Guía de operaciones de Cisco IQ Link v1.2.0

Introducción

Cisco IQ™ le ofrece mejoras y funciones diseñadas para mejorar la visibilidad de los recursos, ofrecer una perspectiva más inteligente de sus entornos y simplificar la gestión de casos. Además, las funciones de inteligencia artificial, como el asistente de inteligencia artificial, optimizan los resultados operativos y la experiencia del usuario de Cisco IQ al proporcionar una comprensión contextual que le permite tomar decisiones proactivas e informadas y agilizar los procesos para lograr el compromiso y el éxito de los clientes.

Cisco IQ Link recopila y transmite de forma segura la telemetría de recursos de su red en las instalaciones a Cisco IQ, lo que permite obtener información predictiva basada en IA que le ayuda a mejorar la visibilidad de la red, anticipar problemas e impulsar la eficacia operativa.

Autenticación local

Los administradores de cuentas deben utilizar las siguientes credenciales para iniciar sesión en Cisco IQ Link:

- Nombre de usuario predeterminado: admin
- Contraseña predeterminada: contraseña que se establece durante el proceso de instalación de Cisco IQ Link; Consulte la Guía de inicio de Cisco IQ Link para obtener más información
- Contexto de cuenta predeterminado: Cliente predeterminado

Al iniciar sesión, el usuario predeterminado, "admin", y el nombre de cuenta, "Default-Customer", se muestran en la página de inicio.

Configuración de la seguridad del administrador local

Puede cambiar su contraseña y configurar preguntas de seguridad mediante el menú Perfil del usuario en la página de inicio.

Configuración de bloqueo

Se pueden configurar los siguientes ajustes de bloqueo de cuentas durante la implementación:

- Estado de bloqueo: habilita o deshabilita la función de bloqueo de cuentas.
- Número máximo de intentos de inicio de sesión: establece el número máximo de intentos fallidos consecutivos permitidos antes de que se bloquee una cuenta (valor predeterminado: 3; Rango: 0-10).
- Ventana Tiempo de Acumulación: Define el período de tiempo para realizar un seguimiento de los intentos fallidos (Valor por Defecto: 15 minutos; Rango: 0-60 minutos).
- Duración: establece la duración durante la que una cuenta permanece bloqueada después de alcanzar el número máximo de intentos (valor predeterminado: 30 minutos; Rango: 0-60 minutos).

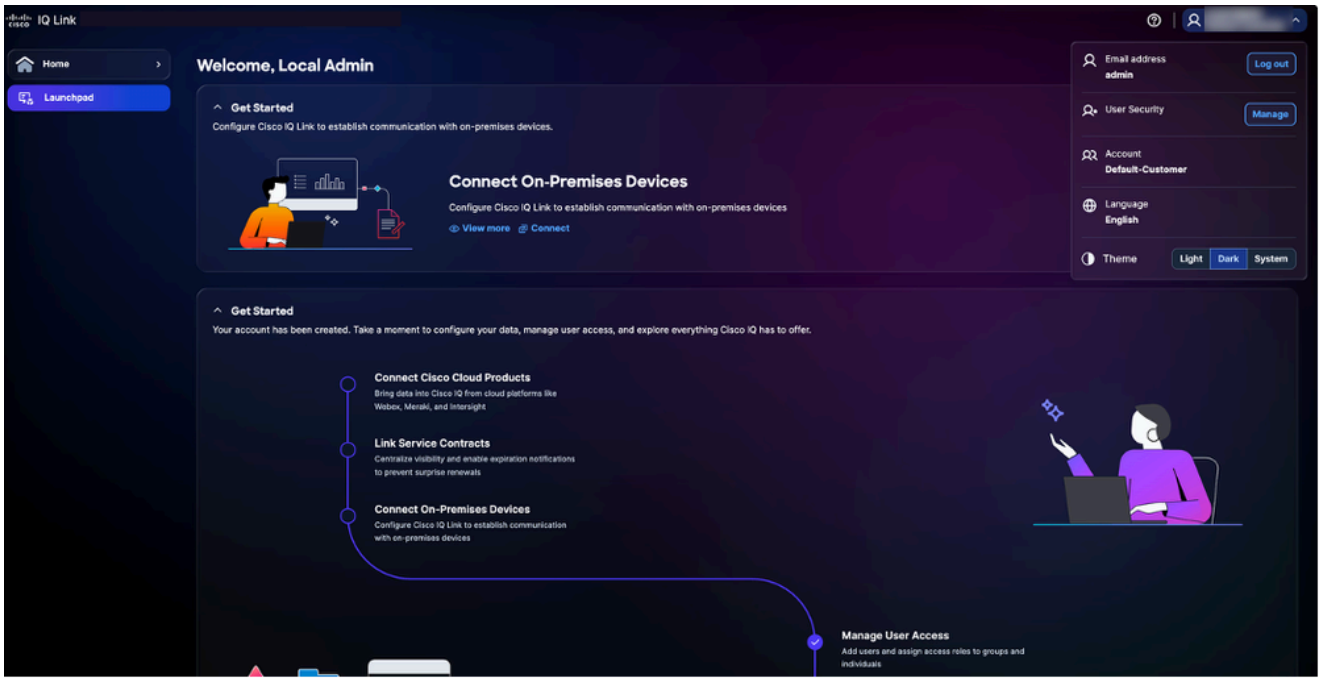
Nota: Tiene tres (3) intentos para introducir la contraseña correcta en un período de 15 minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 30 minutos para proteger su seguridad.
No puede intentar iniciar sesión durante el período de bloqueo. El sistema muestra el mensaje: "Cuenta bloqueada debido a demasiados intentos fallidos. Inténtelo de nuevo más tarde", incluida la hora a la que caduca el bloqueo.
La cuenta se desbloquea automáticamente transcurridos 30 minutos, momento en el que puede intentar iniciar sesión o restablecer la contraseña.

Configuración de preguntas y respuestas de seguridad

Las preguntas de seguridad ayudan a verificar su identidad si olvida su contraseña. Los administradores de cuentas deben configurar respuestas a cinco (5) preguntas de seguridad para habilitar la función de restablecimiento de contraseña. Esta es una configuración única.

Para configurar preguntas de seguridad:

1. En la página de inicio, haga clic en el icono Perfil del usuario. Se abre el menú desplegable.

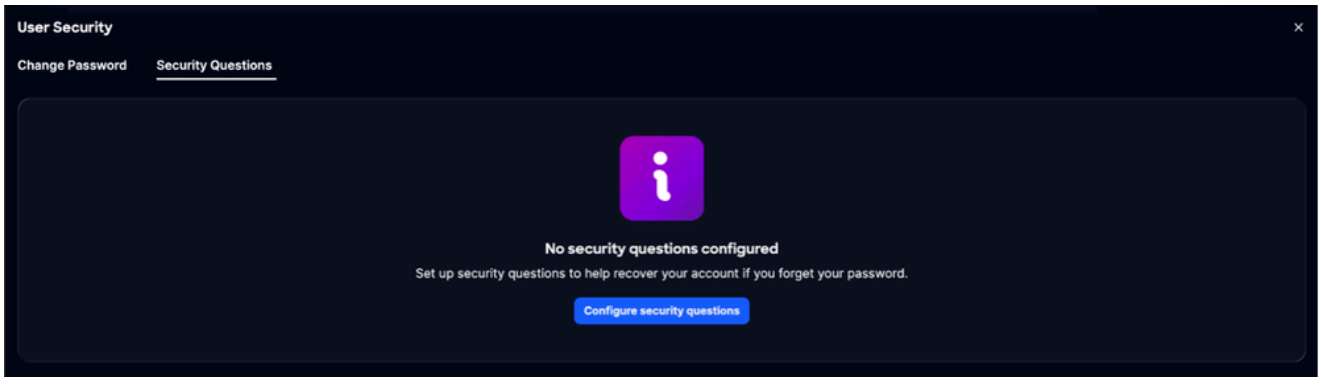


Menú Perfil de usuario

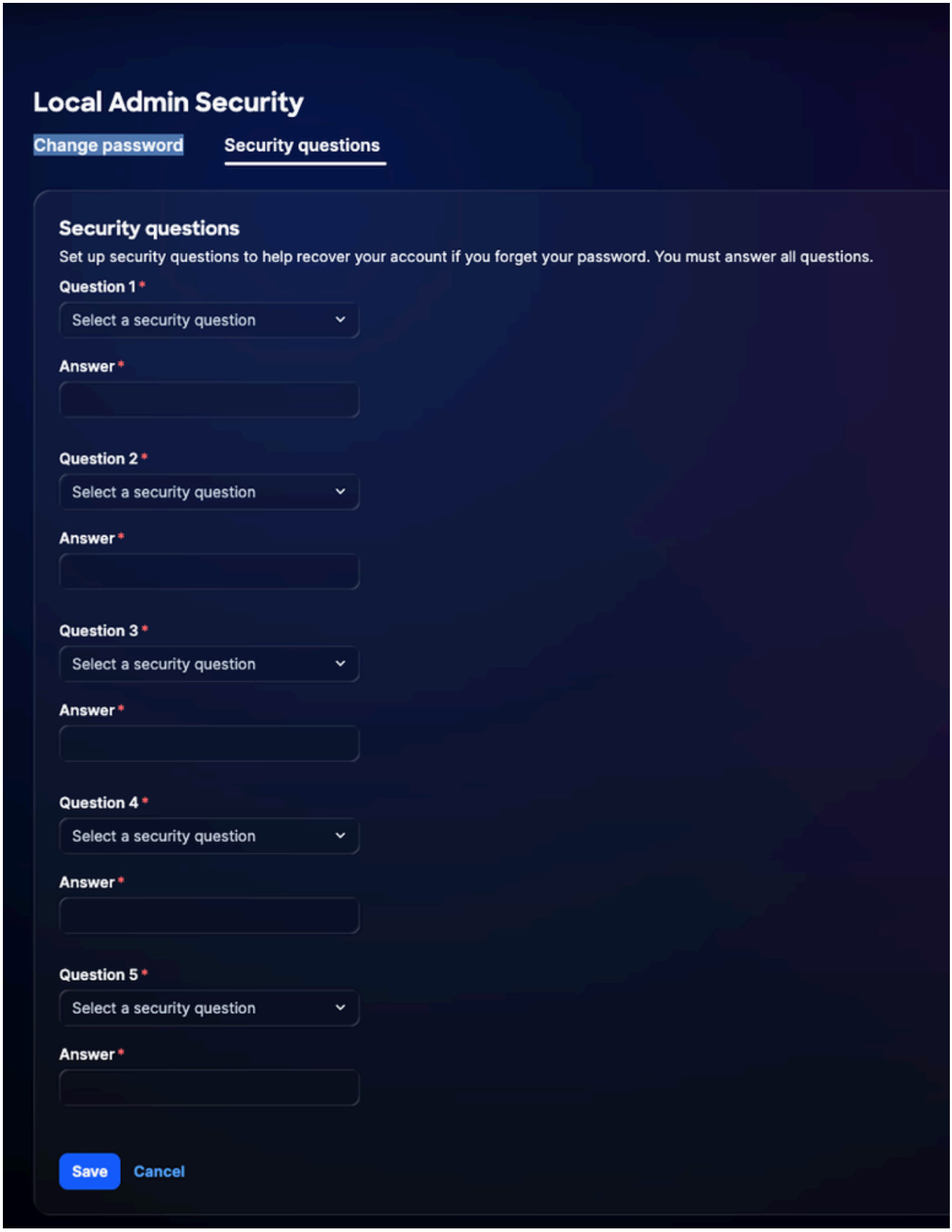
2. Haga clic en Administrar en Seguridad del usuario. Se muestra la página User Security.

Cambiar contraseña

3. Haga clic en Preguntas de seguridad para abrir la ficha.



4. Haga clic en Configurar preguntas de seguridad.



5. Elija cinco (5) preguntas de seguridad cualesquiera de las listas desplegables.
6. Introduzca la respuesta para cada pregunta.
7. Click Save.

Nota: Las respuestas no distinguen entre mayúsculas y minúsculas; por ejemplo, "SMITH" y "smith" se consideran iguales.
Se omiten los espacios adicionales; por ejemplo, " Smith" y "smith" se consideran iguales.

Nota: Si es necesario, puede actualizar las respuestas más adelante. Al actualizar las respuestas, se sustituyen todas las respuestas anteriores, por lo que debe volver a proporcionar las respuestas a las cinco (5) preguntas y no solo a las que desea cambiar.

Administración de contraseñas

Los administradores de cuentas y los usuarios locales pueden administrar las contraseñas de Cisco IQ.

Para garantizar la seguridad de su cuenta, se aplican las siguientes políticas de contraseñas:

- Restricción de reutilización: Su nueva contraseña no puede coincidir con ninguna de las cinco (5) contraseñas anteriores. Esta política se aplica a los flujos Suscripción, Contraseña olvidada y Cambiar contraseña.
- Variación de caracteres: al cambiar la contraseña mientras está autenticado, la contraseña nueva debe tener al menos ocho (8) caracteres diferentes de la contraseña actual.
- Intervalo mínimo de cambio: de forma predeterminada, debe esperar 24 horas antes de volver a cambiar la contraseña. Si se configura un intervalo diferente, no podrá actualizar la contraseña hasta que haya transcurrido ese tiempo.
- Vencimiento de contraseña: Las contraseñas caducan cada 60 días. La primera vez que inicie sesión después de la fecha de vencimiento, se le pedirá que establezca una nueva contraseña antes de poder acceder al sistema. (Si se configura en 0, la caducidad de la contraseña está deshabilitada.)

Prerequisites

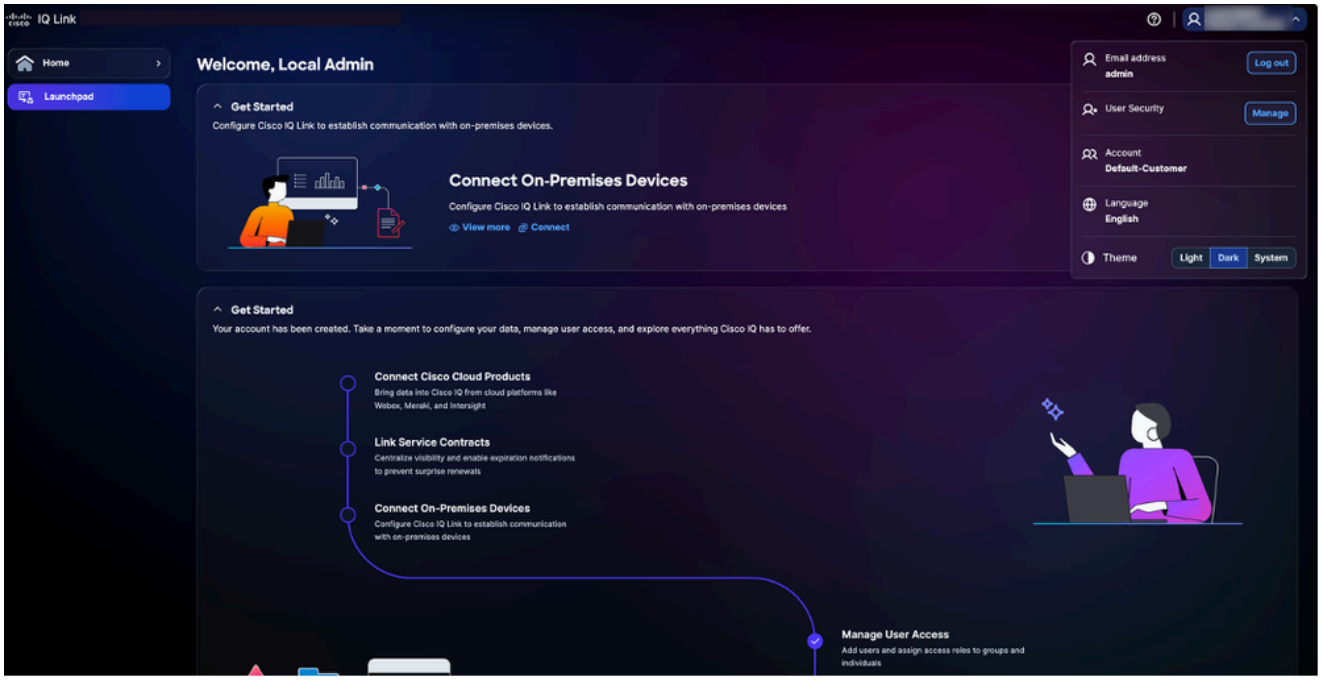
Para administrar contraseñas, se deben cumplir las siguientes condiciones:

- Es un usuario o administrador de cuenta local
- Está utilizando una cuenta local (no un inicio de sesión único (SSO) ni autenticación externa)
- Ha iniciado sesión en Cisco IQ Link
- Conoce la contraseña actual

Cambio de contraseñas

Para cambiar una contraseña:

1. En la página de inicio, haga clic en el icono Perfil del usuario. Se abre el menú desplegable.



Menú Perfil de usuario

2. Haga clic en Administrar en Seguridad del usuario. Se muestra la página User Security.

Cambiar contraseña

3. Introduzca la contraseña actual.
4. Introduzca la nueva contraseña.
5. Vuelva a introducir la nueva contraseña para confirmarla.
6. Click Save.

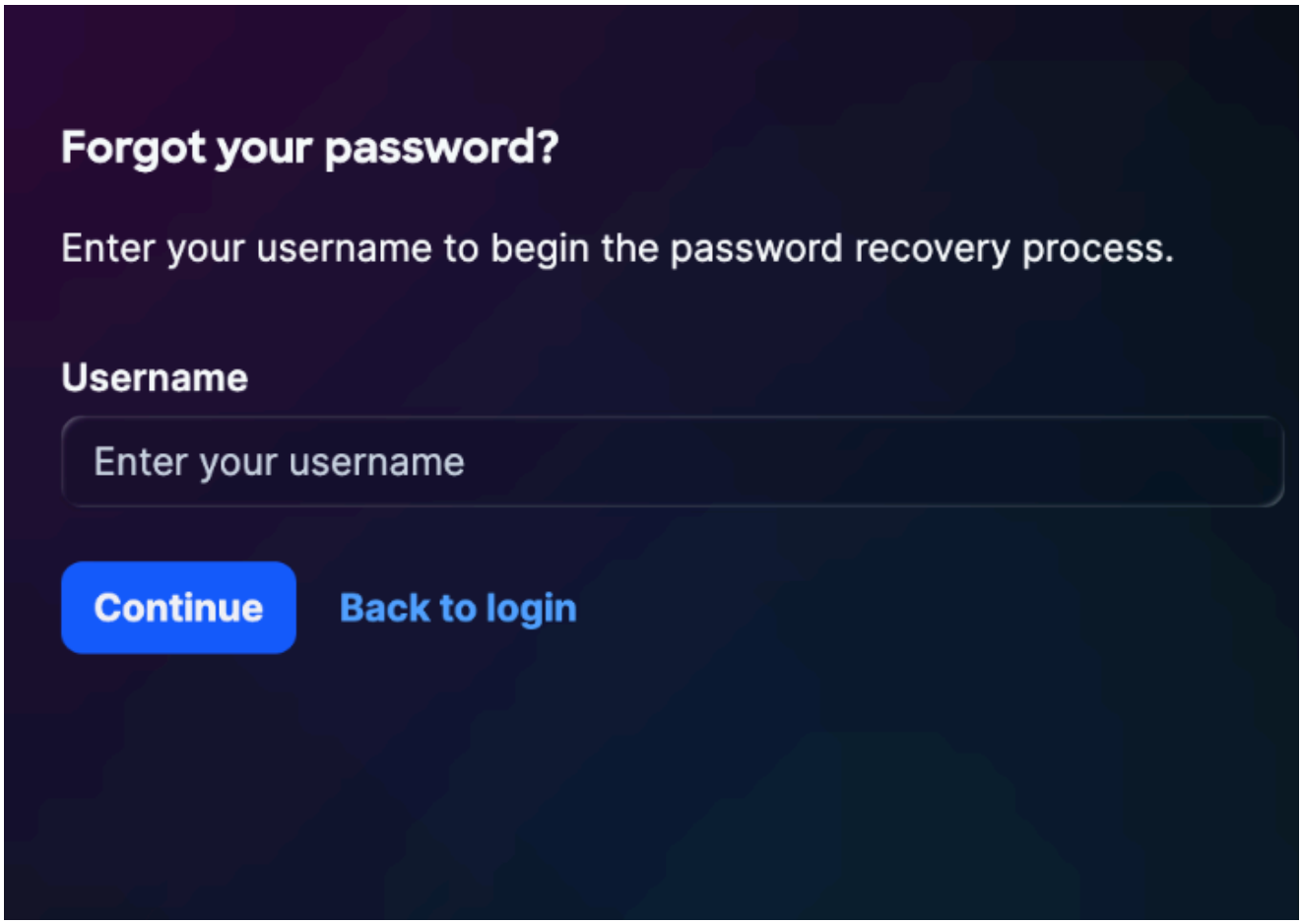
La contraseña se actualiza en el sistema Cisco IQ, incluida la máquina virtual (VM) de Cisco IQ.

Restablecimiento de una Contraseña Olvidada

Puede restablecer una contraseña olvidada mediante el proceso de verificación de preguntas de seguridad, si ha configurado las preguntas de seguridad anteriormente. Consulte Configuración de preguntas y respuestas de seguridad para obtener más información.

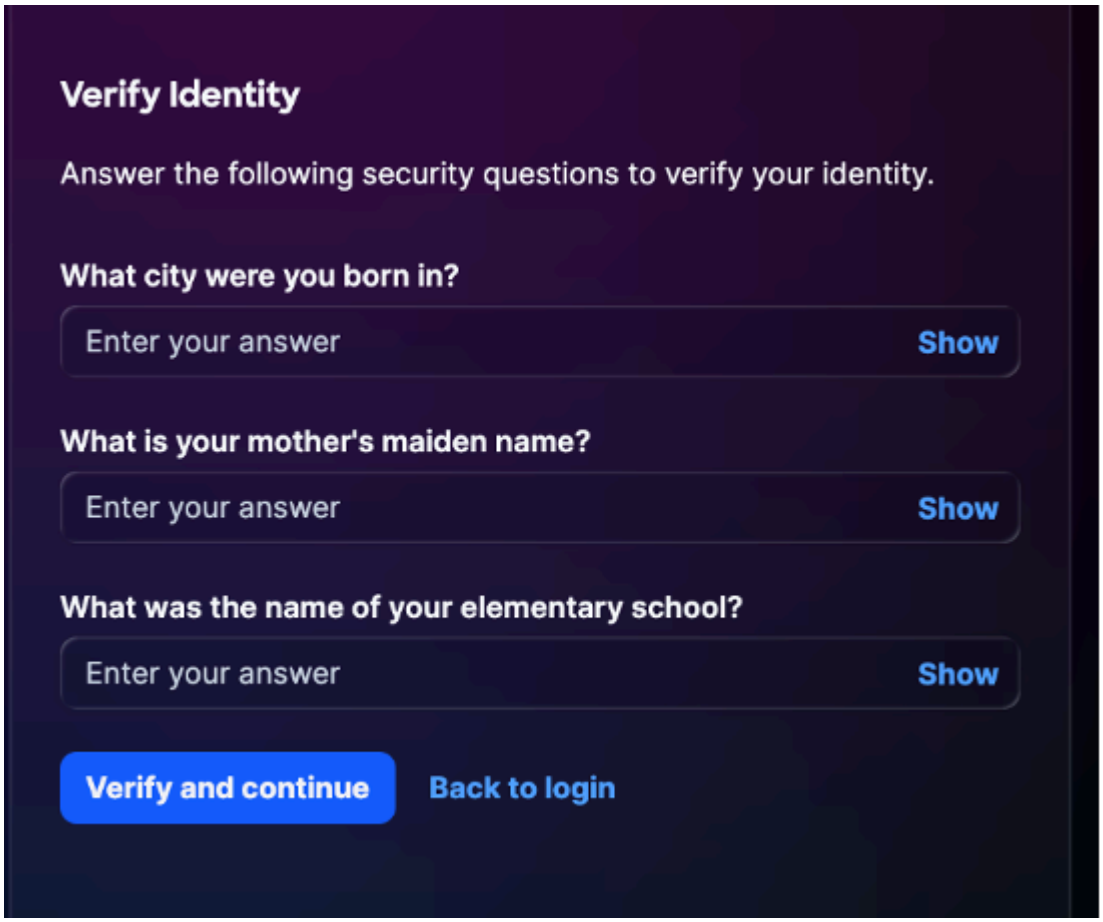
Para restablecer una contraseña olvidada:

1. Vaya a la página de inicio de sesión de Cisco IQ Link.
2. Haga clic en Olvidó su contraseña.



Contraseña olvidada

3. Introduzca el nombre de usuario.
4. Haga clic en Continue (Continuar). La página Verificar identidad muestra tres (3) preguntas de seguridad aleatorias de las cinco (5) preguntas configuradas anteriormente.



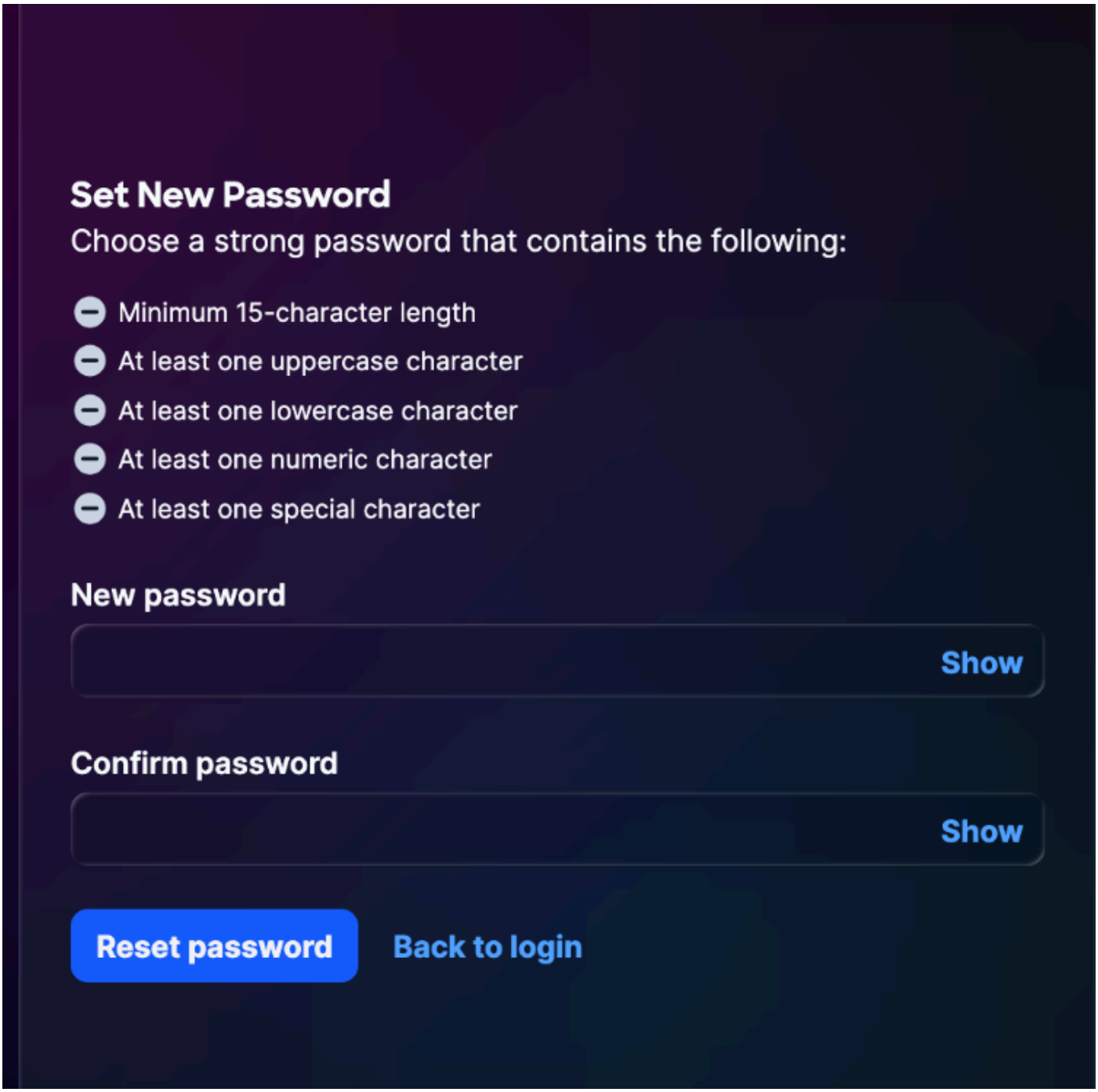
Verificar identidad

Nota: Las preguntas de seguridad mostradas arriba son específicas del usuario y variarán en consecuencia.

---

5. Introduzca las respuestas de las tres (3) preguntas mostradas.

6. Haga clic en Verificar y continúe. Si la respuesta enviada coincide con las respuestas guardadas anteriormente, se le solicitará que introduzca una nueva contraseña.



Restablecer contraseña

Tiene tres (3) intentos de responder correctamente a las preguntas de seguridad en un período de 15 minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 30 minutos para proteger su seguridad. No puede restablecer la contraseña durante el período de bloqueo.
El sistema muestra el mensaje: "Cuenta bloqueada debido a demasiados intentos de verificación fallidos. Inténtelo de nuevo más tarde", incluida la hora a la que caduca el bloqueo.
La cuenta se desbloquea automáticamente transcurridos 30 minutos, momento en el que puede intentar iniciar sesión o restablecer la contraseña.

7. Introduzca la nueva contraseña.

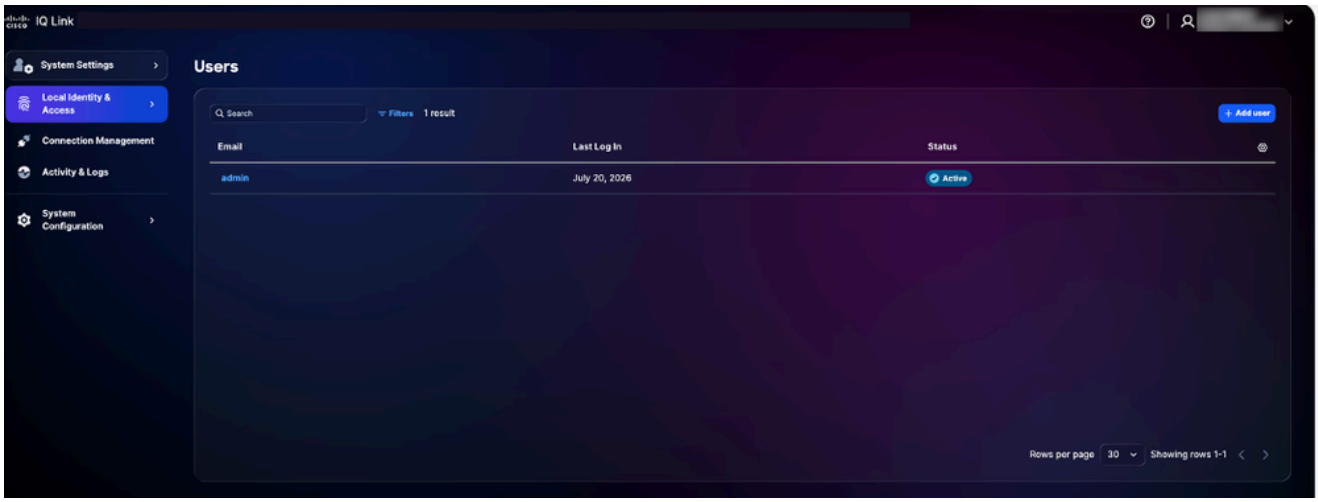
8. Vuelva a introducir la contraseña para confirmarla.

