Guía de operaciones de Cisco IQ Link v1.1.1

Introducción

Cisco IQ™ ofrece a los clientes 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 Cisco IQ AI Assistant, optimizan los resultados operativos y la experiencia del usuario de Cisco IQ al proporcionar una comprensión contextual que permite a los usuarios tomar decisiones proactivas e informadas, y simplifica 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 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

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 a través del menú Local Admin Security en System Configuration.

Tiene tres (3) intentos de introducir la contraseña correcta en un período de diez (10) minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 60 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.

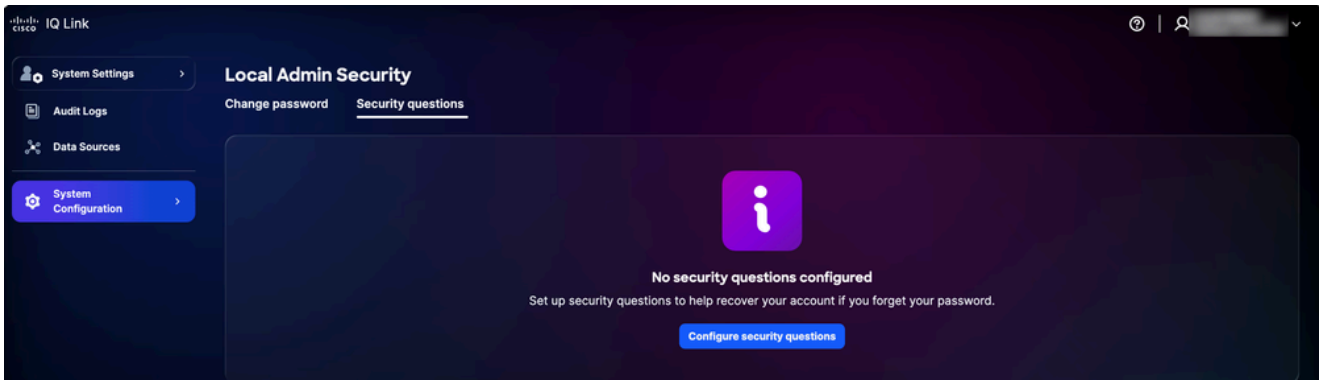
La cuenta se desbloquea automáticamente transcurridos 60 minutos, momento en el que puede intentar iniciar sesión o restablecer la contraseña.

Configuración de preguntas y respuestas de seguridad

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

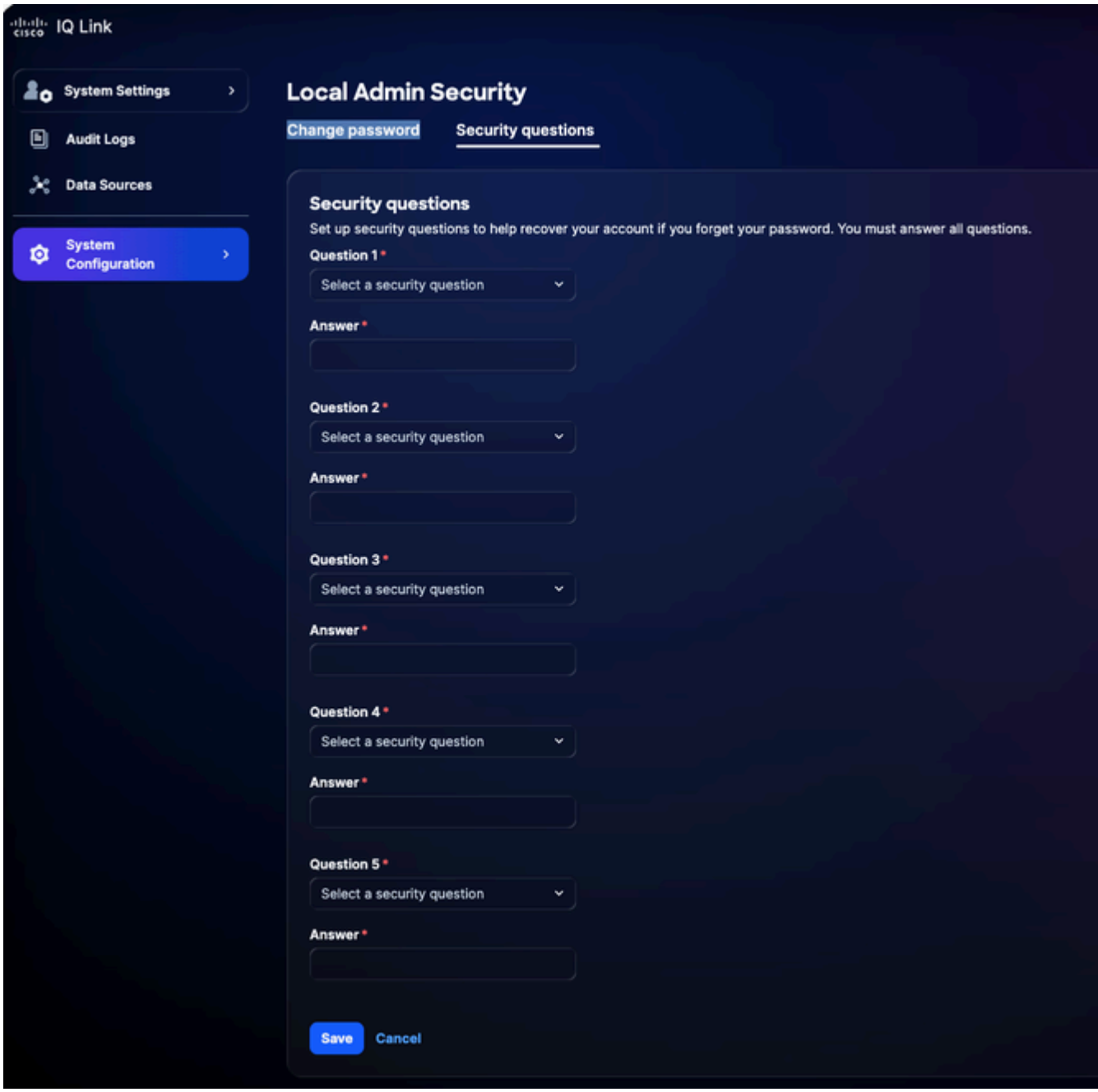
Para configurar preguntas de seguridad:

1. En System Settings, elija System Configuration > Local Admin Security > Security Questions.



Preguntas de seguridad

2. Haga clic en Configurar preguntas de seguridad.



Preguntas de seguridad

3. Elija cinco (5) preguntas de seguridad cualesquiera de las listas desplegables.

4. Introduzca la respuesta para cada pregunta.

5. Click Save.

Notas:
· Las respuestas no distinguen entre mayúsculas y minúsculas; por ejemplo, "SMITH" y "smith" se consideran iguales
· Los espacios adicionales son ignorados, lo que significa que "Smith" y "Smith" son tratados de manera idéntica

---

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

Solo los administradores locales pueden administrar la contraseña de Cisco IQ.

Prerequisites

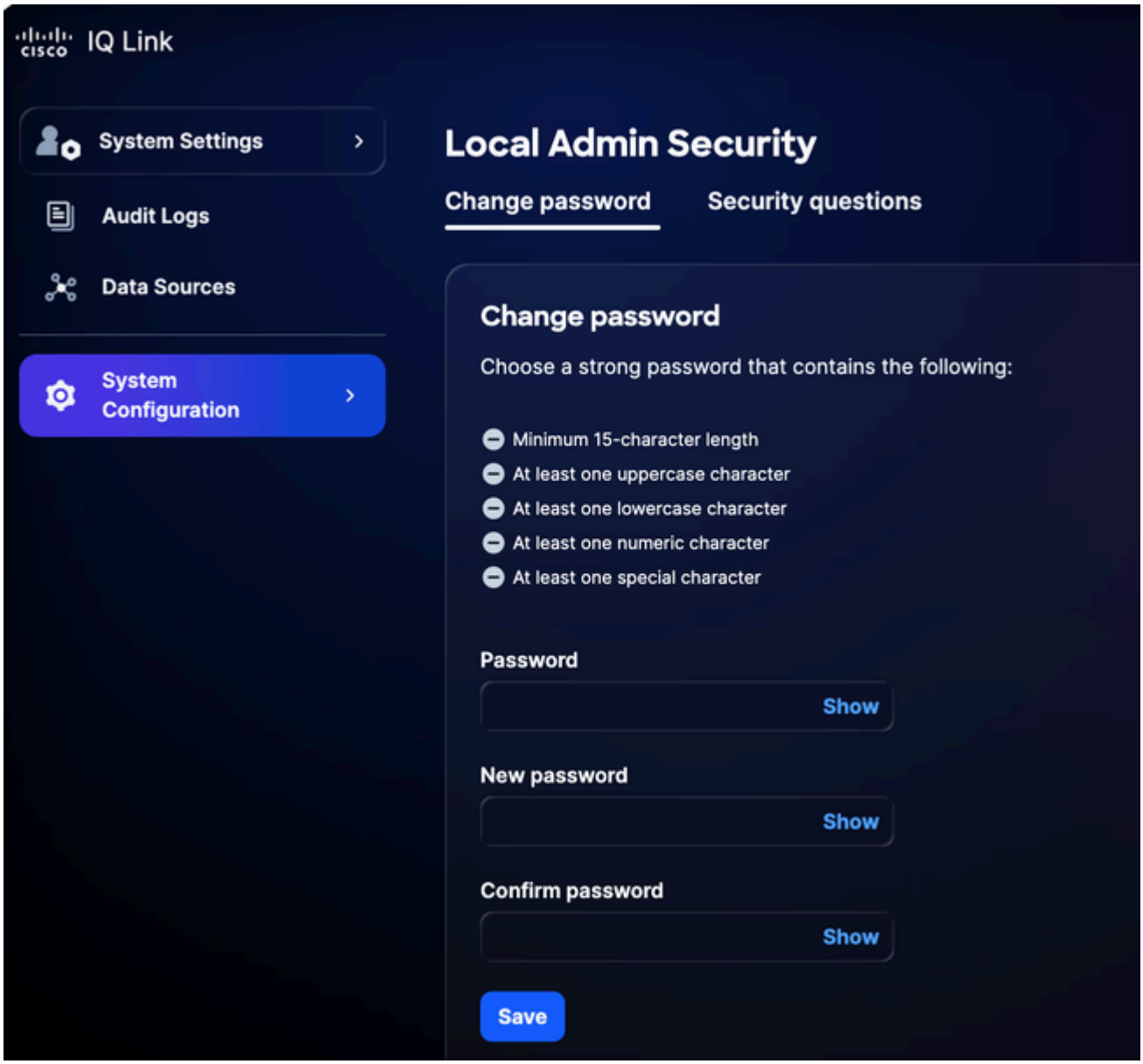
Para administrar contraseñas, se deben cumplir las siguientes condiciones:

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

Cambio de contraseñas

Para cambiar la contraseña:

1. Desde System Settings, navegue hasta System Configuration > Local Admin Security > Change Password.



Cambiar contraseña

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

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

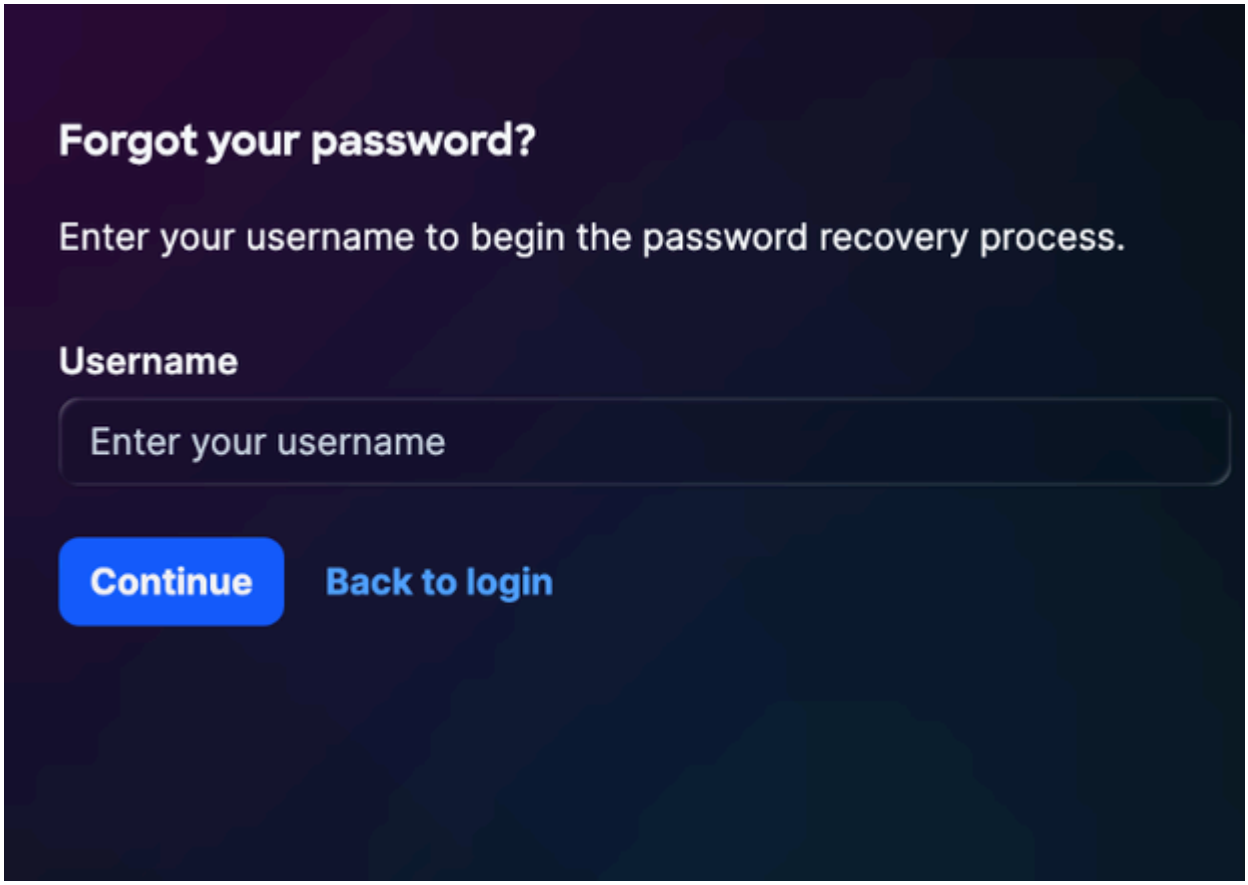
Restablecimiento de una Contraseña Olvidada

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.

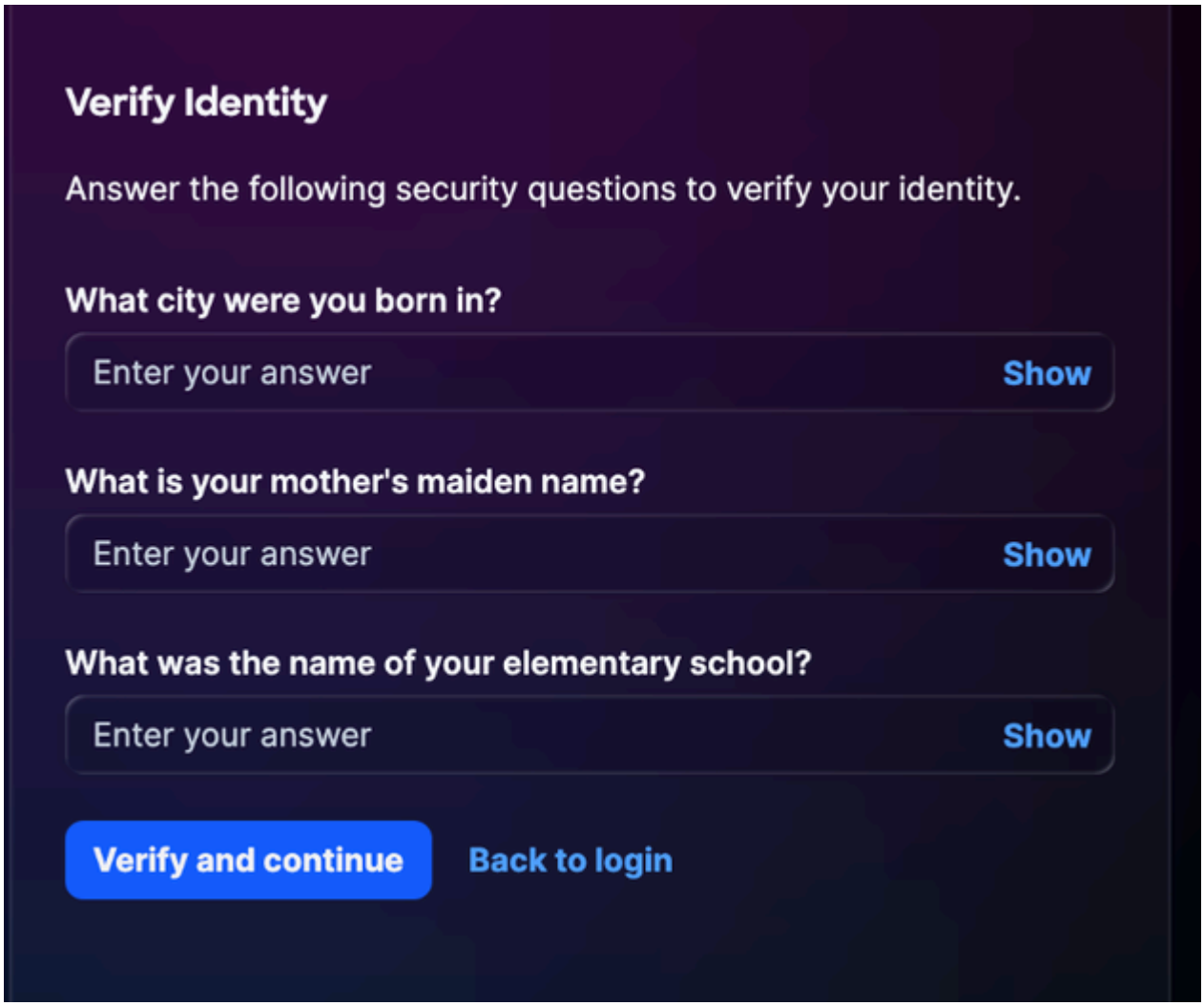
Para restablecer una contraseña olvidada:

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.

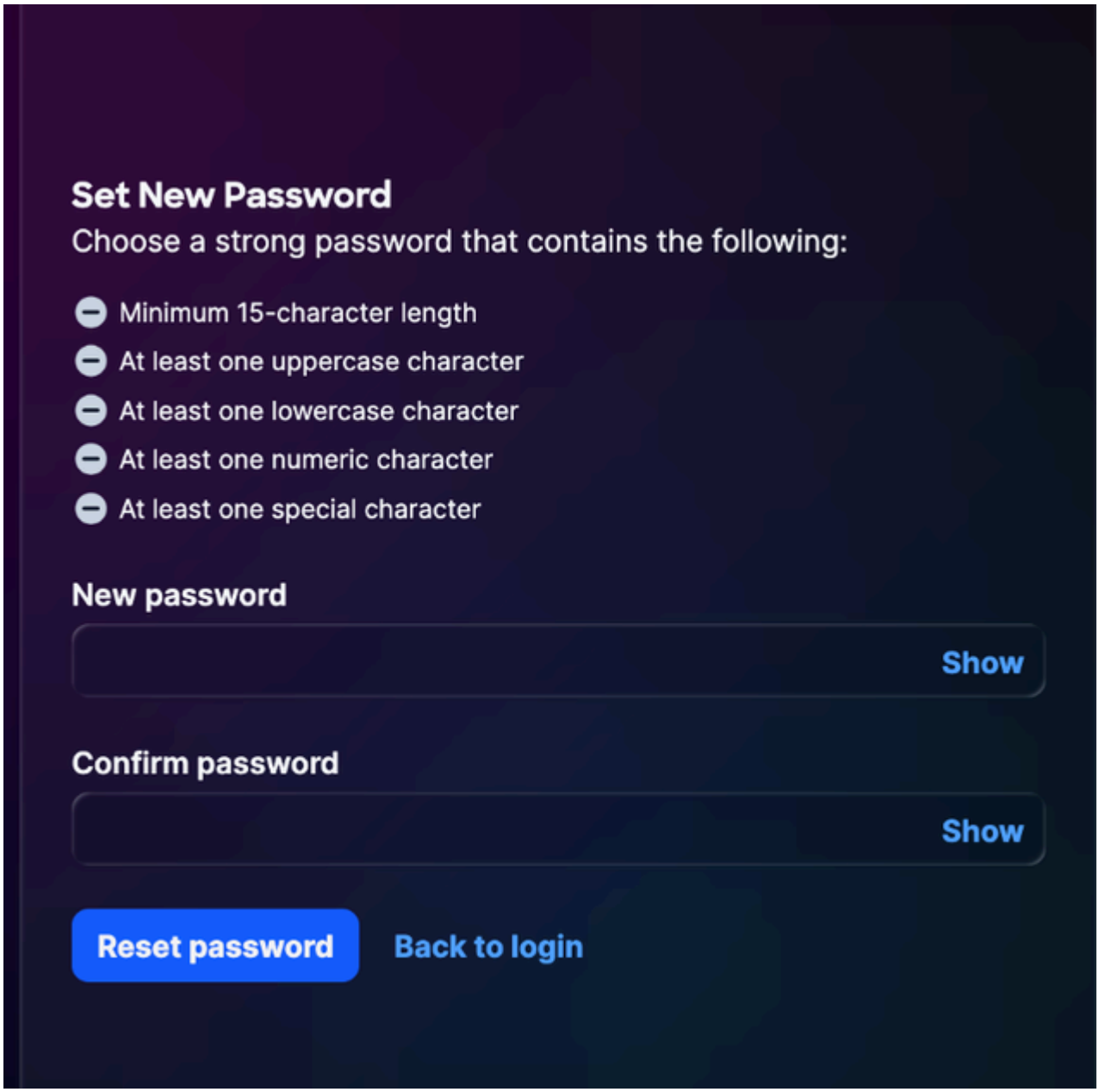


Verificar identidad

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

---

5. Introduzca las respuestas para 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

Notas:
· Tiene tres (3) intentos de responder correctamente a las preguntas de seguridad en un período de diez (10) minutos. Si los tres (3) intentos no tienen éxito, su cuenta se bloquea temporalmente durante 60 minutos para proteger su seguridad.
· No puede restablecer su 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.
· Su cuenta se desbloquea automáticamente después de 60 minutos, momento en el que puede intentar iniciar sesión o restablecer su contraseña.

