Solución de problemas comunes de acceso de invitado ISE

Contenido

Introducción

Este documento describe cómo resolver problemas comunes de invitados en la implementación, cómo aislar y verificar el problema y soluciones alternativas sencillas para intentar.

Requisito previo

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- configuración de invitado ISE
- Configuración de CoA en dispositivos de acceso a la red (NAD)
- Se requieren herramientas de captura en las estaciones de trabajo.

Componentes Utilizados

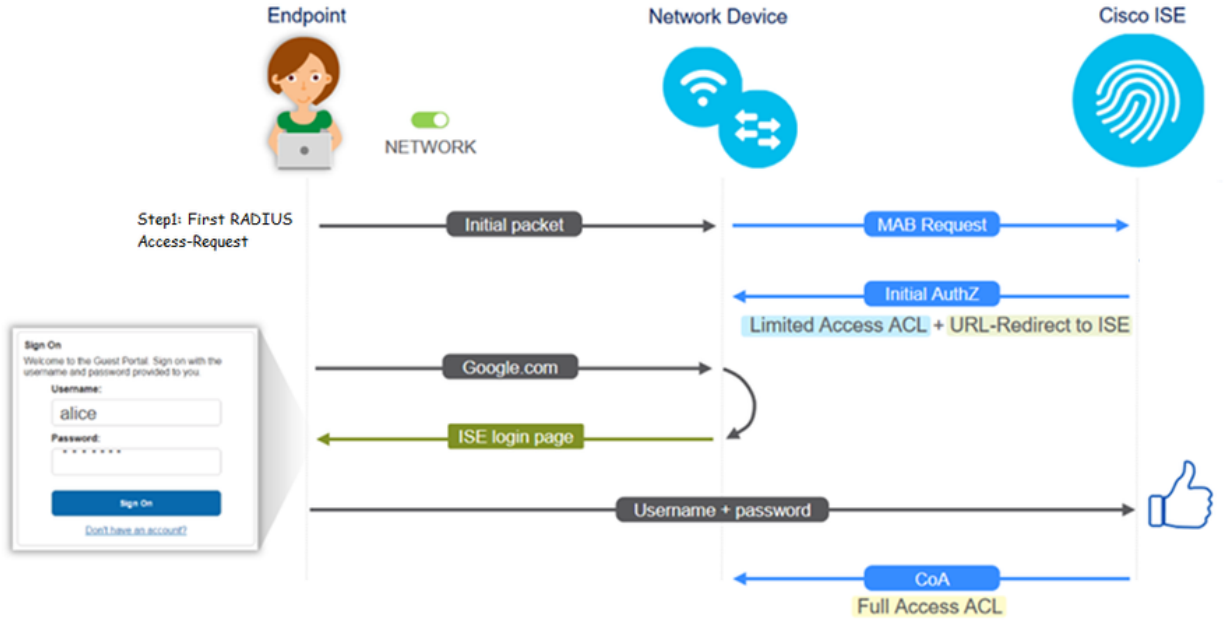
La información de este documento se basa en Cisco ISE, versión 2.6 y:

- WLC 5500
- Catalyst switch 3850 versión 15.x
- estación de trabajo Windows 10

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.

Flujo de invitados

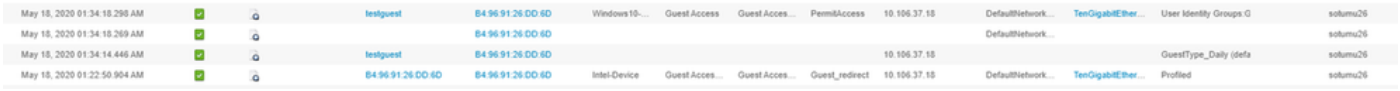
La descripción general del flujo de invitados es similar a las configuraciones por cable o inalámbricas. Esta imagen del diagrama de flujo se puede utilizar como referencia en todo el documento. Ayuda a visualizar el paso y la entidad.



El flujo también se puede seguir en los registros en directo de ISE [**Operations > RADIUS Live Logs**] filtrando el ID del terminal:

- Autenticación MAB correcta- el campo de nombre de usuario tiene la dirección MAC- La URL se envía al NAD - El usuario obtiene el portal
- Autenticación de invitado correcta: el campo de nombre de usuario tiene el nombre de usuario de invitado, se ha identificado como GuestType_Daily (o el tipo configurado para el usuario invitado)
- Iniciado por CoA - el campo de nombre de usuario está en blanco, el informe detallado muestra autorización dinámica correcta
- Acceso de invitado proporcionado

Secuencia de eventos de la imagen (de abajo arriba)



Guías de implementación comunes

Estos son algunos enlaces para obtener ayuda sobre la configuración. Para cualquier solución de problemas de casos prácticos específicos, ayuda conocer la configuración ideal o esperada.