9. Haga clic en Enviar.

Adición de usuarios locales

Los administradores de cuentas pueden agregar usuarios a la cuenta de Cisco IQ. Para agregar un nuevo usuario:

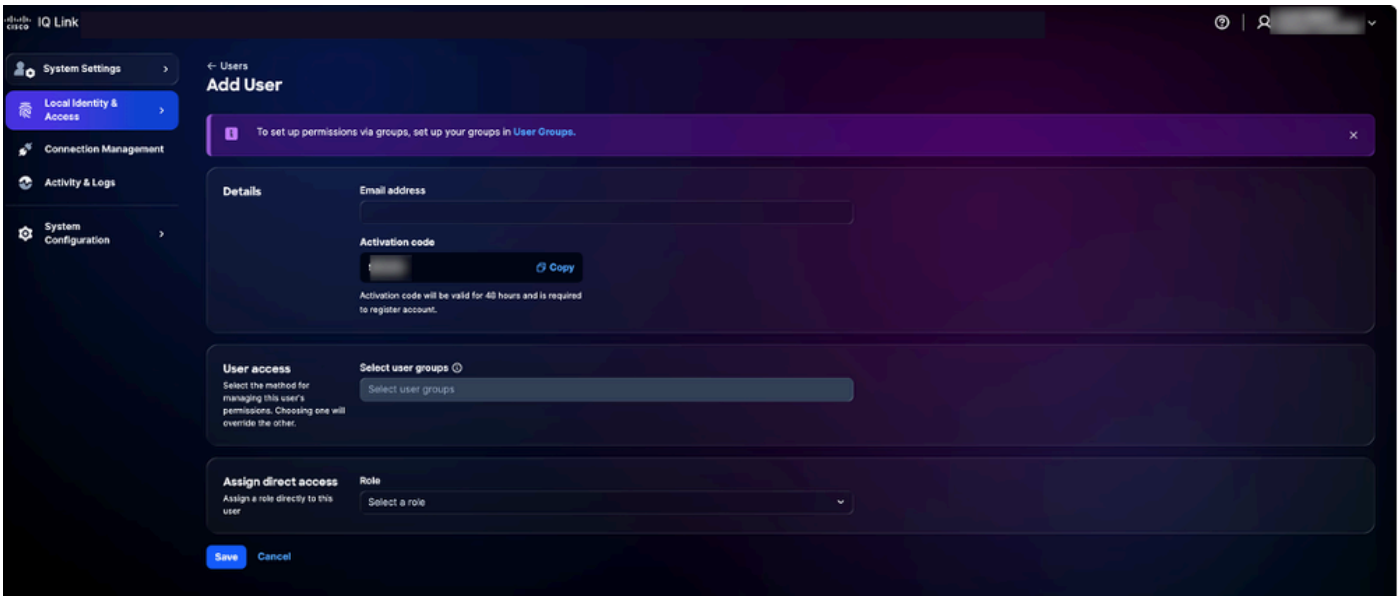
1. Vaya a System Settings > Local Identity & Access > Users. Se muestra la página Users. Enumera todos los usuarios locales existentes junto con su estado.



Página Usuarios

Nota: El icono Más opciones no se muestra para los administradores de cuentas (como se muestra en la imagen anterior).

2. Haga clic en Agregar usuarios. Se muestra la página Add User.



Agregar usuario

3. Introduzca la dirección de correo electrónico.

4. Introduzca el código de activación.

Nota: El código de activación se muestra de forma predeterminada. Compártalo con el usuario, ya que es necesario para completar el registro.

---

5. En el campo Acceso de Usuario, seleccione el grupo de usuarios de la lista desplegable Seleccionar Grupos de Usuarios.

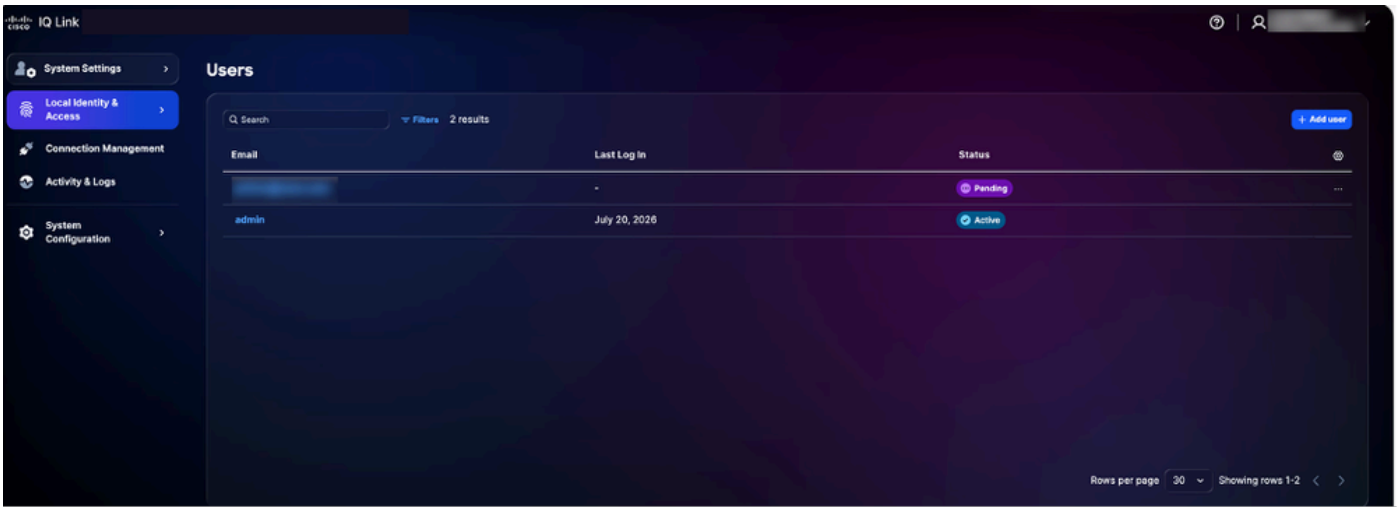
Nota: Los usuarios heredan el acceso del grupo seleccionado.

---

6. En Asignar acceso directo, seleccione un rol de la lista desplegable Rol. Hay dos (2) funciones disponibles:

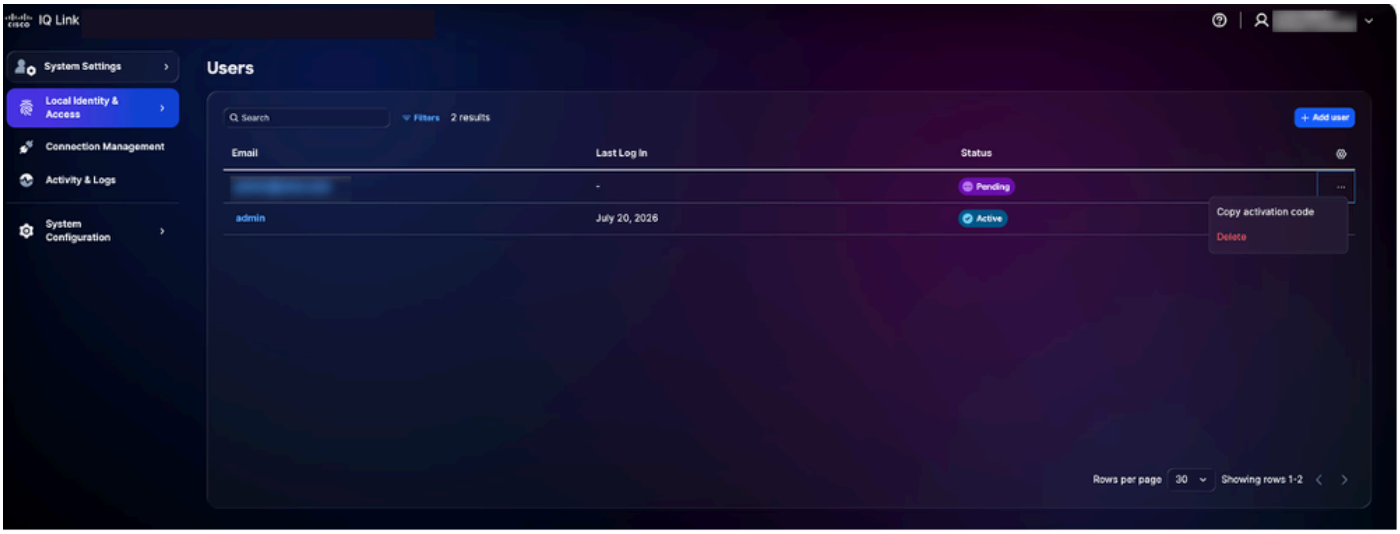
- Visor: Ver y acceder a aplicaciones
- Administrador: Acceder a las aplicaciones y gestionar la configuración del sistema, excepto la gestión del sistema y el IDP

7. Haga clic en Guardar. Se crea el nuevo usuario y se muestra en la lista de usuarios con el estado Pendiente. Pendiente indica que el usuario aún no ha completado la autoactivación.



Usuario recién agregado

8. Localice el usuario recién creado en la lista y confirme que la columna Estado muestra Pendiente.



Copiar código de activación

9. Haga clic en el icono Más opciones > Copiar código de activación junto al usuario recién creado. El código de activación se copia en el portapapeles.

10. Comparta este código con el usuario de forma segura (por ejemplo, mediante un canal interno seguro). El código de activación es para un solo uso y es necesario para completar el registro.

Nota: No comparta el código de activación a través de canales inseguros. Si el código se pierde o se ve comprometido, utilice el icono Menú para volver a generar un nuevo código de activación, que invalida el anterior

---

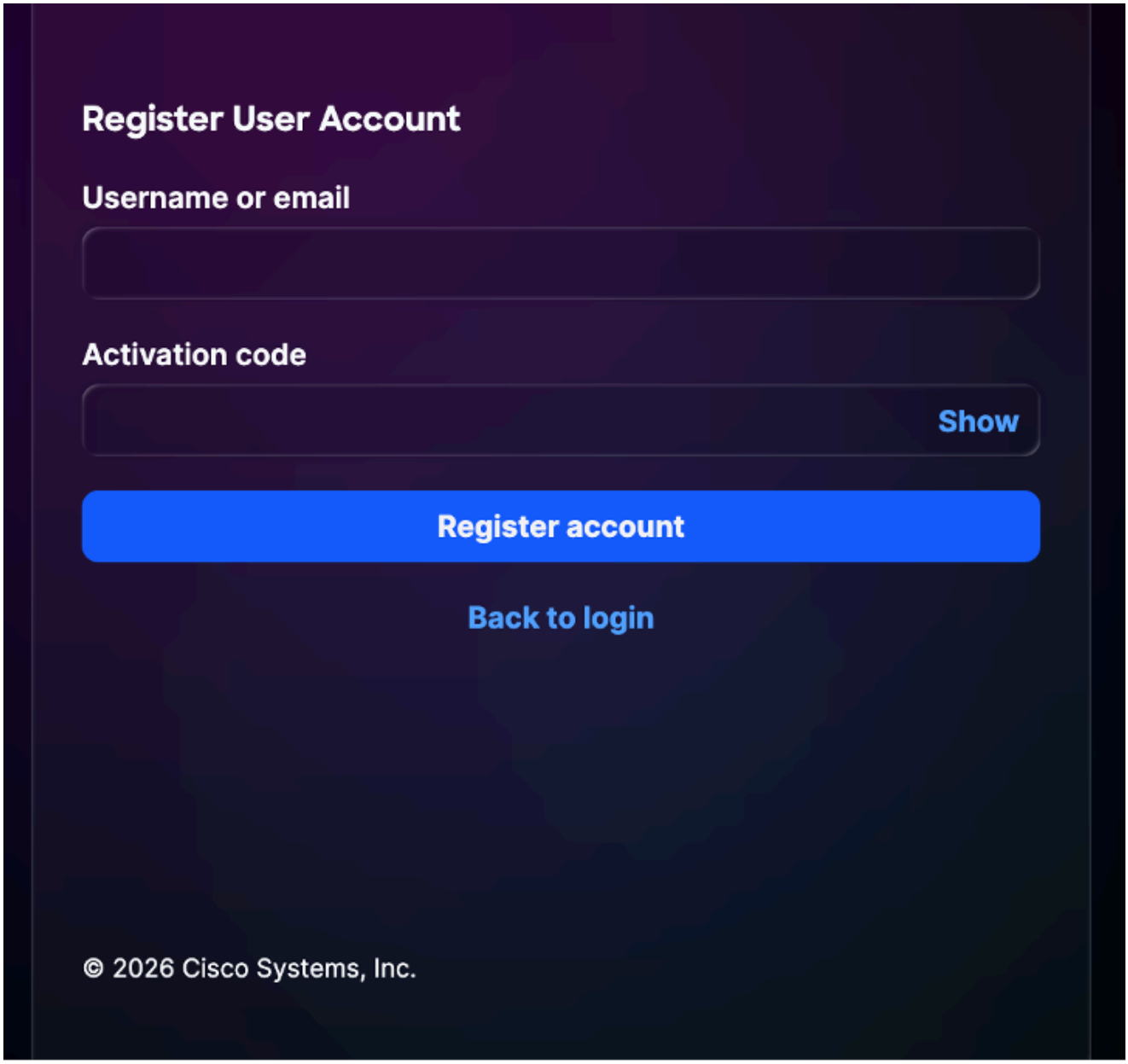
Nota: Los códigos de activación son válidos durante 48 horas. Si su código caduca, póngase en contacto con el administrador de su cuenta para solicitar uno nuevo.

11. Para cerrar sesión, haga clic en el icono User en la esquina superior derecha y seleccione Logout. Volverá a la página de inicio de sesión de Cisco IQ.

Registro de una nueva cuenta de usuario

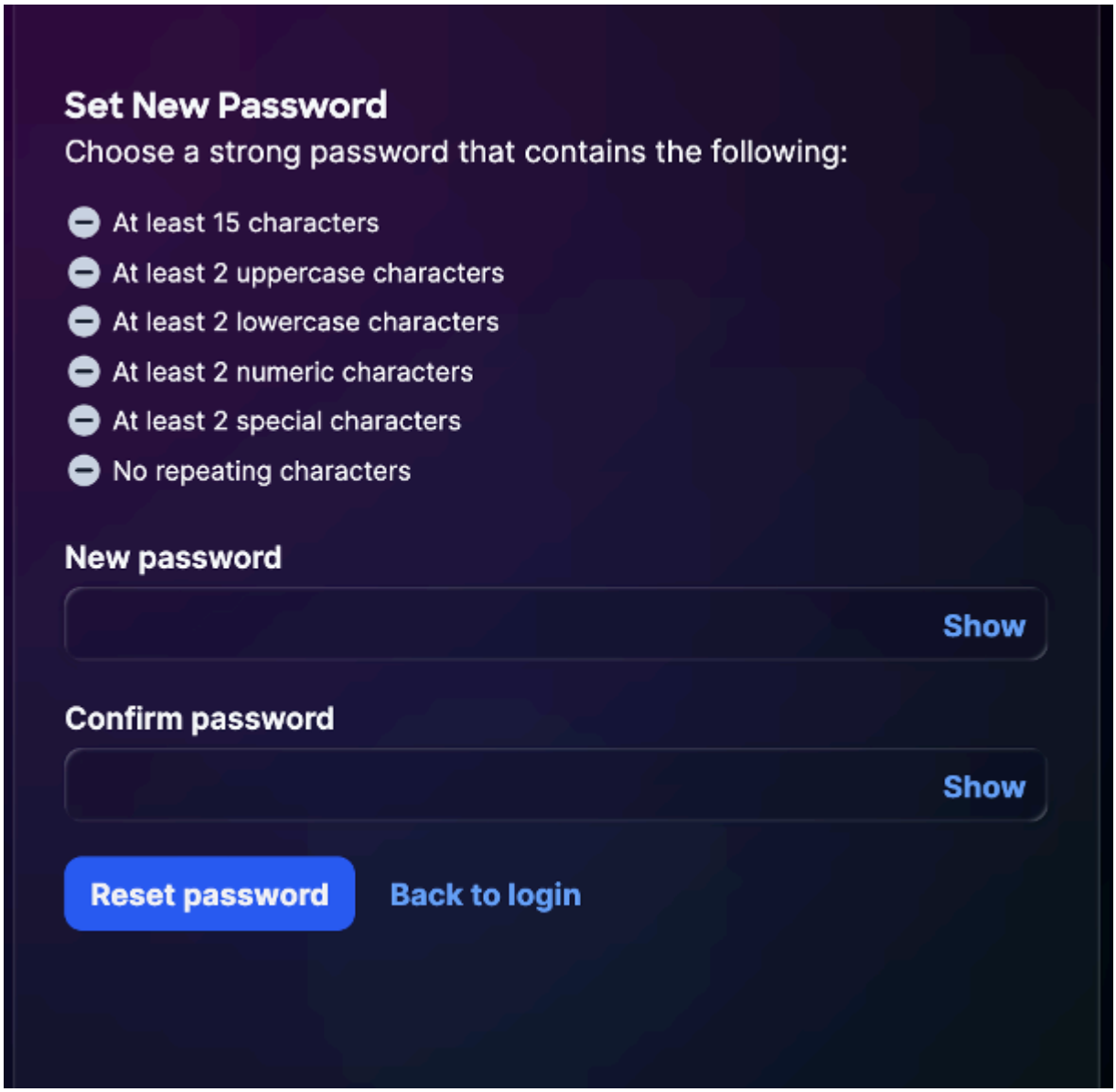
Para registrar la nueva cuenta de usuario:

1. En la página de inicio de sesión, haga clic en el enlace Registrar una nueva cuenta de usuario.



Nueva cuenta de usuario

2. Introduzca el nombre de usuario o la dirección de correo electrónico utilizada cuando se creó el usuario (por ejemplo, user1@abc.com).
3. Introduzca el código de activación compartido por el administrador de la cuenta.
4. Haga clic en Registrar cuenta. Se muestra la ventana Set New Password.



Contraseña de cuenta de usuario nueva

5. Introduzca una nueva contraseña.
6. Vuelva a introducir la contraseña en Confirmar contraseña.
7. En el primer inicio de sesión correcto, se le pide al usuario que configure cinco (5) preguntas de seguridad (consulte Configuración de preguntas y respuestas de seguridad para obtener más información).

Administración de grupos de usuarios locales

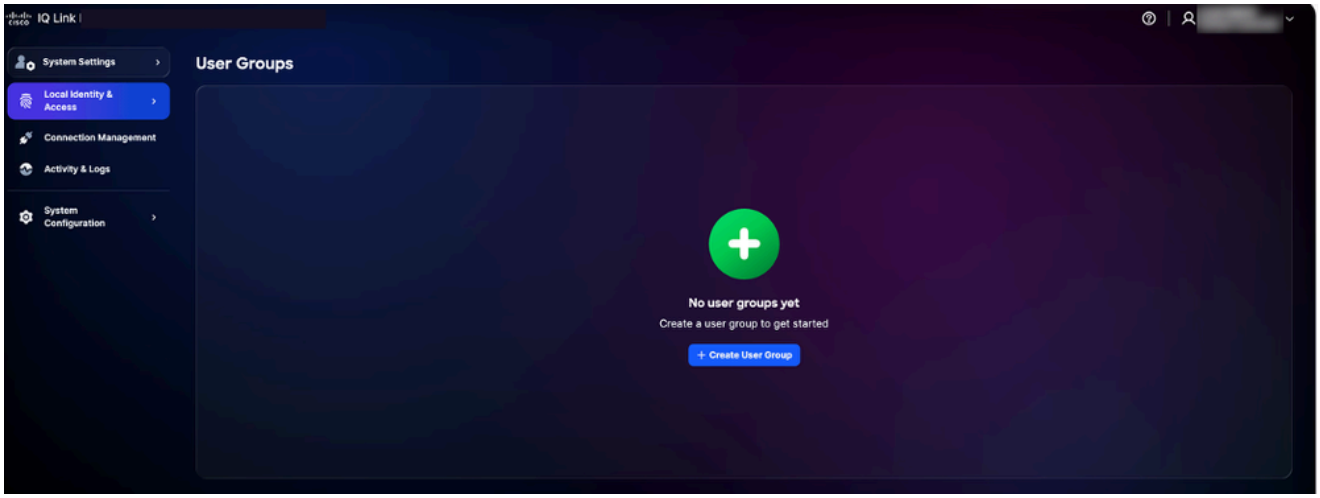
Los grupos de usuarios permiten a los administradores de cuentas administrar las funciones de varios usuarios locales juntos. En lugar de asignar una función a cada usuario de forma individual, un administrador de cuentas puede crear un grupo, adjuntarle una función y un conjunto de usuarios, y actualizar la función o la pertenencia en un único lugar. Toda la gestión de grupos de usuarios se realiza desde la página Identidad local y acceso.

Nota: Sólo un administrador de cuentas puede crear, editar o eliminar grupos de usuarios. Los grupos están formados por usuarios locales existentes; los usuarios deben crearse antes de poder agregarlos a un grupo.

Creación de un grupo de usuarios

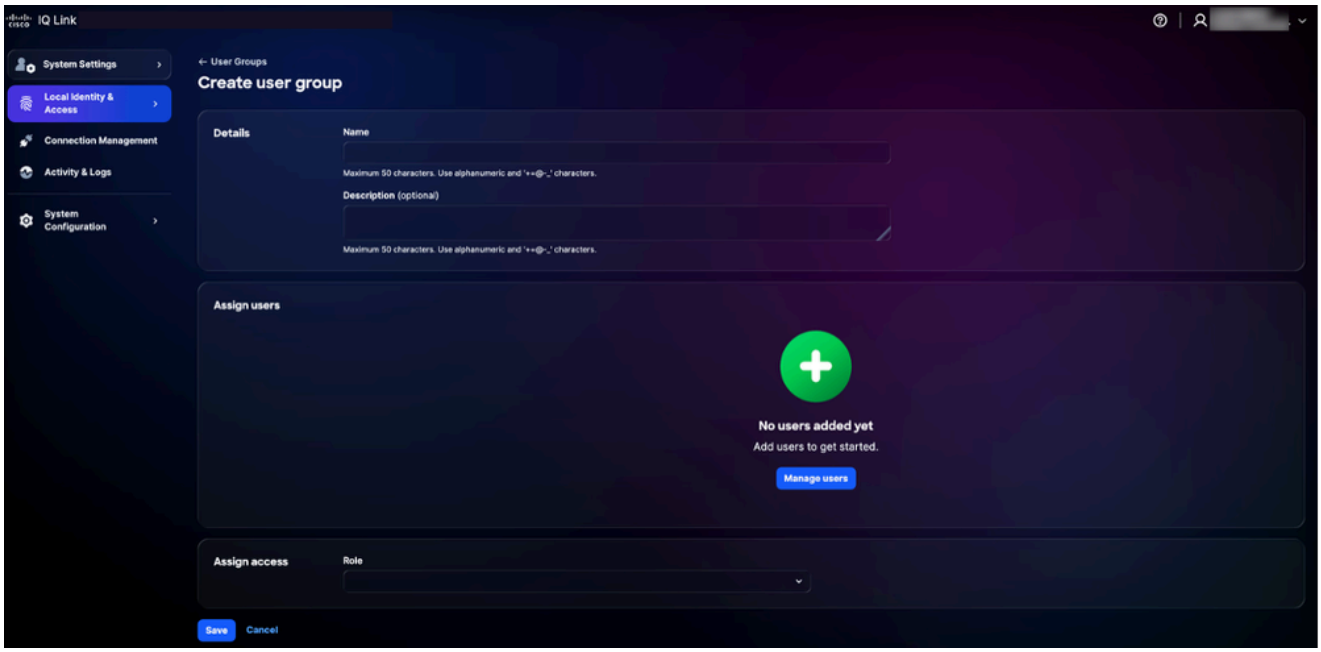
Para crear un grupo de usuarios:

1. En System Settings, elija Local Identity & Access > User Groups. Se muestra la página Grupos de usuarios.



Grupos de usuarios

2. Haga clic en Create User Group. Se muestra la página Crear grupo de usuarios.



Crear grupo de usuarios

3. Complete las siguientes secciones:

- Detalles
  - Nombre: Introduzca un nombre único para el grupo (por ejemplo, Operadores de sólo lectura)
  - Descripción (opcional): Breve descripción del grupo (máximo 50 caracteres; alfanumérico y + = @ - _ (se permiten caracteres)

- Asignar usuarios

  Busque y seleccione uno o varios usuarios locales existentes para agregarlos al grupo.

  Nota: Para agregar usuarios que aún no aparezcan en la lista, haga clic en Administrar usuarios.

- Asignar acceso
  - Función: Seleccione el rol del sistema que desea asignar a todos los miembros de este grupo. Están disponibles los siguientes roles:
    - Visor: Visualización y acceso a aplicaciones (solo lectura)
    - Administrador: Acceder a las aplicaciones y administrar la configuración del sistema

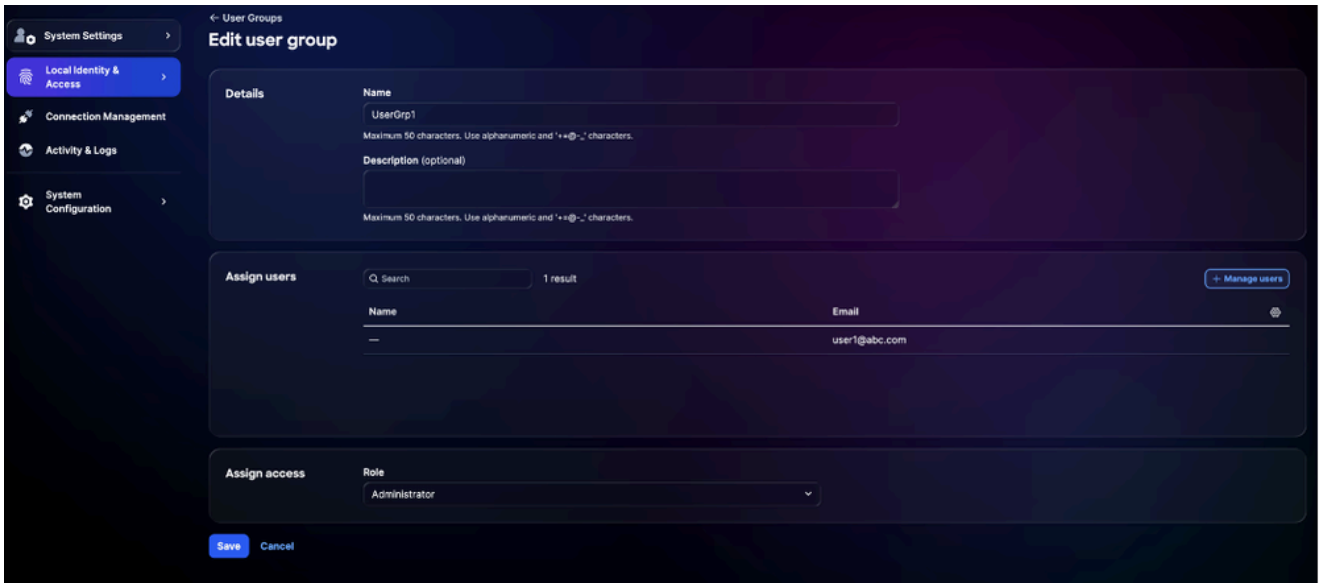
4. Haga clic en Guardar.

El nuevo grupo de usuarios se muestra en la lista Grupos de usuarios junto con su función asignada y número de miembros.

Edición de un grupo de usuarios

Para editar un grupo de usuarios:

1. En la lista Grupos de usuarios, localice el grupo que desea modificar.
2. Haga clic en el icono Más junto al grupo y elija Editar. Se muestra la página Editar grupo de usuarios.



Editar grupo de usuarios

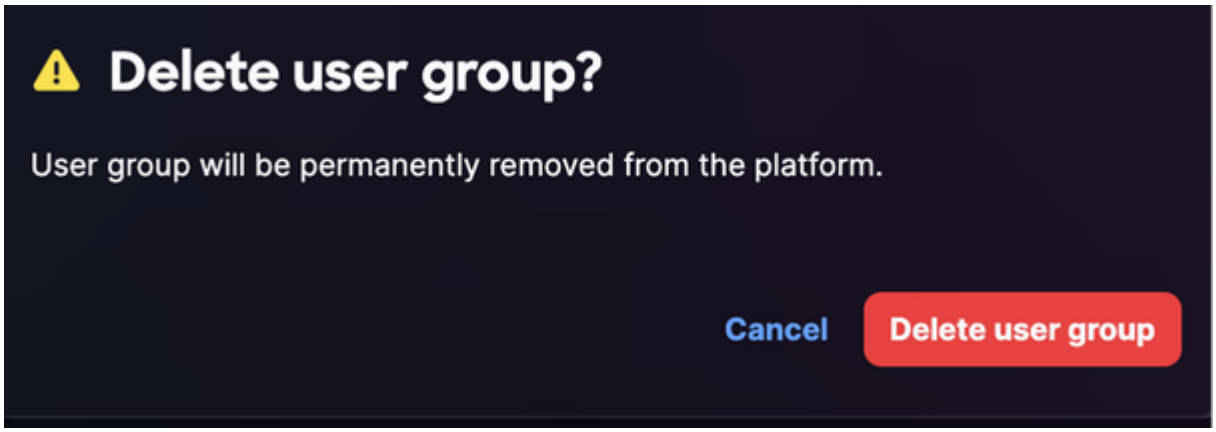
3. Realice los cambios que desee.
4. Click Save.

El grupo actualizado se muestra en la lista Grupos de usuarios. La nueva función surte efecto para todos los miembros del grupo.

Eliminación de un grupo de usuarios

Para eliminar un grupo de usuarios:

1. En la lista Grupos de usuarios, localice el grupo que desea eliminar.
2. Haga clic en el icono Más opciones junto al grupo y seleccione Eliminar.



Eliminar grupo de usuarios

3. Confirme la eliminación cuando se le solicite.

El grupo se elimina de la lista Grupos de usuarios.

Nota: Al eliminar un grupo de usuarios, se quita la asignación de función basada en grupo de todos los miembros. Las cuentas de usuario individuales no se eliminan.

Configuración del proveedor de identidad

Una vez que haya iniciado sesión en Cisco IQ Link, los administradores de cuentas pueden configurar diversos parámetros. Los administradores de cuentas pueden iniciar sesión en Cisco IQ Link mediante la administración local o la configuración del proveedor de identidad (IDP).

Configuración SAML de IDP Okta para SSO

Prerrequisitos para Configurar IDP SAML

- Acceso de administrador de cuenta local a Cisco IQ Link
- Acceso al portal IDP

Configuración SAML de IDP para SSO

Para configurar el Lenguaje de marcado de aserción de seguridad (SAML) IDP para SSO:

1. Desplácese hasta el portal IDP.

2. Establezca los siguientes atributos para la instancia de Cisco IQ Link.
Tabla 1: Atributos de enlace de Cisco IQ

Campo	Valor
Nombre de aplicación	<Application Name>
Entorno	Aplicación empresarial ESP
Grupos de propietarios de aplicaciones	Propietario de la configuración de IDP
Correo del equipo	Correo para el equipo
Destinatarios	Personal no laboral
Categoría de incorporación	Seleccione "Nueva incorporación"

Tabla 2: Parámetros de configuración de SAML

Parámetro	Configuración	Ejemplo:
Audiencia (ID de entidad)	Nombre de dominio completo (FQDN)	mymanagementhost.mydomain.com
URL de inicio de sesión único	Extremo de servicio al consumidor de aserción (ACS) de SAML	https://mymanagementhost.mydomain.com/saml/acs
Formato de ID de nombre	Dirección de correo	NA
Nombre de usuario de aplicación	Nombre de usuario	NA

3. Configure las siguientes sentencias de atributo obligatorias.

Nota: Los cambios en el atributo IDP dependen del proveedor y la configuración específicos. Cisco IDP y sus atributos se comparten a continuación como ejemplo.

- Primera entrada
  - Nombre: Nombre de usuario
  - Valor: user.login

- Segunda entrada
  - Nombre: Correo electrónico principal
  - Valor: usuario.correo electrónico

- Sentencias de Atributo de Grupo
  - Nombre: grupos
  - Filtro: REGEX
  - Valor: .*

4. Configure los parámetros de cierre de sesión único (SLO) en la aplicación.

Tabla 3: Parámetros de configuración de SLO

Campo	Valor
Certificado de firma	Para Okta, este certificado solo es necesario si elige habilitar SLO. Descargue el certificado de firma mediante Download SP Certificate en Identity Providers. Guarde el archivo como sp-public-key.crt. Consulte Configuración de cierre de sesión único para obtener más detalles.
Metadatos SP	Los metadatos SP sólo son necesarios para ADFS IDP (y no para Okta).
¿Desea activar el cierre de sesión único?	Sí o No
URL de cierre de sesión único	https://mymanagementhost.mydomain.com/saml/logout
Emisor SP (ID de entidad/público o URL ACS)	https://mymanagementhost.mydomain.com

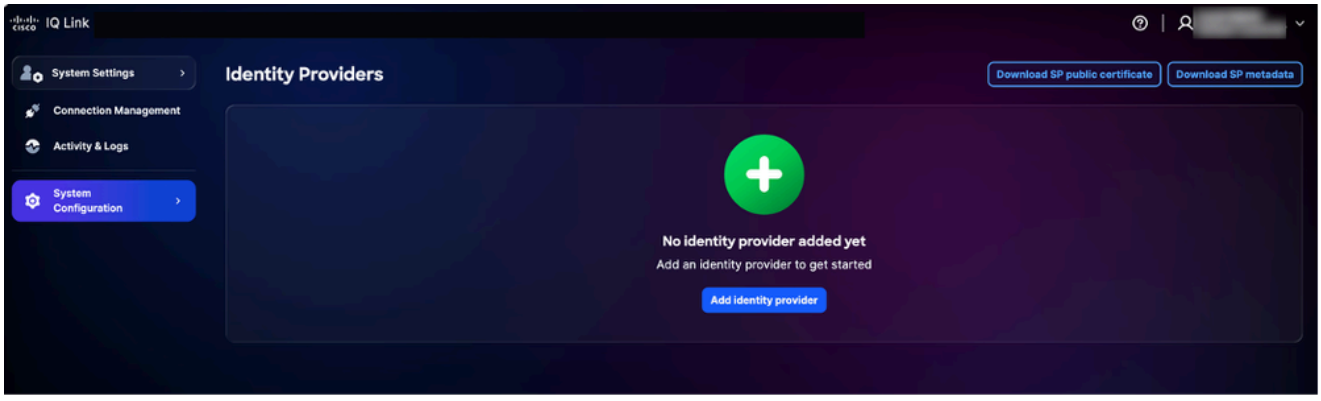
5. Haga clic en el icono Download para descargar el archivo "SP Metadata".

