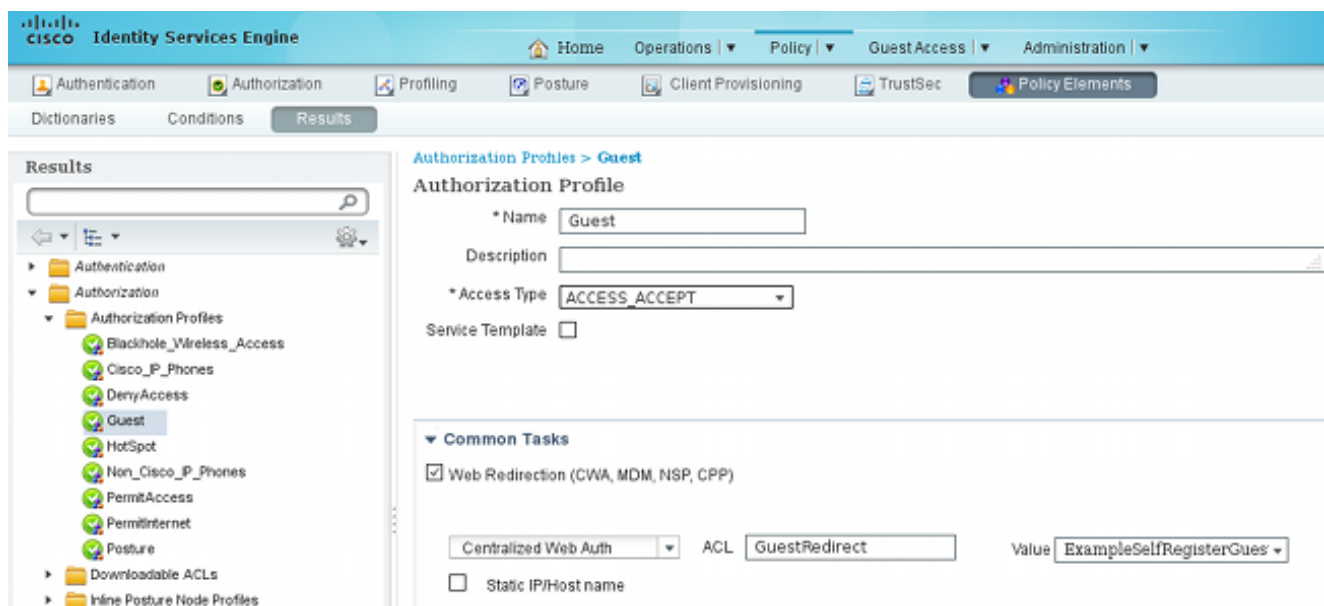
ISE

1. Navegue al **acceso de invitado > a la configuración > a los portales del invitado**, y cree un nuevo tipo porta, portal registrado uno mismo del invitado:

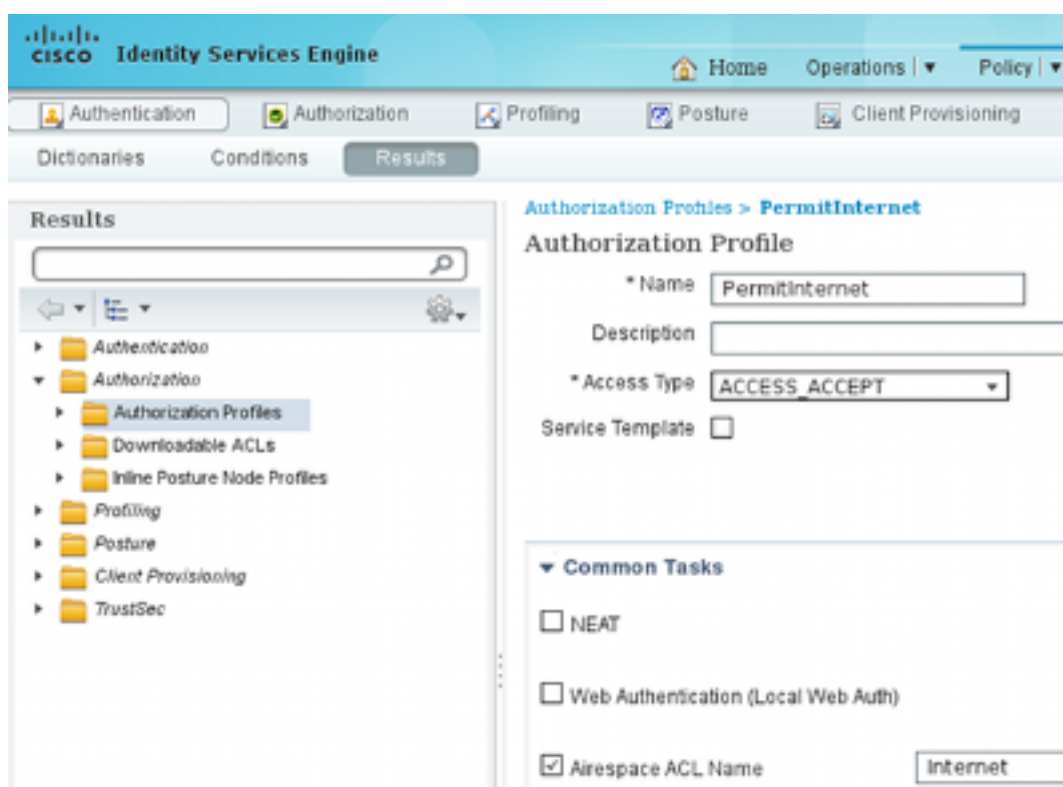


2. Elija el nombre porta que será referido al perfil de la autorización. Fije todas las otras configuraciones para omitir. Bajo arreglo para requisitos particulares porta de la página, todas las páginas presentadas pueden ser personalizadas.
3. Perfiles de la autorización de la configuración:

Invitado (con el cambio de dirección al nombre porta y a ACL GuestRedirect del invitado)



PermitInternet (con Internet del igual del Airespace ACL)



- Para verificar las reglas de la autorización, navegue a la **directiva > a la autorización**. En la versión 1.3 ISE por abandono para la autenticación fallada del acceso de puente de la autenticación de MAC (MAB) (dirección MAC no encontrada) se continúa (no rechazado). Esto es muy útil para los portales del invitado porque no hay necesidad de cambiar cualquier cosa en las reglas de la autenticación predeterminada.

Authorization Policy

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

First Matched Rule Applies

▶ Exceptions (0)

Standard

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

Los usuarios nuevos que se asocian al invitado SSID no son todavía parte de cualquier grupo de la identidad. Esta es la razón por la cual hacen juego la segunda regla, que utiliza el perfil de la autorización del invitado para reorientarlos al portal correcto del invitado.

Después de que un usuario cree una cuenta y abra una sesión con éxito, el ISE envía un CoA RADIUS y el WLC realiza la reautenticación. Esta vez, la primera regla se corresponde con junto con el perfil PermitInternet de la autorización y vuelve el nombre ACL que se aplica en el WLC.

5. Agregue el WLC como dispositivo de acceso a la red de la **administración > de los recursos de red > de los dispositivos de red**.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

1. Después de que usted se asocie al invitado SSID y teclee un URL, después le reorientan a la página de registro:

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

CISCO Sponsored Guest Portal

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

Username:

Password:

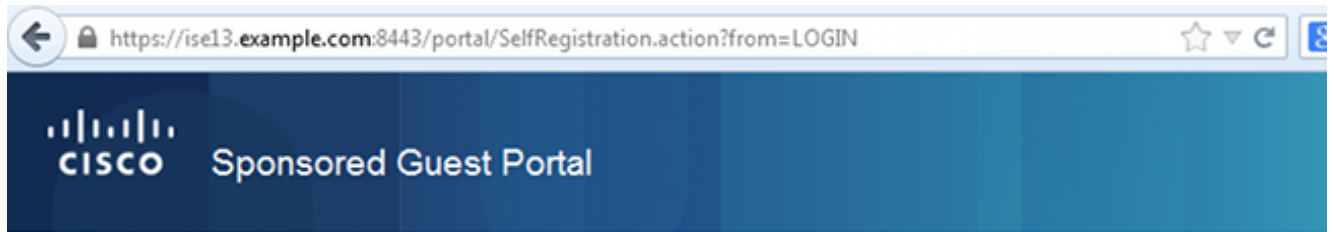
Passcode:

Sign On

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

[Contact Support](#)

2. ¿Puesto que usted no tiene ningunas credenciales todavía, usted debe elegir **no tiene una cuenta?** opción. Una nueva página que permite las visualizaciones de la creación de una cuenta. Si la opción del código del registro fue habilitada bajo configuración porta del invitado, se requiere ese valor secreto (éste se asegura de que solamente no prohiban la gente con los permisos correctos el uno mismo-registro).