---

7. Introduzca la nueva contraseña.

8. Vuelva a introducir la contraseña para confirmarla.

9. Haga clic en Submit (Enviar).

Configuración del proveedor de identidad

Una vez que haya iniciado sesión en Cisco IQ Link, los administradores pueden configurar diversos parámetros. Los administradores 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 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.

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

Campo	Valor
Destinatarios	Personal no laboral
Categoría de incorporación	Seleccione "Nueva incorporación"

Parámetros de configuración de SAML

Parámetro	Configuración	Ejemplo:
Audiencia (ID de entidad)	nombre FQDN	mymanagementhost.mydomain.com
URL de inicio de sesión único	punto final ACS 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 Single Logout (SLO) en la aplicación.

Parámetros de configuración de SLO

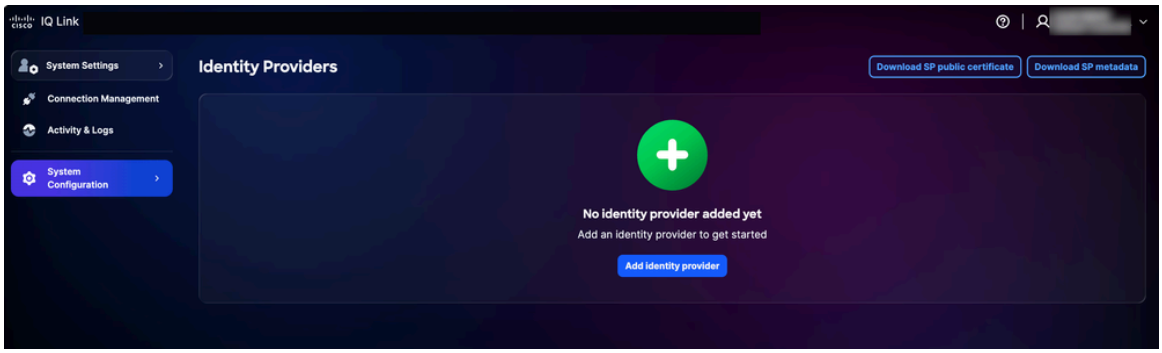
Campo	Valor
Certificado de firma	Para Okta, este certificado solo es necesario si elige habilitar SLO. Descargue el certificado de firma mediante Download SP Certificate en Identity Providers. Guarde el archivo como sp-public-key.crt. Consulte Configuración de cierre de sesión único para obtener más 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 IDP

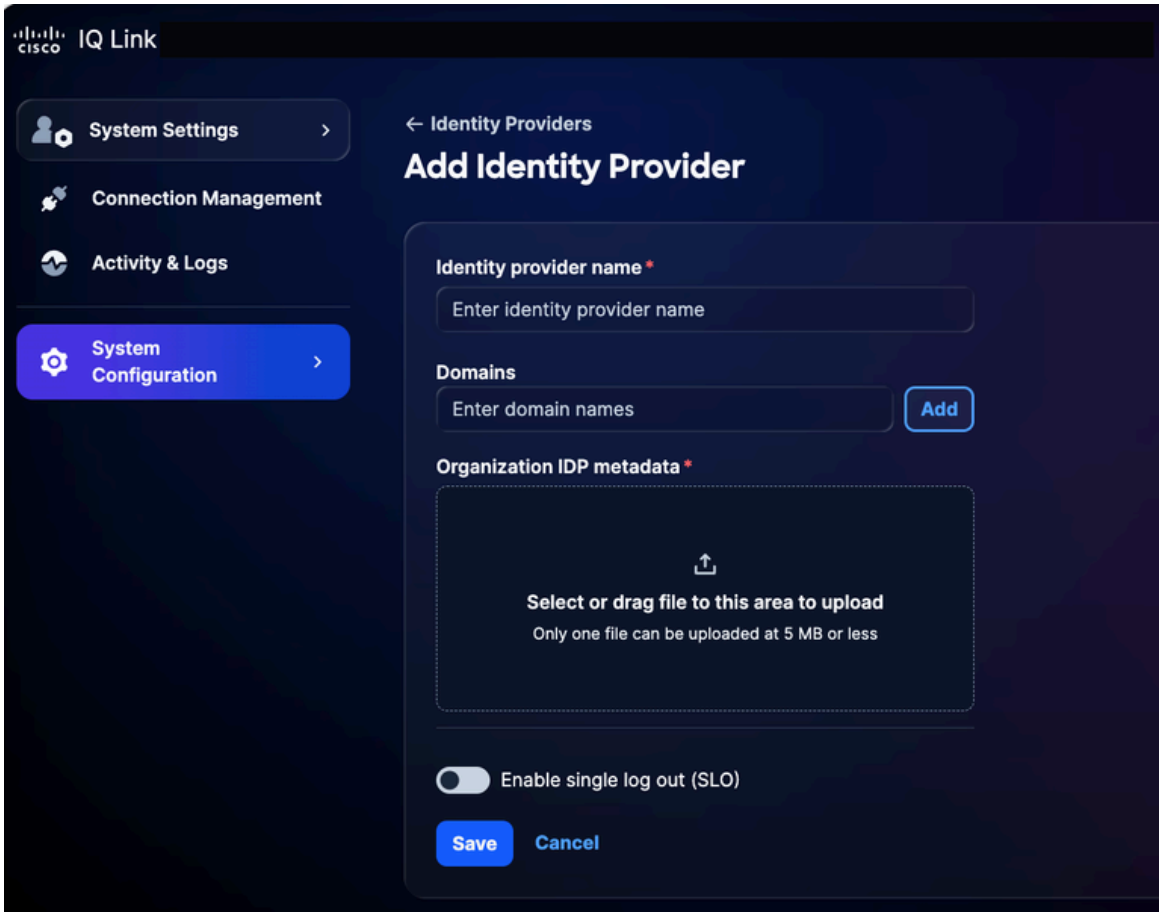
Para agregar un IDP en Cisco IQ Link:

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.



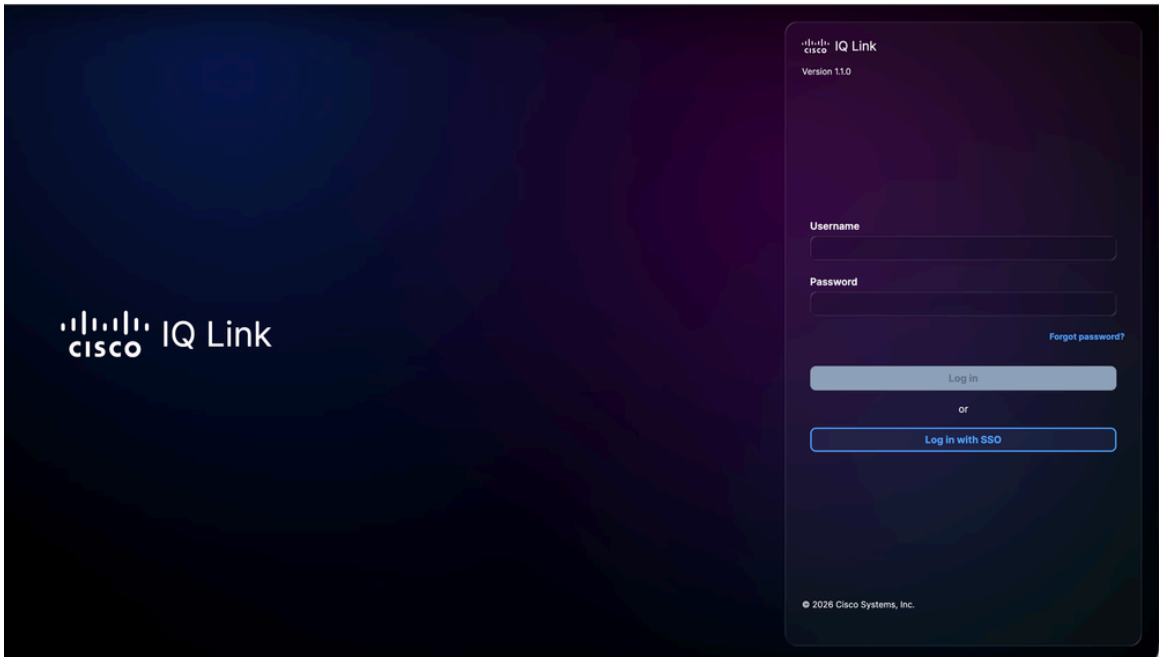
Agregar proveedor de identidad

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.