6. Aprovisione o cree la aplicación según lo requiera el proveedor.

Adición de Okta IDP

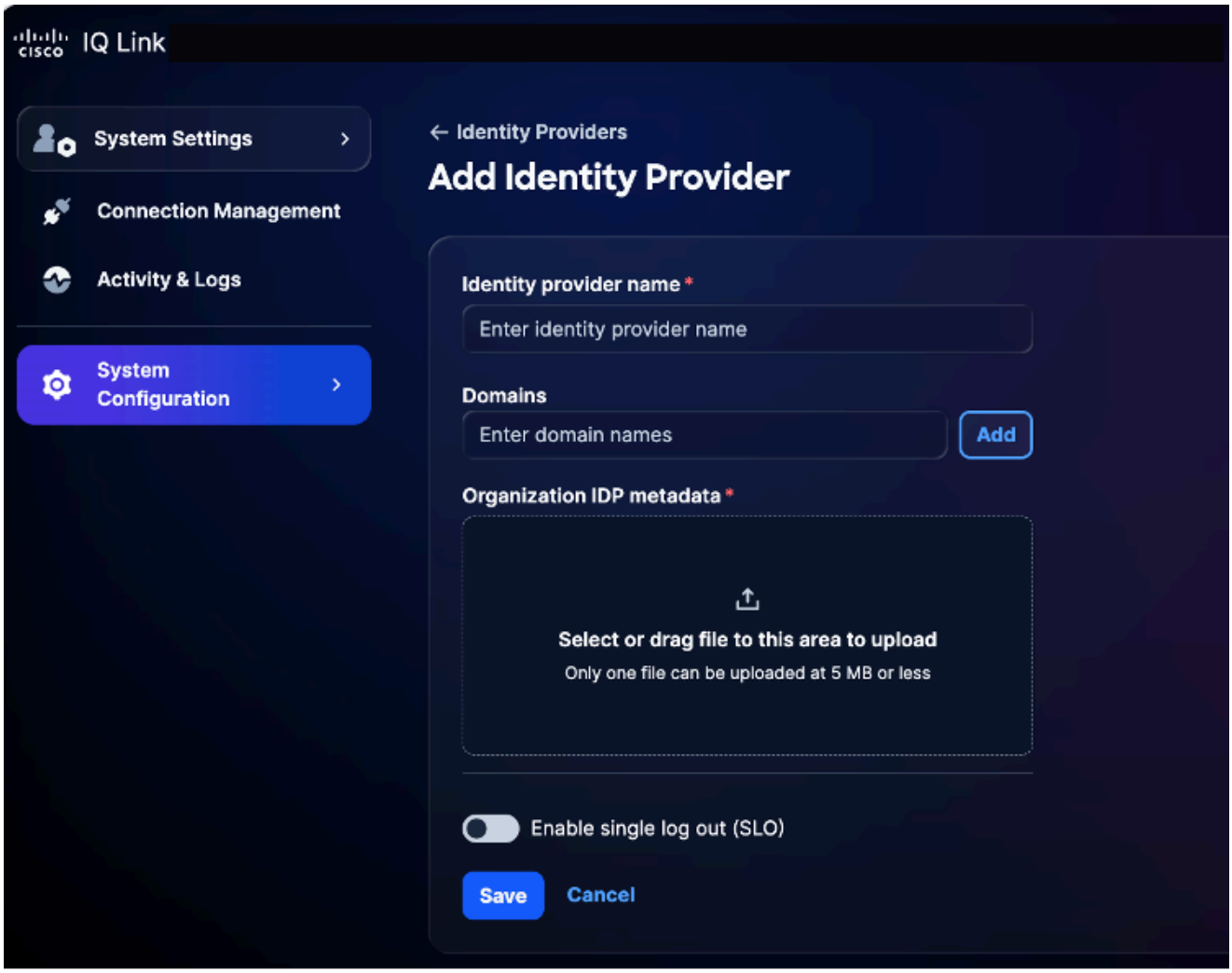
Para agregar un IDP en Cisco IQ Link:

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página Identity Providers.



Página de inicio de IDP

2. Haga clic en Agregar proveedor de identidad. Se muestra la página Add Identity Provider.



Agregar proveedor de identidad

Nota: Solo se puede agregar un (1) IDP en un momento dado.

3. Introduzca el nombre del proveedor de identidad.

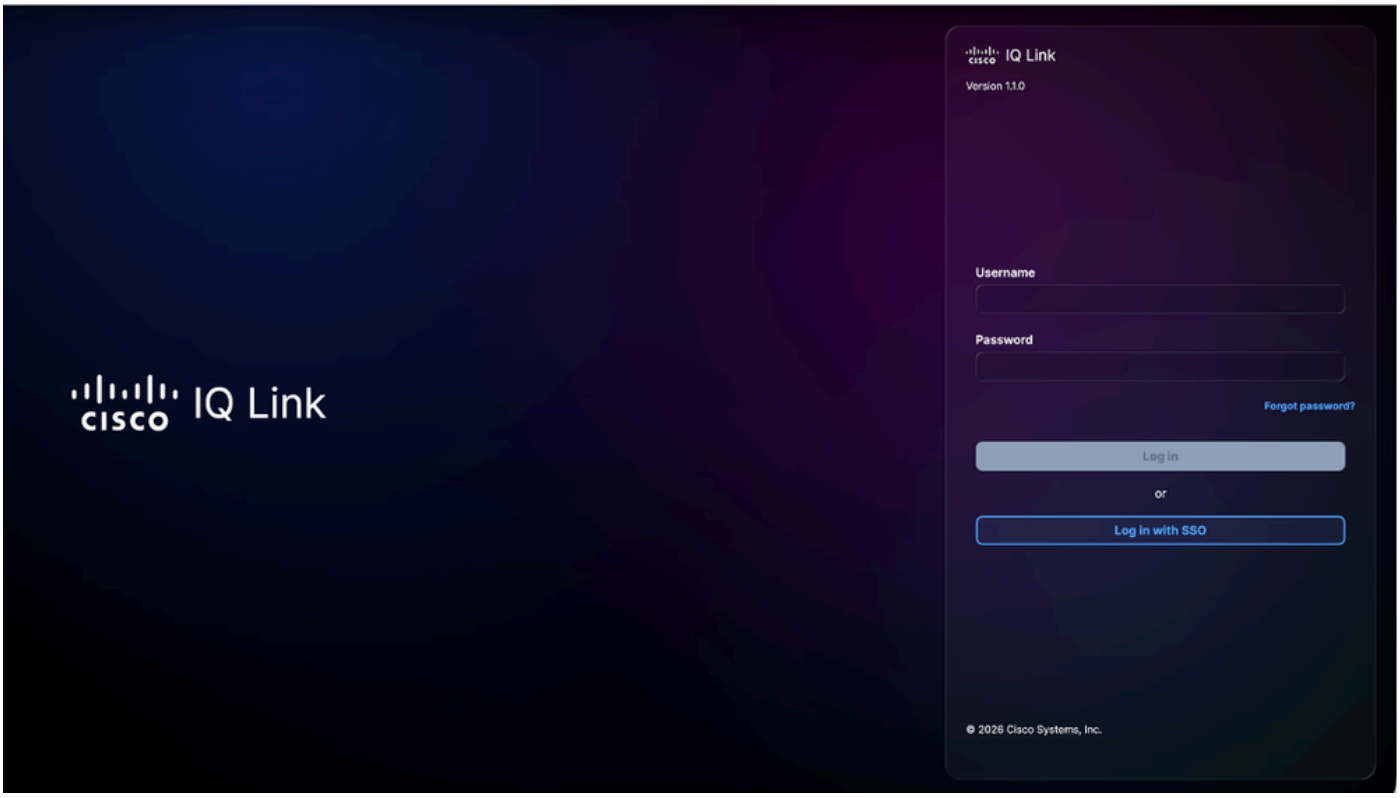
4. Haga clic en Agregar para agregar un nombre de dominio configurado de Cisco IQ Link al campo Dominios.

5. Arrastre y suelte o cargue el archivo de metadatos SAML obtenido de la aplicación IDP en el campo de metadatos Organization IDP. Este archivo contiene los detalles del certificado y los detalles de la entidad Proveedor de servicios (SP).

6. (Opcionalmente) Active el botón de alternancia Enable single logout. También puede activar el SLO más adelante.

7. Haga clic en Guardar.

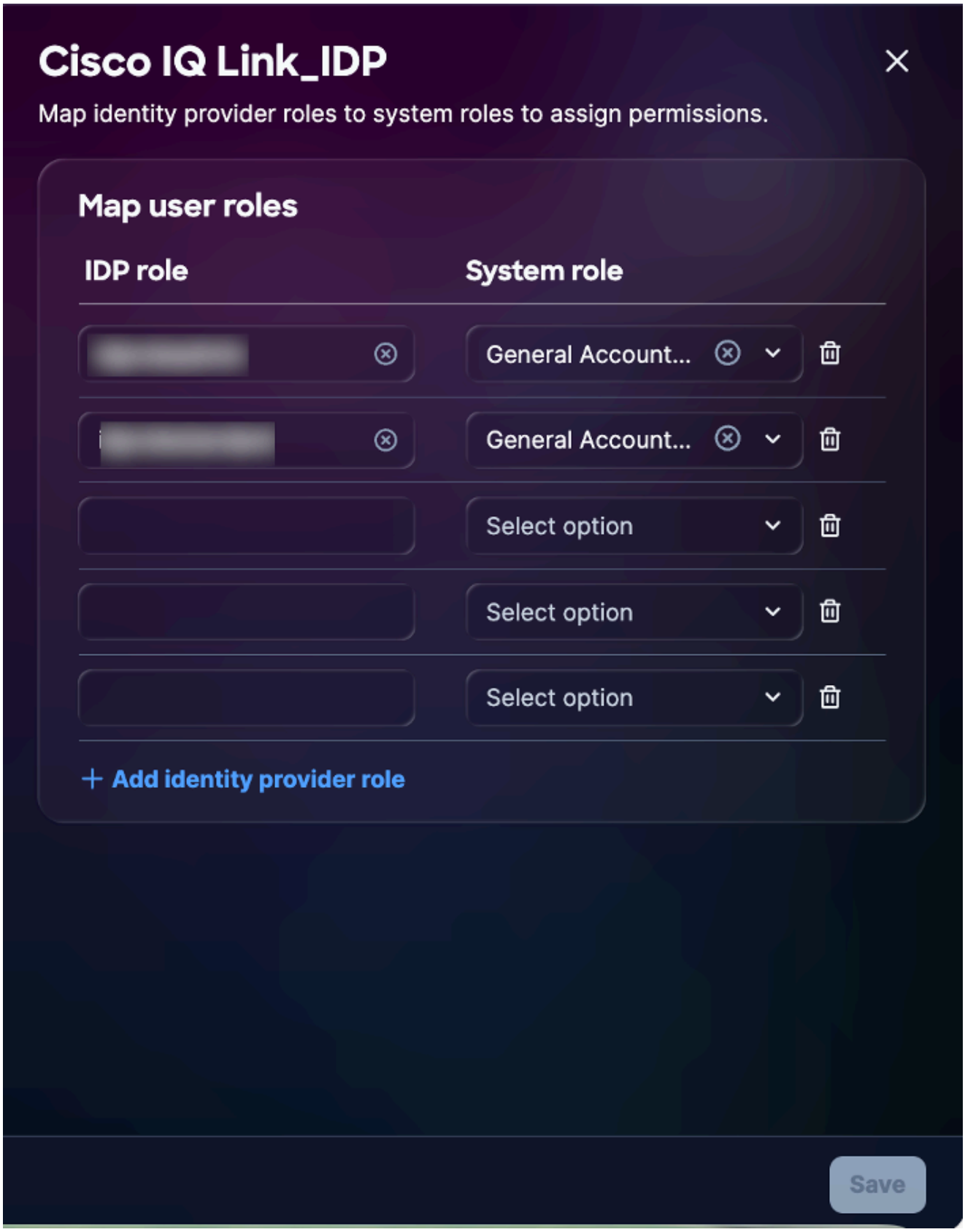
Una vez configurada, la página de inicio de sesión muestra una opción para iniciar sesión con SSO (mediante IDP).



Conexión a Cisco IQ Link

Configuración de asignación de roles

1. En el IDP agregado, seleccione el icono Más opciones > Asignar roles. Se muestra la página Asignar roles de usuario.



Asignación de funciones de usuario

2. Introduzca un rol IDP para el rol de sistema seleccionado. Se admiten los siguientes roles del sistema:

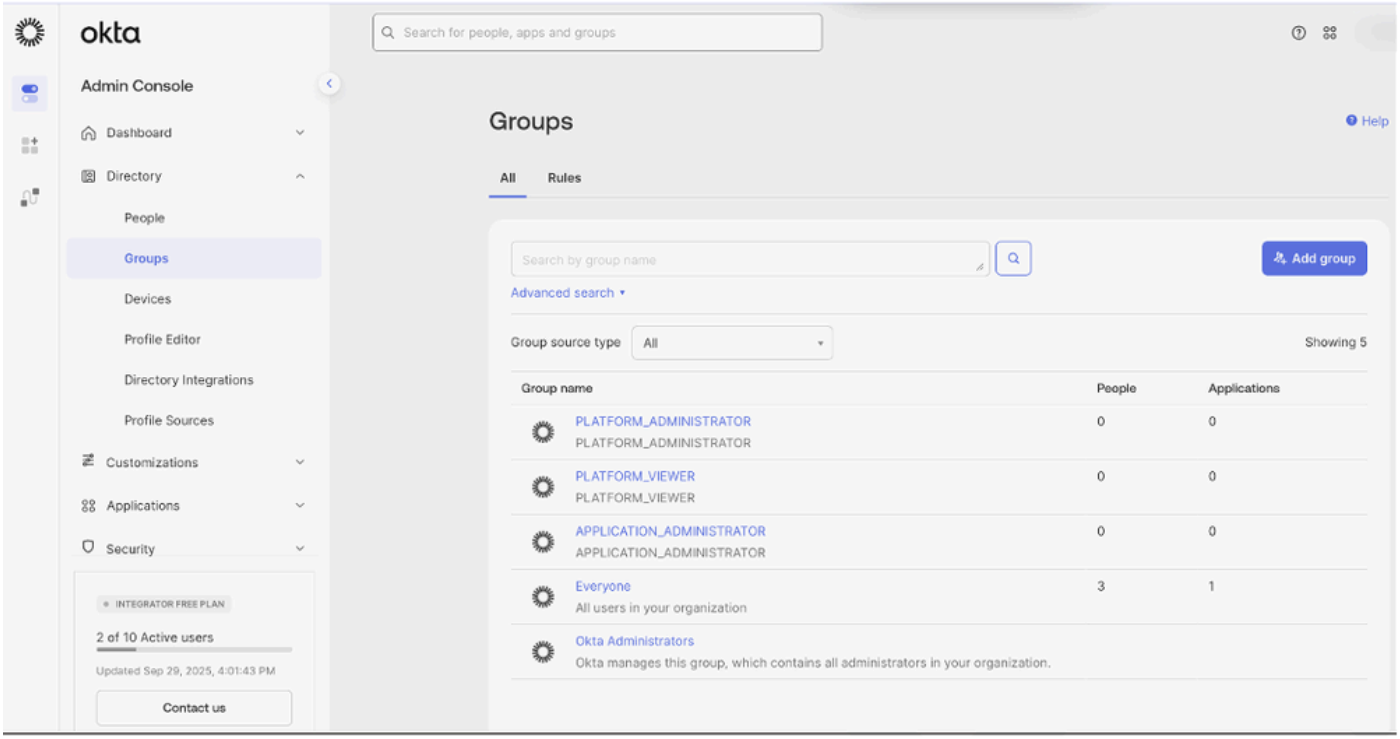
- Administrador general de cuentas: El administrador de cuentas general tiene permisos

completos para realizar todas las acciones del producto

- Visor de cuentas general: El Visor de cuentas general tiene acceso de solo lectura

---

Nota: El rol IDP es un campo de texto abierto. Debe coincidir exactamente con el nombre de grupo o rol configurado en el IDP de su organización. A continuación se comparte un ejemplo de grupos Okta.



Referencia de asignación de roles

3. Asigne roles adicionales según sea necesario haciendo clic en Agregar rol de proveedor de identidad.

4. Haga clic en Guardar.

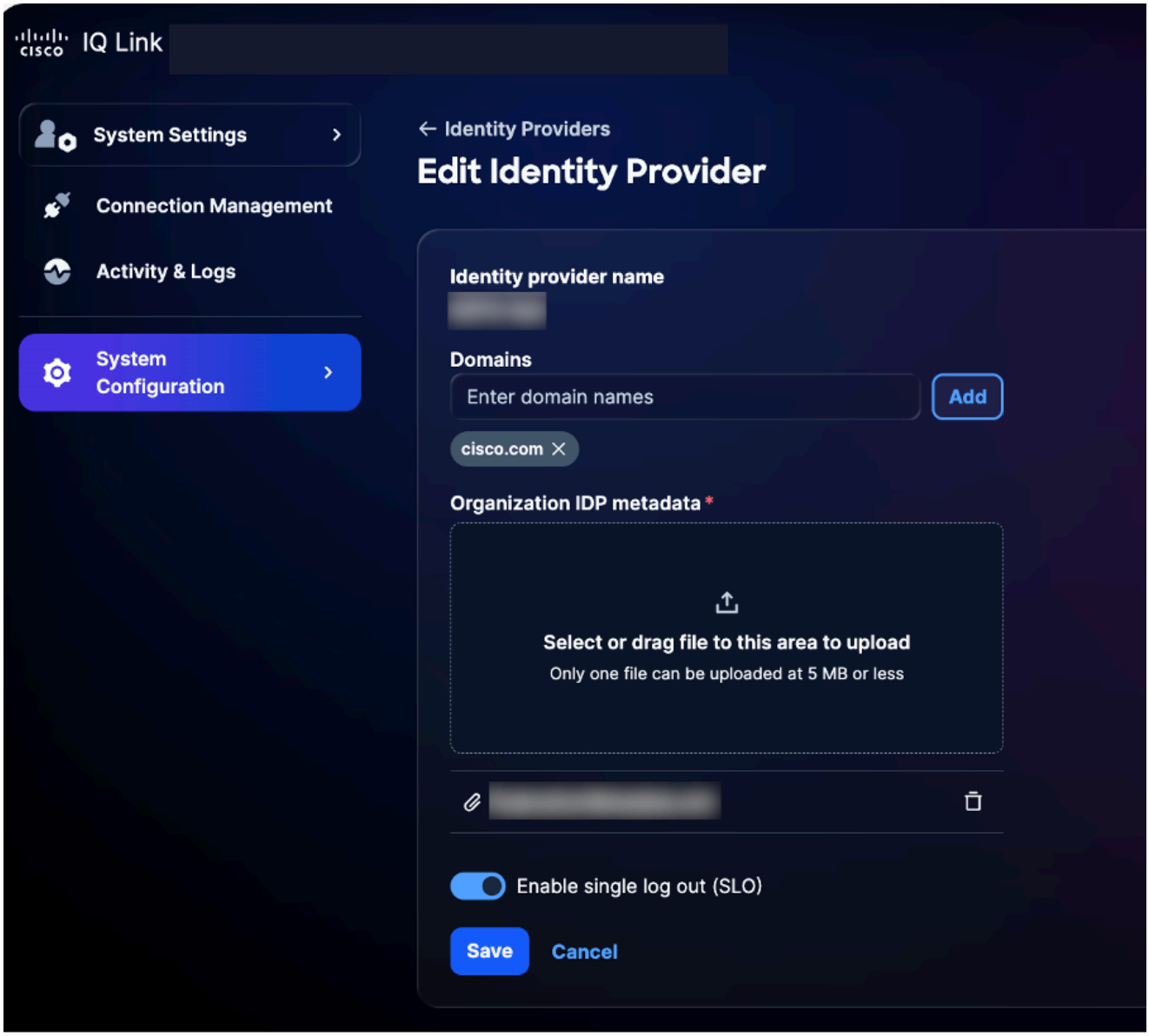
Configuración de cierre de sesión único

Si decide activar la configuración de cierre de sesión único (SLO), debe cargar metadatos que incluyan la URL de SLO. Puede configurarlo editando la configuración del proveedor de identidad y activando la opción Enable Single Log Out. Para completar la configuración de SLO:

1. En la página Identity Providers, haga clic en Download SP public certificate.

Descargar certificado público

2. Guarde el archivo de descarga como sp-public-key.crt.
3. Desplácese hasta el portal IDP.
4. Cargue el archivo de certificado de firma generado en IDP SAML Configuration for SSO.
5. Vuelva a descargar el archivo de metadatos IDP.
6. En la página Identity Providers, elija el icono More Options > Edit del IDP agregado.



Editar proveedor de identidad

7. Active el botón de alternancia Enable single log out (SLO).
8. Cargue el archivo de metadatos recién descargado.
9. Utilice la siguiente lista de comprobación para verificar la funcionalidad de SSO y SLO:

Lista de verificación:

- El inicio de sesión del administrador de cuenta local se ha realizado correctamente
- Se configura y se aprovisiona el portal IDP
- IDP se agrega a Cisco IQ con el estado "Correcto"
- Las asignaciones de funciones se configuran y se prueban
- Se descargan los metadatos SP y se extrae el certificado
- Si SLO está habilitado, la configuración de SLO se completa con el certificado de firma real
- El flujo de SSO/SLO de extremo a extremo se ha probado correctamente

Solución de problemas de IDP

La siguiente lista describe los problemas comunes y las posibles soluciones para ayudar a identificar y resolver rápidamente los problemas relacionados con el estado de IDP, errores de certificado, fallas de inicio de sesión de SSO y configuración de SLO:

Tabla 4: Resolución de problemas

Problema	Solución
El estado de IDP aparece como "Incompleto"	Verificar las configuraciones de asignación de roles
Errores de certificado	Comprobar el formato y la validez del certificado
Fallos de inicio de sesión SSO	Validar asignación de atributos y asignaciones de grupos
SLO no funciona como se esperaba	Asegúrese de que el certificado se haya cargado correctamente y de que las URL de SLO estén configuradas

Configuración ADFS IDP SAML para SSO

Esta sección proporciona una guía para configurar los Servicios de federación de Microsoft Active Directory (AD) (ADFS) como el IDP de SAML para Cisco IQ.

Prerrequisitos para Configurar ADFS IDP SAML for SSO

- Se recomienda ADFS 6.0+
- Windows Server 2012 R2+
- Integración de AD configurada
- Certificados SSL/TLS (Transport Layer Security) en ADFS
- Acceso de administrador de cuenta a Cisco IQ
- Acceso administrativo al servidor ADFS (Windows Server)
- Acceso a PowerShell en servidor ADFS
- Conectividad de red entre ADFS y Cisco IQ
- Detalles de la configuración del servidor ADFS (como se indica en la tabla siguiente)

Tabla 5: Configuración del servidor ADFS

Ítem	Descripción	Ejemplo:
FQDN de Cisco IQ	Nombre de host de implementación de usuario	devxx-23.cx-xxx-xxx.cisco.com
URL del servidor ADFS	Dirección del servidor ADFS del usuario	https://ad-fs.dev.local
Dominio de la empresa	Dominio de correo electrónico	company.com
Grupos AD	Nombres de dominio (DN) del grupo AD	CN=Función: desarrolladores de CXIQ

Configuración de servidores ADFS

Para configurar ADFS:

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página

Identity Providers.

Opciones de descarga

2. Haga clic en Download SP public certificate y Download SP metadata para descargar estos archivos.
3. Copie y guarde los archivos service-provider-metadata.xml y service-provider-certificate.crt en el directorio ADFS (por ejemplo, C:-certificate.crt).
4. Inicie sesión en el servidor ADFS.
5. En el menú Administración de ADFS, haga clic en Confianza de terceros.
6. En el menú Confianzas de usuario de confianza, haga clic en Agregar confianzas de usuario de confianza. Se abrirá el nuevo asistente.
7. Haga clic en el botón de opción Reclamaciones.
8. Haga clic en Start para continuar con la configuración.
9. Haga clic en Importar datos sobre el usuario de confianza desde un archivo para obtener detalles del archivo que se guarda como parte del paso 3.
10. Haga clic en Examinar para seleccionar el archivo de metadatos SP y completar la carga del archivo.
11. Haga clic en Next (Siguiente).
12. Introduzca un nombre para mostrar (por ejemplo, "CIQ-Stage"), añada las notas pertinentes y haga clic en Next (Siguiente).
13. En la página Choose Access Control Policy, haga clic en Permit everyone (o la política requerida por la configuración de seguridad de su organización).
14. Haga clic en Next en las pantallas restantes.
15. Haga clic en Cerrar para completar la configuración de Confianza de usuario de confianza.

Nota: No seleccione "Permitir a todos con MFA" a menos que el servidor ADFS tenga un adaptador Multi-Factor Authentication (MFA) registrado (por ejemplo, Azure MFA o

*Contraseña de un solo uso basada en tiempo (TOTP) configurada).
Si esta directiva está habilitada sin un proveedor MFA configurado, ADFS autentica al usuario pero, en última instancia, deniega la solicitud con el estado urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Dado que la respuesta SAML no contiene aserción, el plugin falla e informa de un error de "correo electrónico faltante".

Problema: "Permitir a todos con MFA" está seleccionado.

Solución alternativa: En PowerShell, compruebe la directiva actual ejecutando el comando siguiente.

```
Get-AdfsRelyingPartyTrust -Name “

     ”).AccessControlPolicyName
```

Para establecer "Permitir a todos" (sin requisito de MFA), ejecute el siguiente comando:

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

También puede crear la confianza de usuario de confianza a través de PowerShell:

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

      ” `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol SAMLAssertionConsumer -Uri “
```

```
    ") `
-AccessControlPolicyName "Permit everyone" `
-IssuanceAuthorizationRules '=> issue(Type = "http://schemas.microsoft.com/authorization/claims/per
```

Configuración de reglas de reclamación de ADFS

Para configurar las reglas de reclamación de ADFS, lleve a cabo los pasos que se indican en las secciones siguientes.

Reclamaciones necesarias

Consulte la tabla siguiente para obtener información sobre las reclamaciones necesarias.

Tabla 6: Reclamaciones necesarias

Afirmación	Propósito	Fuente
Correo electrónico	Identificador de usuario	Correo AD
Mostrar nombre:	Nombre completo del usuario	Nombre para mostrar de AD
UPN	Infraestructura de clave pública (PKI)/autenticación de certificados	ADFS asigna el certificado de cliente a un usuario de AD a través del nombre principal de usuario (UPN)
ID de nombre	asunto SAML	Transformado a partir del correo electrónico
Grupos	Acceso basado en roles	Pertenencia a grupos AD (memberOf)

Aplicación de reglas de reclamación

1. Defina el nombre de su fideicomiso de usuario de confianza (por ejemplo, "Cisco IQ - Stage").

```
$relyingPartyName = "Cisco IQ - Stage"
```

2. Defina las reglas de reclamación para enviar la información de usuario y la pertenencia al grupo a Cisco IQ.

```
$claimRules = @'

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@RuleName = “Transform Email to NameID”
c:[Type == “http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress ”]
=> issue(Type = “http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ”, Issuer = c.Iss

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;mem
'@@
```

3. Aplique las reglas de reclamación ejecutando el siguiente comando:

```
Set-AdfsRelyingPartyTrust -TargetName $relyingPartyName -IssuanceTransformRules $claimRules

Write-Host “Claim rules configured successfully!” -ForegroundColor Green
```

Advertencia: Cada cuenta de usuario de AD debe tener el atributo de correo rellenado. Si falta este atributo, la afirmación SAML no contiene una notificación de correo electrónico, lo que provoca un rechazo de autenticación.

Para actualizar la dirección de correo electrónico de un usuario, ejecute el siguiente comando de PowerShell:

```
Set-ADUser -Identity “


     ” -EmailAddress “


      ”
```

Verificación de grupos de usuarios

1. Establezca el nombre de usuario para comprobar la pertenencia al grupo del usuario.

```
$username = “testuser”
```

2. Ejecute los siguientes comandos para buscar la cuenta del usuario:

```
$searcher = [adsisearcher]“(samaccountname=$username)”
$user = $searcher.FindOne()
```

3. Muestra los grupos a los que pertenece el usuario.

```
$user.Properties.memberof
```

Ejemplo de salida:

```
CN=Role - CXIQ Developers,OU=Role Groups,DC=dev,DC=local
```

Configuración de ADFS para Confiar en el Certificado de Firma SP

1. En el servidor ADFS, importe el certificado SP en el almacén TrustedPeople.

```
Import-Certificate -FilePath “C:-provider-certificate.crt” -CertStoreLocation “Cert:”
```

2. Seleccione una de las siguientes opciones:

Nota: El certificado SP lo emite una autoridad de certificación (CA) interna que ADFS no puede validar a través de la cadena de confianza estándar.

- Deshabilitar la validación de cadena globalmente para este usuario de confianza

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


     ” `
    -SigningCertificateRevocationCheck None `
    -EncryptionCertificateRevocationCheck None
```

O

- Si el certificado SP lo emite una CA (no autofirmada), importe el certificado de CA emisor en el almacén de certificados raíz:

```
Import-Certificate -FilePath “C:-iq-onprem-ca.cer” -CertStoreLocation “Cert:”
```

3. Aplique los cambios reiniciando el servicio ADFS.

```
Restart-Service adfssrv
```

Configuración de la Autenticación PKI/de Certificados

En esta sección se describe cómo agregar autenticación basada en certificados (es decir, tarjeta inteligente o certificado de software) junto con contraseñas. Esta sección se puede omitir si la autenticación de solo contraseña es suficiente.

Instalación del rol CA de AD CS

Para instalar el rol de CA de Servicios de certificados de AD (CS):

1. Verifique si ya existe una CA empresarial en su dominio ejecutando el siguiente comando:

```
certutil -config - -ping
```

Si el comando devuelve una respuesta válida, puede omitir el resto de esta sección. Su entorno ya está configurado. Si el comando indica que no se ha encontrado ninguna CA, vaya al paso 2.

2. Instale el rol CA ejecutando el siguiente comando:

```
install-WindowsFeature AD-Certificate -IncludeManagementTools
```

3. Configure el rol CA ejecutando el siguiente comando:

```
Install-AdcsCertificationAuthority `
    -CAType EnterpriseRootCA `
    -CACommonName “


     ” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. Instalación mediante la ejecución del siguiente comando:

```
certutil -ca
```

5. Confirme que el servicio está activo y accesible ejecutando el siguiente comando:

```
certutil -config - -ping
```

Configuración de una Plantilla de Certificado

Para configurar una plantilla de certificado con el Uso mejorado de claves de autenticación de cliente (EKU):

1. Abra certsrv.msc y expanda el nodo CA.
2. Haga clic con el botón derecho en Plantillas de certificado > Administrar.
3. Duplicar la plantilla de usuario.

Nota: La plantilla de usuario integrada es funcional o válida sólo si el certificado emitido desde ella incluye EKU de autenticación de cliente.

---

4. Configure los parámetros de las siguientes fichas:

- General: Introduzca "Autenticación de usuario CIQ" en el campo Nombre con un período de validez de un (1) año
- Gestión de solicitudes: Seleccione Signature and encryption en la lista desplegable Purpose y marque la casilla de verificación Allow private key to be export
- Nombre del sujeto: Seleccione Build from Active Directory Information e incluya un correo electrónico en los campos Subject y SAN

Advertencia: Los campos Subject y SAN deben contener el UPN de un usuario o un correo electrónico que coincida con una cuenta de AD. ADFS asigna el certificado a un usuario de AD mediante estos campos.

- Extensiones: Asegúrese de que las políticas de aplicación incluyen "Autenticación de cliente (1.3.6.1.5.5.7.3.2)"
- Seguridad: Agregue usuarios de dominio y conceda permisos de lectura e inscripción

5. Publique la plantilla mediante el siguiente comando:

```
Add-CATemplate -Name “CIQUserAuthentication” -Force
```

Inscripción de un Certificado de Usuario

1. Inicie sesión como usuario de destino.
2. Inscriba el certificado ejecutando el siguiente comando:

```
certreq -enroll -user “CIQUserAuthentication”
```

3. Verifique la instalación del certificado ejecutando el siguiente comando:

```
Get-ChildItem Cert:| Where-Object {
    $_.EnhancedKeyUsageList.ObjectId -contains “1.3.6.1.5.5.7.3.2”
} | Format-Table Subject, Thumbprint, NotAfter -AutoSize
```

Exportación de un certificado de usuario desde Windows e instalación en el cliente (Mac)

Para exportar un certificado de usuario de Windows a Mac:

1. Exporte el certificado de Windows como un archivo PFX ejecutando los siguientes comandos:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like “*

     *” }

$password = ConvertTo-SecureString -String “

      ” -Force -AsPlainText

Export-PfxCertificate -Cert $cert -FilePath “C:-cert.pfx” -Password $password
```

2. Transfiera el archivo user-cert.pfx a su dispositivo Mac.

3. Importe el certificado en el llavero Mac ejecutando el siguiente comando:

```
security import user-cert.pfx -k ~/Library/Keychains/login.keychain-db -P “

     ”
```

Nota: Después de importar el certificado, el explorador debe cerrarse y abrirse de nuevo para que se reconozca.