Create Account

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

Registration Code*

cisco

Username

guest1

First name

michal

Last name

garcarz

Email address

mgarcarz@cisco.com

Phone number

666666666

3. Si hay algunos problemas con la contraseña o la política de usuario, navegue al **acceso de invitado > a las configuraciones > a la política de contraseña del invitado** o el **acceso de invitado > las configuraciones > la directiva del nombre de usuario del invitado** para cambiar las configuraciones. Aquí tiene un ejemplo:

▶ Guest Email Settings

Identify the SMTP server and specify

▶ Guest Locations and SSIDs

Specify the locations where you want

▶ Guest Password Policy

Specify the policy settings that will

▼ Guest Username Policy

Specify the policy settings that will

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

Username Length

Minimum username length: (1-64 characters)

Username Criteria for Known Guests

If data is available, base username on:

- First name and last name
- Email address

Characters Allowed in Randomly-Generated Usernames

Alphabetic:

Minimum alphabetic: (0-64)

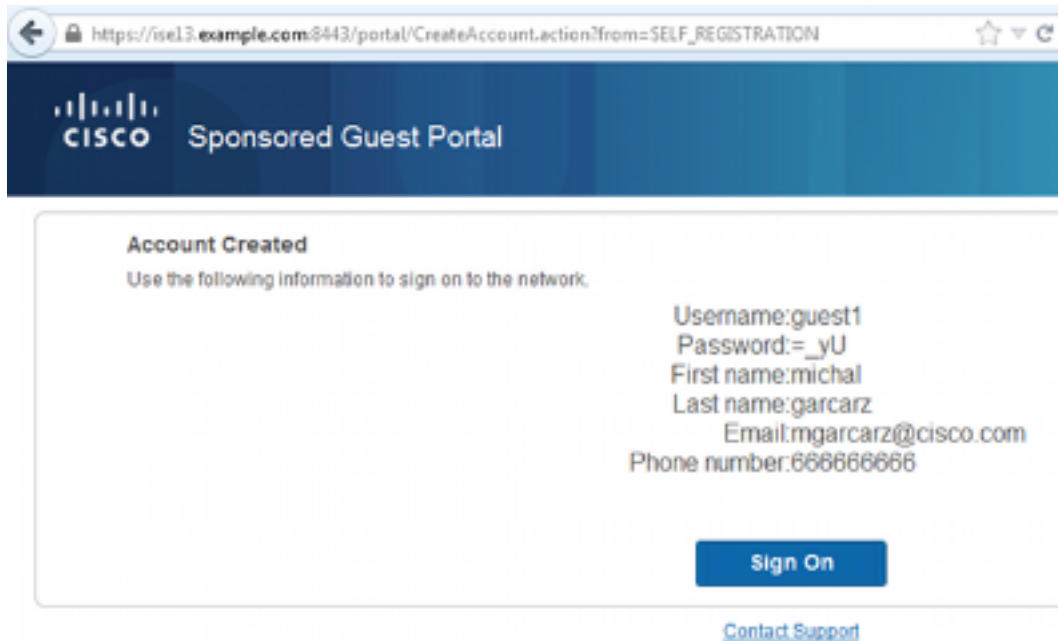
Numeric:

Minimum numeric: (0-64)

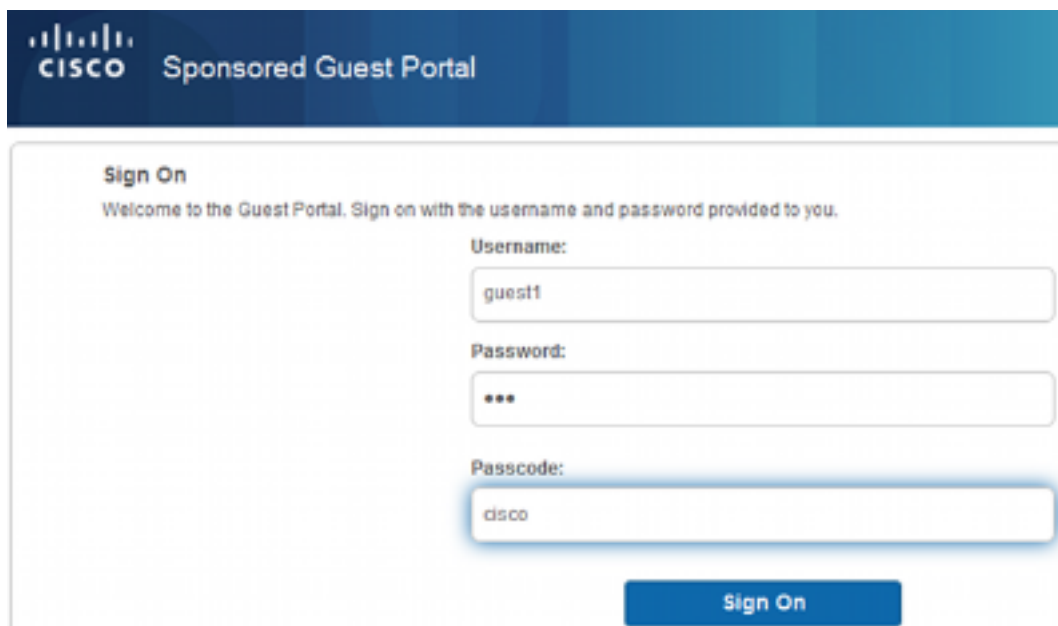
Special:

Minimum special: (0-64)

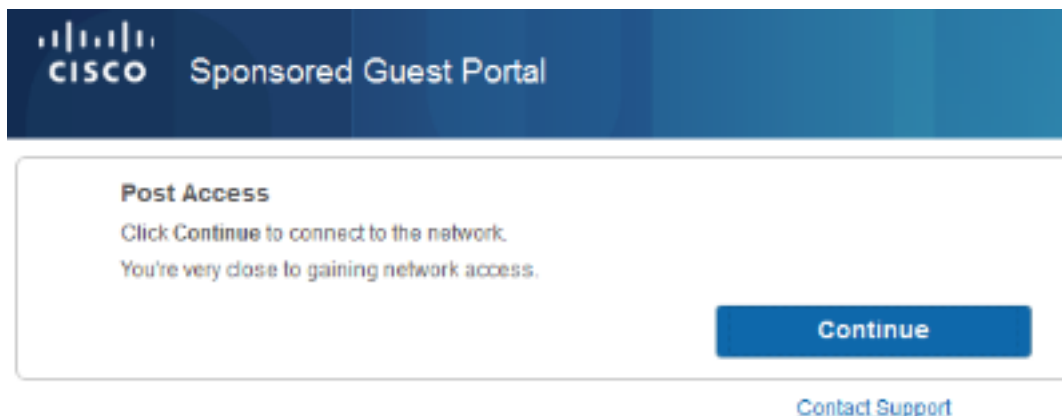
4. Después de la creación de una cuenta acertada, le presentan con las credenciales (contraseña generada según las políticas de contraseña del invitado):



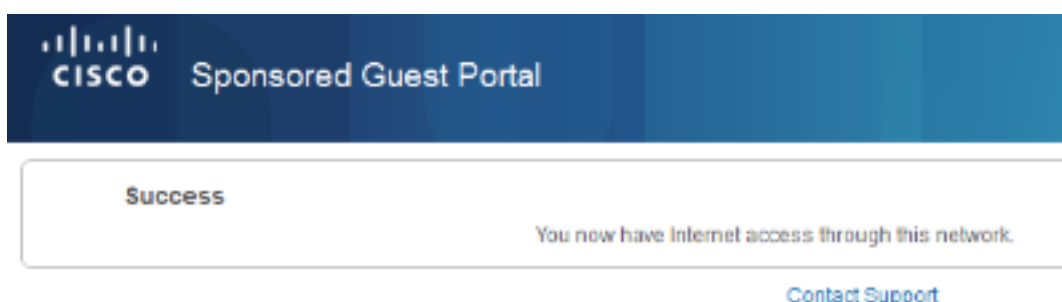
5. Haga clic la **muestra encendido** y proporcione las credenciales (la contraseña adicional del acceso pudo ser requerida si estuvo configurada bajo el portal del invitado; éste es otro mecanismo de seguridad que permite solamente a los que conozcan la contraseña para iniciar sesión).



6. Cuando es acertado, un Acceptable Use Policy opcional (AUP) pudo ser presentado (si está configurado bajo el portal del invitado). La página del acceso del poste (también portal inferior configurable del invitado) pudo también visualizar.



La página más reciente confirma que se ha concedido el acceso:



Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

En esta etapa, el ISE presenta estos registros:

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	🔴		0	quest1					Session State is Started
2014-08-01 13:19:52...	🟢			quest1	Default >> MAB	Default >> Guest	PermitInternet	User Identity Gro...	Authorize-Only succeeded
2014-08-01 13:19:52...	🟢			quest1					Dynamic Authorization succeeded
2014-08-01 13:18:29...	🟢			quest1				GuestType_DAILY	Guest Authentication Passed
2014-08-01 13:16:31...	🟢			64:66:B3:08:23	Default >> MAB >> ..	Default >> Guest_...	Guest		Authentication succeeded

Aquí está el flujo:

- El Usuario invitado encuentra la segunda regla de la autorización (Guest_Authenticate) y se reorienta al invitado (“Authenticación tuvo éxito”).
- Reorientan al invitado para el uno mismo-registro. Después de que con éxito el login (con la cuenta creada recientemente), ISE envíe el CoA Reauthenticate, que es confirmado por el WLC (“autorización dinámica tenida éxito”).