- Configuración de invitado por cable
- Configuración de invitado inalámbrico
- CWA de invitado inalámbrico con AP FlexAuth

Problemas encontrados frecuentemente

Este documento aborda principalmente estos problemas:

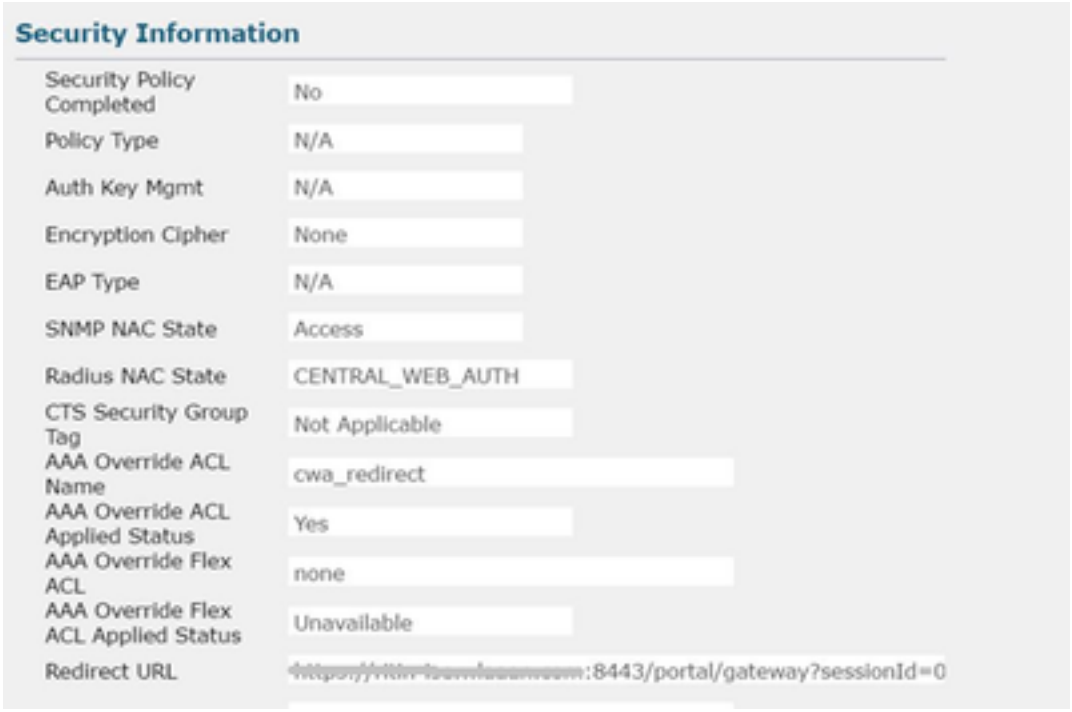
La redirección al portal de invitados no funciona

Una vez que la URL de redirección y la ACL se envíen desde ISE, verifique lo siguiente:

1. El estado del cliente en el switch (si tiene acceso de invitado por cable) con el comando **show authentication session int <interface> details**:

```
guestlab#sh auth sess int T1/0/48 de
            Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
    URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

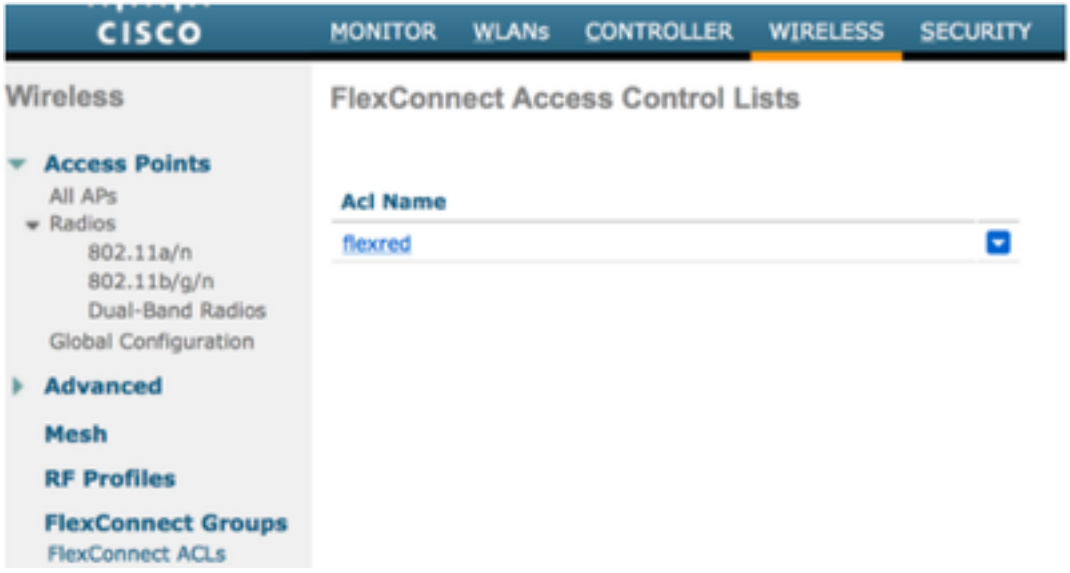
2. El estado del cliente en el controlador del Wireless LAN (si el acceso del invitado inalámbrico): **Monitor > Client > MAC address**



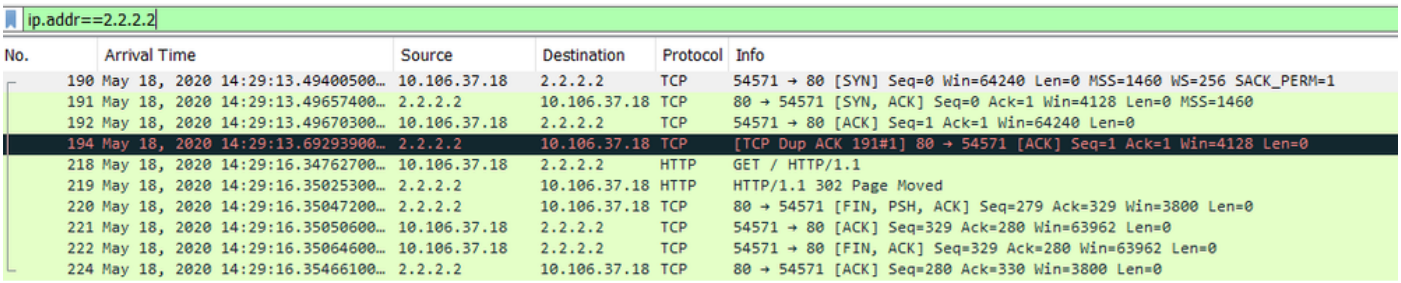
3. El alcance desde el terminal al ISE en el puerto TCP 8443 con la ayuda del símbolo del sistema: **C:\Users\user>telnet <ISE-IP> 8443**