4. Confíe en la CA en Mac ejecutando:

```
sudo security add-trusted-cert -d -r trustRoot \
-k /Library/Keychains/System.keychain ca-certificate.cer
```

Habilitación de los Extremos de Autenticación de Certificado ADFS

Para habilitar los extremos de autenticación de certificados ADFS:

1. Habilite los extremos de certificado ADFS requeridos ejecutando los siguientes comandos:

```
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2. Compruebe que todos los terminales están habilitados ejecutando el siguiente comando:

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like “*cert*” } |

Format-Table AddressPath, Enabled, Proxy -AutoSize
```

Habilitación de la Autenticación de Certificados como Principal

Para habilitar la autenticación de certificados como principal:

1. Configure los proveedores de autenticación principales para el acceso a la intranet y a la extranet mediante el siguiente comando:

```
Set-AdfsGlobalAuthenticationPolicy `
-PrimaryIntranetAuthenticationProvider @(“CertificateAuthentication”, “WindowsAuthentication”, “FormsAu
```

```
-PrimaryExtranetAuthenticationProvider @("CertificateAuthentication", "FormsAuthentication", "Microsoft
```

2. Compruebe que ambas listas incluyen CertificateAuthentication y FormsAuthentication mediante los siguientes comandos:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Verifique la configuración actual del puerto del cliente TLS mediante el siguiente comando:

```
Get-AdfsProperties | Select-Object HostName, HttpsPort, TlsClientPort
```

4. Si el valor de TlsClientPort no es 49443, actualice el puerto y reinicie el servicio ADFS con los siguientes comandos:

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

Correcciones SChannel/TLS (CRÍTICO para PKI)

Los pasos de las siguientes secciones resuelven los errores CERT_E_UNTRUSTEDROOT (0x800B0109), que impiden que funcione la autenticación de certificados.

Enlace de certificados SSL en el puerto 49443

Para enlazar certificados SSL en el puerto 49443:

1. Elimine cualquier enlace de certificado SSL existente en el puerto 49443 mediante el siguiente comando:

```
netsh http delete sslcert hostnameport=
```

```
     :49443
```

2. Cree un nuevo enlace con la negociación de certificado de cliente habilitada mediante el siguiente comando:

```
netsh http add sslcert hostnameport=
```

```
     :49443 `
    certhash=
```

```
       `
    appid="{5d89a20c-beab-4389-9447-324788eb944a}" `
    certstorename=MY `
    clientcertnegotiation=enable `
    verifyclientcertrevocation=disable
```

3. Verifique que la negociación de certificado de cliente esté habilitada mediante el siguiente comando:

```
netsh http show sslcert hostnameport=
```

```
     :49443
```

Limpieza del almacén de certificados (CRÍTICO)

Para limpiar el almacén de certificados:

Advertencia: Windows SChannel rechaza todos los certificados de cliente si hay certificados no autofirmados en el almacén raíz de confianza. Esta es la causa principal de las fallas de PKI.

---

1. Identifique los certificados no autofirmados en el almacén raíz de confianza ejecutando el siguiente comando:

```
$bad = Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
$bad | ForEach-Object { Write-Host “PROBLEM: $($_.Subject) | Issuer: $($_.Issuer)” -ForegroundColor Red
```

2. Mueva estos certificados al almacén de CA intermedio ejecutando el siguiente comando:

```
$bad | Move-Item -Destination Cert:
Write-Host “Moved $($bad.Count) cert(s) from Root to Intermediate CA store” -ForegroundColor Green
```

3. Compruebe que no queden certificados no autofirmados en el almacén raíz ejecutando el siguiente comando:

```
Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
```

Correcciones de registro de SChannel (CRÍTICO)

Para configurar los valores del Registro de SChannel para garantizar una autenticación de certificado adecuada:

1. Defina la variable de ruta de acceso del Registro mediante el siguiente comando:

```
$regPath = “HKLM:”
```

2. Aplique la configuración del registro definida en la tabla siguiente utilizando los siguientes comandos:

```
Set-ItemProperty -Path $regPath -Name “ClientAuthTrustMode” -Value 2 -Type DWord

Set-ItemProperty -Path $regPath -Name “SendTrustedIssuerList” -Value 0 -Type DWord
```

Tabla 7: Configuración del Registro de Schannel

Configuración	Valor	Propósito
ClientAuthTrustMode	2	Habilita la confianza exclusiva de la CA para corregir la ruta de validación predeterminada.
SendTrustedIssuerList	0	Impide que el servidor envíe la lista completa de emisores de confianza durante el intercambio de señales TLS.

Verificación del almacén de certificados de la CA

Para comprobar el almacén de certificados de la CA:

Nota: El certificado de CA que emite los certificados de usuario debe estar en el almacén de certificados del sistema para garantizar que se reconoce correctamente.

1. Defina la huella digital de su certificado de CA mediante el siguiente comando:

```
$caThumbprint = “

    ”
```

2. Compruebe que el certificado de la CA ya está presente en el almacén de equipo local mediante el siguiente comando:

```
$exists = Test-Path “HKLM:\caThumbprint”
```

Si no se encuentra el certificado, impórtelo al LocalMachinestore:

```
if (-not $exists) {
Import-Certificate -FilePath “C:\YOUR-CA-CERT>.cer” `
-CertStoreLocation “Cert:”
}
```

Reinicio del servidor ADFS (OBLIGATORIO)

Reinicie el servidor ADFS con el siguiente comando:

```
Restart-Computer -Force
```

Nota: El cambio de registro ClientAuthTrustMode sólo tiene efecto después de reiniciar el servidor.

Exportación de metadatos ADFS

Puede descargar los metadatos de ADFS mediante PowerShell o el explorador web.

PowerShell

Para exportar metadatos de ADFS mediante PowerShell:

1. Abra PowerShell en el servidor ADFS.
2. Ejecute los siguientes comandos para descargar el archivo de metadatos.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq “Federation Metadata”}).FullUrl

Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile “C:-metadata.xml”

Write-Host “ADFS metadata exported to C:-metadata.xml” -ForegroundColor Green
```

Después de ejecutar los comandos, el archivo de metadatos se guarda en C:-metadata.xml.

Explorador web

Para exportar metadatos de ADFS mediante un explorador web:

1. Vaya a https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Sustituya <your-adfs-server> por el nombre de host del servidor ADFS.
3. Guarde el archivo XML de metadatos en el equipo cuando se le solicite.

Configuración en Cisco IQ

Para configurar en Cisco IQ:

1. Transfiera adfs-metadata.xml a su estación de trabajo.
2. En Cisco IQ, navegue hasta System Settings > System Configuration > Identity Providers.
3. Cargue el archivo de metadatos ADFS para extraer automáticamente el certificado IDP, la ID de entidad y la URL SSO.
4. Guarde la configuración.

Nota: Si ADFS realiza una renovación automática del certificado de firma de tokens, debe volver a exportar el archivo de metadatos y cargarlo en Cisco IQ para garantizar una autenticación continua.

Adición de IDP de ADFS

1. En la página Proveedores de identidad, haga clic en Agregar proveedor de identidad.
2. Introduzca el nombre del proveedor de identidad.
3. Introduzca el dominio o dominios (por ejemplo, company.com).
4. (Opcionalmente) Active el botón de alternancia Enable single logout, si es necesario.
5. Arrastre y suelte o cargue el archivo de metadatos SAML obtenido de la aplicación IDP en el campo Upload IDP Metadata.
6. Click Save.

Nota: El estado se muestra como "Incompleto" hasta que se complete la asignación de roles; debe ocurrir lo siguiente.

Configuración de mapeo de roles

Antes de continuar con la configuración de la asignación de funciones, asegúrese de que puede encontrar grupos de AD para utilizarlos en la asignación. Para buscar grupos desde AD, ejecute el siguiente comando de PowerShell.

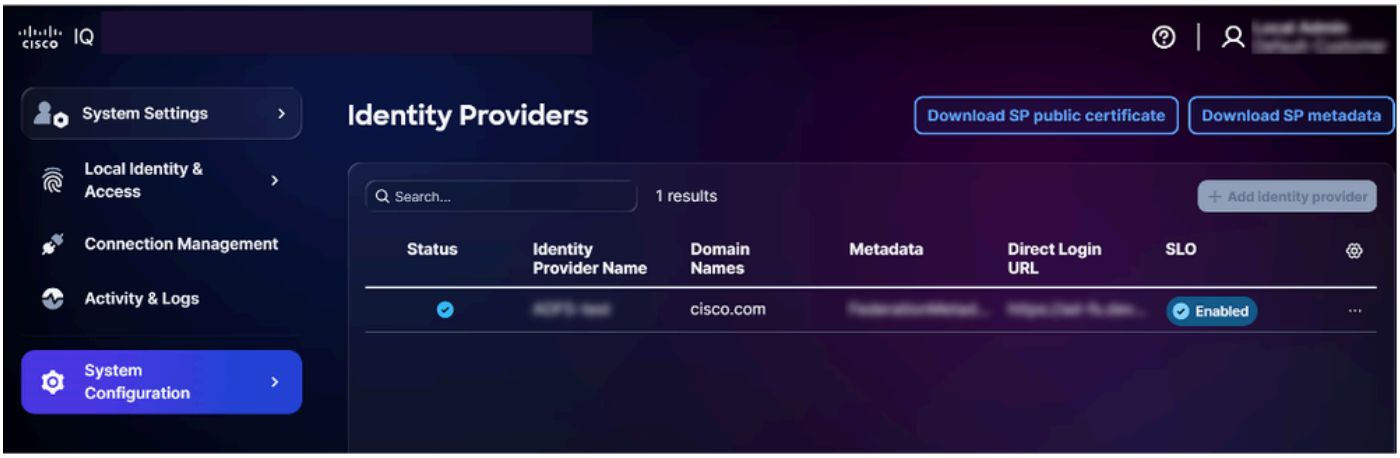
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”] }
```

El sistema consulta a AD directamente a través del protocolo ligero de acceso a directorios (LDAP), sin necesidad de módulos adicionales. La información de grupo se devuelve en formato completo de nombre distinguido, por ejemplo:

CN=Role - CXIQ Developers,OU=Groups,DC=dev,DC=example,DC=com CN=Role - CXIQ Viewers,OU=Groups,DC=dev,DC=example,DC=com

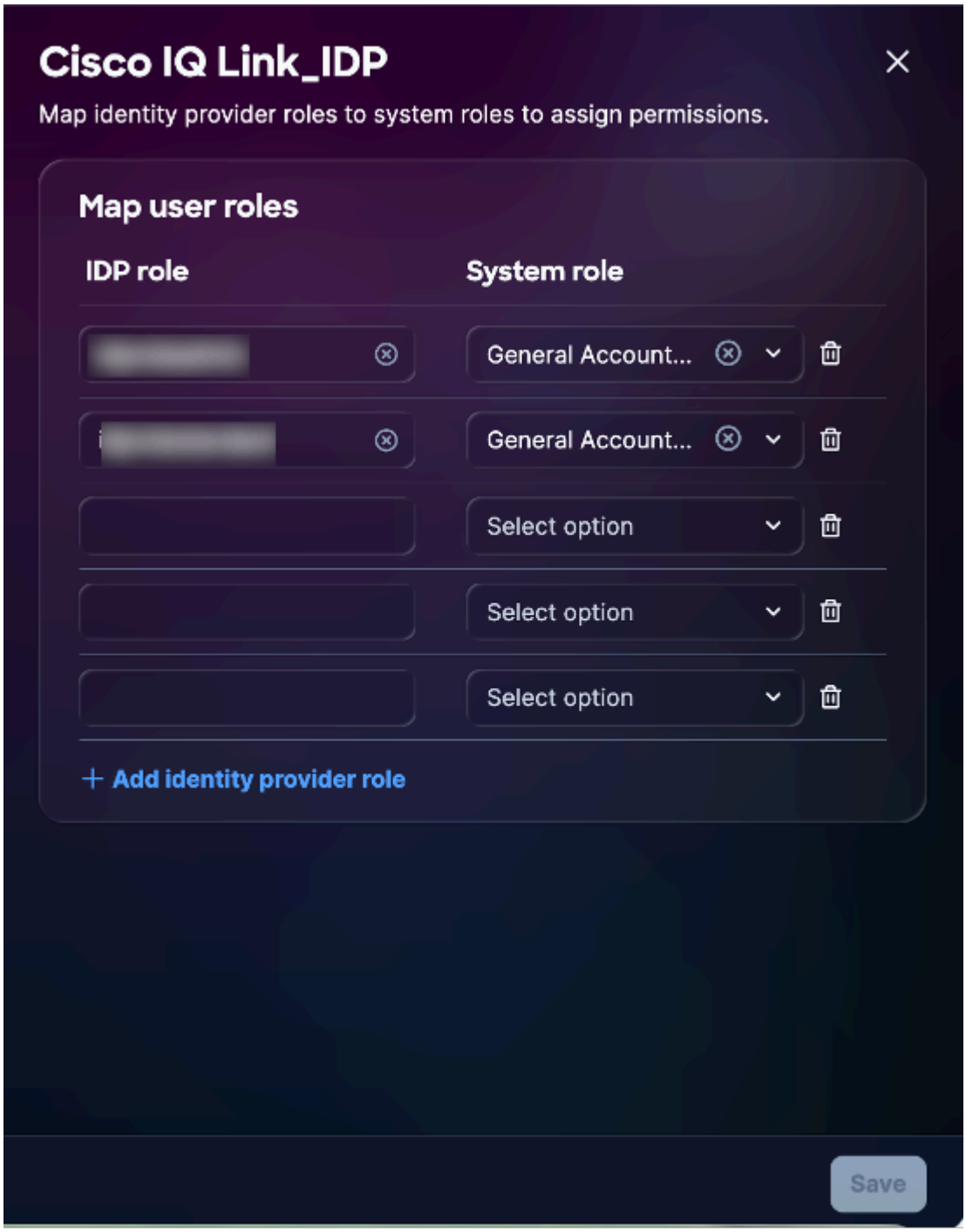
Si los grupos requeridos no aparecen en la lista, un administrador de cuentas debe crearlos en AD para que pueda completar la asignación de funciones de ADFS.

Para configurar la asignación de roles:



Asignar funciones

1. En el IDP agregado, elija el icono Más opciones > Asignar roles. Se muestra la página Asignar roles de usuario.



Asignación de funciones

2. Introduzca un rol IDP para el rol System seleccionado. Se admiten los siguientes roles del sistema:

- Administrador general de cuentas: El administrador de cuentas general tiene permisos completos para realizar todas las acciones del producto. El rol IDP (nombre analizado) es CXIQ Admins.
- Visor de cuentas general: El Visor de cuentas general tiene acceso de sólo lectura. El rol IDP (nombre analizado) es CXIQ Developers y CXIQ Viewers.

Nota: Utilice nombres analizados (por ejemplo, CXIQ Developers) y no nombres de dominio completos.

3. Haga clic en Guardar. El estado se actualiza a Correcto.

Prueba de certificado de cliente SChannel

Para comprobar que SChannel está correctamente configurado para aceptar certificados de cliente, abra una nueva ventana de PowerShell y ejecute el siguiente comando:

```
curl.exe –insecure `
    –cert “CurrentUser\YOUR-USER-CERT-THUMBPRINT>” `
    -v “https://


     :49443/adfs/ls/”
```

El resultado esperado es una respuesta HTTP (por ejemplo, una redirección o la página ADFS). Si se produce un error de intercambio de señales TLS, la conexión ha fallado.

Prueba de explorador de extremo a extremo para flujo PKI

Antes de comenzar la prueba del explorador de extremo a extremo para el flujo PKI, asegúrese de que el certificado de usuario esté instalado en la cadena de claves macOS (consulte Importación del certificado de usuario en la máquina cliente (macOS) en Configuración de la autenticación basada en certificados para obtener más información).

Para probar:

1. Navegue hasta la URL de inicio de sesión de SAML de la aplicación. ADFS presenta opciones de certificado y contraseña.
2. Elija Certificate Authentication. El explorador solicita el certificado.
3. Cargue el certificado. ADFS autentica al usuario, redirige la solicitud con una respuesta SAML y establece una nueva sesión.

Prueba de explorador de extremo a extremo para flujo de contraseña

Antes de comenzar con la prueba del navegador de extremo a extremo para el flujo de contraseñas:

1. Navegue hasta la URL de inicio de sesión de SAML de la aplicación. ADFS presenta opciones de certificado y contraseña.
2. Seleccione Password/Forms Authentication .
3. Ingrese Username.
4. Ingrese la contraseña.
5. Compruebe que el inicio de sesión se ha realizado correctamente.

Nota: Ambos flujos deben funcionar simultáneamente.

Solución de problemas de ADFS

La siguiente lista describe los problemas comunes y las posibles soluciones para ayudar a identificar y resolver rápidamente los problemas relacionados con el estado de ADFS, los errores de certificado, los errores de inicio de sesión de SSO y la configuración de SLO.

Tabla 8: Problemas de ADFS

Problema	Síntomas / Descripción	Causas / Comprobaciones / Soluciones temporales y soluciones
Grupos no extraídos	No hay roles después de iniciar sesión	• Falta la regla de reclamación: Vuelva a ejecutar las instrucciones de Configuración de reglas de reclamación de ADFS • Atributo de grupo incorrecto: Debe ser http://schemas.xmlsoap.org/cla ims/Group • El usuario no está en los grupos AD
Error de descifrado	"Error al descifrar la aserción" en los registros	Comprobar la configuración del certificado ADFS
Bucle de inicio	Atascado en el bucle de autenticación o inicio de sesión	• URL ACS no válida: Verificar: https://your-

Problema	Síntomas / Descripción	Causas / Comprobaciones / Soluciones temporales y soluciones
		fqdn/saml/acs • Discordancia de cookies: Compruebe las cookies del navegador para el dominio correcto

Comandos de diagnóstico para solucionar problemas

Para garantizar una integración correcta entre su entorno ADFS y Cisco IQ, utilice los siguientes comandos de diagnóstico. Estos comandos ayudan a comprobar la accesibilidad de los metadatos, las configuraciones de certificados y la configuración de extremos.

- Verificar accesibilidad de metadatos de ADFS: Confirma que los metadatos de federación de ADFS son accesibles al público; este es un paso crítico para establecer la confianza inicial

```
curl -k https://

    /FederationMetadata/2007-06/FederationMetadata.xml
```

- Validar el certificado de cifrado: Garantiza que el certificado de cifrado correcto esté asociado a la confianza de usuario de confianza de Cisco IQ

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object EncryptionCertificate | Format-List
```

- Revisar configuración de terminal SAML: Verifica que los terminales SAML para la confianza de Cisco IQ estén correctamente configurados y que las solicitudes de autenticación y las aserciones se enruten a las URL esperadas

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

Configuración SAML de Microsoft Entra ID para SSO

Esta sección proporciona una guía para configurar Microsoft Entra ID (Entra ID) como SAML IDP para Cisco IQ, soportando tanto la autenticación basada en contraseña como la autenticación basada en PKI/certificados (CBA).

Prerrequisitos para Configurar Entra ID SAML for SSO

- Arrendatario de ID de Microsoft Entry (por ejemplo, "ciqtestdev.onmicrosoft.com")
- Acceso a Cisco IQ con la función de administrador global o administrador de aplicaciones
- Conectividad entre Entra ID (nube) y Cisco IQ
- CA empresarial instalada o accesible (sólo se requiere para PKI)
- Punto de distribución de la lista de revocación de certificados (CRL) accesible desde Internet (sólo se requiere para PKI)

Tabla 9: Configuración del servidor de ID de entrada

Ítem	Descripción	Ejemplo:
ID de arrendatario	Identificador de arrendatario de ID de entrada	37352d8f-0ebe-4762-8161-8775ffe897cb
FQDN de Cisco IQ	Nombre de host de implementación	<YOUR-CIQ-FQDN>
ID de entidad IDP	URL del emisor de ID de entrada	https://sts.windows.net/<TENANT-ID>/
URL SSO IDP	terminal de inicio de sesión SAML	https://login.microsoftonline.com/<TENANT-ID>/saml2
Dominio de la empresa	Dominio de correo electrónico para usuarios	<YOUR-DOMAIN>

Configuración de la Aplicación SAML Entra ID

Crear una aplicación empresarial

1. Inicie sesión en el centro de administración de Microsoft Entra.
2. Navegue hasta Identidad > Aplicaciones > Aplicaciones de empresa.

3. Haga clic en Nueva aplicación > Crear su propia aplicación.
4. Introduzca el nombre (por ejemplo, "Cisco IQ").
5. Elija Integrar cualquier otra aplicación que no encuentre en la galería (No galería).
6. Haga clic en Crear.

Configuración de SAML Single Sign-On

Para configurar el inicio de sesión único SAML, debe cargar el archivo de metadatos SP. Puede obtenerla realizando los siguientes pasos desde el dispositivo virtual (VA):

1. En System Settings, elija System Configuration > Identity Providers. Se muestra la página Identity Providers.

Opciones de descarga

2. Haga clic en Descargar metadatos SP para descargar. Este archivo de metadatos SP descargado se carga para completar la configuración de inicio de sesión único de SAML.
3. Haga clic en el botón Cargar archivo de metadatos para cargar el archivo de metadatos SP. Los datos del archivo de metadatos SP se rellenarán automáticamente en la pantalla Single Sign-on basado en SAML después de una carga correcta.

También puede optar por introducir manualmente estos detalles para configurar los parámetros de inicio de sesión único. Para configurar manualmente el inicio de sesión único de SAML:

1. En la aplicación Enterprise, navegue hasta Single Sign-on y elija SAML.
2. En la sección Configuración SAML Básica, haga clic en Editar e ingrese lo siguiente:
    a. Identificador (Id. de entidad): <YOUR-CIQ-FQDN>
    b. URL de respuesta (URL de ACS): https://<YOUR-CIQ-FQDN>/saml/acs
    c. URL de inicio de sesión: https://<YOUR-CIQ-FQDN>/saml/login

d. URL de cierre de sesión: https://<YOUR-CIQ-FQDN>/saml/logout

3. Click Save.

Nota: El ID de entidad debe coincidir exactamente con lo que Cisco IQ utiliza como su ID de entidad SP. Este suele ser el FQDN de la implementación.

---

4. Para configurar atributos y reclamaciones SAML, en la sección Atributos y reclamaciones, haga clic en Editar.

5. Configure las siguientes notificaciones:

Tabla 10: Reclamaciones SAML necesarias

Afirmación	Atributo de origen	Espacio de nombres
Identificador de usuario único (NameID)	user.userprincipalname	(predeterminado)
correo electrónico	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
nombre dado	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
apellidar	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
nombre	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
grupos	user.assignedroles	(EMPTY: borra el espacio de nombres)

Nota: Para la reclamación de grupos:
- Utilice user.assignedroles como el origen, no user.groups
- El campo Espacio de nombres debe estar vacío. Esto garantiza que el nombre de atributo en la afirmación SAML sea simplemente grupos en lugar de un identificador uniforme de recursos (URI) completo
- No agregue una notificación de grupo duplicada con user.groups, ya que esto provoca conflictos

---

Configuración de funciones de aplicaciones

Los roles de aplicación se configuran en el registro de aplicación (no en la aplicación de empresa); para configurar las funciones de aplicación:

1. Navegue hasta Identidad > Aplicaciones > Registros de aplicaciones.
2. Busque y seleccione su aplicación.
3. Vaya a Funciones de aplicación > Crear función de aplicación.

4. Para cada función necesaria, configure lo siguiente:

- Nombre para mostrar: Por ejemplo, Cisco IQ Admins
- Tipos de miembros permitidos: Usuarios/grupos
- Valor: Por ejemplo, Cisco IQ Admins
- Descripción: Por ejemplo, Cisco IQ Administrators

5. Haga clic en Aplicar.

✎ Nota: Cree funciones que coincidan con los requisitos de asignación de funciones de Cisco IQ (por ejemplo, administradores CXIQ, desarrolladores CXIQ, visores CXIQ).

Los roles de aplicación se utilizan en lugar de las notificaciones de grupo por los siguientes motivos:

- Los arrendatarios solo en la nube no pueden enviar nombres para mostrar de grupo sin una licencia P1 o P2
- sAMAccountName solo funciona para grupos sincronizados desde AD en las instalaciones
- El origen de ID de grupo envía identificadores únicos universales (UUID) difíciles de asignar
- Los roles de aplicación envían valores de cadena exactos que coinciden con las expectativas de rol de Cisco IQ

Asignación de usuarios a funciones de aplicaciones

Para asignar usuarios a funciones de aplicación:

1. Vuelva a Aplicación empresarial > Usuarios y grupos.
2. Haga clic en Agregar usuario/grupo.
3. Elija el usuario o usuarios y asigne el rol de aplicación correspondiente.
4. Haga clic en Asignar. Los valores de rol se muestran como cadenas legibles en el atributo de grupos de aserción SAML.

Descarga de metadatos y certificados de IDP

Para descargar metadatos y certificados de IDP:

1. Desde la aplicación Enterprise, vaya a la sección Single Sign-on > SAML Signing Certificate.
2. Descargar XML de metadatos de federación (guardar como entra-id-metadata.xml).

   O bien

   Descargue el certificado (Base64) para la entrada manual del certificado.
3. Tome nota de los siguientes valores de la sección Configuración:

- URL de inicio de sesión (URL SSO IDP)
- Azure AD Identifier (ID de entidad IDP)
- URL de desconexión (URL de IDP SLO)

Nota: Dado que el ID de entrada rota los certificados de firma periódicamente, debe volver a descargar los metadatos y cargarlos en el dispositivo virtual cada vez que cambie el certificado activo para garantizar un servicio SSO ininterrumpido.

Adición de IDP de ID de entrada

Nota: Las rutas APISIX para SAML se crean automáticamente cuando se agrega un IDP en Cisco IQ, lo que elimina la necesidad de una configuración de ruta manual.

Para agregar el ID de entrada IDP:

1. Inicie sesión en VA como administrador de cuenta.
2. Vaya a System Settings > System Configuration > Identity Providers.
3. Haga clic en Agregar proveedor de identidad.
4. Introduzca el nombre del IDP (por ejemplo, "ID de entrada").
5. Ingrese el Dominio(s) (por ejemplo, "ciqtestdev.onmicrosoft.com" o el dominio de su compañía).
6. (Opcionalmente) Active el botón de alternancia Enable single logout, si es necesario.
7. Arrastre y suelte o cargue el archivo entra-id-metadata.xml obtenido de Entra ID en el campo Upload IDP Metadata.
8. Click Save.

Nota: El estado sigue siendo "Incompleto" hasta que finalice la asignación de roles; ésta es la conducta esperada.

Configuración de mapeo de roles

Para configurar la asignación de funciones:

1. En el IDP agregado, elija el icono Más opciones> Asignar roles. Se muestra la página Asignar roles de usuario.
2. Introduzca un rol IDP para cada rol del sistema. Se admiten los siguientes roles del sistema:

Tabla 11: Funciones del sistema

Función del sistema	Función IDP (App Role Value)	Descripción
Administrador general de cuentas	Administradores de CXIQ	Permisos completos para todas las acciones
Visor de cuentas general	Desarrolladores de CXIQ	Acceso de sólo lectura
Visor de cuentas general	Visores CXIQ	Acceso de sólo lectura

Nota: Utilice las cadenas App Role Value exactamente como se configuraron en Entra ID (consulte Configuración de Roles de Aplicación en Configuración de Aplicación SAML de Entra ID para obtener más detalles).

3. Haga clic en Guardar. El estado se actualiza a Correcto.

Verificación del Flujo SAML (Autenticación de Contraseña)

Para verificar el flujo SAML:

1. Abra un navegador en modo Incógnito o Privado.
2. Vaya a https://<YOUR-CIQ-FQDN>/saml/login.
3. Compruebe que se le redirige a la página de inicio de sesión de Microsoft.
4. Realice la autenticación con sus credenciales (y MFA si se ha configurado).
5. Después de la autenticación, verifique que se le redireccione nuevamente a /saml/acs y que

se muestre la aplicación Cisco IQ.

6. Verifique la extracción del grupo ejecutando el siguiente comando:

```
kubectl -ncxue logs deployment/apisix –since=5m | grep -E “authentication successful|Extracted group|To
```

Resultado esperado

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 1
```

Configuración de la autenticación basada en certificados

En esta sección se describe cómo agregar CBA junto con las contraseñas. Esta sección se puede omitir si la autenticación de solo contraseña es suficiente.

Prerrequisitos de CBA

- Windows Server con Servicios de certificados de AD (CS) con CA empresarial configurada (por ejemplo, "DEV-ADCS-CA")
- Acceso de administrador de PowerShell en el servidor de la CA
- El UPN del certificado debe coincidir con el ID de entrada userPrincipalName
- El punto de distribución CRL debe estar accesible desde Internet

Creación de una plantilla de certificado en AD CS

1. Abra certtmpl.msc en el servidor de la CA.
2. Duplique la plantilla User y asígnele el nombre "EntraUserCert".
3. Configuración de la plantilla:

- General: Nombre para mostrar EntraUserCert, validez 1-2 años
- Gestión de solicitudes: Objetivo = Firma y cifrado

- Nombre del sujeto: Seleccione Aprovisionar en la solicitud
- Extensiones: Las políticas de aplicación deben incluir autenticación de cliente (1.3.6.1.5.5.7.3.2)
- Seguridad: Conceder permisos de lectura e inscripción a usuarios autenticados

4. Publique la plantilla mediante el siguiente comando:

```
Add-CATemplate -Name “EntraUserCert” -Force
```

Solicitud y emisión de un certificado de usuario

1. Cree un archivo de configuración de certificados (INF) (por ejemplo, C:-cert.inf) mediante el siguiente script de PowerShell:

```
@”
[Version]
Signature = “`$Windows NT`$”

[NewRequest]
Subject = “CN=



     ”
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10

[RequestAttributes]
CertificateTemplate = EntraUserCert

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2

[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=



      &”
_continue_ = “email=
```

```
      ”
“@ | Out-File -FilePath C:-cert.inf -Encoding ASCII
```

2. Sustituya **<**USER-UPN**>** por su ID de usuario UPN (por ejemplo, user@ciqtestdev.onmicrosoft.com).

3. Para generar el certificado, ejecute el siguiente comando:

```
certreq -new C:-cert.inf C:-cert.csr
```

4. Para enviar la solicitud a la CA, ejecute el siguiente comando:

```
certreq -submit -config “

     \CA-NAME>” C:-cert.csr C:-cert.cer
```

5. Para instalar el certificado en la CA, ejecute el siguiente comando:

```
certreq -accept C:-cert.cer
```

Exportación de certificados

- Para exportar el certificado de usuario como un archivo PFX (para el cliente), ejecute la siguiente secuencia de comandos:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like “*

     *” }
```

```
$password = ConvertTo-SecureString -String “

      ” -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password
```

- Para exportar el certificado raíz de la CA (para el ID de entrada), ejecute el siguiente script:

```
Get-ChildItem Cert:| Where-Object { $_.Subject -like “*

     *” } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

Importación del certificado de usuario en la máquina cliente (macOS)

- Para importar el certificado de usuario (PFX), ejecute el siguiente comando:

```
security import /path/to/entra-cert.pfx -k ~/Library/Keychains/login.keychain-db -P “

     ”
```

- Para importar el certificado raíz de la CA, ejecute el siguiente comando:

```
security import /path/to/ca-root.cer -k ~/Library/Keychains/login.keychain-db
```

- Para establecer el certificado de la CA en Confiar siempre en el Acceso mediante Cadena de Llave:

    1. Abra Acceso mediante llavero.

2. Busque el certificado de la CA y haga clic en Obtener información.

3. En Confianza, establezca en "Confiar siempre".

Nota: Después de la importación, salga del explorador y vuelva a abrirlo para que se reconozca el certificado.