- El WLC realiza la reautenticación con el atributo del autorizar-Solamente y se vuelve el nombre ACL (“Autorizar-Solamente tuvo éxito”). Proporcionan el invitado el acceso a la red correcto.

Los informes (las **operaciones > señalan que > el ISE señala > los informes del acceso de invitado > informe del invitado del master**) también confirman eso:

Master Guest Report								Favorite
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM								Page << 1 >>
Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance	
2014-08-01 13:18:49.9	guest1	64-66-83-08-23-A3	10.221.0.218				Guest user has accepted the use policy	
2014-08-01 13:18:08.7	guest1	64-66-83-08-23-A3	10.221.0.218	Add	SelfRegistration			

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

Este ejemplo confirma que la cuenta está creada, pero el usuario nunca ha abierto una sesión (“aguardando la conexión con el sistema inicial”):

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

First name:	michal
Last name:	garcarz
Username:	guest1
Password:	=_yU
Email address:	mgarcarz@cisco.com
Company:	
Phone number:	666666666
Person being visited(email):	
Reason for visit:	
Guest type:	DAILY
SMS provider:	
State:	Awaiting Initial Login
From date:	08/01/2014 12:58
To date:	08/02/2014 12:58
Location:	
SSID:	
Language:	English
Group tag:	
Time left:	0,23,47

Configuración optativa

Para cada etapa de este flujo, diversas opciones pueden ser configuradas. Todo el esto se configura por el portal del invitado en el **acceso de invitado > la configuración > los portales > PortalName del invitado > edita > las configuraciones porta del comportamiento y del flujo**. Configuraciones más importantes incluyen:

Configuraciones del Uno mismo-registro

- Tipo del invitado - Describe cuánto tiempo la cuenta es activo, las opciones del vencimiento de la contraseña, las horas de inicio de sesión y las opciones (ésta es la mezcla de perfil y de rol de invitado del tiempo de la versión 1.2 ISE)
- Código del registro - Si están habilitados, solamente no prohíben los usuarios que conocen el código secreto el uno mismo-registro (debe proporcionar la contraseña cuando se crea la cuenta)
- AUP - Valide la directiva del uso durante el uno mismo-registro
- El requisito para que el patrocinador apruebe/activa la cuenta de invitado

Configuraciones del invitado del login

- Código de acceso - Si están habilitados, solamente se permite a los Usuarios invitados que conocen el código secreto iniciar sesión
- AUP - Valide la directiva del uso durante el uno mismo-registro
- Opción del cambio de la contraseña

Configuraciones del registro del dispositivo

- Por abandono, el dispositivo se registra automáticamente

Configuraciones de la conformidad del dispositivo del invitado

- Tiene en cuenta una postura dentro del flujo

Configuraciones BYOD

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

Cuentas Patrocinador-aprobadas

Si seleccionan a los **invitados uno mismo-registrados** **Require a ser** opción **aprobada**, después la cuenta creada por el invitado se debe aprobar por un patrocinador. Esta característica pudo utilizar el correo electrónico para entregar la notificación al patrocinador (para la aprobación de la cuenta de invitado):

Si el servidor o el valor por defecto del Simple Mail Transfer Protocol (SMTP) de la notificación del correo electrónico no se configura, después la cuenta no será creada:

Account Created

Use the following information to sign on to the network.

Email send failure

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

Sign On

El registro de guest.log confirma que el global del direccionamiento usado para la notificación falta:

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

Cuando usted tiene la configuración apropiada del correo electrónico, se crea la cuenta:

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for Guest Email Settings. The page has a blue header with the Cisco logo and the text "Identity Services Engine". Navigation links for "Home" and "Operations" are visible. Below the header, there are tabs for "Configure", "Manage Accounts", and "Settings". The "Settings" tab is active. The main content area shows a list of settings with "Guest Email Settings" expanded. The "SMTP server" is set to "outbound.cisco.com". There is a link to "Administration > System > Settings > SMTP". The "Enable email notifications to guests" checkbox is checked. The "Use default email address" radio button is selected, and the "Default email address" field contains "ise_notification@cisco.com". The "Use email address from sponsor" radio button is unselected.