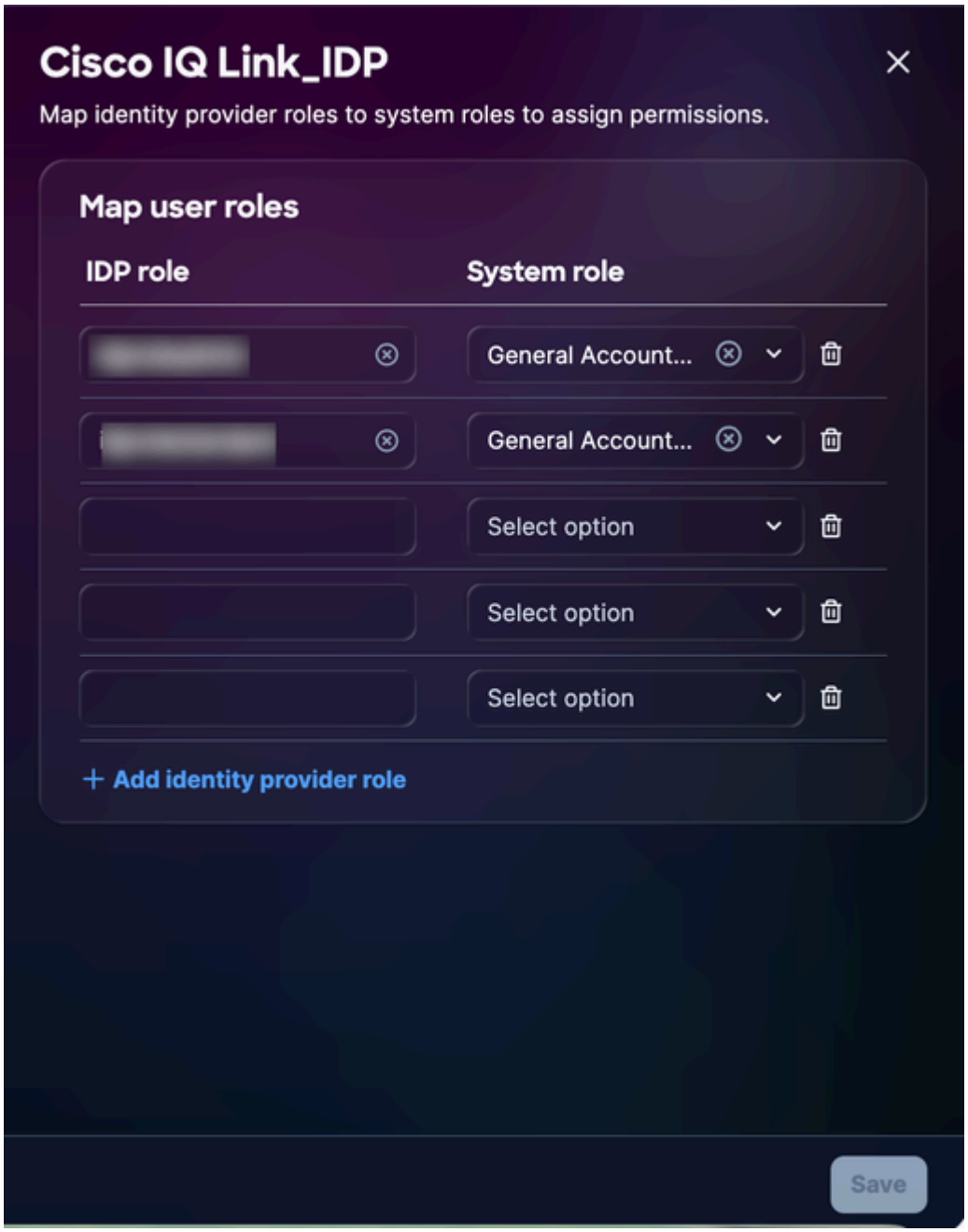
5. Arrastre y suelte o cargue el archivo de metadatos SAML obtenido de la aplicación IDP en el campo de metadatos Organization IDP. Este archivo contiene los detalles del certificado y los detalles de la entidad Proveedor de servicios (SP).
6. (Opcionalmente) Active el botón de alternancia Enable single logout. También puede activar el SLO más adelante.
7. Click Save.
8. 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.



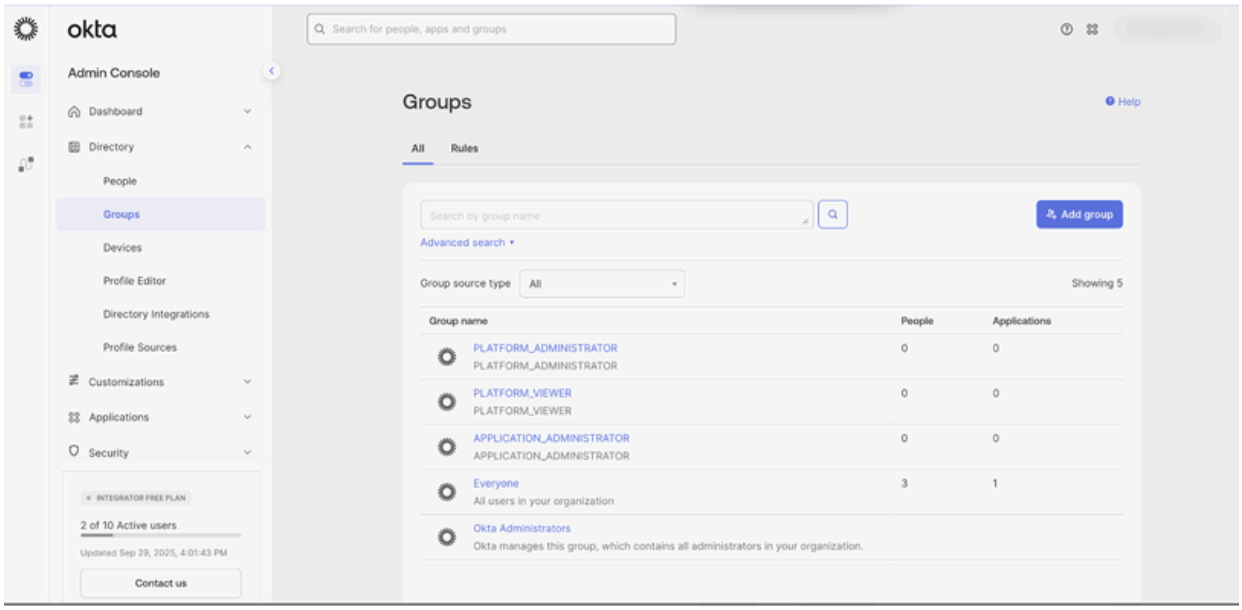
Asignación de funciones de usuario

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

    - administrador_cuenta_general: El administrador de la cuenta general tiene permisos completos para realizar todas las acciones del producto
    - general_account _viewer: El visor general de cuentas 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.



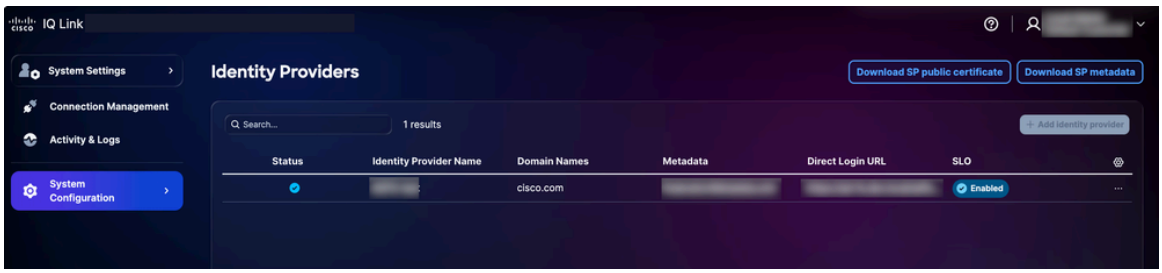
Referencia de asignación de roles

3. Asigne funciones adicionales según sea necesario haciendo clic en Agregar función de proveedor de identidad.
4. Click Save.

Configuración de cierre de sesión único

Si elige habilitar 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:

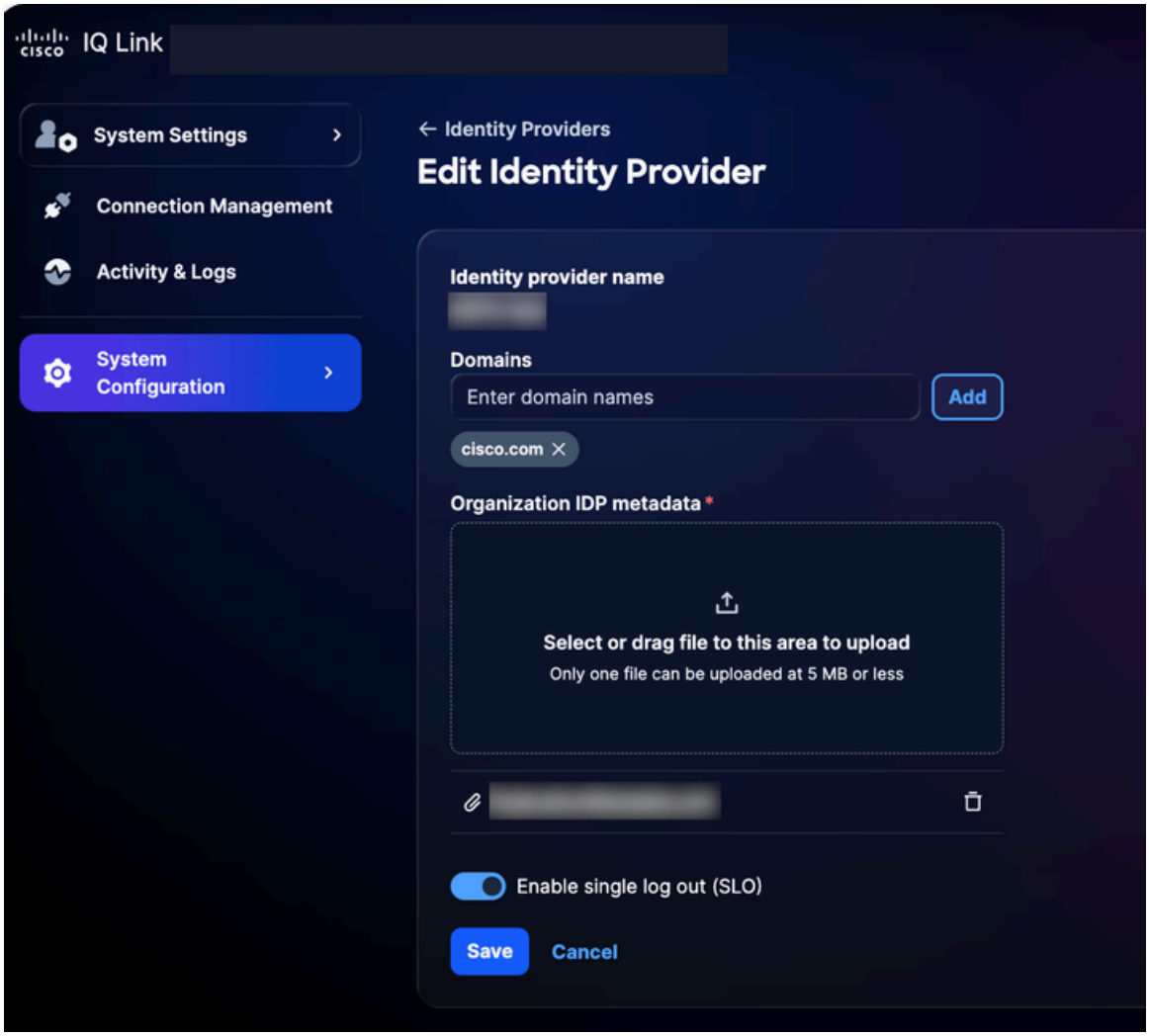
1. En la página Identity Providers, haga clic en Download SP public certificate.