Carga del certificado raíz de la CA en la ID de entrada

1. Inicie sesión en el centro de administración de Microsoft Entra.
2. Navegue hasta Protección > Seguridad > Autoridades de certificados.
3. Haga clic en Upload y seleccione el archivo ca-root.cer.
4. Marcarlo como certificado de CA raíz.
5. Introduzca la URL del punto de distribución de CRL (debe ser accesible públicamente).

Habilitación de CBA en Métodos de Autenticación de Entra ID

1. Navegue hasta Protección > Métodos de autenticación > Políticas.
2. Haga clic en Autenticación basada en certificados para configurar.
3. Active CBA y agregue los usuarios o grupos de destino.
4. En Configurar, establezca el nivel de protección en Autenticación de factor único.

Configuración de Username Binding

En la configuración de CBA, vaya a la pestaña Enlace de nombre de usuario y establezca el siguiente enlace:

- Campo de certificado: NombrePrincipal
- Atributo de usuario: userPrincipalName

De este modo, se asigna el UPN en el nombre alternativo de asunto del certificado al usuario de ID de entrada.

Verificación del flujo de CBA

1. Abra un navegador en modo Incógnito o Privado.
2. Vaya a https://<YOUR-CIQ-FQDN>/saml/login.
3. En la página de inicio de sesión de Microsoft, introduzca el correo electrónico del usuario y haga clic en Next (Siguiente).
4. Elija Utilizar un certificado o una tarjeta inteligente (o puede que se solicite automáticamente).
5. Elija el certificado de usuario aplicable cuando el explorador solicite la selección de certificados.
6. Verifique que Entra ID valida el certificado, redirige con una respuesta SAML y crea una sesión.

Nota: Asegúrese de seleccionar el certificado de cliente correcto. La selección de un certificado incorrecto (por ejemplo, un certificado de otro usuario o un certificado caducado) provoca un error de autenticación.

Resolución de problemas de ID entrante

La siguiente lista describe los problemas comunes y las posibles soluciones para ayudar a identificar y resolver rápidamente los problemas relacionados con la configuración SAML de Entra ID.

Tabla 12: Resolución de problemas

Problema	Causa	Corregir
Respuesta SAML no válida; falta correo electrónico	La afirmación SAML no tiene ningún atributo NameID o email	Verifique la configuración de notificaciones de ID de entrada (vea Configuración de SAML Single Sign-On bajo Configuración de Aplicación SAML de ID de entrada para obtener más detalles). Compruebe que el usuario tiene el atributo de correo rellenado.
Total de grupos extraídos: 0	Reclamaciones de grupo no configuradas o origen incorrecto	Utilice user.assignedroles como origen. Asegúrese de que el usuario esté asignado a un rol de aplicación (consulte Asignación de usuarios a roles de aplicación en Configuración de la aplicación SAML Entra ID para obtener más detalles).
Reclamaciones de grupo	Tanto user.groups	Quite la notificación user.groups. Conservar

Problema	Causa	Corregir
duplicadas	como user.assignedroles activos	sólo user.assignedroles.
Grupos que se muestran como UUID	El atributo de origen es "Group ID"	Utilice el enfoque de los roles de la aplicación (consulte Configuración de los roles de la aplicación en Configuración de la Aplicación SAML de Entra ID para obtener más detalles).
El nombre del atributo muestra un URI largo	El campo Espacio de nombres no está vacío	Borre el campo Espacio de nombres en la configuración de notificación de grupos.
Firma SAML no válida	Certificado IdP girado o no coincide	Vuelva a descargar los metadatos de la ID de entrada y vuelva a cargarlos en Cisco IQ.
ADSTS500191	CRL no accesible desde Internet	Publique la CRL en una URL de acceso público o utilice el enfoque de CA autofirmada (consulte Solución alternativa de CRL para entornos de laboratorio para obtener más detalles).
Certificado no solicitado	El certificado no está en la cadena de claves, la CA no es de confianza en el cliente o el CBA no está habilitado	Verifique que el certificado de usuario se importe en macOS Keychain Access (vea Importación del Certificado de Usuario en la Máquina Cliente (macOS) bajoConfiguración de la Autenticación Basada en Certificados para obtener más detalles), CBA se habilita en Entra ID con las configuraciones requeridas (vea Habilitación de CBA en Métodos de Autenticación de Id. Inicial bajo Configuración de la Autenticación Basada en Certificados para obtener más detalles) y Chrome se reinicia para aplicar los cambios.
Afirmación SAML caducada	Diferencia de reloj entre sistemas	Aumente clock_skew_seconds en plugin config (valor predeterminado 300, use 30000 para lab).
Estado "Incompleto" en VA	Asignación de roles aún no configurada	Completar la asignación de funciones (consulte Configuración de la asignación de funciones para obtener más detalles).

Solución alternativa de CRL para problemas de disponibilidad

Si el punto de distribución de CRL de su CA no está accesible desde Internet (lo habitual en las configuraciones de laboratorio), utilice una CA autofirmada sin requisitos de CRL:

```
powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject “CN=CIQ-Test-CA” `
-CertStoreLocation “Cert:” `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @(“2.5.29.19={text}ca=TRUE”)

# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
    -Subject “CN=



     ” `
    -CertStoreLocation “Cert:” `
    -Signer $rootCA `
    -KeyUsage DigitalSignature `
    -KeyLength 2048 `
    -NotAfter (Get-Date).AddYears(2) `
    -TextExtension @(
        “2.5.29.37={text}1.3.6.1.5.5.7.3.2”,
        “2.5.29.17={text}upn=



      &email=



       ”
)
```

Cargue sólo el certificado de CA raíz en la ID de entrada. Dado que se firma automáticamente sin CDP, el ID de entrada no intenta la validación de CRL.

Lista de comprobación de configuración completa

En esta sección se describe una lista de comprobación de configuración completa para configurar el AV con la aplicación SAML Microsoft Entra ID y CBA opcional.

Configuración de aplicación SAML de ID de entrada

- Crear aplicación empresarial (no de galería) en Id. de entrada

- Configurar la configuración básica de SAML introduciendo manualmente los metadatos SP
- Configurar atributos y reclamaciones (incluidos correo electrónico, nombre y grupos con user.assignedroles)
- Crear funciones de aplicaciones en el registro de aplicaciones
- Asignar usuarios a funciones de aplicación
- Descargar XML de metadatos de federación

Configuración de Cisco IQ

- Agregue el proveedor de identidad en Cisco IQ cargando los metadatos de la ID de entrada
- Configuración de la asignación de funciones para asignar valores de funciones de aplicaciones a funciones del sistema Cisco IQ
- Verificar que el inicio de sesión basado en contraseña funcione de extremo a extremo
- Comprobar que los grupos se extraen correctamente en los registros

Autenticación basada en certificados (opcional)

- Crear plantilla de certificado en AD CS con EKU de autenticación de cliente
- Emitir certificado de usuario con UPN que coincida con el usuario de ID de entrada
- Exportar certificado de usuario como PFX e instalarlo en el equipo cliente
- Confiar en el certificado de la CA en el equipo cliente
- Cargue el certificado raíz de la CA en el ID de entrada en Protección > Autoridades de certificados
- Habilitar CBA en métodos de autenticación
- Configurar enlace de nombre de usuario (PrincipalName y userPrincipalName)
- Verificar que el inicio de sesión de CBA funciona de extremo a extremo

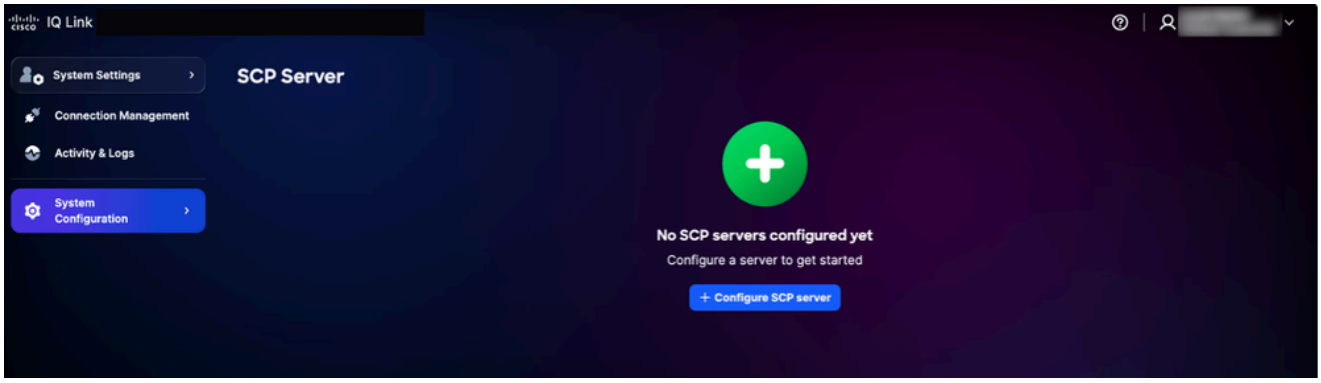
Adición de servidores SCP

Este servidor de protocolo de copia segura (SCP) es un requisito previo para importar archivos de actualización que son esenciales para agregar, actualizar o aplicar parches a la instalación de

Cisco IQ.

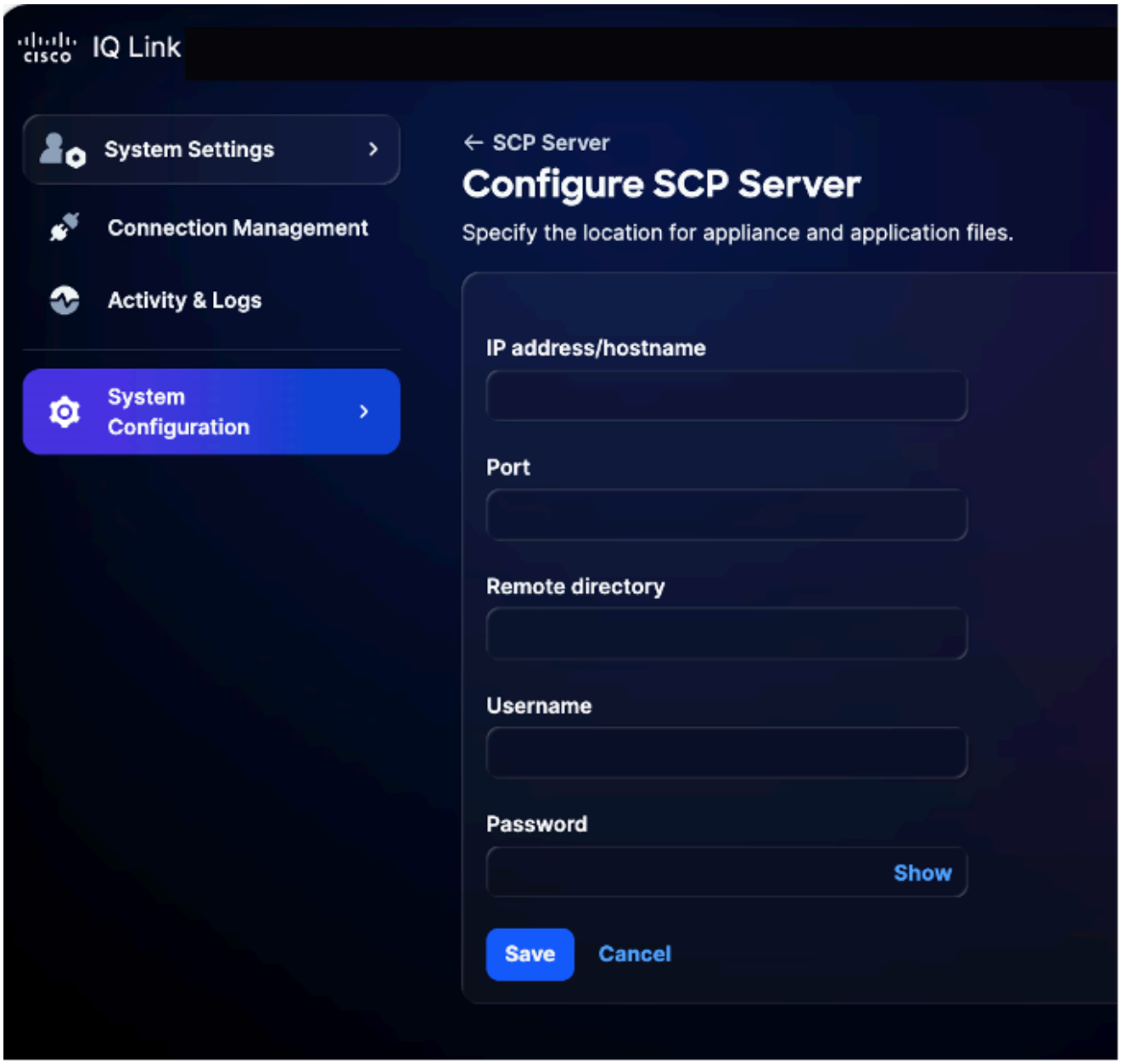
Para agregar un servidor SCP:

1. En System Settings, elija System Configuration > SCP Server. Se muestra la página SCP Server.



Página de inicio del servidor SCP

2. Haga clic en Configure SCP Server.



Configuración del servidor SCP

3. Introduzca la dirección IP/nombre de host.
4. Introduzca un número de puerto.
5. Introduzca el directorio remoto.
6. Introduzca un nombre de usuario.
7. Ingrese una contraseña.
8. Click Save. Aparecerá una confirmación.

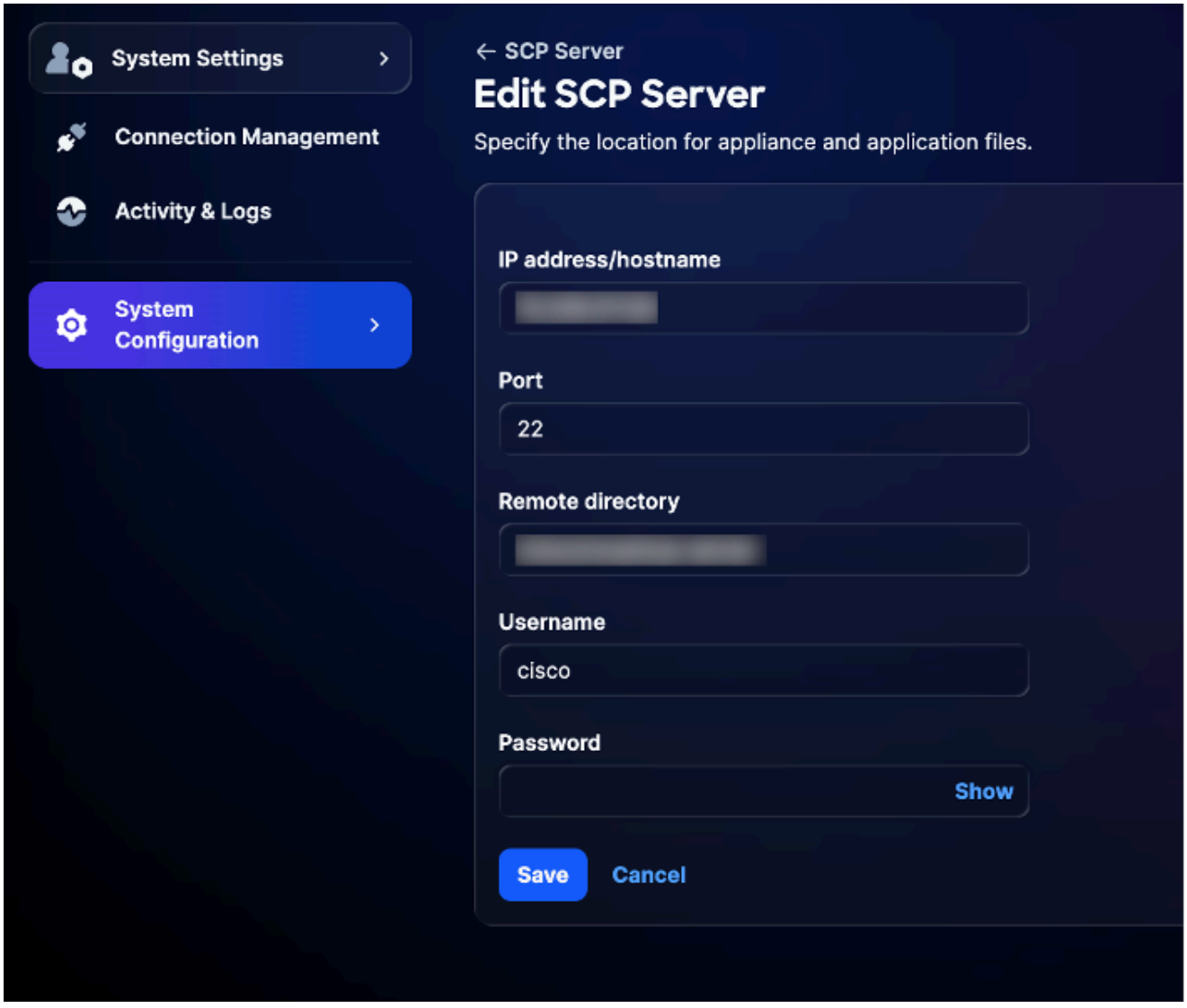
Edición de servidores SCP existentes

Para editar un servidor SCP existente:

1. Vaya a la página SCP Server.

Servidor SCP

2. Haga clic en Editar para el servidor SCP existente que desee.



Edición del servidor SCP

3. Modifique los detalles según sea necesario.

4. Click Save.

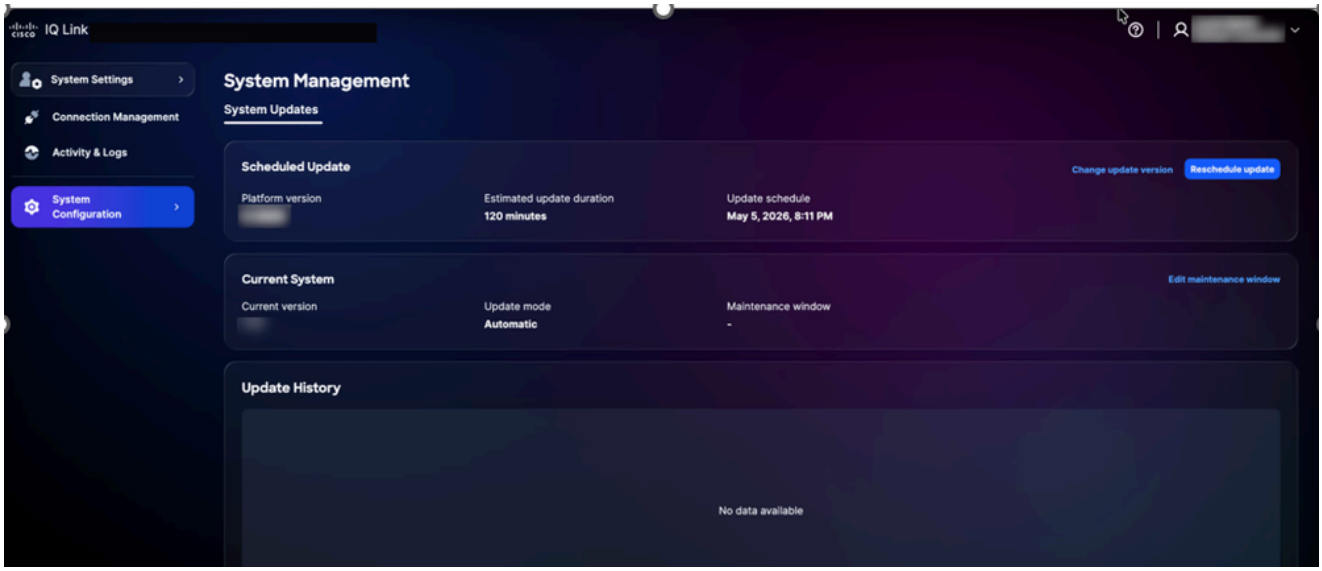
Administración del sistema

Puede actualizar a la última versión de Cisco IQ Link a través de la interfaz de usuario. También puede verificar desde la página Cisco IQ Data Connectors.

Reprogramación de actualización del sistema

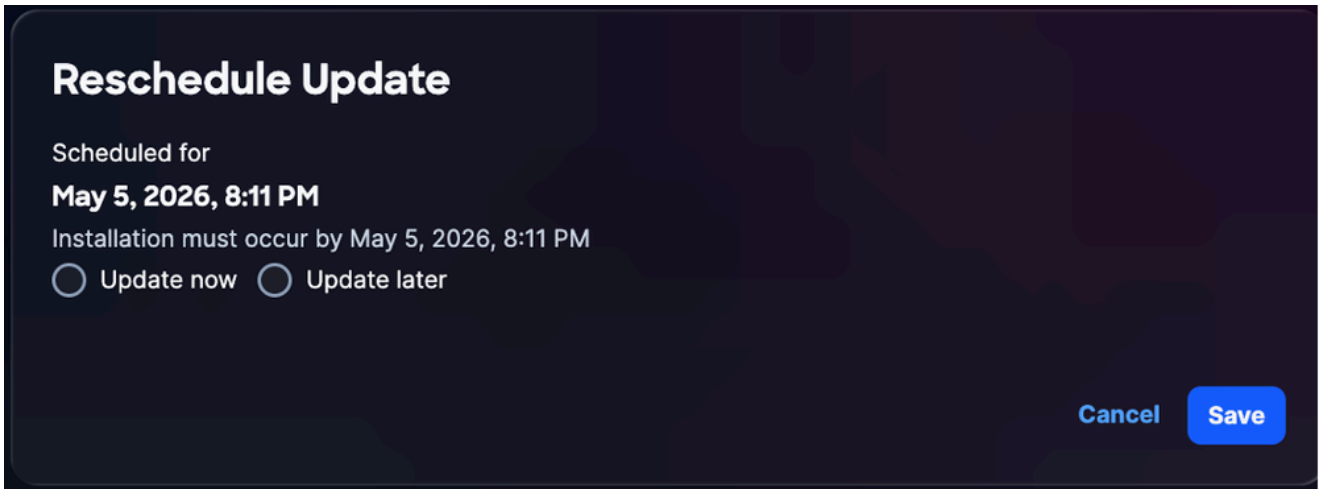
Para reprogramar la actualización del sistema:

1. En Administración, elija Configuración del sistema > Administración del sistema. Se muestra la página Administración del sistema. Esta página muestra la versión del sistema que se está ejecutando actualmente; si no se ha configurado ninguna actualización, la sección Historial de actualizaciones está vacía.



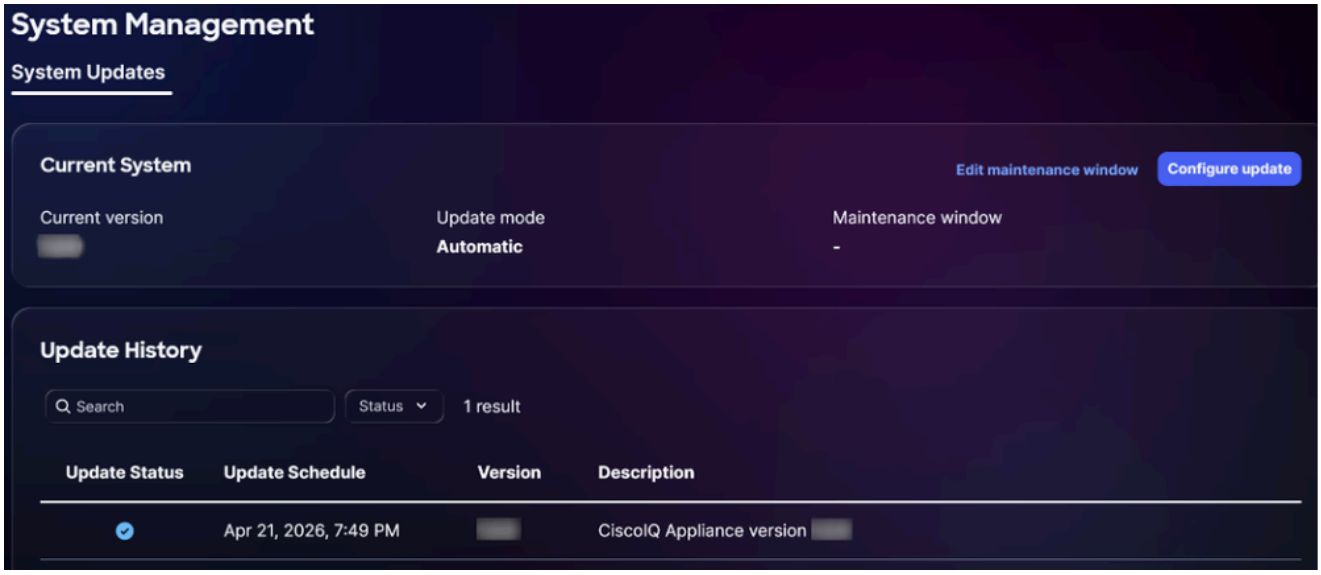
Actualización del sistema

2. Haga clic en Reprogramar actualización.



Reprogramar actualización

3. Elija el botón de opción Update Now para la reprogramación inmediata o el botón de opción Update Later para programar otra hora.
4. Click Save. Aparecerá una confirmación y se le redirigirá a la página de inicio de Actualización del sistema.

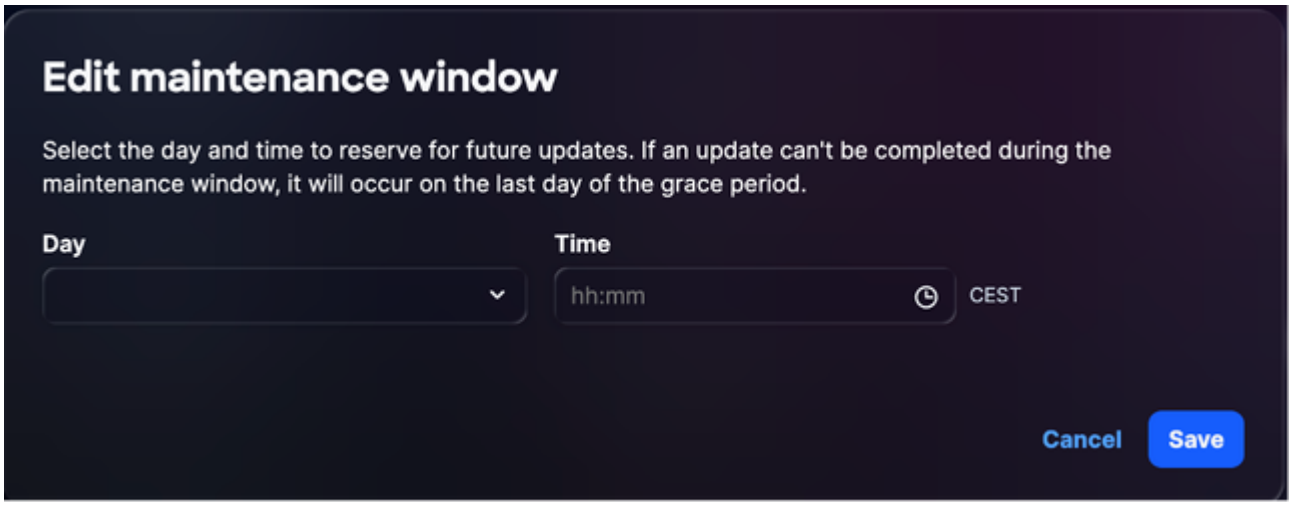


Actualización correcta

Edición de programaciones de actualización del sistema

Puede crear una programación personalizada para las actualizaciones del sistema. Si se configura una programación personalizada, las actualizaciones se realizan en fechas definidas por el usuario, siempre que permanezcan dentro del período de gracia máximo. Para crear una programación de actualización del sistema:

1. En la sección Sistema actual de la página Administración del sistema, haga clic en Editar ventana de mantenimiento.



Editar ventana de mantenimiento

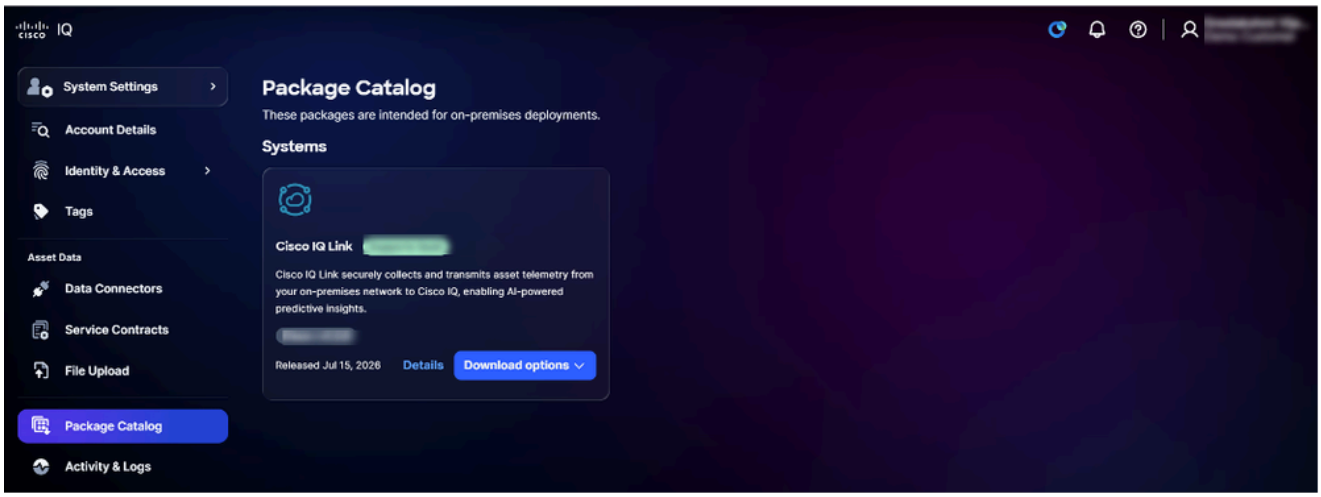
2. Elija una opción de las listas desplegables Día y Hora.
3. Haga clic en Guardar. La ventana de mantenimiento se ha programado correctamente. La actualización se desencadena según la programación mostrada.

Nota:
- Si no se configura ninguna programación de actualización, el sistema establece de forma predeterminada períodos de gracia de dos (2) semanas para las actualizaciones sin reinicio y de cuatro (4) semanas para las actualizaciones que requieren reinicio. Después de estos períodos de gracia, las actualizaciones se deben realizar manualmente.
- En caso de fallo de actualización, el sistema realiza hasta dos (2) reintentos automáticos. Se ha programado un tercer intento, pero es necesario iniciarlo manualmente.