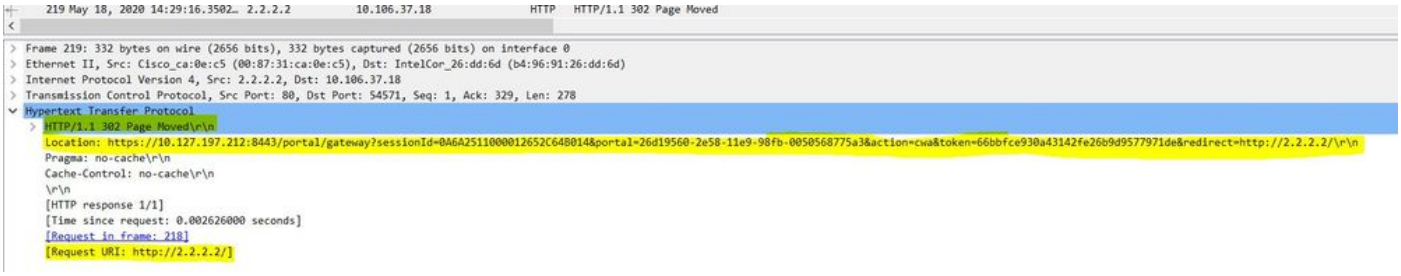
4. Si la URL de redirección del portal tiene un FQDN, verifique si el cliente puede resolver desde el símbolo del sistema: **C:\Users\user>nslookup guest.ise.com**

5. En la configuración de flex connect, asegúrese de que el mismo nombre de ACL esté configurado en ACL y ACL flexibles. Además, verifique si la ACL está asignada a los AP. Consulte la guía de configuración de la sección anterior, Pasos 7 b y c, para obtener más información.



6. Tome una captura de paquetes del cliente y verifique la redirección. El paquete HTTP/1.1 302 Page Moved se utiliza para indicar que