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 la sección Configuración SAML de IDP para 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 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:

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 Microsoft Active Directory Federation Services (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 Active Directory configurada
- Certificados SSL/TLS en ADFS
- Acceso de administrador 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)

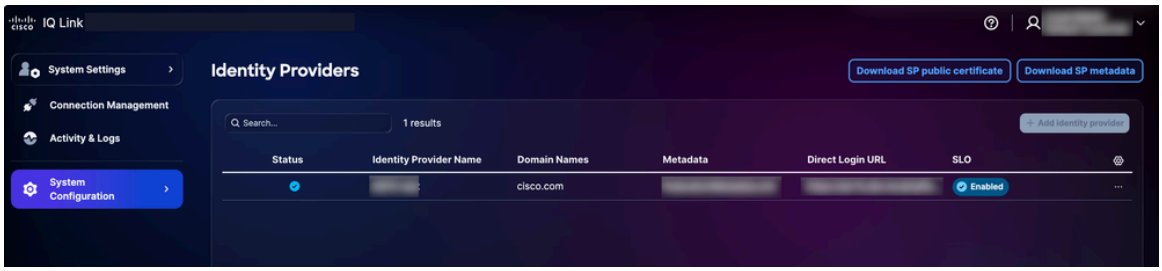
Configuración del servidor ADFS

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	Grupo de Active Directory Nombres de dominio (DN)	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 de un archivo acerca de la persona que confía.
10. Haga clic en Browse para seleccionar el archivo de metadatos del proveedor de servicios 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.

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.

Reclamaciones necesarias

Afirmación	Propósito	Fuente
Correo electrónico	Identificador de usuario	Correo AD
Mostrar nombre:	Nombre completo del usuario	Nombre para mostrar de AD
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 reglas de reclamación para enviar información de usuario y pertenencia a grupos 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 A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema

@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.Issu
```

```
@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname”, Issuer == “AD A
=> 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
```

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. Elija una de las opciones siguientes:

Nota: El certificado SP es emitido por una autoridad de certificación 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

- Importar el certificado de la CA emisora en el almacén Entidades de certificación raíz de confianza

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

3. Aplique los cambios reiniciando el servicio ADFS.

```
Restart-Service adfssrv
```

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.

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 Enable single logout toggle, 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 Active Directory para utilizarlos en la asignación. Para buscar grupos desde Active Directory, 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”] }
```

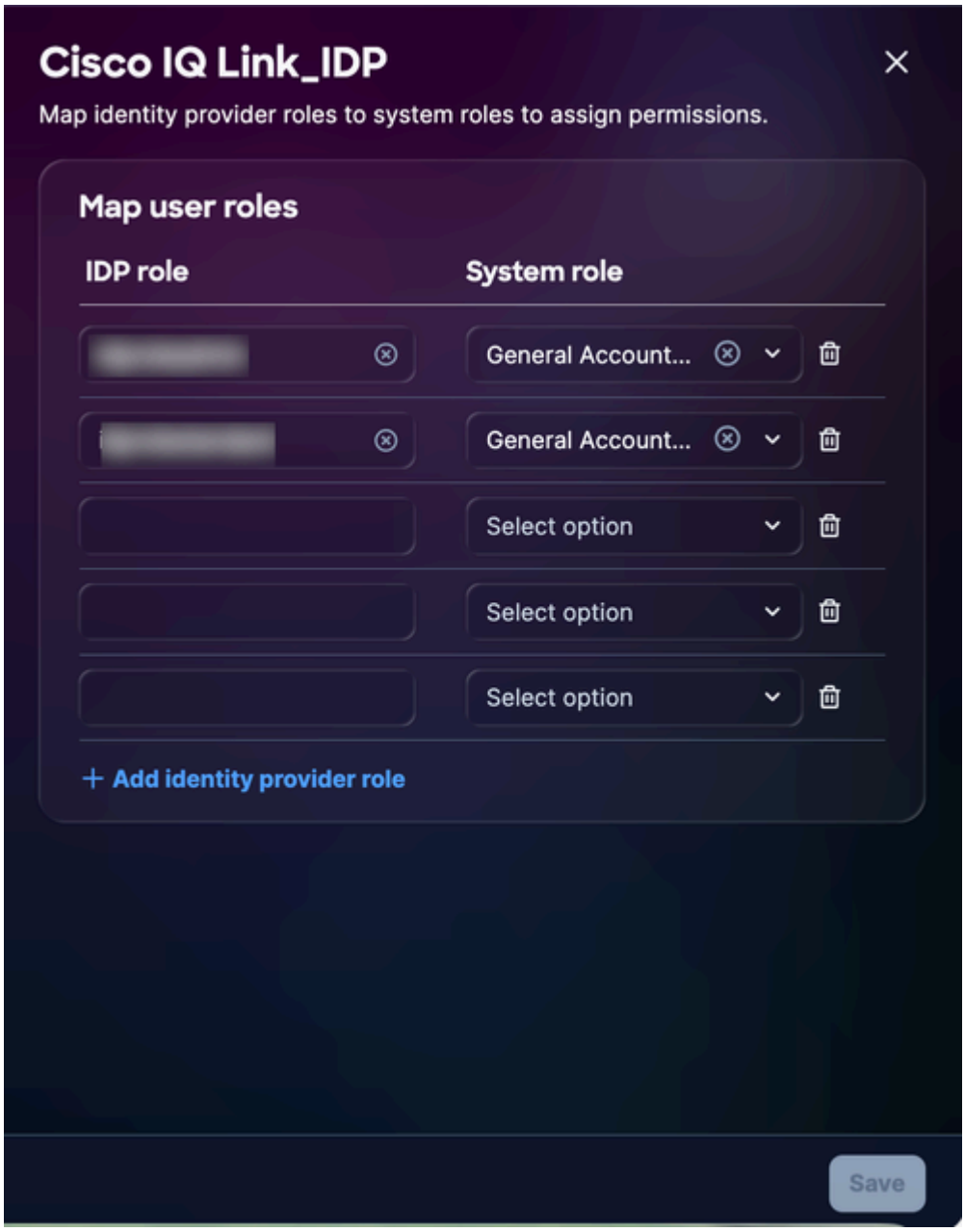
El sistema consulta a Active Directory directamente a través de LDAP, sin necesidad de módulos adicionales. La información de grupo se devuelve en formato completo de nombre distinguido (DN), por ejemplo:

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 debe crearlos en Active Directory para poder completar la asignación de funciones de ADFS.

Para configurar la asignación de roles:

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 del sistema seleccionado. Se admiten los siguientes roles del sistema:

   - administrador_cuenta_general: El administrador de cuentas general dispone de permisos completos para realizar todas las acciones del producto. El rol IDP (nombre analizado) es CXIQ Admins.
   - general_account__viewer: El visor general de cuentas tiene acceso de solo 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. Click Save. El estado se actualiza a Correcto.

Verificación y pruebas

Probando autenticación

1. En un navegador en modo Incógnito o Privado, navegue hasta https://your-cisco-iq-domain.com/login.
2. Inicie sesión con sus credenciales de Active Directory en el formato dominio\nombre de usuario o user@domain.local.
3. Verifique que se le redirige a la página de inicio de Cisco IQ (después de una autenticación exitosa).
4. Confirme que los roles asignados muestren los nombres de grupo analizados correctos (por ejemplo, CXIQ Developers) en su perfil de usuario.

Probar cierre de sesión

Para probar el cierre de sesión, haga clic en Cerrar sesión en Cisco IQ. Se muestra el mensaje "Logging out, please wait..." (Cerrando sesión, espere...) y se le redirige a la página de inicio de sesión de Cisco IQ. El sistema también finaliza la sesión de ADFS. Si intenta acceder directamente a ADFS, se le solicitará que vuelva a iniciar sesión.

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.

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

Problema	Síntomas / Descripción	Causas / Comprobaciones / Soluciones temporales y soluciones
		• Atributo de grupo incorrecto: Debe ser http://schemas.xmlsoap.org/claims/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-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

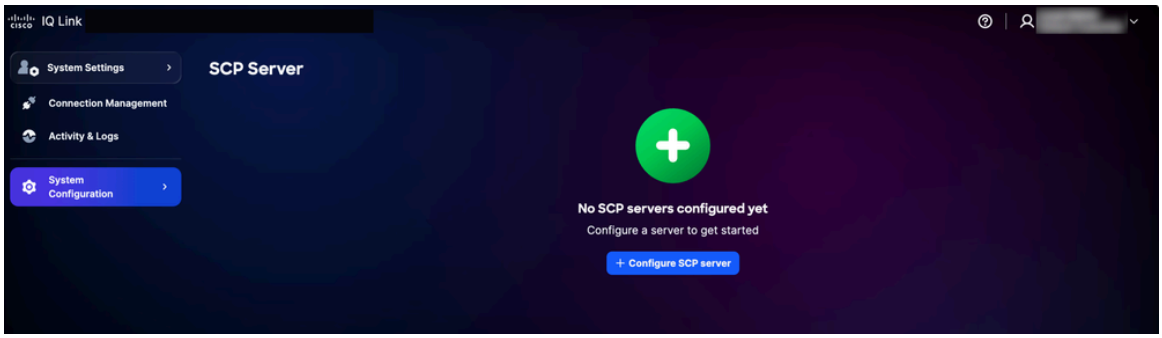
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

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 reparar la instalación de Cisco IQ.