Actualización manual del sistema

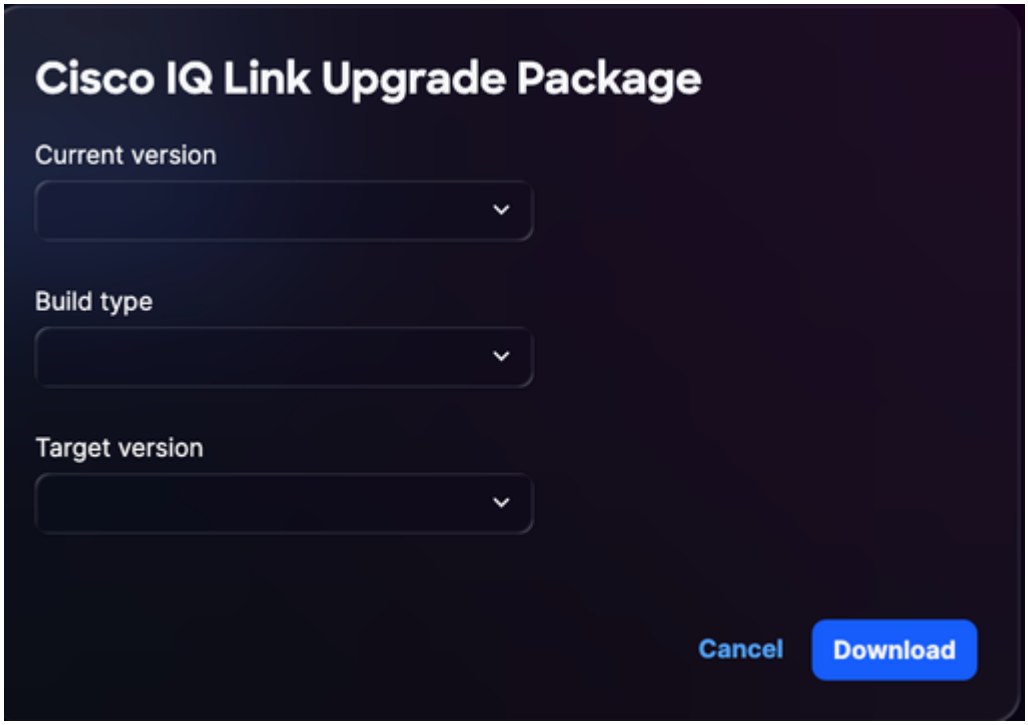
En situaciones en las que la distribución automática de Cisco IQ SaaS no está disponible o se ha retrasado, puede realizar manualmente una actualización del sistema descargando el paquete de actualización directamente desde Cisco IQ SaaS. Para actualizar manualmente el sistema:

1. Inicie sesión en Cisco IQ SaaS y elija Home > System Settings > Package Catalog.



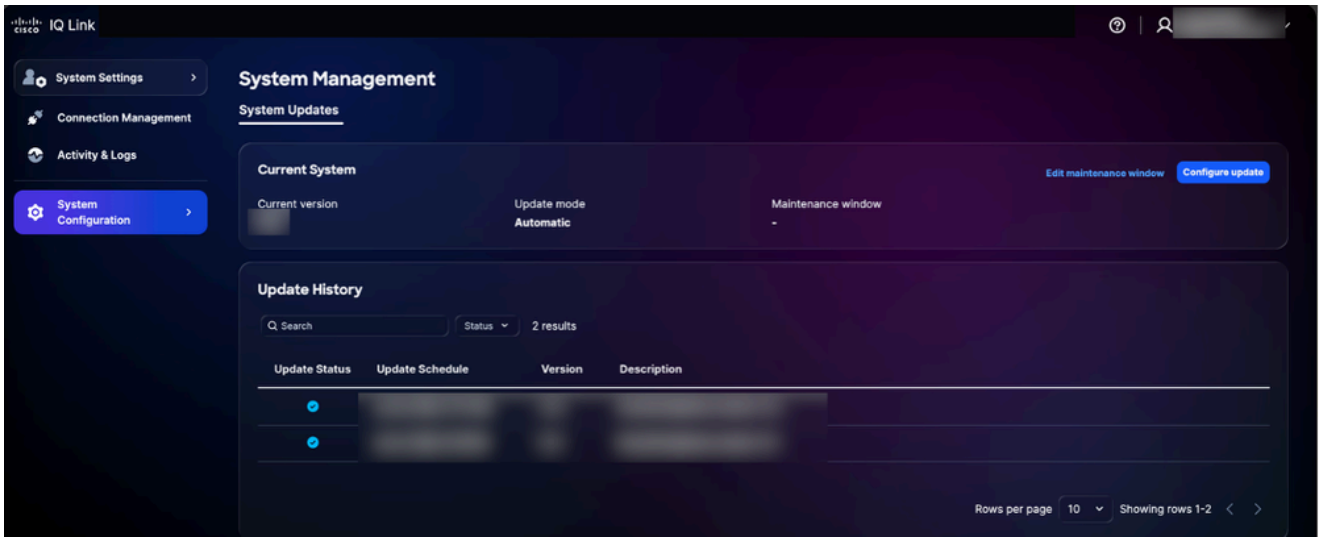
Catálogo de paquetes

2. En la sección Cisco IQ Link, haga clic en Opciones de descarga > Paquetes de actualización.



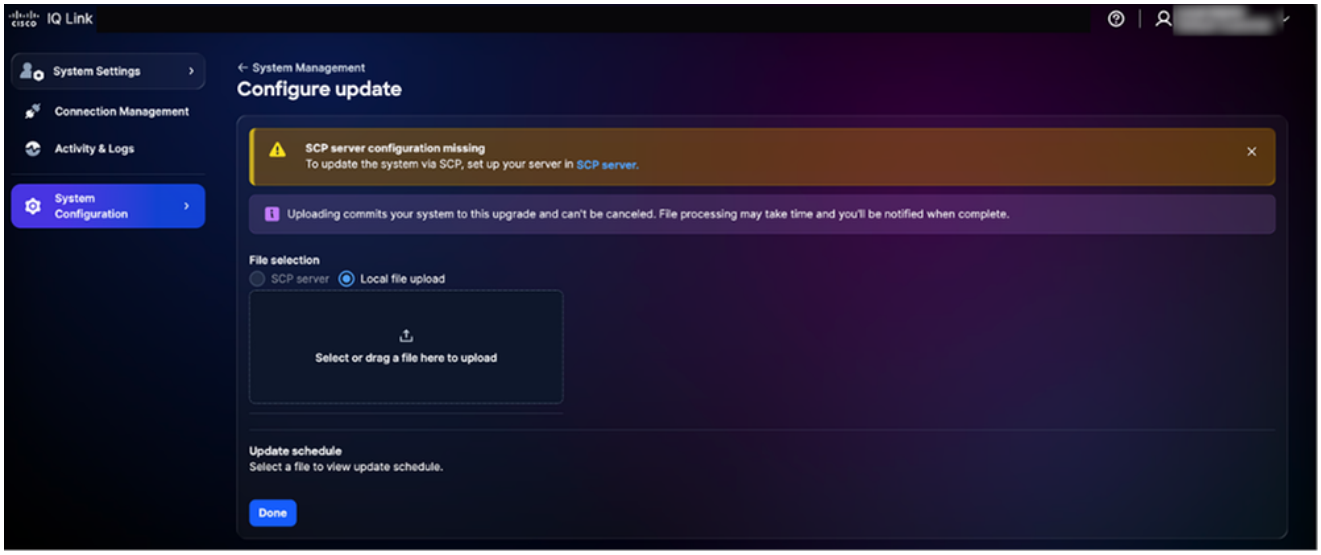
Paquete de actualización

3. Elija la versión actual en la lista desplegable.
4. Elija el tipo de generación en la lista desplegable.
5. Elija la versión de destino en la lista desplegable.
6. Haga clic en Descarga. Se descarga el paquete de actualización.
7. Navegue hasta Cisco IQ Link.
8. En System Settings, elija System Configuration > System Management.



Configurar actualización

9. Haga clic en Configurar actualización.



Carga de archivos locales

10. Haga clic en el botón de opción Carga de archivo local.

11. Seleccione o arrastre el archivo de paquete de actualización descargado al campo de carga.
12. Haga clic en Done (Listo). Aparecerá un mensaje de confirmación una vez que el sistema se haya actualizado correctamente.

Configuración de certificados SSL

Un certificado autofirmado predeterminado está preinstalado y habilitado en Cisco IQ, pero puede cargar certificados SSL personalizados. Cuando se habilita un certificado SSL personalizado, se utiliza para conexiones HTTPS; si el certificado está deshabilitado o eliminado, el sistema vuelve automáticamente al certificado predeterminado.

El certificado SSL predeterminado no se puede editar ni eliminar.

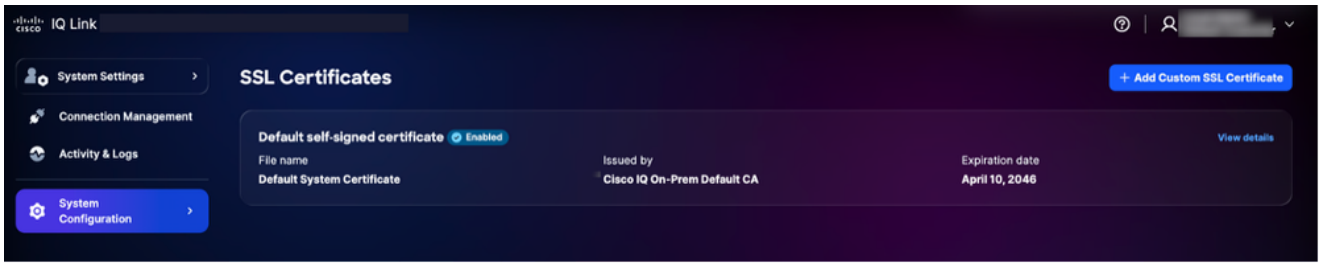
Nota: El certificado debe tener al menos 90 días de validez restantes. Se considera que un certificado está "a punto de caducar" cuando le quedan menos de 90 días para su caducidad.

Después de agregar, editar o eliminar un certificado SSL, debe cargar el nuevo certificado SSL como se describe en Single Logout Configuration para Okta IDP o ADFS IDP.

Agregar certificado SSL personalizado

Para agregar un certificado SSL personalizado:

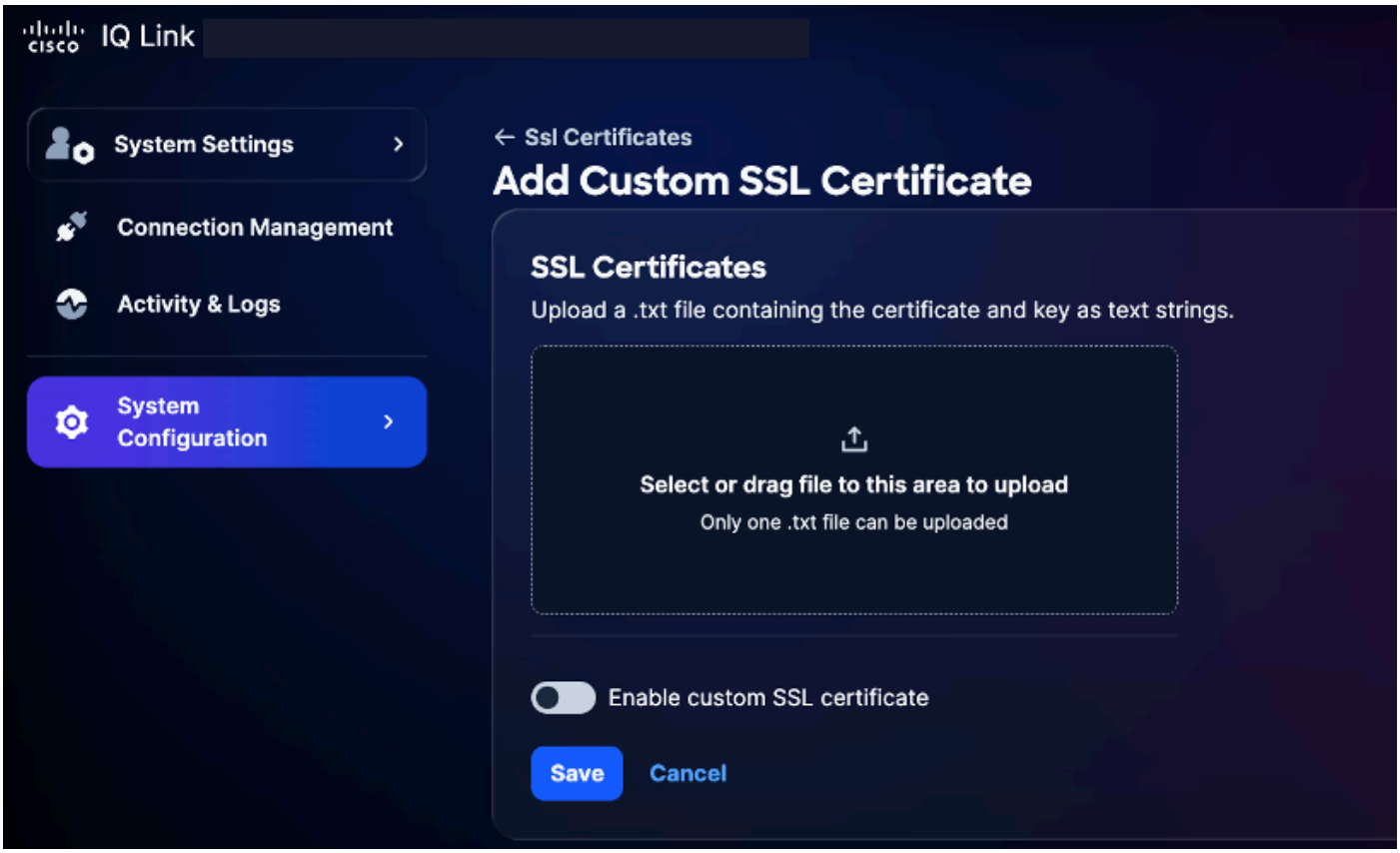
1. En System Settings, elija System Configuration > SSL Certificates. Se muestra la página SSL Certificates, que enumera todos los certificados SSL del sistema.



Agregando certificado SSL

2. Haga clic en Agregar certificado SSL personalizado.

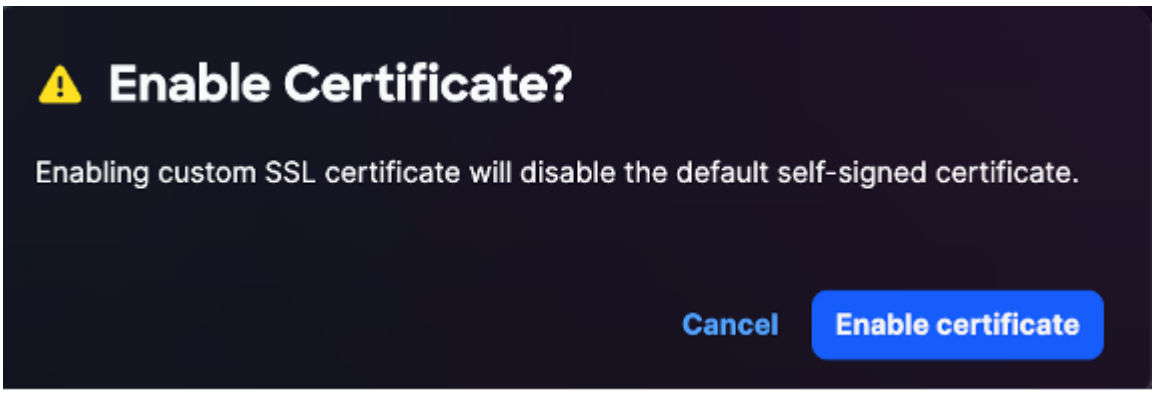
Notas:
- Cargue un archivo .txt que incluya el certificado y la clave codificados en Privacy-Enhanced Mail como cadenas de texto
- Sólo se puede cargar un archivo .txt a la vez
- El archivo debe contener el certificado y la clave privada



Cargar certificado SSL

3. Arrastre y suelte o cargue el certificado SSL personalizado en el campo Certificado SSL.

4. Active el botón de alternancia Enable custom SSL certificate.



Editar certificado SSL

Nota: Mantenga la tecla de apagado si desea cargar el certificado sin activarlo inmediatamente.

5. Haga clic en Habilitar certificado.

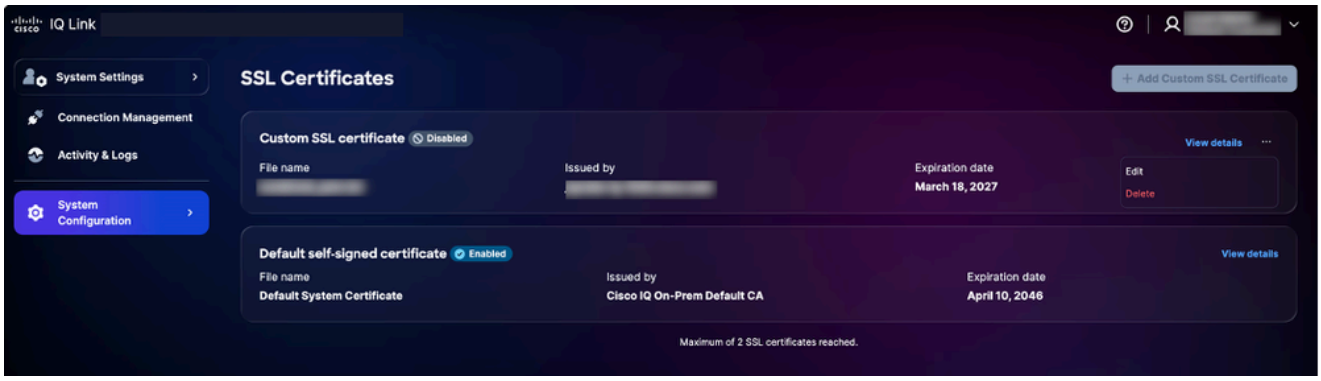
6. Haga clic en Guardar.

El certificado SSL personalizado está activado y activo. El certificado predeterminado del sistema se desactiva automáticamente.

Edición de certificados SSL personalizados

Puede editar el certificado SSL personalizado para cargar un nuevo certificado o para deshabilitar el certificado habilitado actualmente. Para editar:

1. Vaya al certificado SSL personalizado que desee.



Editar certificado SSL

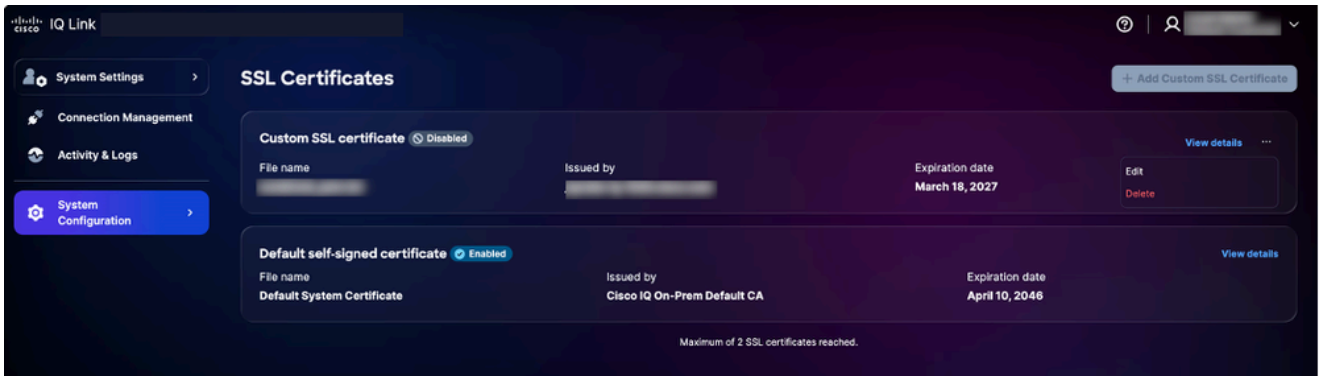
2. Elija el icono Más opciones > Editar. Se muestra la página Editar Certificado SSL.
3. Edite los detalles del certificado según sea necesario.
4. Click Save.

Eliminación de certificados SSL personalizados

Advertencia: Un certificado SSL personalizado se puede eliminar en cualquier momento, pero es una acción irreversible; puede cargar un nuevo certificado personalizado en cualquier momento después de la eliminación.

Para eliminar:

1. Vaya al certificado SSL personalizado que desee.



Eliminar certificado SSL

2. Elija el icono Más opciones > Eliminar.
3. Haga clic en Eliminar certificado. El certificado personalizado se elimina y el certificado predeterminado se reactiva automáticamente.

Configuración del servidor Syslog

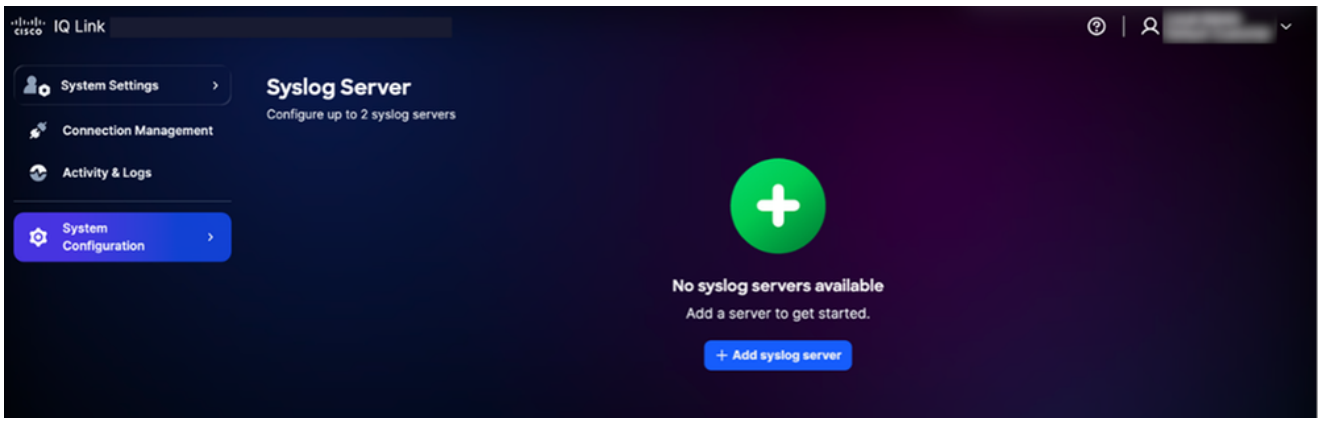
Los usuarios con la función de administrador de cuentas pueden configurar servidores syslog externos para exportar registros del sistema. Se pueden configurar hasta dos (2) servidores syslog.

Nota: El servidor Syslog se debe especificar como una dirección IP, no un FQDN.

Agregar servidores Syslog

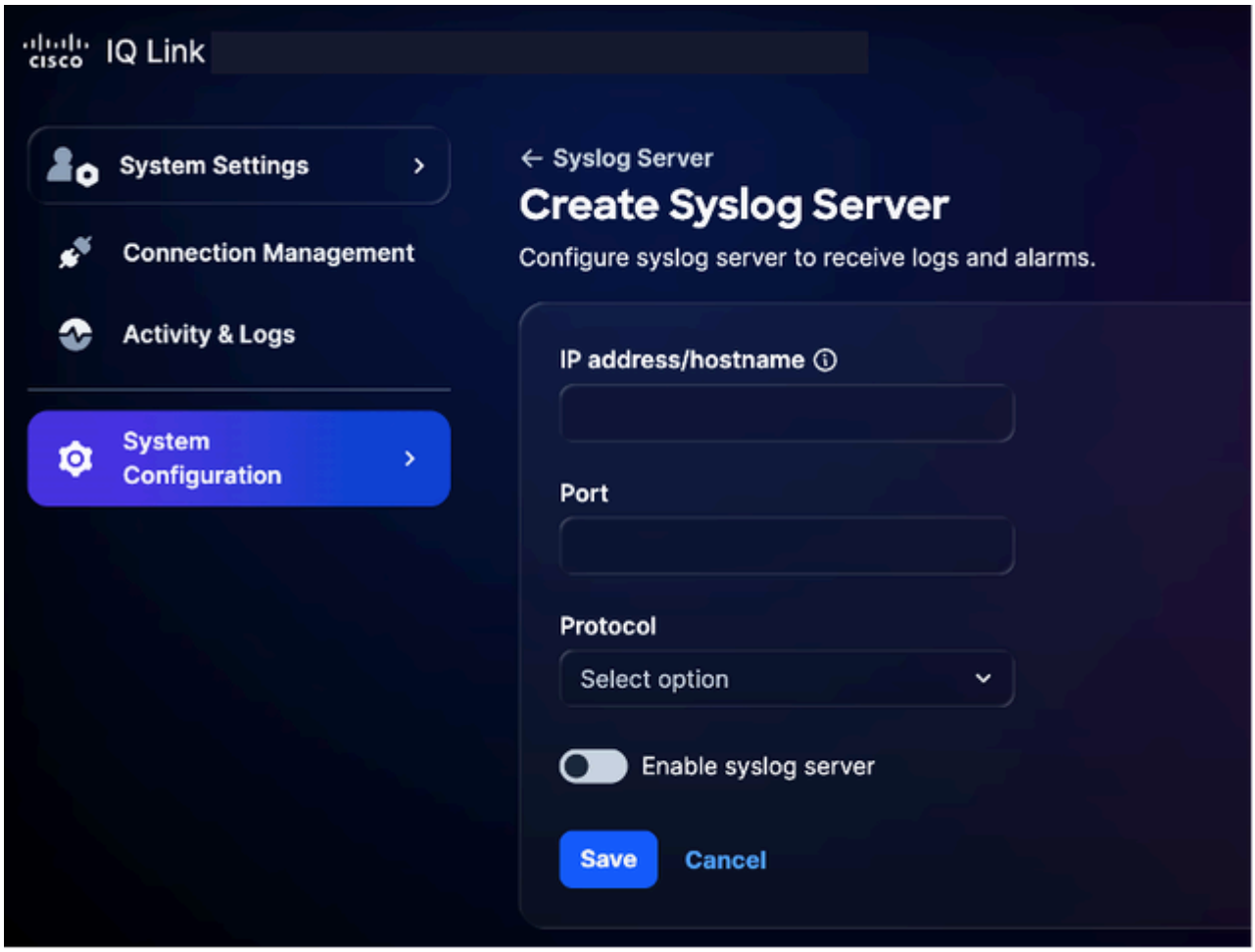
Para agregar un servidor syslog:

1. En System Settings, elija System Configuration > Syslog Server. Se muestra la página Syslog Server.



Agregar servidor Syslog

2. Haga clic en Add syslog server. Se muestra la página Create Syslog Server.



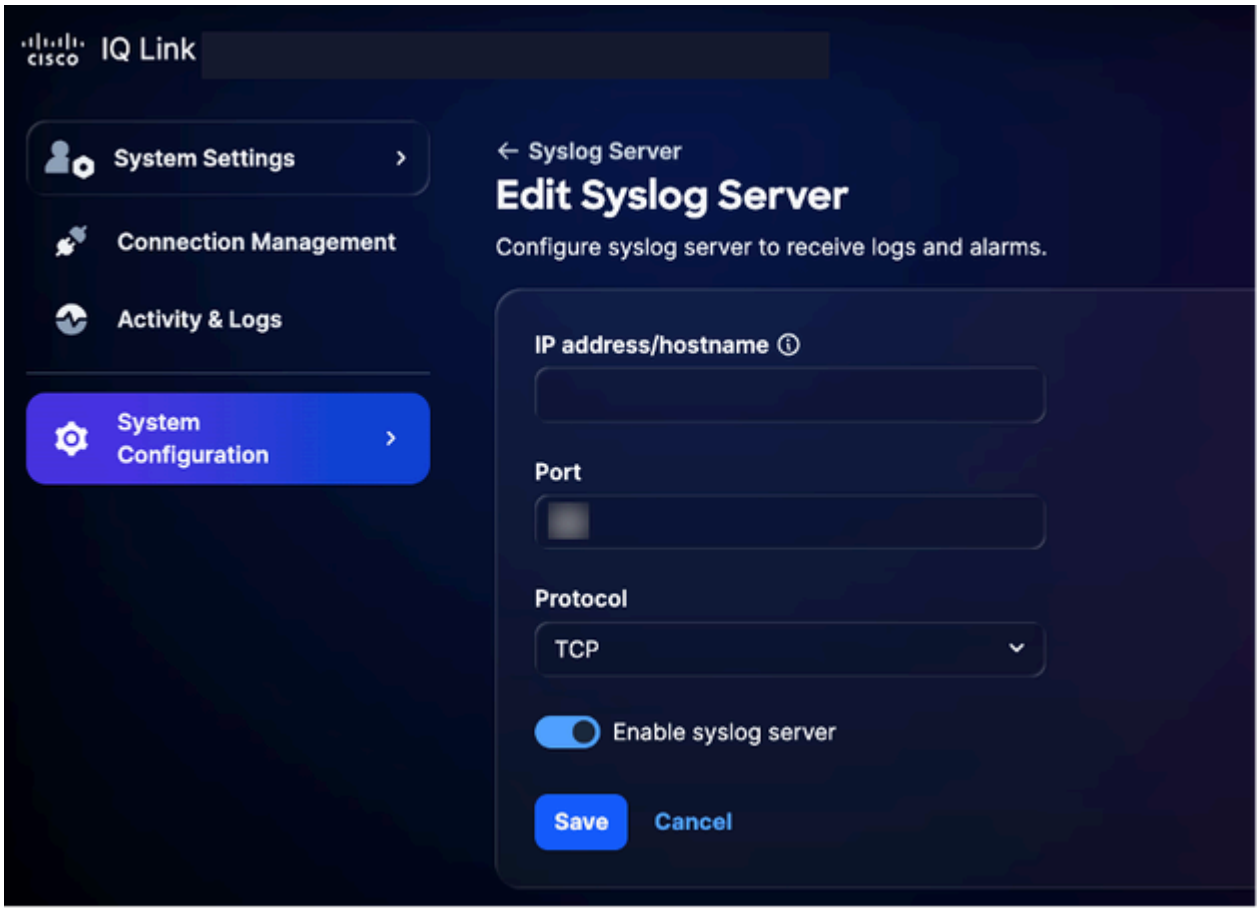
Crear servidor Syslog

3. Introduzca la dirección IP/nombre de host.
4. Introduzca un número de puerto.
5. Seleccione el protocolo aplicable en la lista desplegable Protocol (por ejemplo, UDP o TCP).
6. Active el botón de alternancia Enable syslog server.
7. Click Save. Aparece una confirmación y el servidor syslog recién agregado aparece en la página de inicio del servidor Syslog.

Edición de servidores Syslog configurados

Para editar un servidor syslog configurado:

1. Desplácese hasta el servidor syslog deseado.
2. Elija el icono Más opciones > Editar. Se muestra la página Edit Syslog Server.



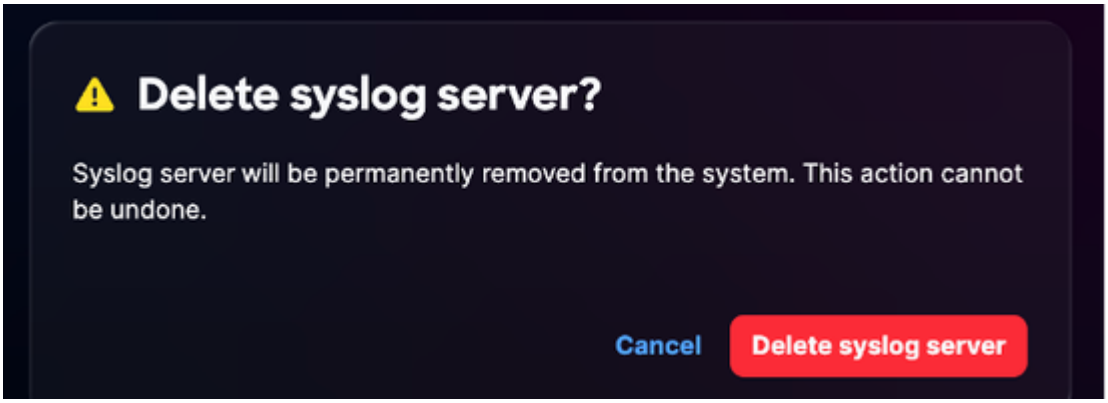
Editar servidor Syslog

3. Edite los detalles o desactive la opción Enable syslog server, según sea necesario.
4. Click Save.

Eliminación de servidores Syslog configurados

Para eliminar un servidor syslog configurado:

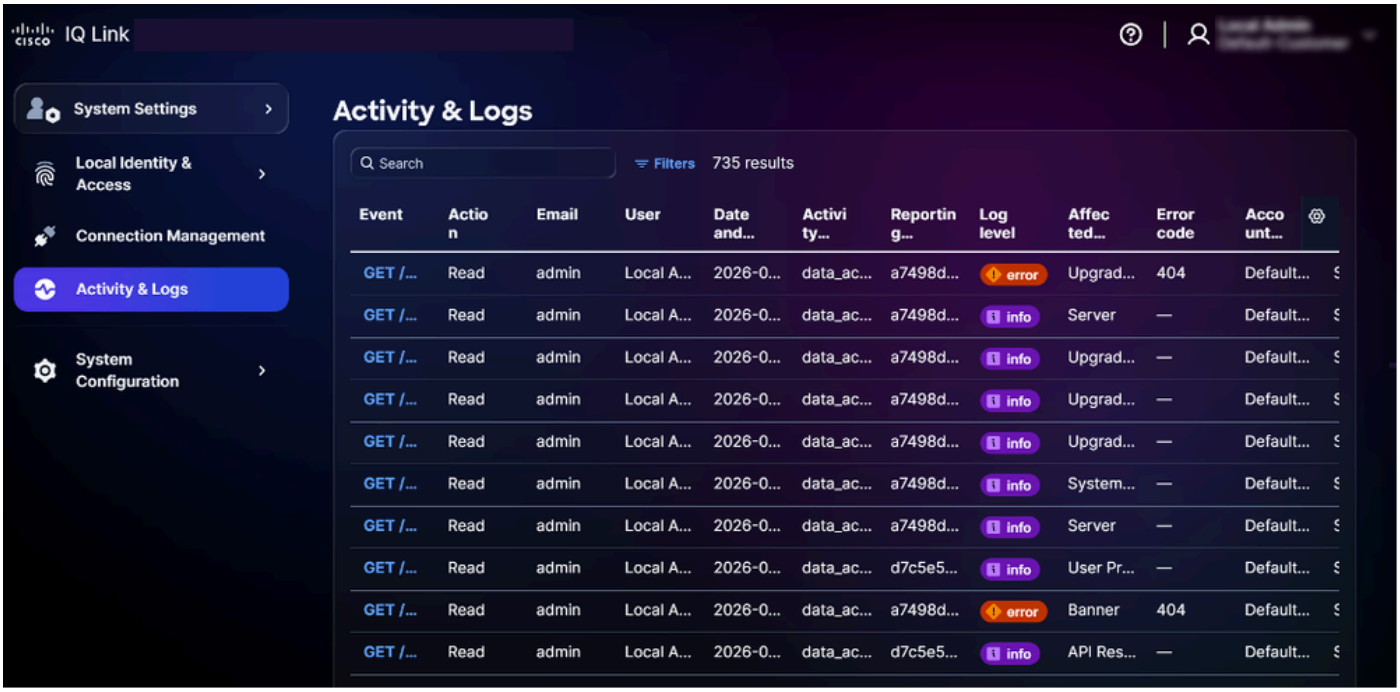
1. Desplácese hasta el servidor syslog deseado.
2. Elija el icono Más opciones > Eliminar. Aparecerá una confirmación.