el WLC/Switch redirigió el sitio al que se accedió al portal de invitados de ISE (URL redirigida):





7. El motor HTTP(s) está activado en los dispositivos de acceso a la red:

En el switch:

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

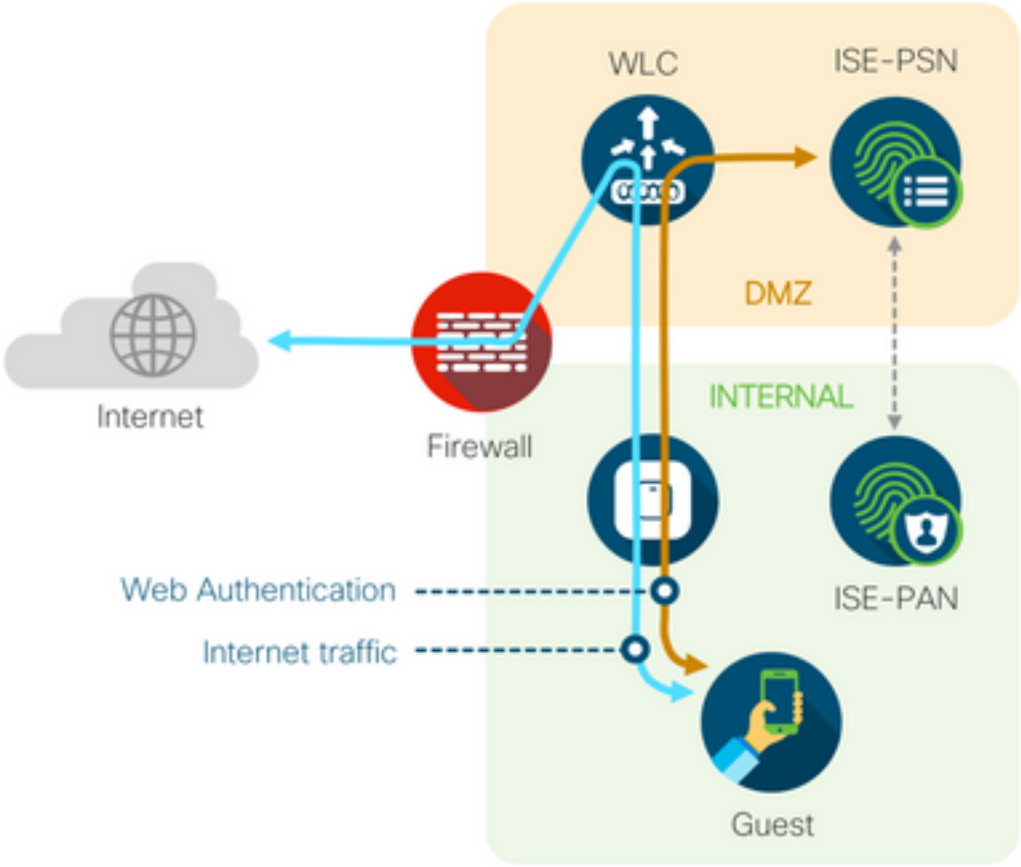
En el WLC:

8. Si el WLC está en una configuración de anclaje externo, verifique esto:

Paso 1. El estado del cliente debe ser el mismo en ambos WLC.

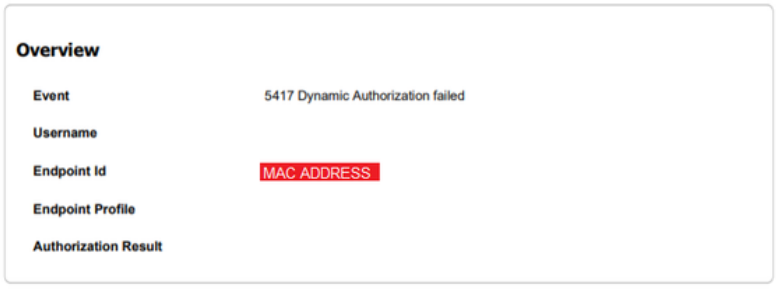
Paso 2. La URL de redireccionamiento debe ser vista en ambos WLC.

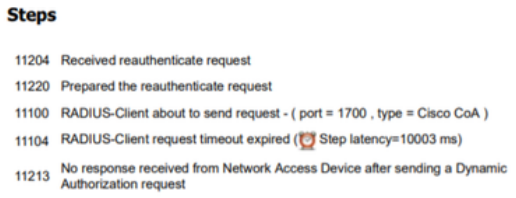
Paso 3. La Contabilización RADIUS debe estar inhabilitada en el WLC de anclaje.