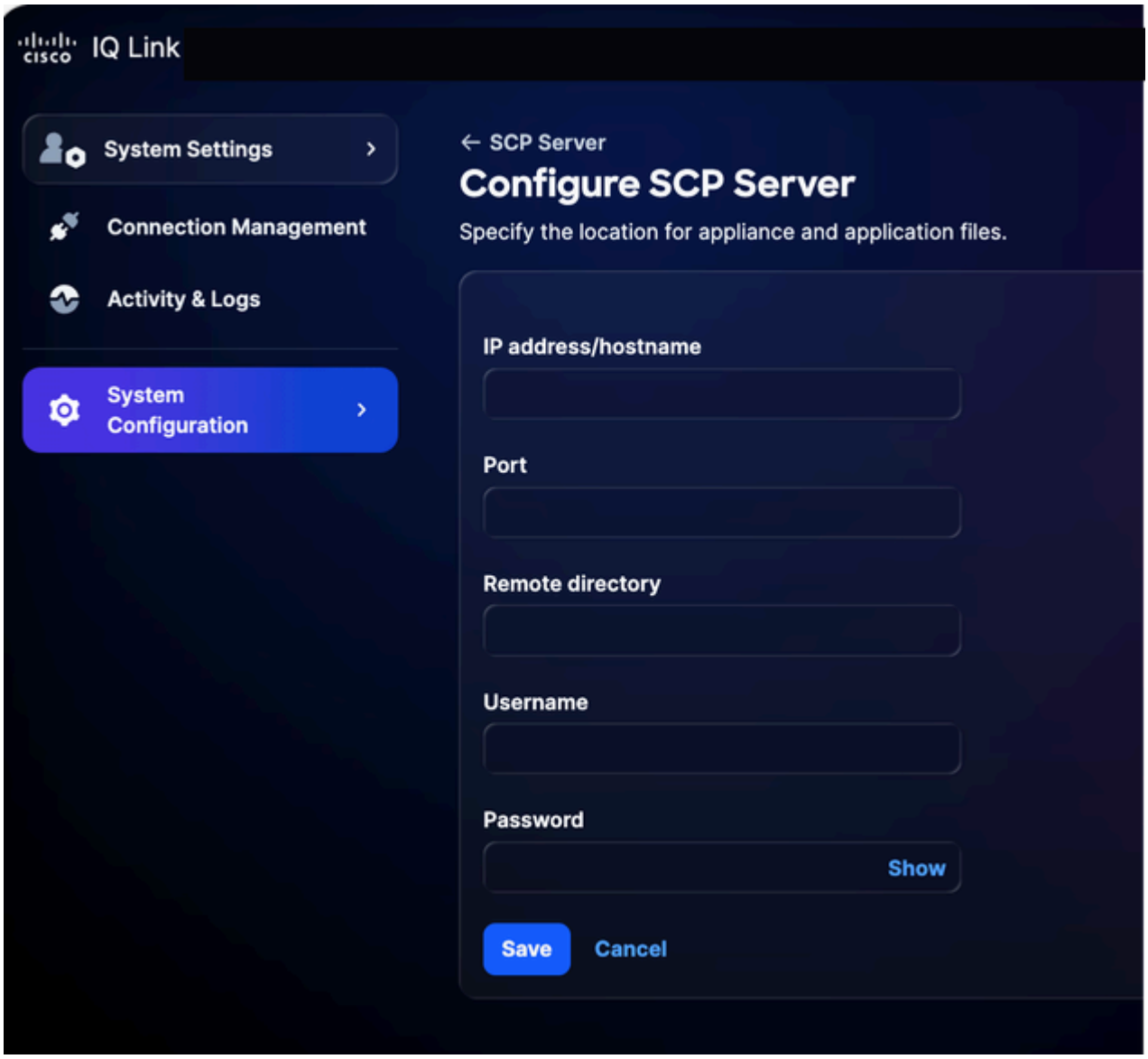
Para agregar un servidor SCP:

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.



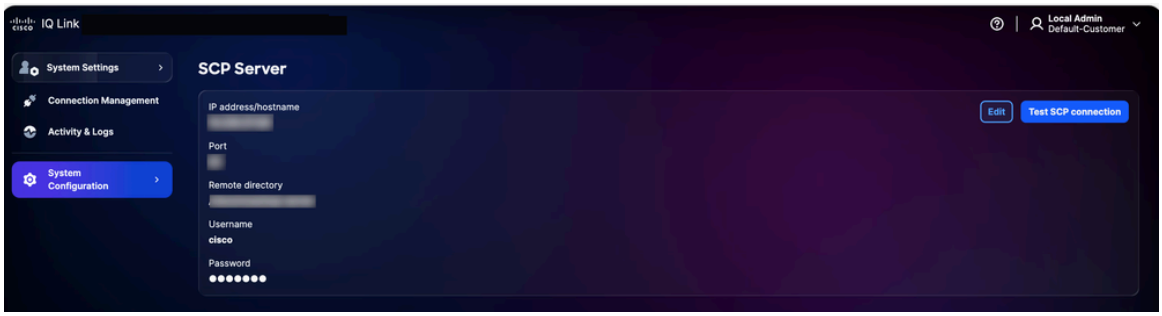
Configuración del servidor SCP

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

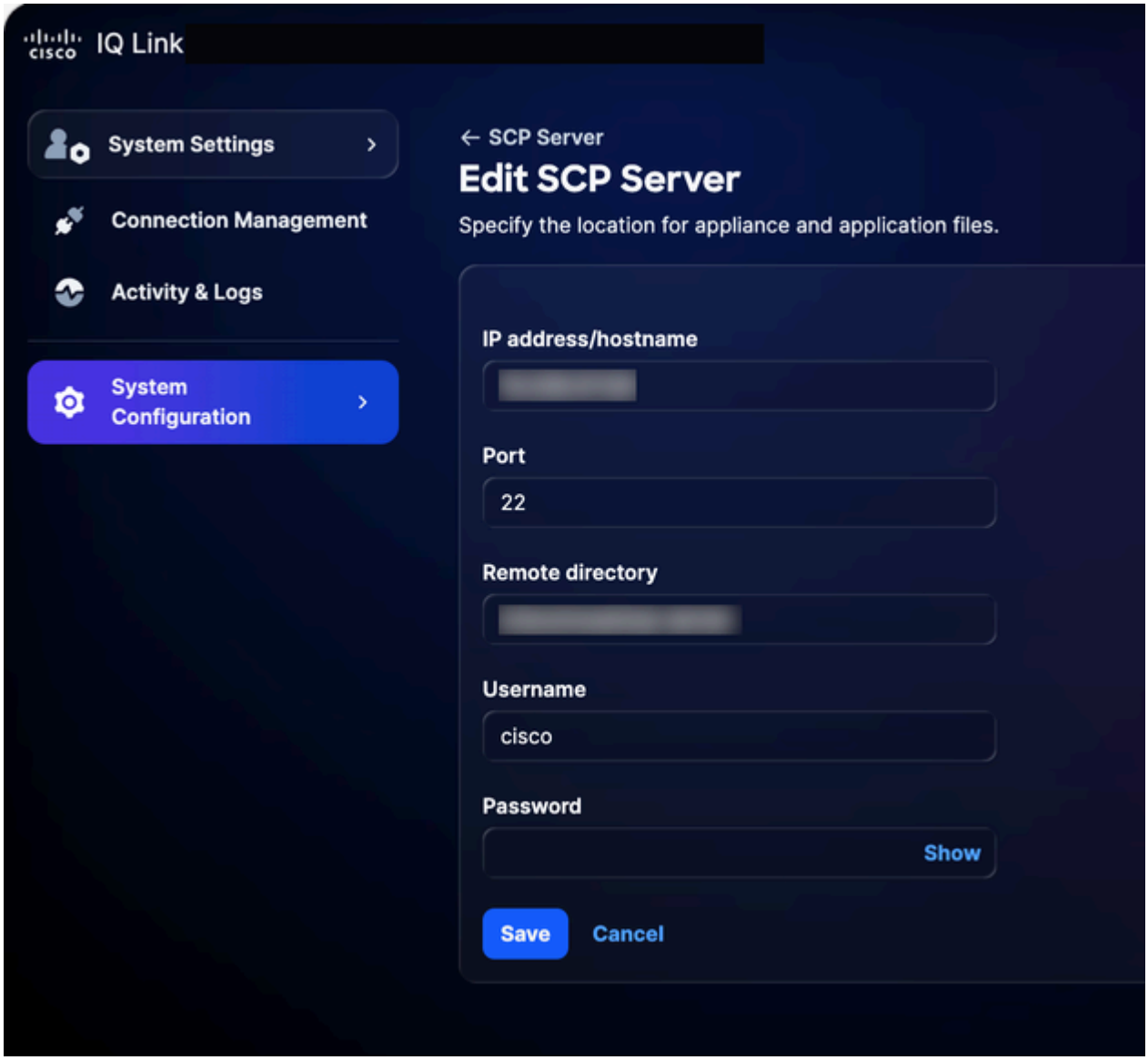
Para editar un servidor SCP existente:

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.

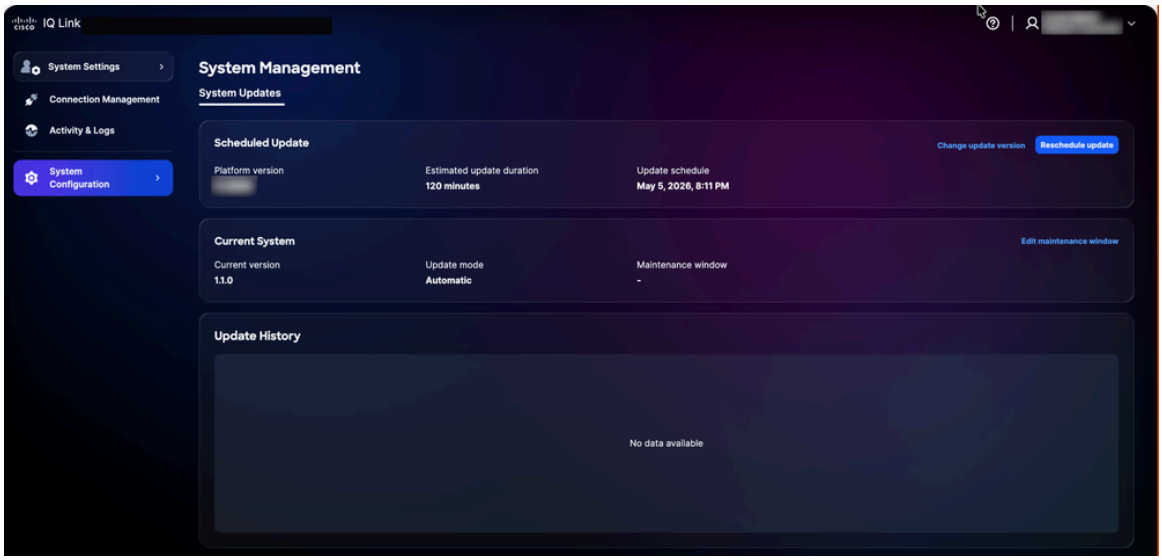
Actualización de administración del sistema

Los clientes pueden 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.

Sistema de reprogramación

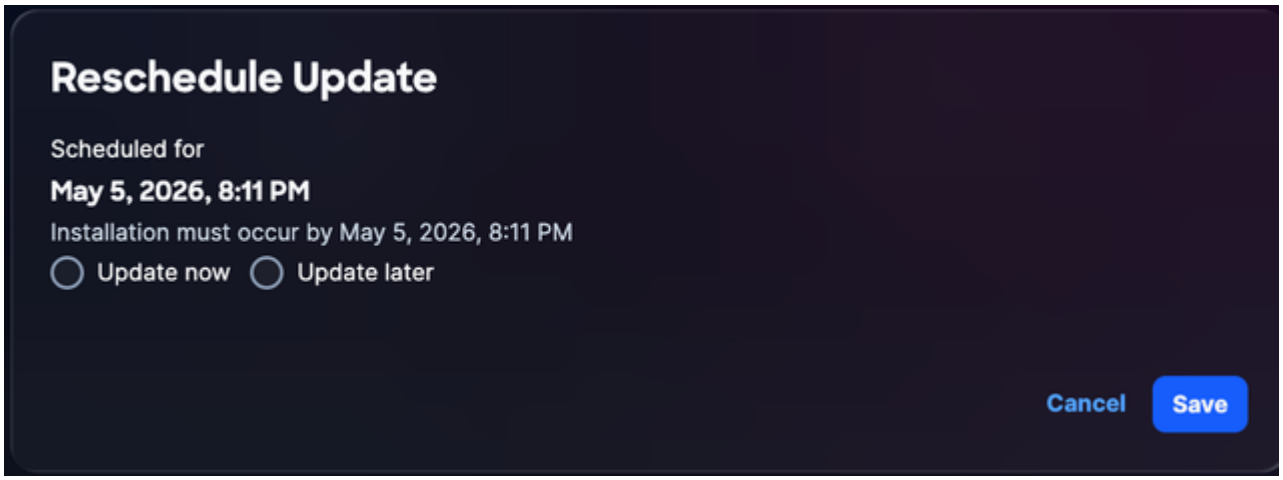
Para reprogramar la actualización del sistema:

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.