3. Haga clic en Eliminar servidor syslog.

Actividad y registros

Activity & Logs proporciona un registro detallado de las acciones y cambios de los usuarios en Cisco IQ, lo que permite a los administradores de cuentas realizar un seguimiento de las actividades de los usuarios y mantener la transparencia.



Actividad y registros

Para ver la actividad y los registros, seleccione Activity & Logs en el menú System Settings.

Actividad y registros:

- Admite filtros, paginación y funciones de búsqueda para facilitar la búsqueda y administración de la información
- Registra todas las operaciones de la API en el nivel de gateway

Están disponibles las siguientes opciones de filtro:

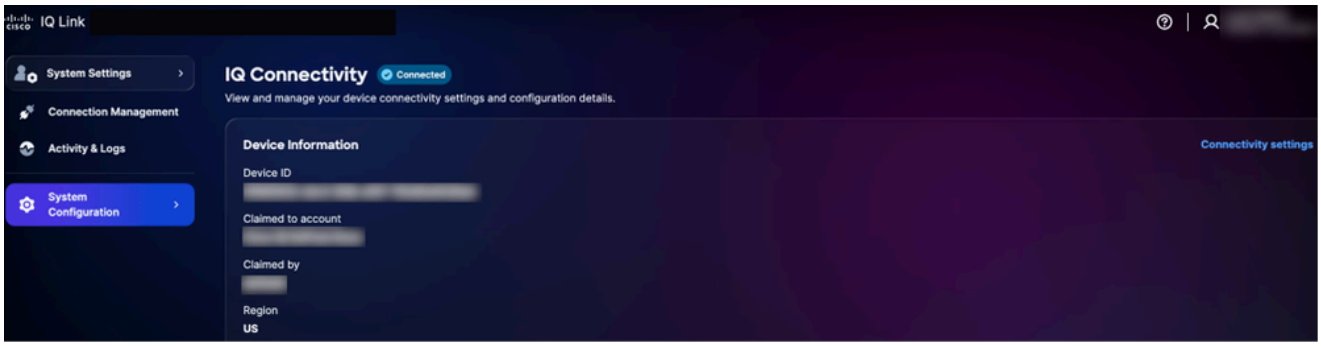
- Fecha: Filtra los registros a un rango de tiempo específico

- Nivel de registro: Filtra los registros por gravedad (por ejemplo, error, advertencia e información)
- Tipo de actividad: Filtra los registros por tipo de actividad del sistema
- Código de error: Filtra los registros de un código de error específico

Conectividad IQ

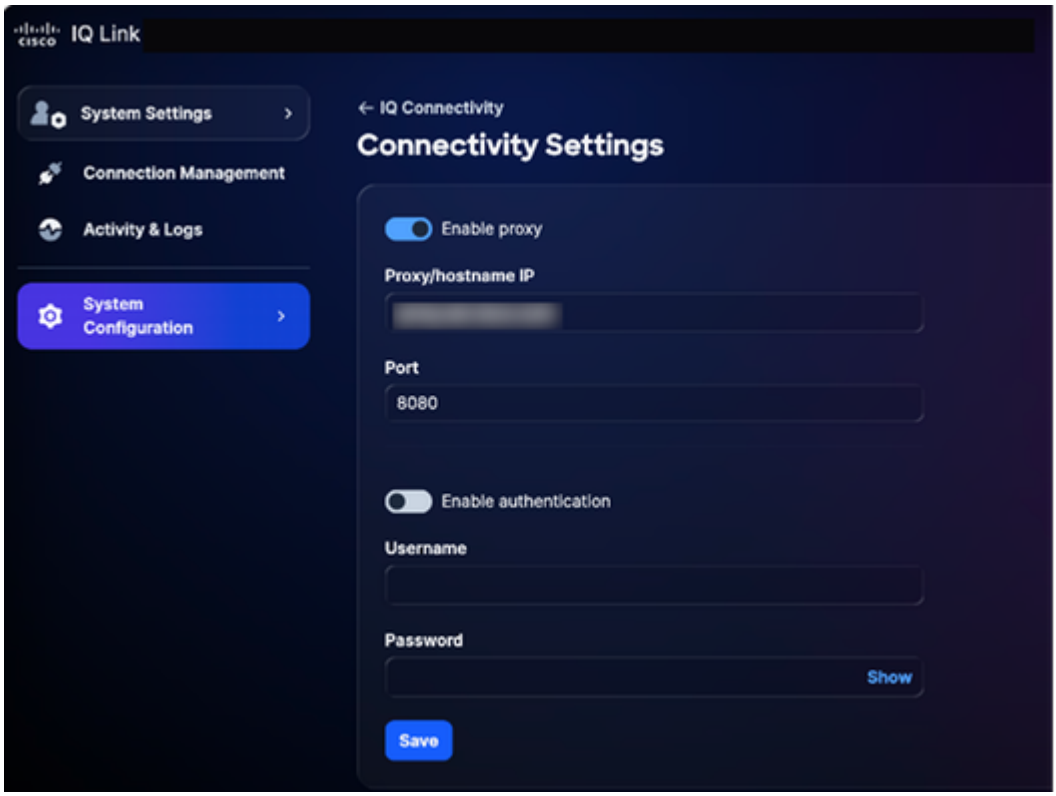
Para ver y administrar los parámetros de conectividad y los detalles de configuración del dispositivo:

1. En System Settings, elija System Configuration > IQ Connectivity. Se muestra la página Conectividad IQ.



Conectividad IQ

2. Haga clic en Configuración de conectividad.



Configuración de conectividad

3. Actualice los detalles según sea necesario.
4. Click Save.

Administración de conexiones (recopilación de datos)

Cisco IQ Link es una solución in situ para la recopilación de datos de red, diseñada para proporcionar una gran visibilidad de su infraestructura. Recopila datos mediante Catalyst Center y Direct Connection. Simplifica la forma de gestionar la autenticación de red y la detección de dispositivos. La configuración de la recolección de datos se resume a continuación:

- Creación de conjuntos de credenciales: Establezca los protocolos de autenticación (por ejemplo, protocolo simple de administración de red (SNMP) v1/v2c/v3) para comunicarse con los dispositivos de red. La centralización de credenciales por zona o ubicación de seguridad (por ejemplo, "SanJose-SNMPv3") permite actualizar contraseñas en una ubicación, con los cambios que se propagan automáticamente a todos los dispositivos asociados.
- Asignación de credenciales al inventario: Asigne sus conjuntos de credenciales a los recursos de inventario para automatizar el proceso de autenticación. Al crear reglas que vinculan rangos de IP específicos a conjuntos de credenciales definidos, el sistema aplica automáticamente la autenticación correcta durante la recopilación de datos. Esto elimina los errores de entrada manual y garantiza que la configuración siga siendo precisa a medida

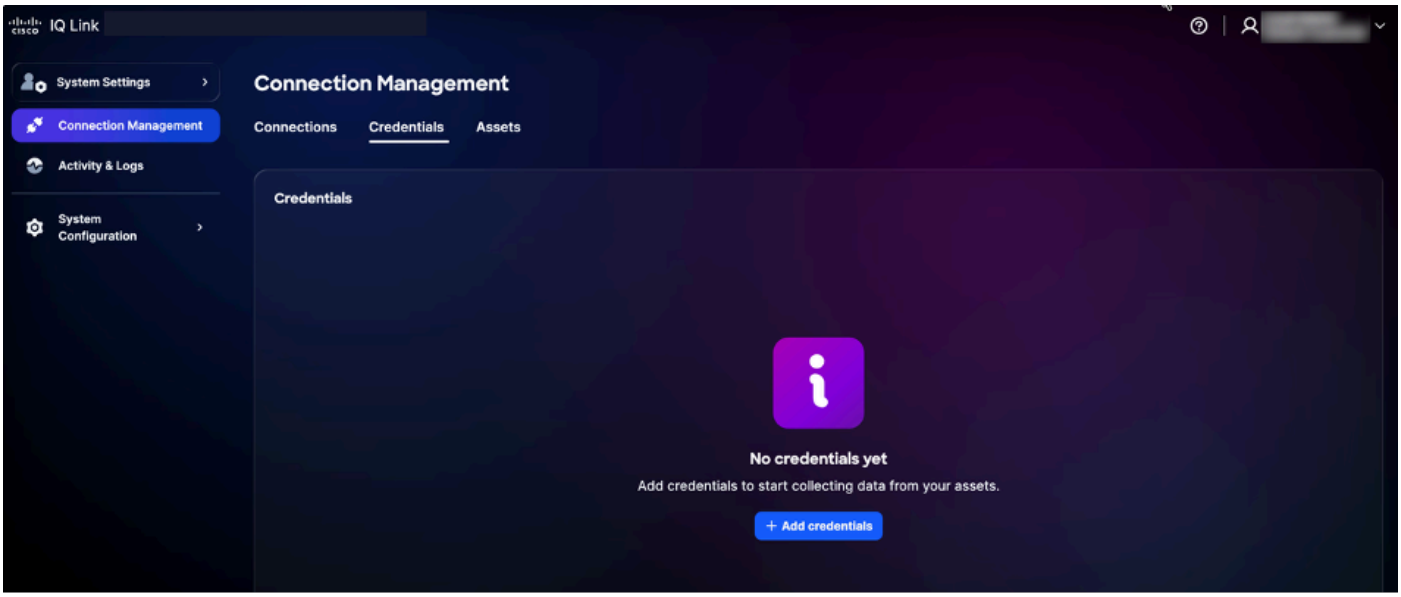
que crece la red.

Nota: Se requieren SNMPv2c/SNMPv3 y SSH para la detección de dispositivos y se deben proporcionar credenciales HTTP/HTTPS antes de configurar Catalyst Center.

Adición de credenciales

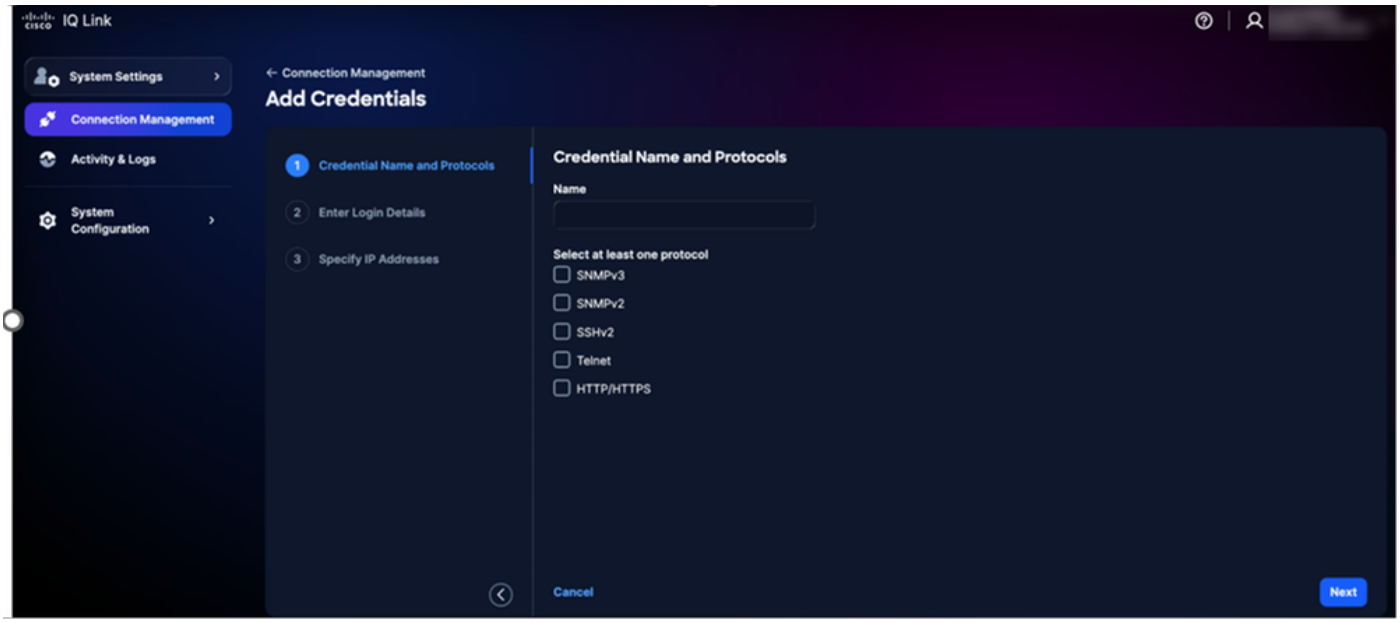
En primer lugar, debe agregar credenciales para realizar la recopilación de datos. Para agregar credenciales:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.
2. Haga clic en la pestaña Credenciales.



Ficha Credenciales

3. Haga clic en Agregar credenciales.

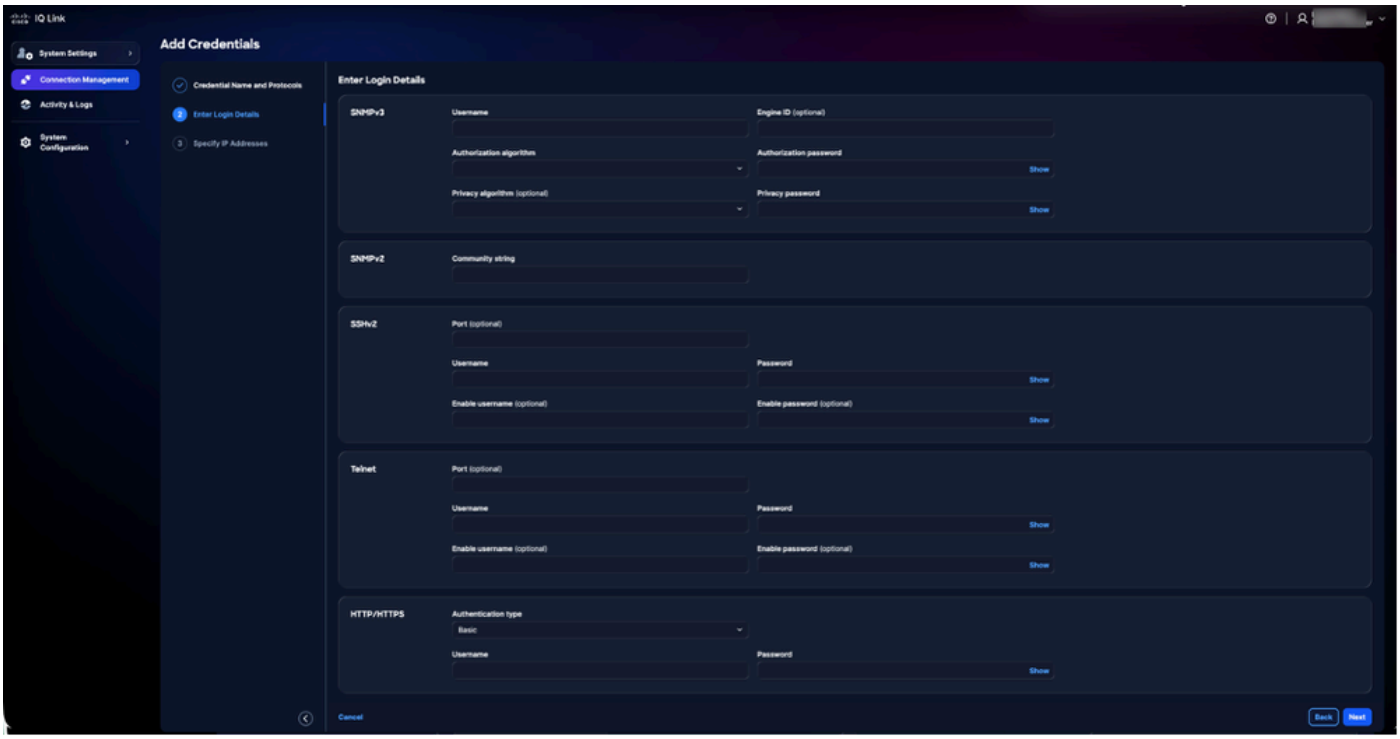


Agregar credenciales

4. Introduzca Nombre.

5. Marque todas las casillas de verificación de protocolo aplicables.

6. Haga clic en Next.

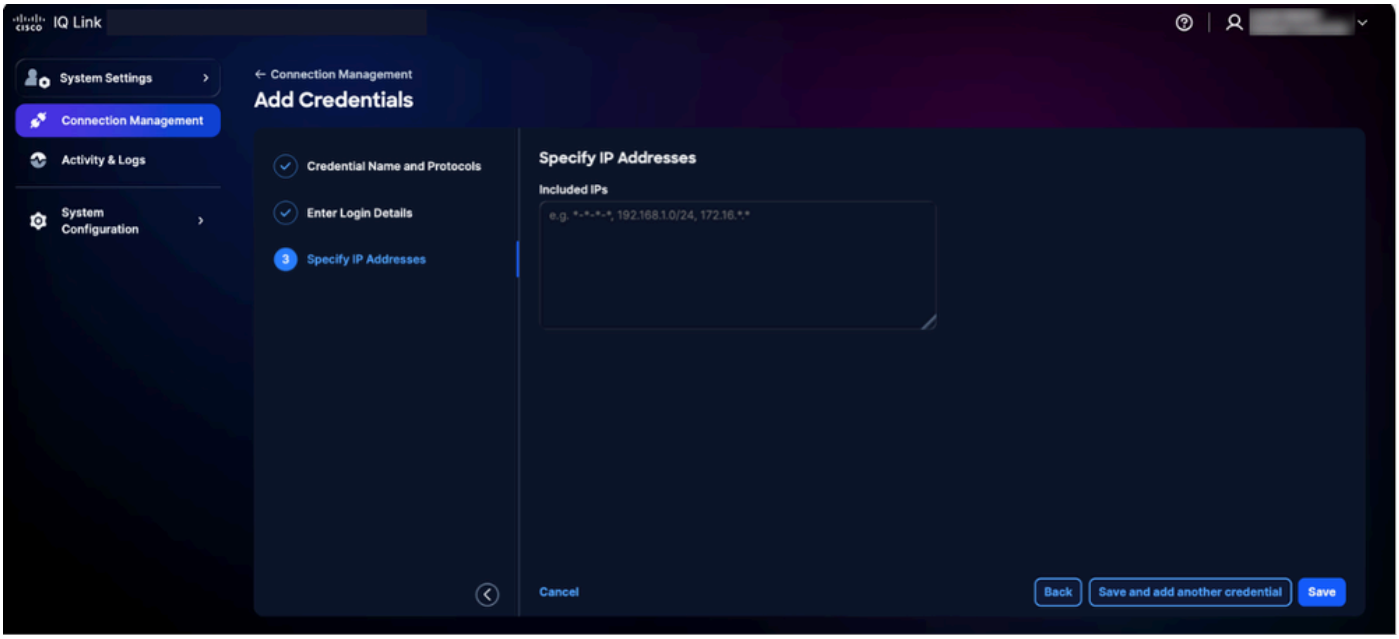


Agregar detalles de credenciales

Nota: Para la imagen anterior, se ilustra la vista en la que se seleccionaron todos los protocolos en el paso anterior. La interfaz mostrará únicamente los protocolos específicos que haya seleccionado.

7. Introduzca los detalles de conexión de cada protocolo seleccionado.

8. Haga clic en Next.

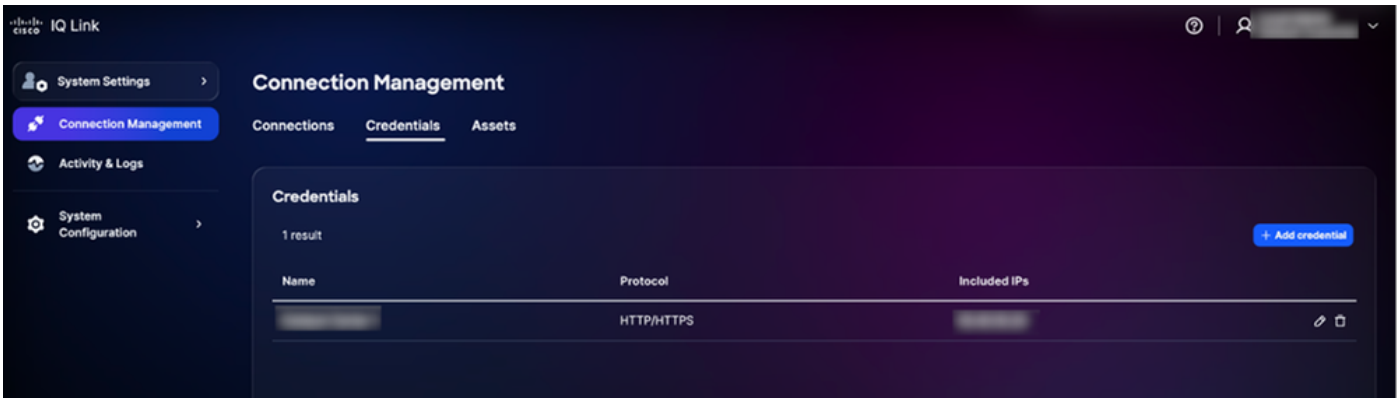


Especificar direcciones IP

9. Introduzca las direcciones IP incluidas.

Nota: Este campo define las direcciones IP o los intervalos IP en los que se pueden utilizar las credenciales para establecer una conexión. Admite una combinación de direcciones IP y máscaras IP (mediante la notación de caracteres comodín). Para obtener más información sobre los formatos compatibles, consulte Selección de credenciales y lógica de coincidencia.

10. Haga clic en Guardar. Se muestra una confirmación y se le redirige a la pestaña Credenciales.



Credenciales agregadas

Puede editar las credenciales haciendo clic en el icono Edit y eliminarlas haciendo clic en el icono Delete.

Selección de credenciales y lógica de coincidencia

El motor de telemetría emplea una lógica de coincidencia basada en prioridades para determinar qué credenciales se deben aplicar durante la detección y la recopilación. La comprensión de esta jerarquía garantiza que se utilicen las credenciales correctas para los dispositivos deseados.

- Clasificación de prioridad: Cuando se aplican varios conjuntos de credenciales a un dispositivo, Cisco IQ los evalúa en función de la coincidencia específica con el dispositivo; el sistema aplica la prioridad siguiente, con mayor prioridad a las coincidencias más específicas:
  - Coincidencia de IP exacta: Prioridad más alta
  - Coincidencia de comodín final: la prioridad depende del número de estrellas finales; menos estrellas indican una coincidencia más específica y, por lo tanto, una prioridad más alta

- Reglas de formato de comodines: Los comodines (*) sólo se admiten como caracteres finales en una dirección IP; deben aplicarse de derecha a izquierda.
  - Formatos admitidos:

    1.2.3.* (Máxima prioridad entre comodines)

    1.2.*

    1.*.*.*

    ..*.* (Prioridad más baja)

  - Formatos no admitidos:

    Caracteres comodín iniciales (por ejemplo, *.1.2.3)

Caracteres comodín entre octetos (por ejemplo, 10.10.*.20)

Uso de guiones u otros delimitadores no estándar

Ejemplo de selección de credenciales:

En la tabla siguiente se muestra cómo el motor de telemetría selecciona el conjunto de credenciales más adecuado cuando un dispositivo coincide con varios patrones definidos.

Tabla 13: Ejemplo de Selección de Credenciales

IP del dispositivo	Conjuntos de credenciales disponibles	Conjunto de credenciales seleccionado
10.10.1.5	10.10.1.5, 10.10.1, 10.10.*	10.10.1.5 (Coincidencia exacta)
10.10.2.15	10.10.2, 10.10.10.*	10.10.2.* (Más específica)
10.10.5.50	10:10 ..., ...	10.10.2010. (Más específica)

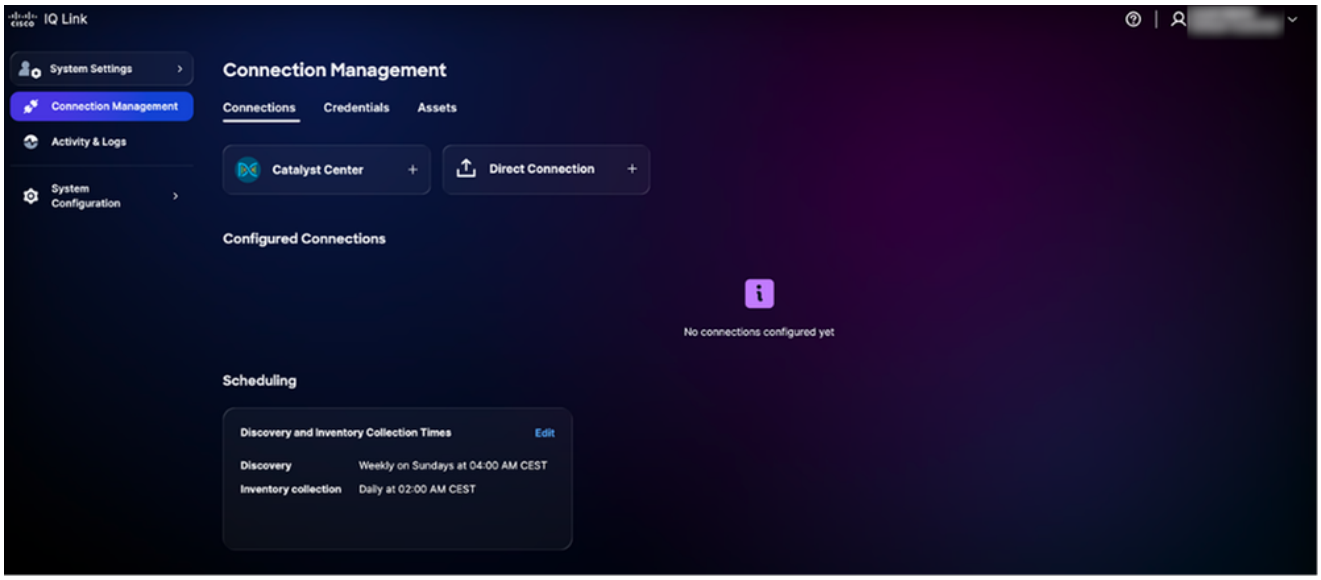
Nota: Si un dispositivo entra en varias categorías superpuestas, el sistema siempre selecciona el conjunto de credenciales con la especificidad más alta (es decir, el menor número de comodines finales).

Recopilación de datos mediante Catalyst Center

Puede conectar hasta 20 Catalyst Centers (no de clúster) para cada instancia de Cisco IQ Link.

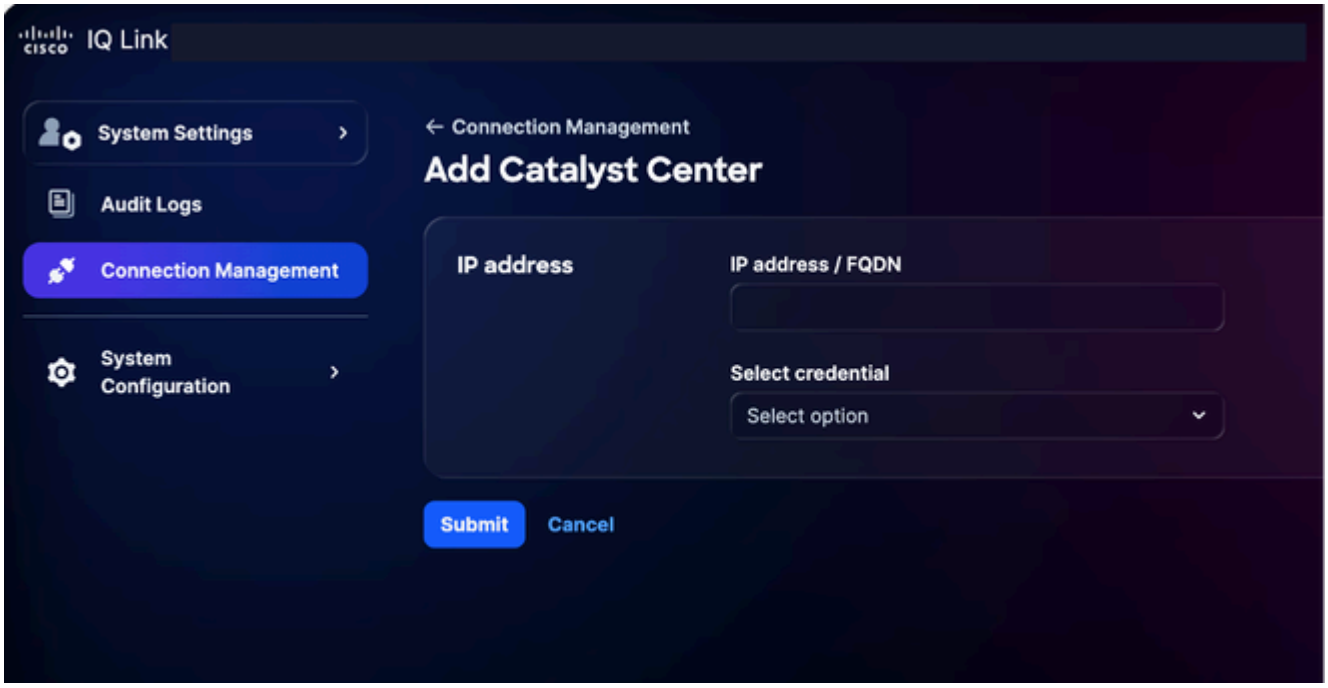
Para la recopilación de datos mediante Catalyst Center:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.



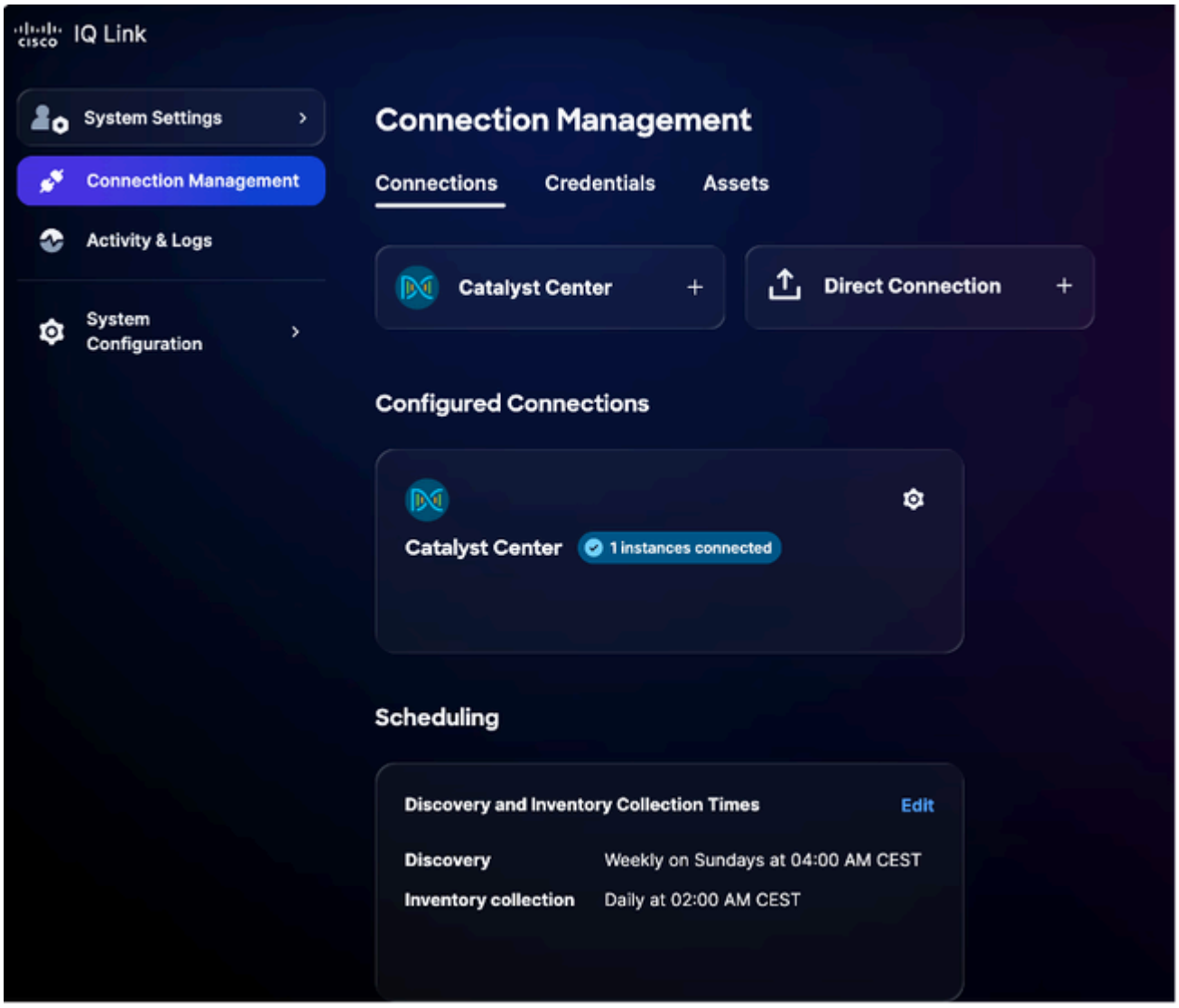
Administración de conexiones

2. Haga clic en la opción Catalyst Center.



Agregar Catalyst Center

3. Introduzca la dirección IP o FQDN.
4. Elija una credencial HTTP/HTTPS configurada en la lista desplegable.
5. Haga clic en Submit (Enviar). Aparecerá una confirmación (puede tardar hasta 75 minutos). Puede ver el Catalyst Center recién agregado en Conexiones configuradas.