CISCO Identity Services Engine Home Operations

Configure Manage Accounts Settings

▶ **Guest Account Purge Policy** Specify when to delete expired guest accounts

▶ **Custom Fields** Add custom fields that can be used for creating

▼ **Guest Email Settings** Identify the SMTP server and specify the email

SMTP server: outbound.cisco.com

Configure SMTP server at:
[Administration > System > Settings > SMTP](#)

Enable email notifications to guests

Use default email address

Default email address:

Use email address from sponsor

Account Created

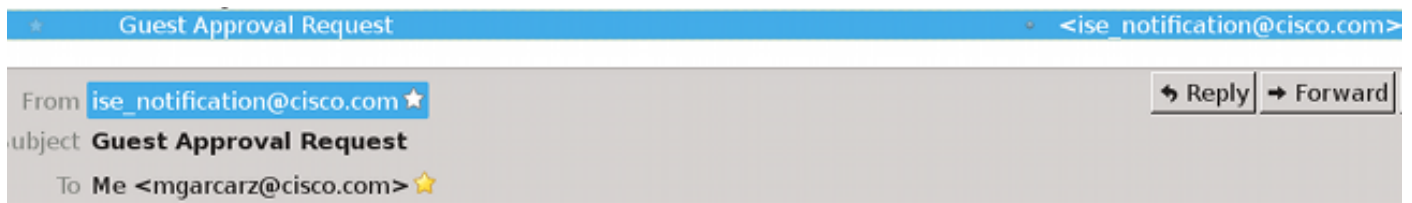
Use the following information to sign on to the network.

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

Sign On

Después de que usted permita a los **invitados uno mismo-registrados** **Require para ser opción aprobada**, los campos del nombre de usuario y contraseña se quitan automáticamente del **incluir esta información sobre la** sección de la **página del éxito del Uno mismo-registro**. Esta es la razón por la cual, cuando la aprobación del patrocinador es necesaria, las credenciales para los Usuarios invitados no se visualizan por abandono en la página web que presenta la información para mostrar que se ha creado la cuenta. En lugar deben ser entregadas por los servicios de mensajería cortos (SMS) o el correo electrónico. Esta opción se debe habilitar en la **notificación credencial del envío sobre la aprobación usando la** sección (marca email/SMS).

Un correo electrónico de notificación se entrega al patrocinador:



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

Los registros del patrocinador en el patrocinador porta y aprueban la cuenta:

CISCO Sponsor Portal Welcome sponsor

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

Approve Deny Refresh

<input type="checkbox"/>	Username	State	First Name	Last Name	Email address	Phone number	Company
<input checked="" type="checkbox"/>	quest7	Pending Approval	michal	garcarz	mgarcarz@cisco.com		

Desde aquí, se permite al Usuario invitado iniciar sesión (con las credenciales recibidas por el correo electrónico o SMS).

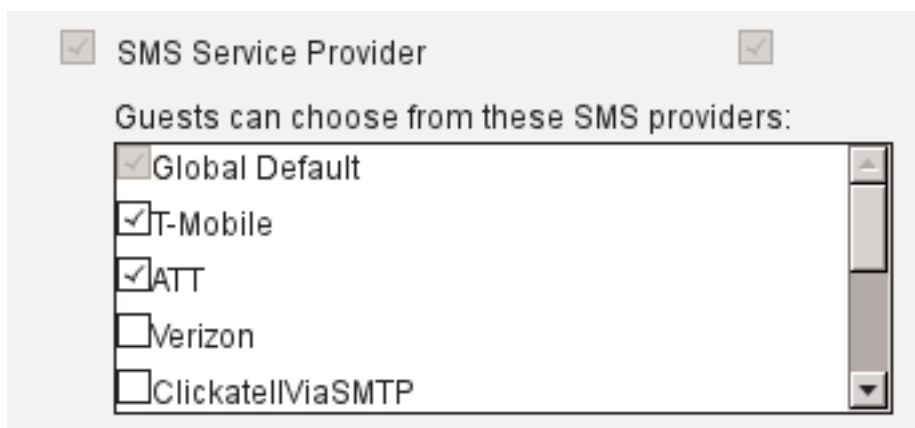
En resumen, hay tres direcciones de correo electrónico usadas en este flujo:

- Notificación "" del direccionamiento. Esto se define estáticamente o se toma de la cuenta del patrocinador y se utiliza como del direccionamiento para ambos: notificación a patrocinar (para la aprobación) y detalles credenciales al invitado. Esto se configura bajo el **acceso de invitado > la configuración > las configuraciones > configuraciones del correo electrónico del invitado**.
- Notificación "" a dirigir. Esto se utiliza para notificar al patrocinador que ha recibido una aprobación del explicar. Esto se configura en el portal del invitado bajo el **acceso de invitado > la configuración > los portales del invitado > los invitados uno mismo-registrados Require porta del name> que se aprobarán > petición de aprobación del correo electrónico a**.
- Invitado "" a dirigir. Esto es proporcionada por el Usuario invitado durante el registro. Si **envíe la notificación credencial sobre la aprobación usando el correo electrónico** se selecciona, el correo electrónico con los detalles credenciales (nombre de usuario y contraseña) se entrega al invitado.