La autorización dinámica falla

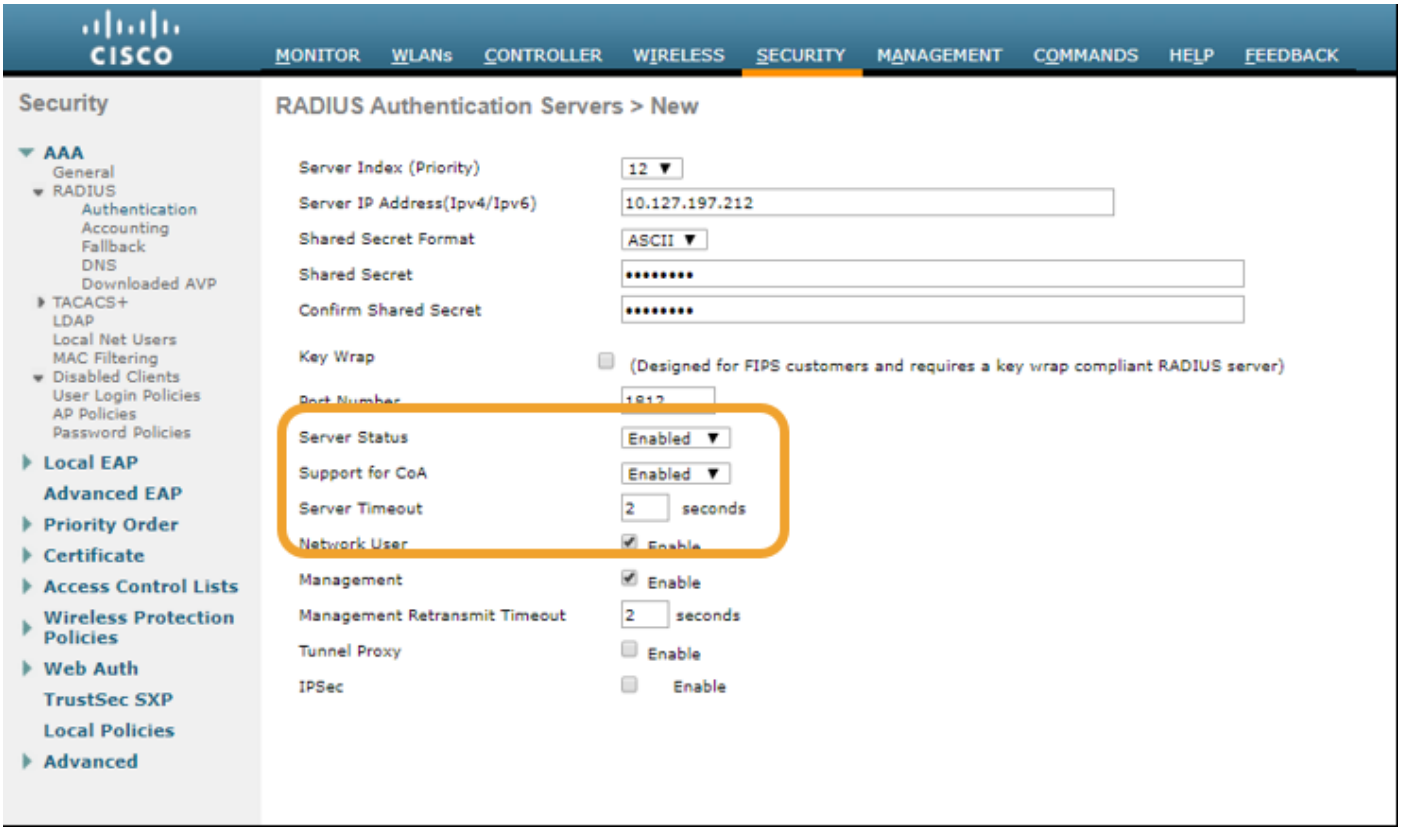
Si el usuario final es capaz de acceder al portal de invitados e iniciar sesión correctamente, el siguiente paso sería un cambio de autorización para proporcionar acceso de invitado completo al usuario. Si esto no funciona, observará un error de autorización dinámica en los registros en directo de ISE Radius. Para solucionar el problema, compruebe lo siguiente:





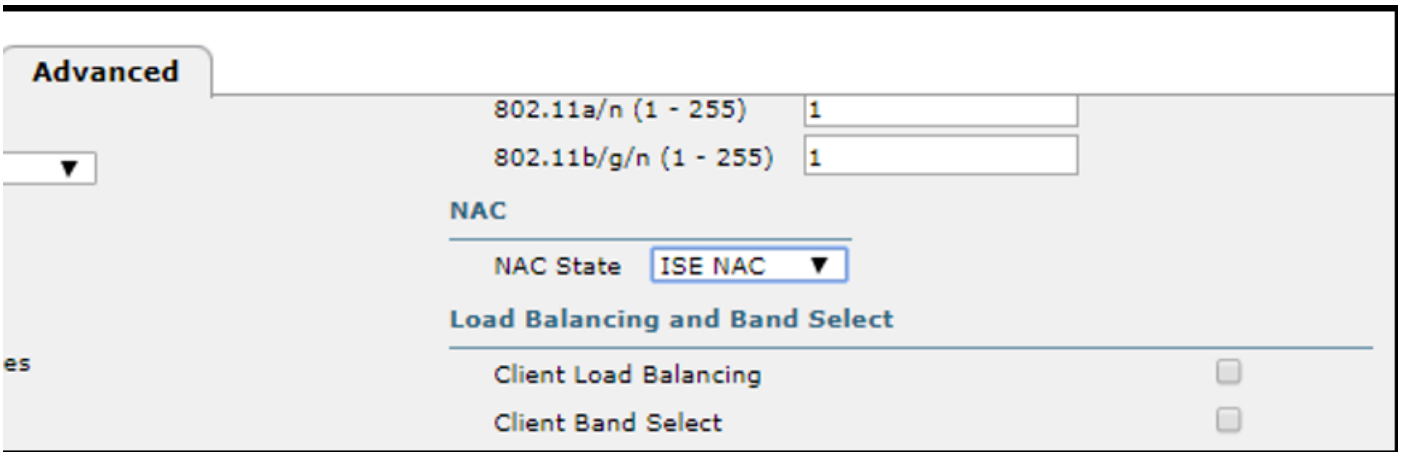
1. El cambio de autorización (CoA) debe estar habilitado/configurado en el NAD:

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
```