Catalyst Center agregado correctamente

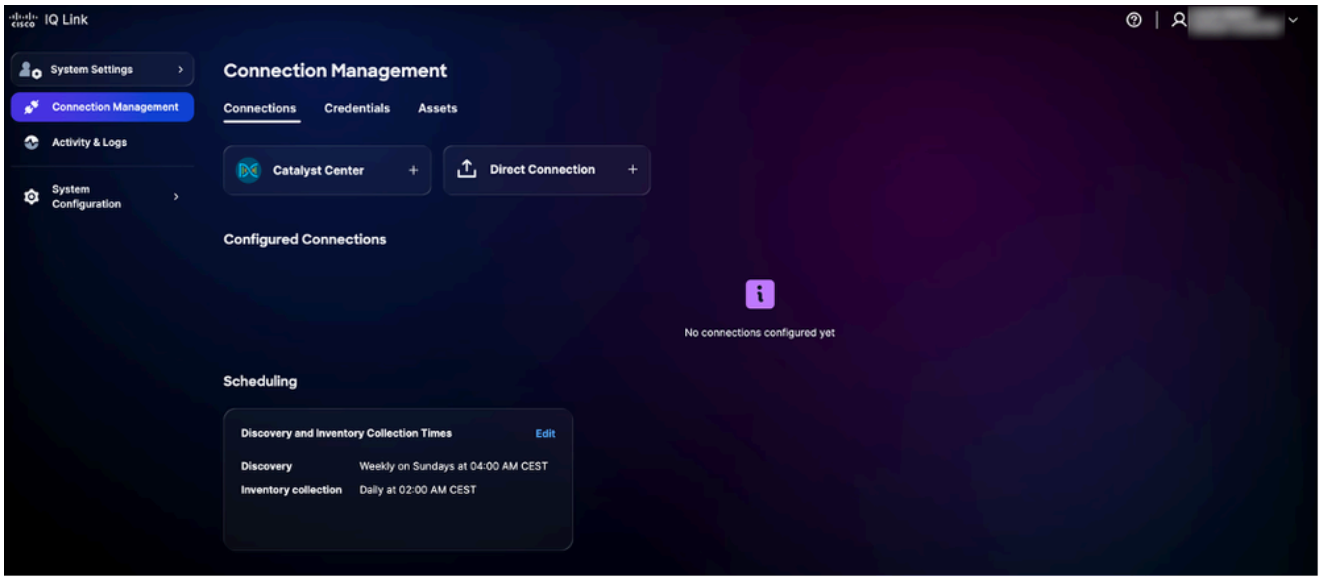
6. Programe una recopilación. Consulte Programación para obtener más detalles.

Nota: Cisco IQ Link está preconfigurado con una configuración de programación automatizada y el sistema inicia una programación de recopilación automatizada predeterminada. Se recomienda encarecidamente que edite la programación para ajustarla a los requisitos y ventanas de mantenimiento de su organización.

Conexión directa

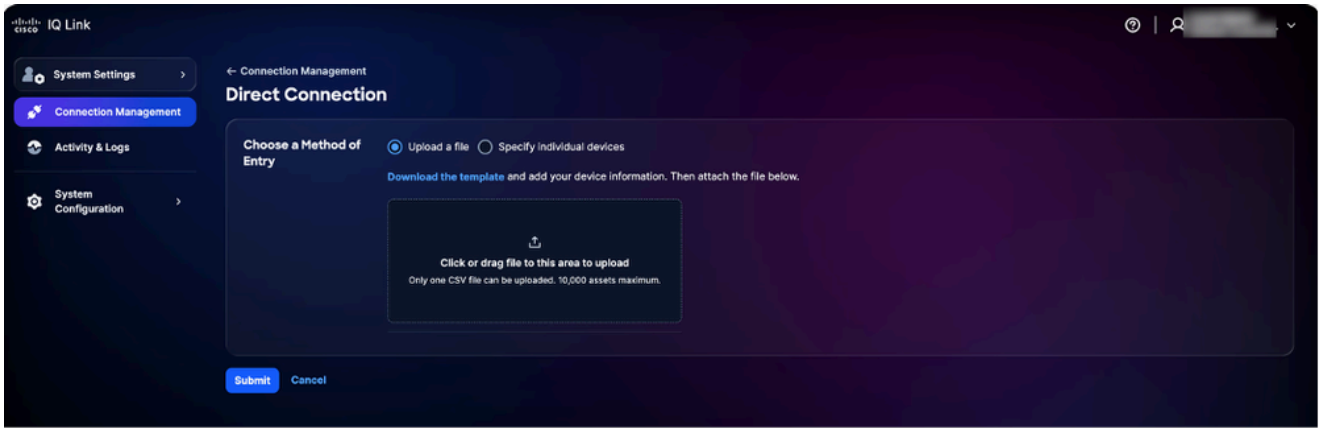
Para agregar dispositivos para la conexión directa:

1. En Configuración del sistema, elija Administración de conexiones. Se muestra la página Connection Management.



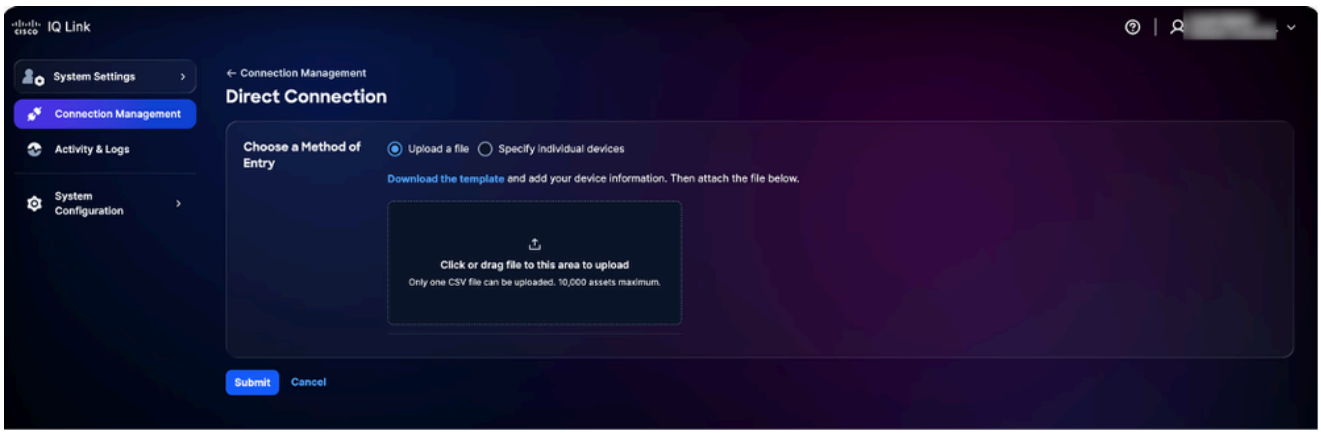
Administración de conexiones

2. Haga clic en Conexión directa. La página Conexión directa se muestra con dos (2) opciones para recopilar datos.



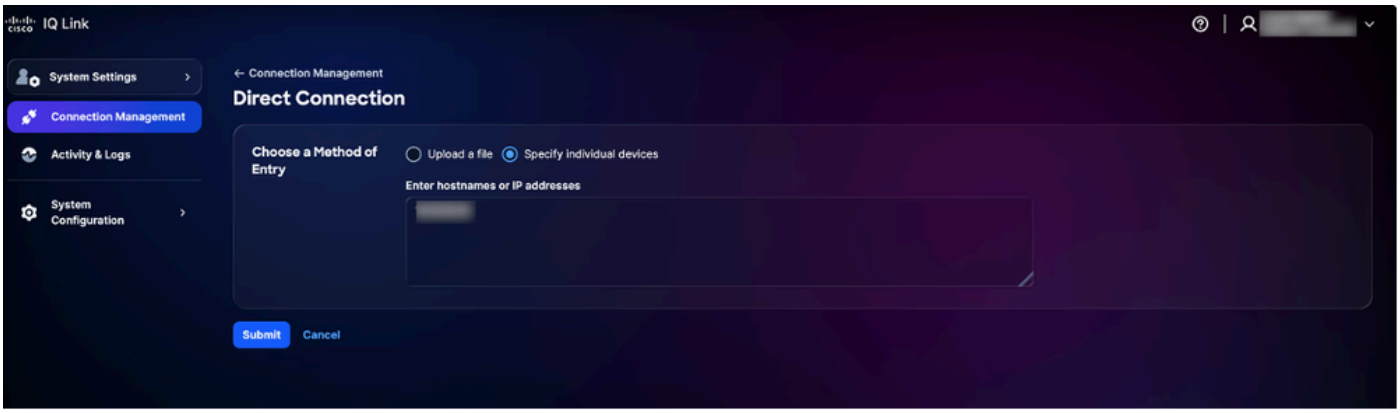
Cargar archivo

3. Haga clic en la opción preferida de Elegir un método de entrada y envíe los dispositivos mediante uno de los siguientes métodos:



Cargar un archivo

- Cargar un archivo: Haga clic o arrastre y suelte el archivo y haga clic en Enviar



Especificar dispositivos individuales

- Especificar dispositivos individuales: Introduzca un único nombre de host, direcciones IP o una lista de nombres de host o direcciones IP separados por comas y, a continuación, haga clic en Enviar

Se le redirigirá a la pestaña Activos tras el envío correcto.

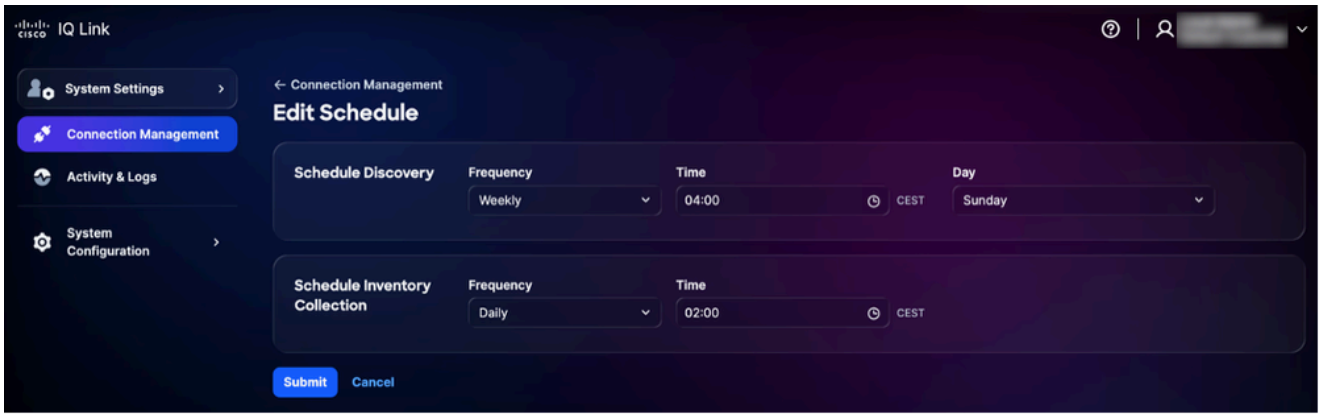
4. Programe una recopilación. Consulte Programación para obtener más detalles.

Nota: Cisco IQ Link está preconfigurado con una configuración de programación automatizada y el sistema inicia una programación de recopilación automatizada predeterminada. Se recomienda encarecidamente que edite la programación para ajustarla a los requisitos y ventanas de mantenimiento de su organización.

Planificación

La programación le permite definir cuándo Cisco IQ Link realiza la recopilación de datos automatizada. Para programar la recopilación:

1. En la sección Programación de la página Administración de conexiones, haga clic en Editar para la programación que desea modificar. Se muestra la página Editar programación.



Editar programación

2. En la sección Programación de Detección, elija su Frecuencia y Día preferidos en las listas desplegables e ingrese la Hora de inicio deseada.
3. En la sección Recopilación de Inventario de Programación, elija su Frecuencia preferida en las listas desplegables e ingrese la Hora de inicio que desee.
4. Haga clic en Submit (Enviar).

Nota: Espere de 5 a 10 minutos para que los cambios realizados en las programaciones de detección o recopilación se sincronicen y reflejen con precisión en Cisco IQ Link.

Banners

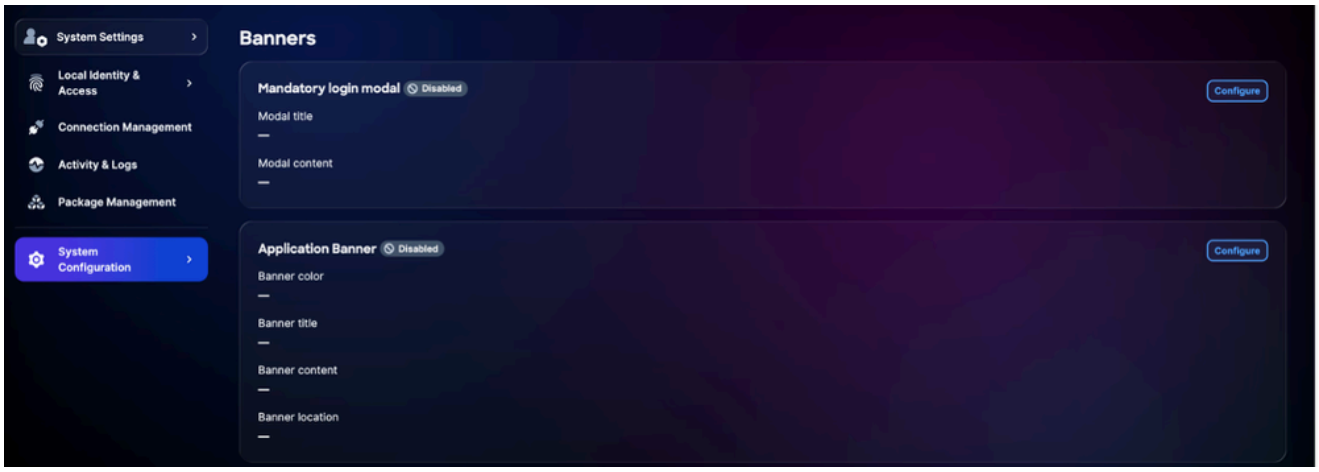
Los administradores de cuentas pueden configurar banners para todo el sistema con el fin de cumplir los estándares de seguridad y cumplimiento.

- Modal de inicio de sesión obligatorio: Debe confirmar el banner obligatorio antes de pasar a la pantalla de inicio de sesión.
- Banners de aplicaciones: Se trata de banners personalizados que se muestran en toda la aplicación después de una autenticación correcta.

Configuración de Banners Modales de Login Obligatorios

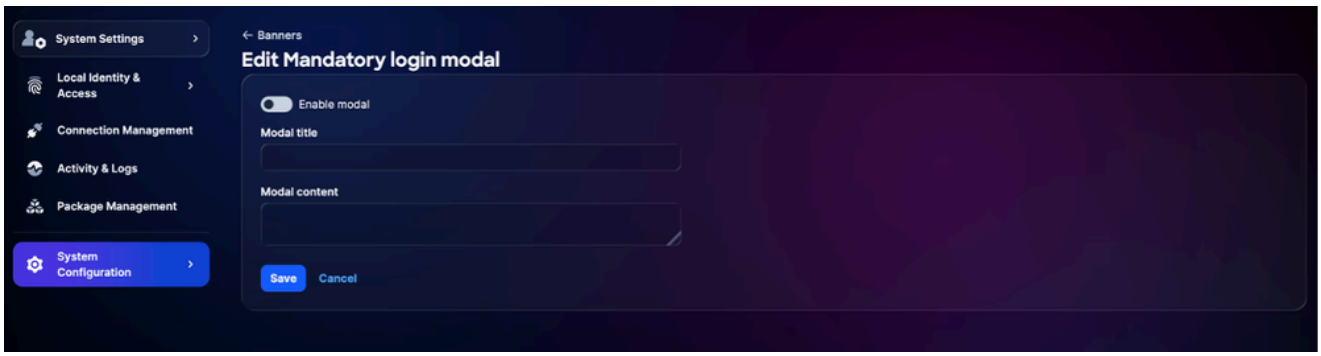
Para configurar un banner obligatorio:

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.



Configurar banner obligatorio

2. Haga clic en Configure en el modal de login obligatorio. Se muestra la página Editar modal de inicio de sesión obligatorio.



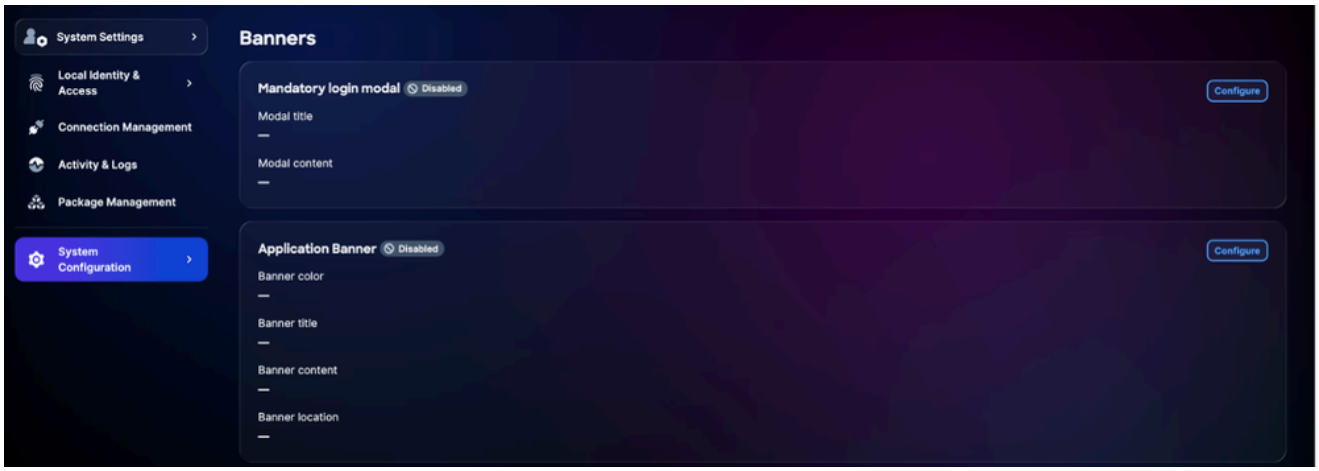
Editar Banner modal de inicio de sesión obligatorio

3. Haga clic en el botón para activar o desactivar el banner.
4. Introduzca el título Modal.
5. Ingrese el contenido Modal.
6. Click Save. Se guarda el modo de inicio de sesión obligatorio.

Configuración de banners de aplicaciones

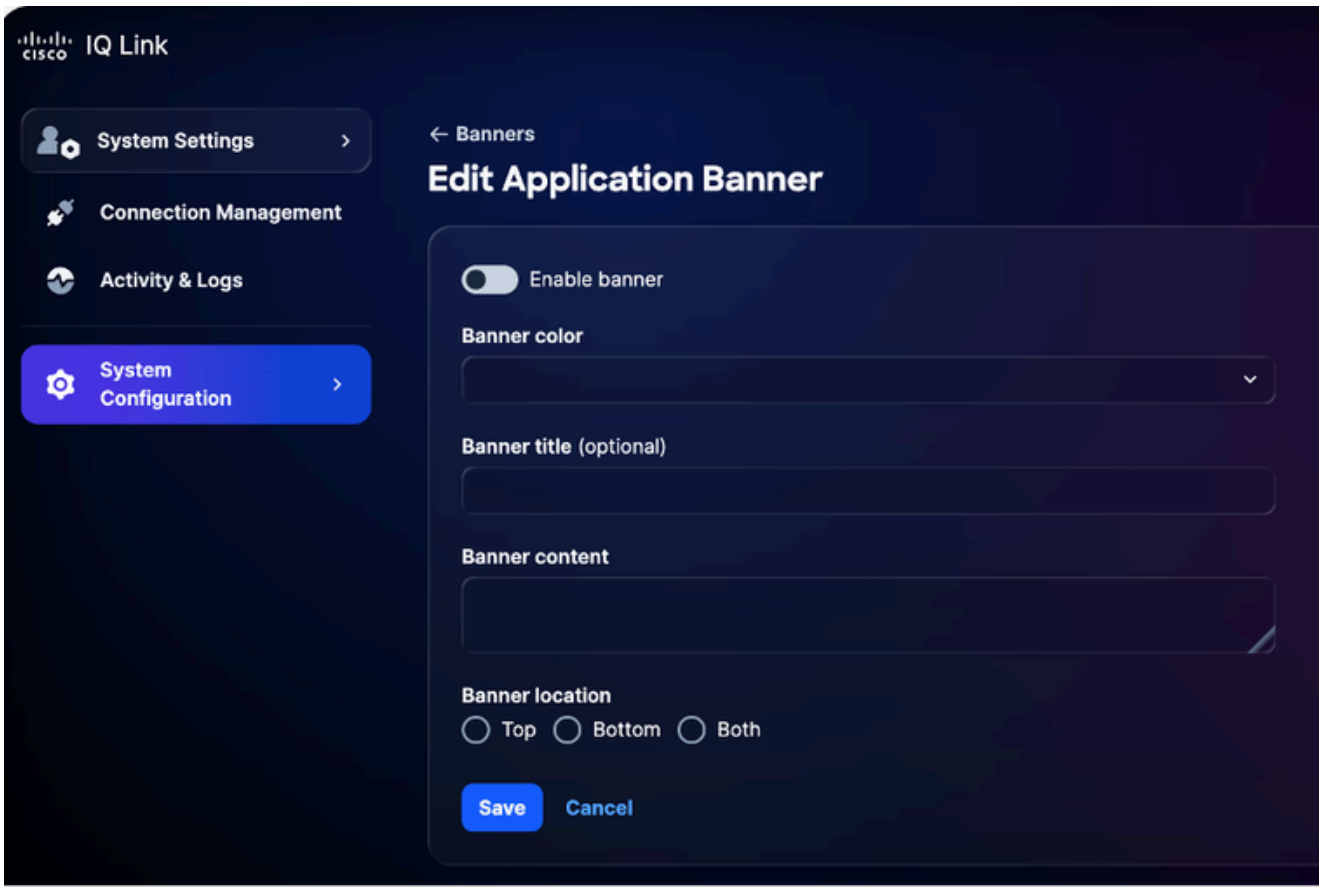
Para configurar un banner de aplicación:

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.



Banner de configuración

2. Haga clic en Configurar en el banner de aplicación. Se muestra la página Editar anuncio de aplicación.



Banner de Editar aplicación

3. Haga clic en el botón para activar o desactivar el banner.
4. Seleccione un color de banner.
5. Introduzca el título del banner.
6. Introduzca el contenido del banner.

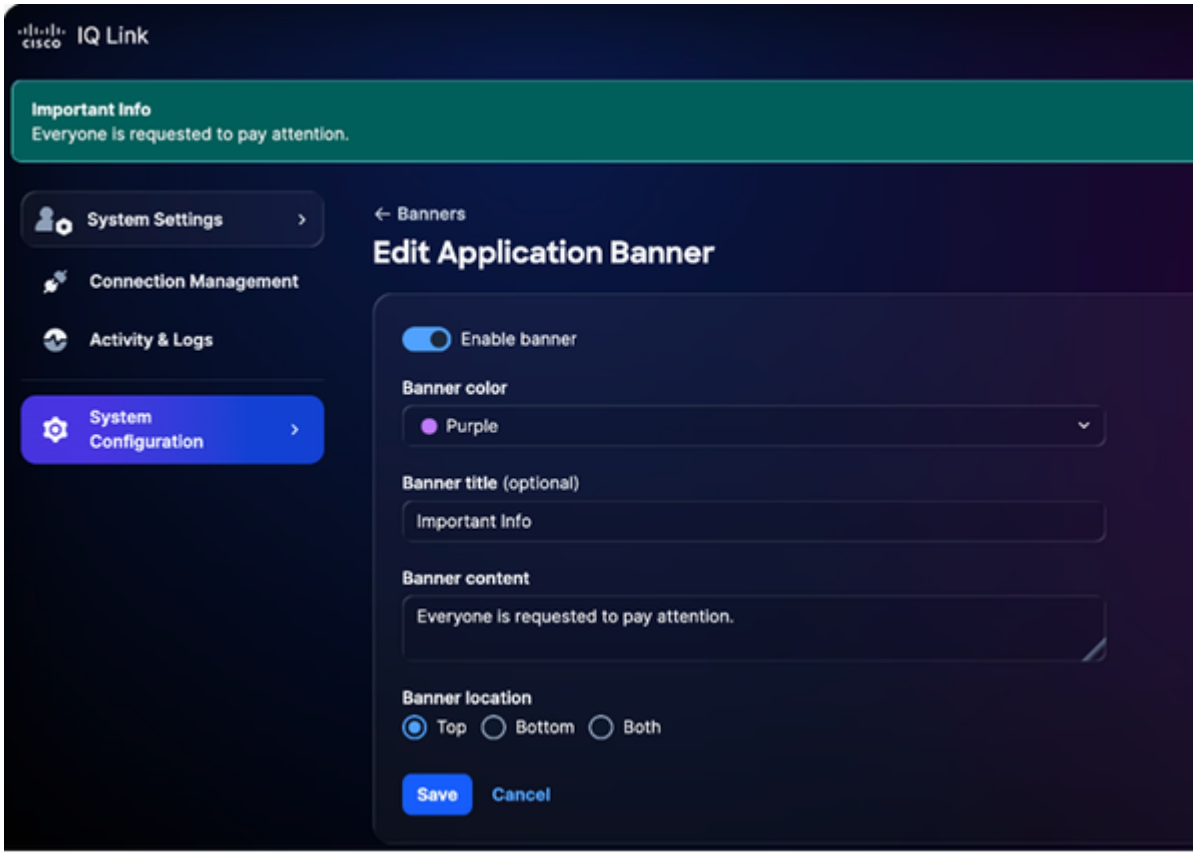
7. Seleccione una ubicación de banner.
8. Click Save. El banner se muestra en toda la aplicación.

Edición de banners

1. En System Settings, elija System Configuration > Banners. Se muestra la página Banners.

Banner de Editar aplicación

2. Haga clic en Editar. Se muestra la página Editar anuncio de aplicación.



Banner de Editar aplicación

3. Edite los detalles que desee.

4. Haga clic en el botón para activar o desactivar el banner.
5. Click Save.

Resolución de problemas

Puede recopilar archivos de diagnóstico y de registro del sistema Cisco IQ y transferirlos de forma segura a un servidor SCP. Estos archivos se pueden compartir con el equipo de soporte técnico al informar sobre problemas para proporcionar un contexto valioso y ayudar con la resolución de problemas.

Para recopilar archivos de diagnóstico y de registro:

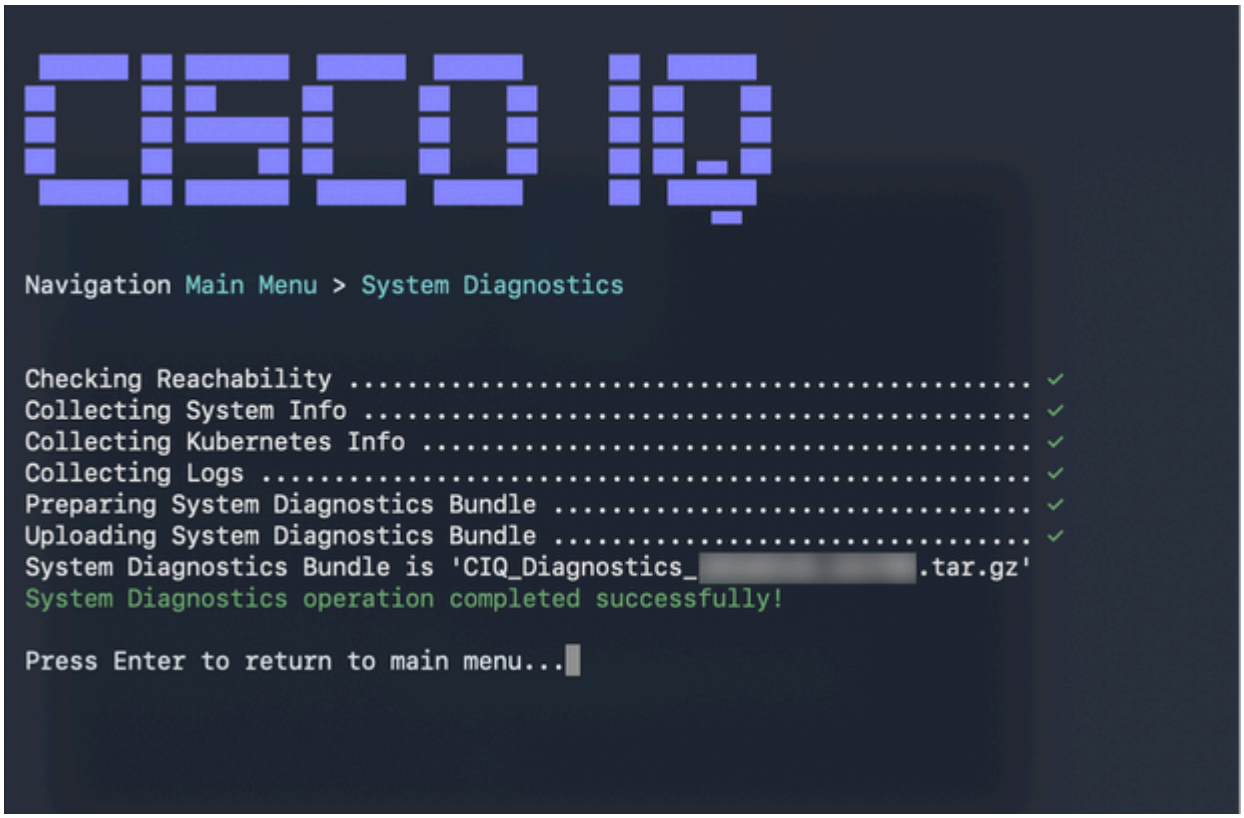
1. Inicie sesión en Cisco IQ.

Menú principal

2. En el menú principal de Cisco IQ, introduzca "3" y pulse Intro para seleccionar Diagnóstico del sistema.

Diagnóstico del sistema

3. Introduzca la dirección del servidor SCP/SFTP.
4. Introduzca el puerto del servidor SCP/SFTP.
5. Introduzca la ruta del servidor SCP/SFTP.
6. Seleccione un protocolo.
7. Introduzca el nombre de usuario.
8. Ingrese la contraseña.
9. Ingrese "C" y presione Enter para continuar con el diagnóstico del sistema.



Operación de diagnóstico del sistema finalizada

El sistema inicia el proceso de diagnóstico y realiza las siguientes acciones:

- Comprobación de disponibilidad
- Recopilación de información del sistema
- Recopilación de información de Kubernetes
- Recopilación de registros
- Preparación del paquete de diagnósticos del sistema
- Cargando paquete de diagnósticos del sistema

Una vez completada, se muestra un mensaje de confirmación que indica el nombre del paquete generado.

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).