Entregue las credenciales vía SMS

Las credenciales del invitado se pueden también entregar por SMS. Estas opciones deben ser configuradas:

1. Elija el proveedor de servicio de SMS:



2. Marque la **notificación credencial del envío sobre la aprobación usando**: Casilla de verificación de **SMS**.
3. Entonces, piden el Usuario invitado elegir el proveedor disponible cuando él crea una cuenta:

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

Phone number*

666666666

Company

SMS provider*

T-Mobile

T-Mobile

ATT

Global Default

Reason for visit

4. SMS se entrega con el proveedor y el número de teléfono elegidos:

Account Created

Use the following information to sign on to the network.

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

Sign On

5. Usted puede configurar los proveedores de SMS bajo la **administración > el sistema > las configuraciones > el gateway de SMS**.

Registro del dispositivo

Si seleccionan a los **invitados de la permit para registrar la opción de dispositivos** después de que un Usuario invitado abra una sesión y valide el AUP, usted puede registrar los dispositivos:

Device Registration

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

Device ID

Device Description

Manage Devices (1)

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

Note que el dispositivo se ha agregado ya automáticamente (está en la lista de dispositivos Manage). Esto es porque los **dispositivos del invitado del registro** fueron seleccionados automáticamente.

Postura

Si se selecciona la opción de la **conformidad del dispositivo del invitado del requerir**, después los Usuarios invitados son aprovisionado con un agente que realice la postura (agente NAC/Web) después de que inicien sesión y validen el AUP (y realice opcionalmente el registro del dispositivo). El ISE procesa las reglas del aprovisionamiento del cliente para decidir a qué agente debe ser aprovisionado. Después el agente que se ejecuta en la estación realiza la postura (según las reglas de la postura) y envía los resultados al ISE, que envía el CoA reauthenticate para cambiar el estatus de autorización si es necesario.

Las reglas posibles de la autorización pudieron parecer similares a esto:

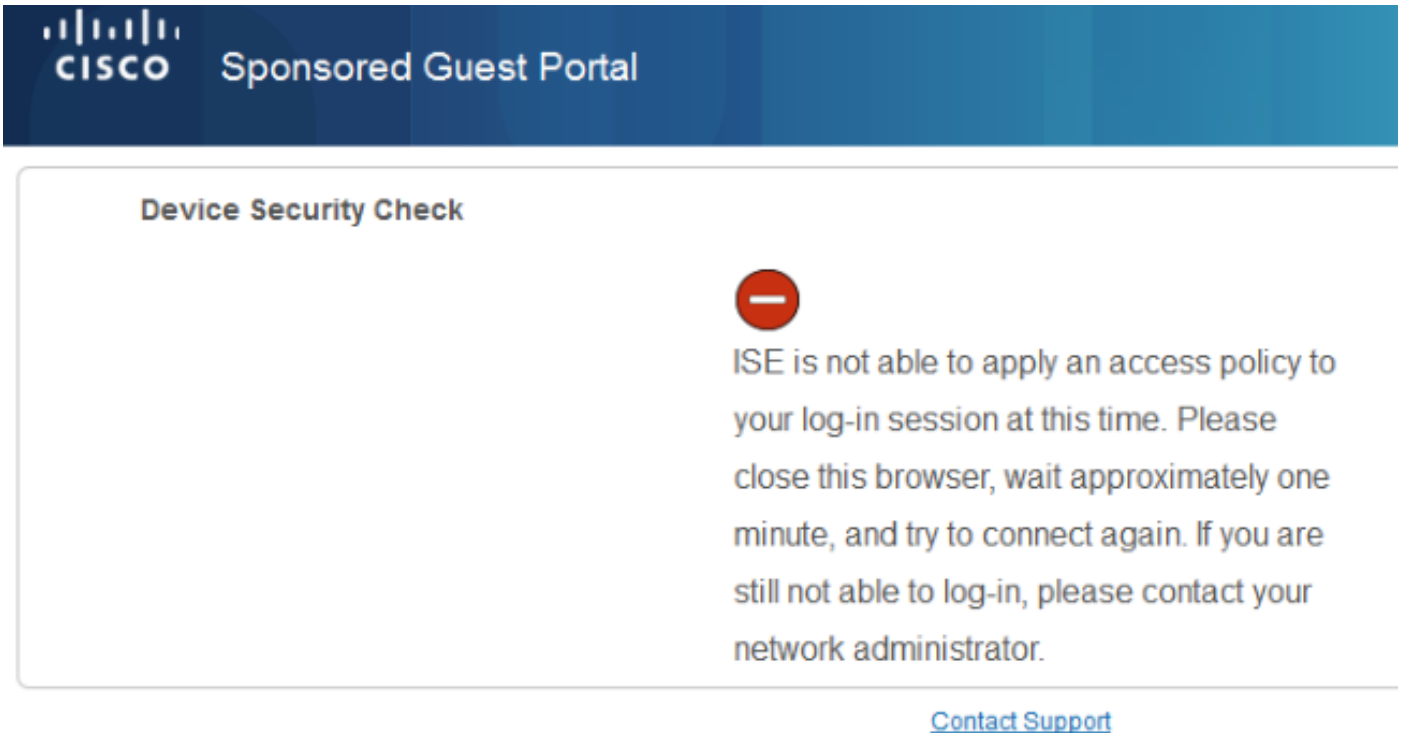
▶ Exceptions (0)