2. El puerto UDP 1700 debe estar permitido en el firewall.

3. El estado NAC en el WLC es incorrecto. En Advanced settings on **WLC GUI > WLAN** cambie el estado de NAC a ISE NAC.

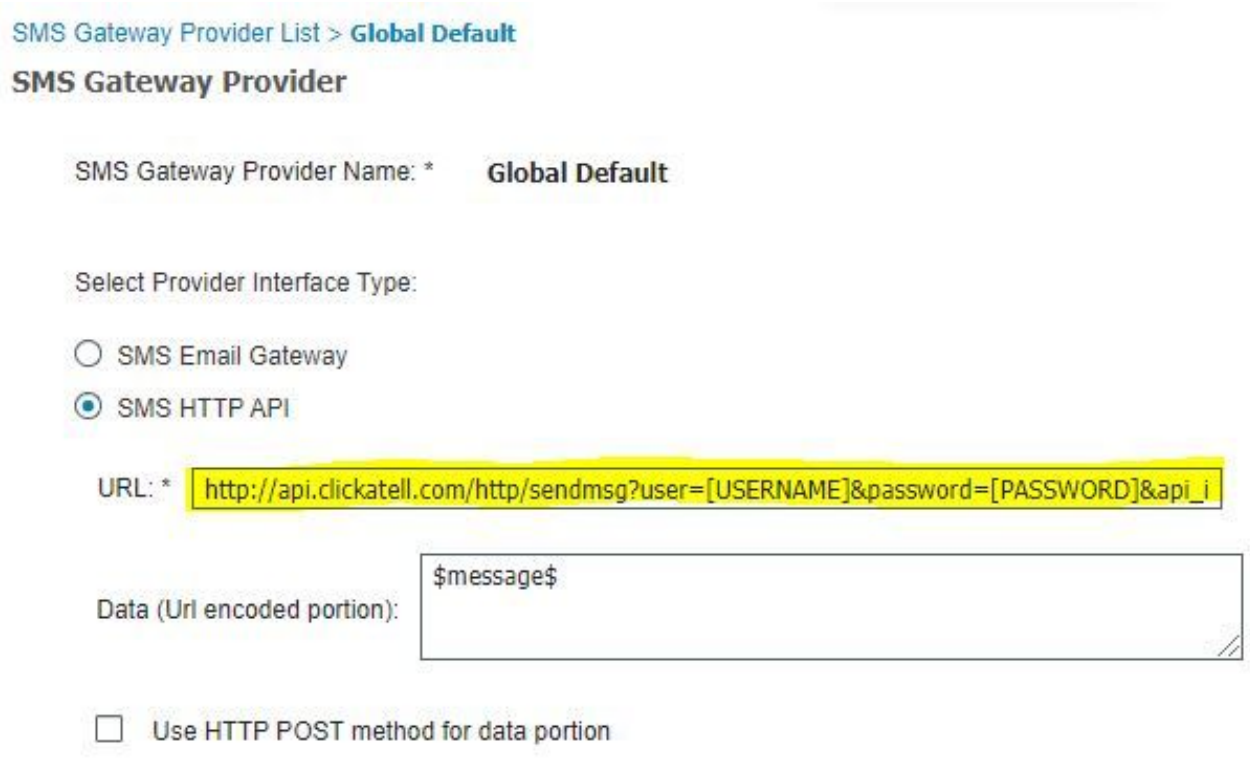


No se envían notificaciones por SMS/CORREO ELECTRÓNICO

1. Verifique la configuración SMTP en **Administration > System > Settings > SMTP**.

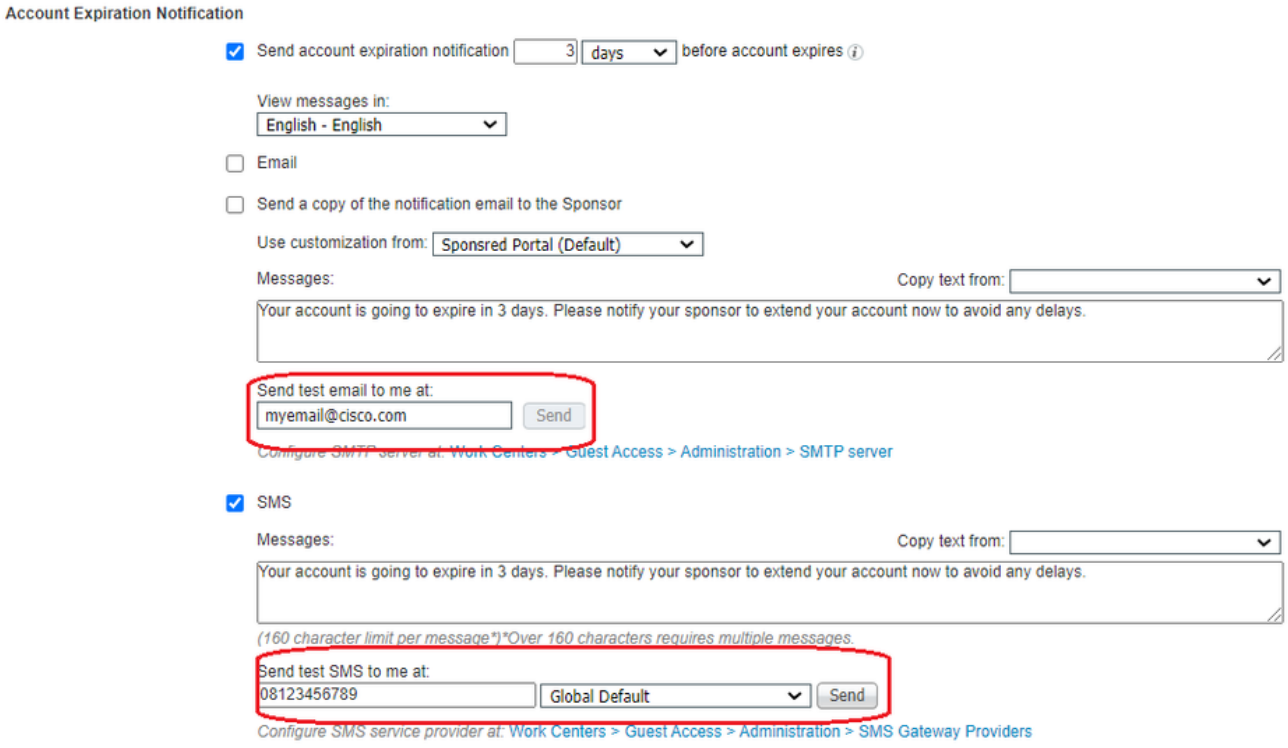
2. Compruebe la API para gateways de SMS/correo electrónico fuera de ISE:

Pruebe las URL proporcionadas por el proveedor en un cliente de API o un navegador, sustituya las variables como nombres de usuario, contraseñas, número de móvil y pruebe el alcance. [**Administration > System > Settings > SMS Gateways**]



Como alternativa, si realiza la prueba desde los grupos patrocinadores de ISE [**Workcenters > Guest Access > Portals and Components > Guest Types**], realice una captura de paquetes en ISE y el gateway SMS/SMTP para comprobar si

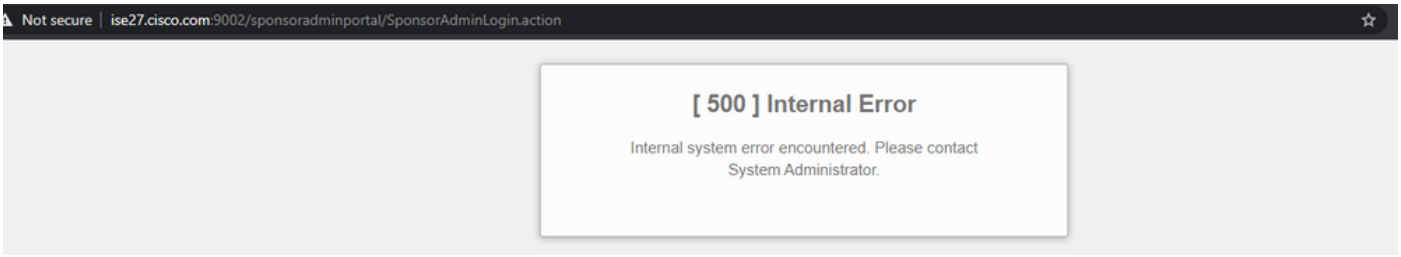
1. El paquete de solicitud llega al servidor sin alteraciones.
2. El servidor ISE tiene los permisos/privilegios recomendados por el proveedor para que la puerta de enlace procese esta solicitud.



No se puede acceder a la página Administrar cuentas

1. En el botón **Workcenters > Guest Access > Manage accounts** se redirige al FQDN de ISE en el

puerto 9002, para que el administrador de ISE acceda al portal del patrocinador:



2. Compruebe si el FQDN lo resuelve la estación de trabajo desde la que se accede al Portal del patrocinador con el comando **nslookup <FQDN de ISE PAN>**.

3. Verifique si el puerto TCP 9002 de ISE está abierto desde la CLI de ISE con el comando **show ports | incluye 9002**.

Prácticas recomendadas de certificados de portal

- Para que la experiencia del usuario sea perfecta, el certificado utilizado para los portales y los roles de administrador debe estar firmado por autoridades de certificados públicas conocidas (por ejemplo: GoDaddy, DigiCert, VeriSign, etc.), de las que suelen confiar los navegadores (por ejemplo: Google Chrome, Firefox, etc.).

- No se recomienda utilizar IP estática para la redirección de invitados, ya que esto hace que la IP privada de ISE sea visible para todos los usuarios. La mayoría de los proveedores no proporcionan certificados firmados por terceros para IP privada.

- Cuando se pasa de ISE 2.4 p6 a p8 o p9, existe un error conocido: ID de error de Cisco CSCvp75207, donde las casillas **Trust for authentication inside ISE** y **Trust for client authentication and Syslog** deben marcarse manualmente después de la actualización del parche. Esto garantiza que ISE envíe la cadena de certificados completa para el flujo TLS cuando se accede al portal de invitados.

Si estas acciones no resuelven los problemas de acceso de invitados, póngase en contacto con el TAC con un paquete de asistencia recopilado con instrucciones del documento: Depuraciones para habilitar en ISE.

Información Relacionada

- Asistencia técnica y descargas de Cisco

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).