Standard


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

Los primeros usuarios nuevos que encuentran la regla de Guest_Authenticate para reorientar al portal del invitado del registro del uno mismo. Después de que los uno mismo-registros del usuario y abran una sesión, el CoA cambia el estatus de autorización y proporcionan el usuario el acceso limitado para realizar la postura y la corrección. Solamente después que es el agente del NAC el aprovisionado y la estación es obedientes hace el estatus de autorización del cambio CoA de nuevo para proporcionar el acceso a Internet.

Los problemas comunes con la postura incluyen la falta de reglas correctas del aprovisionamiento del cliente:



Device Security Check

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

[Contact Support](#)

Esto puede también ser confirmada si usted examina el archivo de guest.log (nuevo en la versión 1.3 ISE):

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

BYOD

Si seleccionan a los **empleados de la permit para utilizar los dispositivos personales en la opción de red**, después los usuarios corporativos que utilizan este portal pueden pasar con BYOD fluyen y registran los dispositivos personales. Para los Usuarios invitados, esa configuración no cambia cualquier cosa.

¿Qué los “empleados que usan el portal como invitado” significan?

Por abandono, los portales del invitado se configuran con el almacén de la identidad de **Guest_Portal_Sequence**:

▼ Portal Settings

HTTPS port: * (8000 - 8999)

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

Certificate Group Tag: *

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

Identity source sequence: *

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

Ésta es la secuencia interna del almacén que intenta a los usuarios internos primero (antes de los Usuarios invitados):

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below it, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. Under 'Identity Management', there are sub-tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The main content area is titled 'Identity Source Sequences List > Guest_Portal_Sequence' and 'Identity Source Sequence'. It shows the configuration for the 'Guest_Portal_Sequence' identity source sequence. The 'Name' field is 'Guest_Portal_Sequence' and the 'Description' is 'A built-in Identity Sequence for the Guest Portal'. There is a section for 'Certificate Based Authentication' with a checkbox for 'Select Certificate Authentication Profile' and a dropdown menu. Below that is the 'Authentication Search List' section, which contains two columns: 'Available' and 'Selected'. The 'Available' column lists 'Internal Endpoints' and 'AD1'. The 'Selected' column lists 'Internal Users', 'Guest Users', and 'All_AD_Instances'. There are arrows between the columns to move items back and forth.

Cuando en esta etapa en el portal del invitado, el usuario proporciona las credenciales que se definen en los usuarios internos salvan y el cambio de dirección BYOD ocurre:

1

2

3

4

BYOD Welcome

Welcome to the BYOD portal.

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

Start

I want guest access only

Los usuarios corporativos de esta manera pueden realizar BYOD para los dispositivos personales.

Cuando en vez de las credenciales de los usuarios internos, se proporcionan se continúan las credenciales de los Usuarios invitados, flujo normal (ningún BYOD).

Cambio de VLAN

Esto es una opción similar al cambio de VLAN configurado para el portal del invitado en la versión 1.2 ISE. Permite que usted ejecute activeX o los subprogramas java, que acciona el DHCP para liberar y para renovar. Esto es necesario cuando el CoA acciona el cambio del VLA N para el punto final. Cuando se utiliza el MAB, el punto final no es consciente de un cambio del VLA N. Una Solución posible es cambiar el VLA N (la versión del DHCP/renueva) con el agente del NAC. Otra opción es pedir una nueva dirección IP vía el applet vuelto en la página web. Un retardo entre la versión/CoA/renueva puede ser configurado. Esta opción no se soporta para los dispositivos móviles.

Información Relacionada

- [Servicios de la postura en la guía de configuración de Cisco ISE](#)
- [Tecnología inalámbrica BYOD con el Identity Services Engine](#)
- [Soporte ISE SCEP para el ejemplo de configuración BYOD](#)
- [Guía de administradores de Cisco ISE 1.3](#)
- [Autenticación Web central en el ejemplo de configuración del WLC y ISE](#)
- [Autenticación Web central con FlexConnect AP en un WLC con el ejemplo de configuración ISE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)