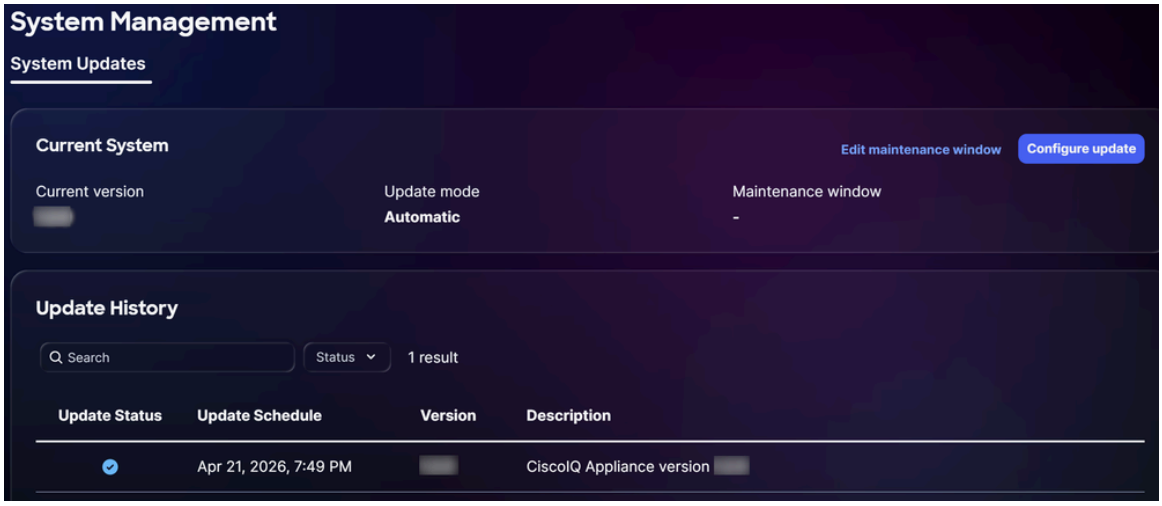
Actualización del sistema

2. Haga clic en Reprogramar actualización.



Reprogramar actualización

3. Haga clic en Update Now para una reprogramación inmediata o en 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.



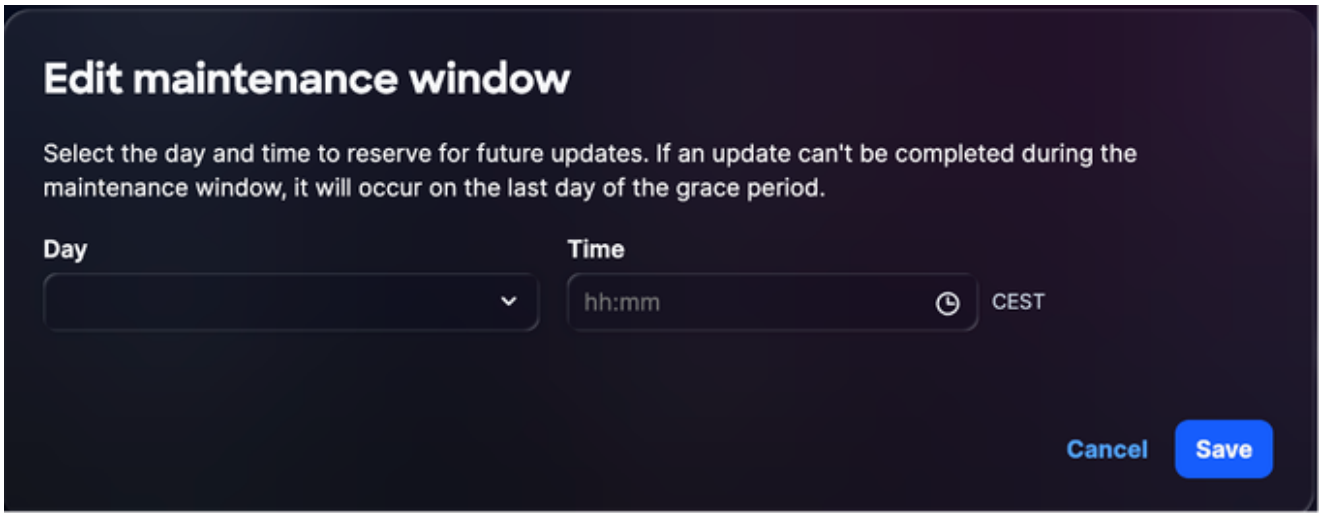
Actualización correcta

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.

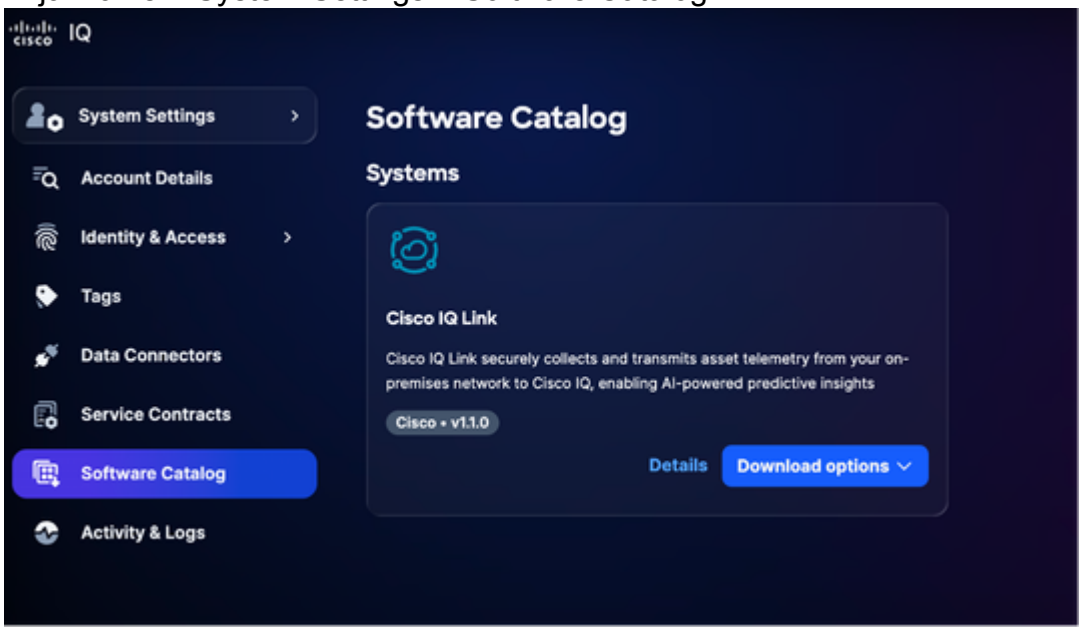
Notas:
· Si no se configura ninguna programación de actualización, el sistema establece de forma predeterminada períodos de gracia de dos (2) semanas para las actualizaciones sin reinicio y de cuatro (4) semanas para las actualizaciones que requieren reinicio. Después de estos períodos de gracia, las 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.

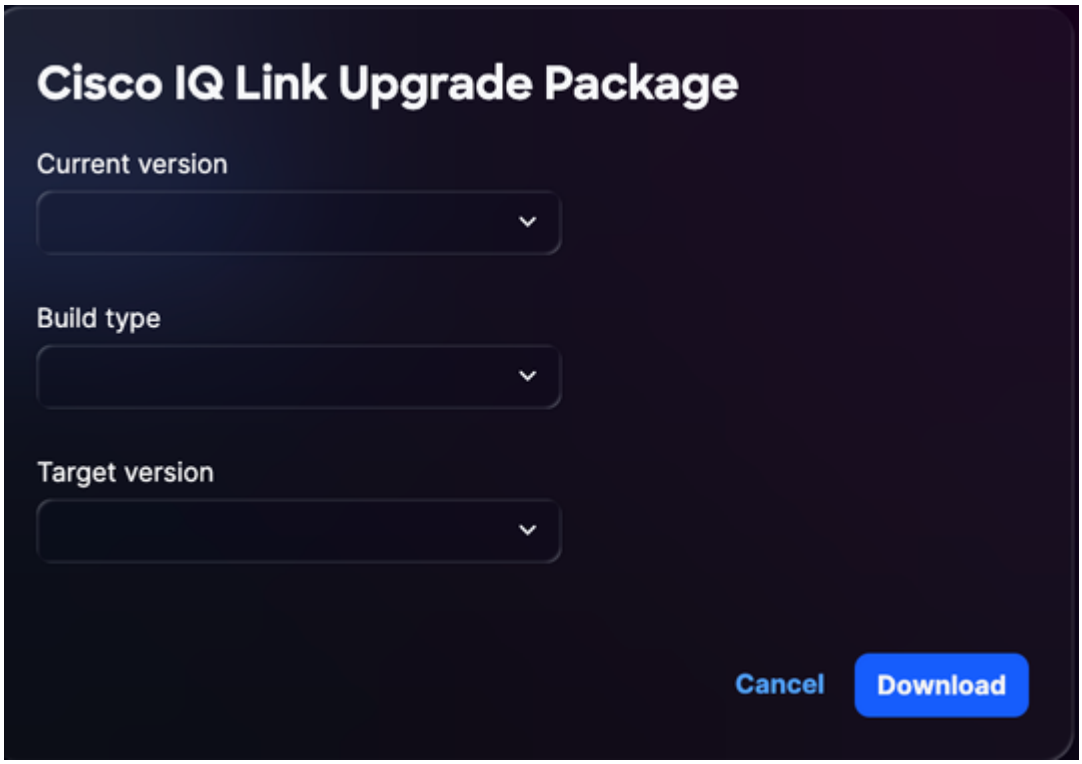
Para actualizar manualmente el sistema:

1. Inicie sesión en Cisco IQ SaaS.
2. Elija Home > System Settings > Software Catalog.



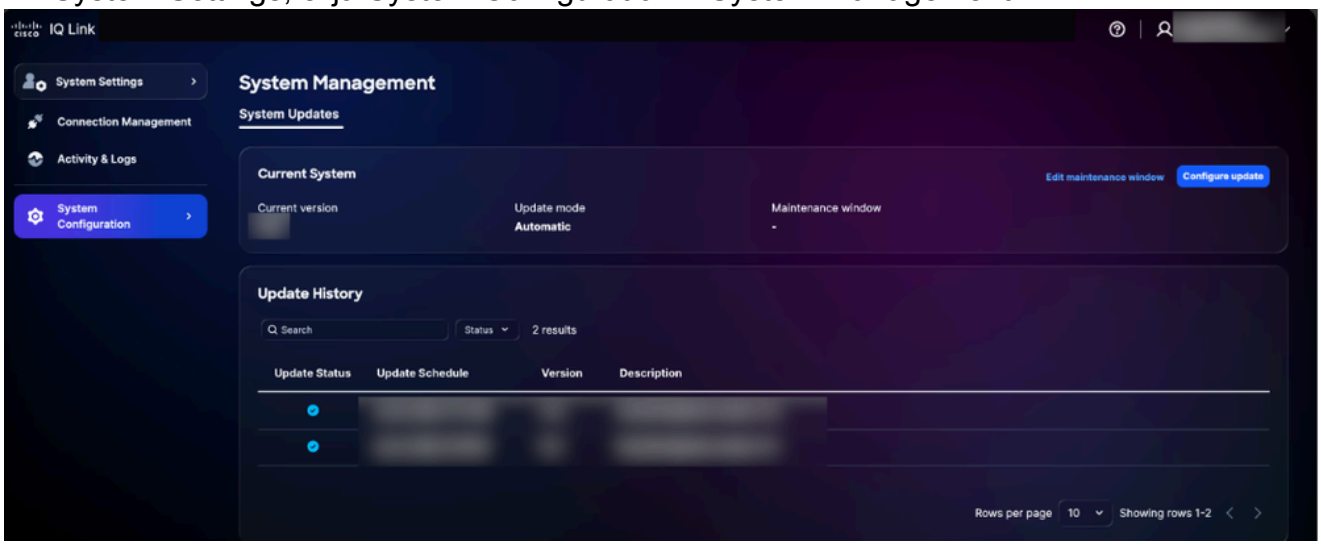
Catálogo de software

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



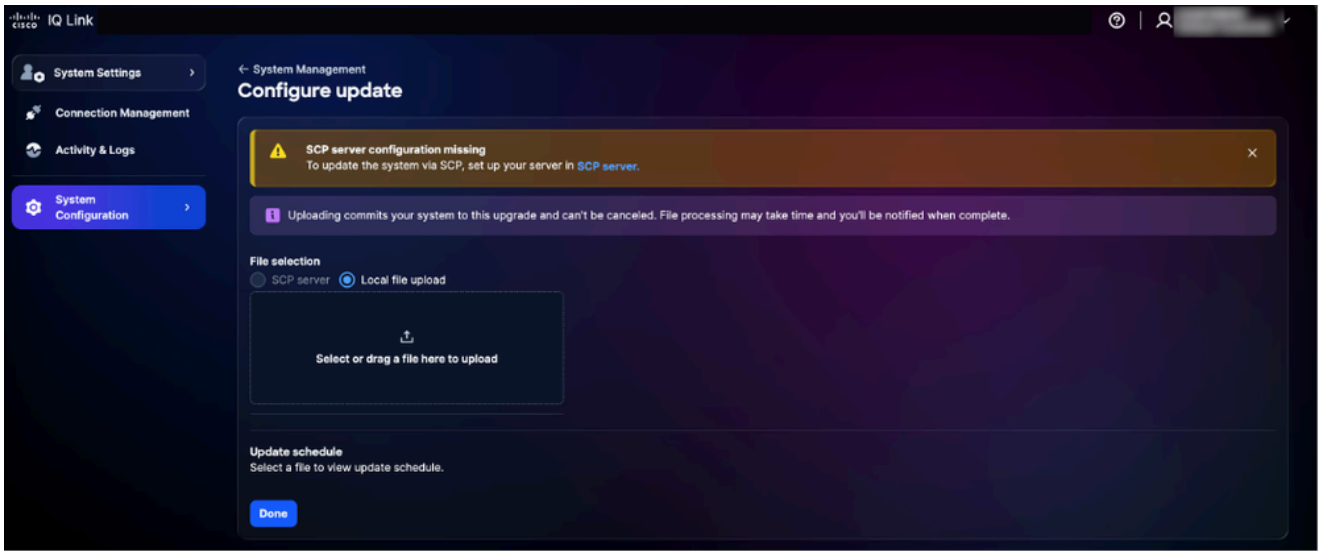
Paquete de actualización

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



Configurar actualización

10. Haga clic en Configurar actualización.



Carga de archivos locales

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

Configuración de certificados SSL

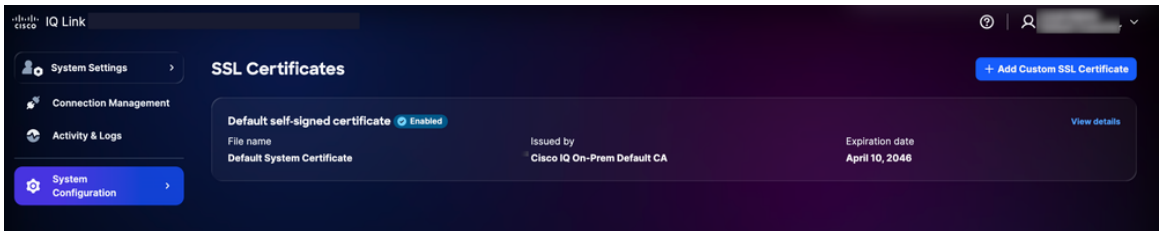
Un certificado autofirmado predeterminado está preinstalado y habilitado en Cisco IQ, pero los usuarios pueden cargar certificados SSL personalizados. Cuando se habilita un certificado SSL personalizado, se utiliza para conexiones HTTPS; si el certificado está deshabilitado o eliminado, el sistema vuelve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

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, el cliente debe cargar el nuevo SSL como se describe en la sección Finalización de la Configuración de SLO 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.

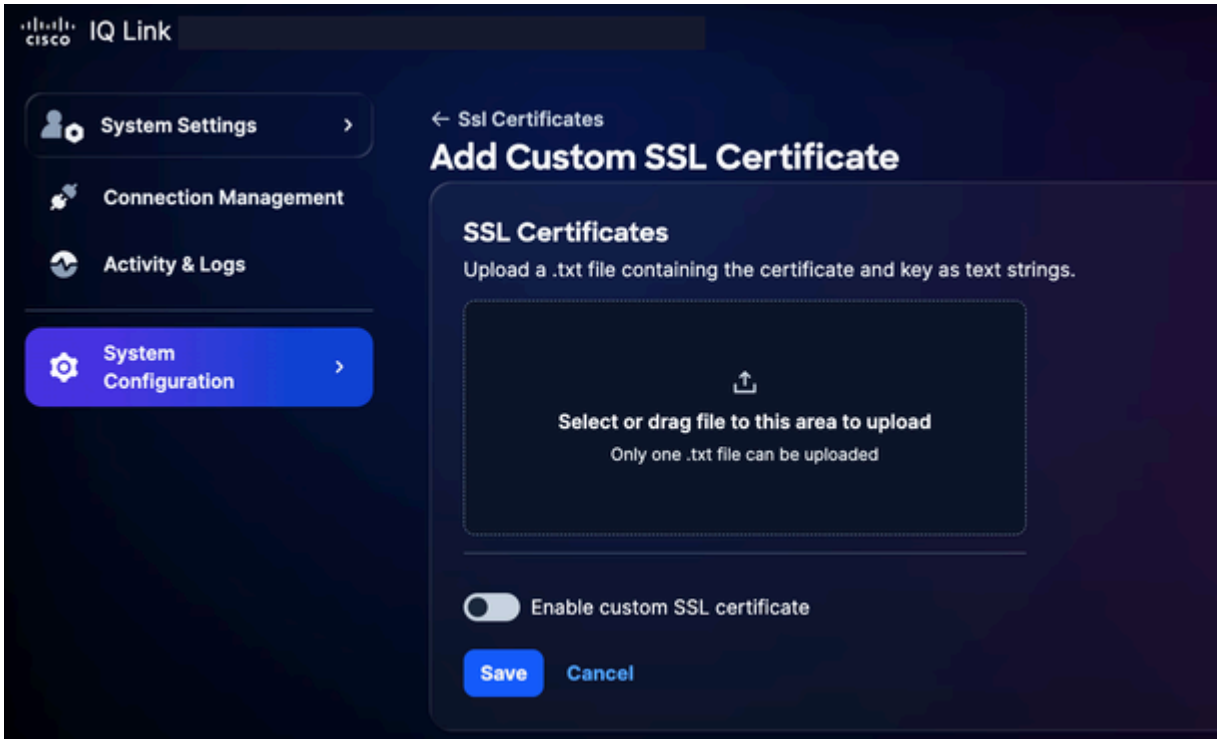


Agregando certificado SSL

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
· Solo se puede cargar un archivo .txt a la vez
· El archivo debe contener tanto el certificado como la clave privada

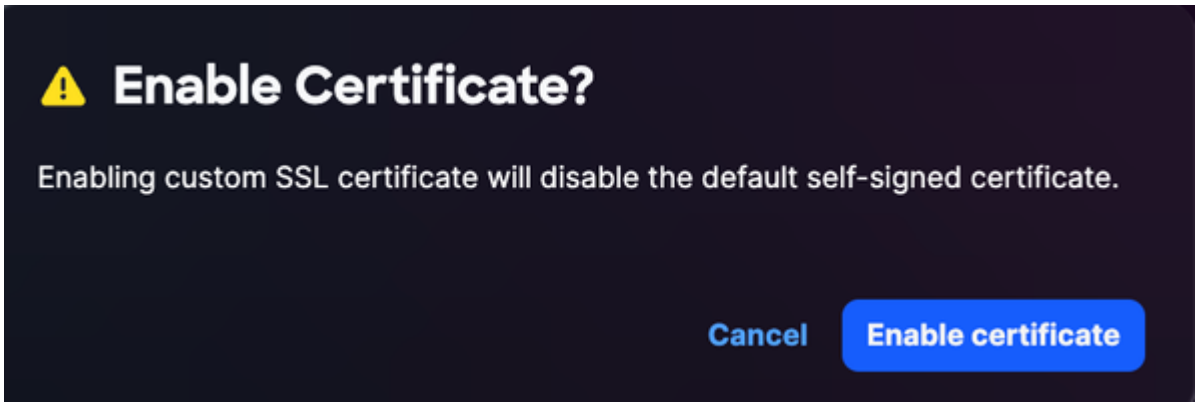
---



Cargar certificados SSL

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

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



Habilitar certificado

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

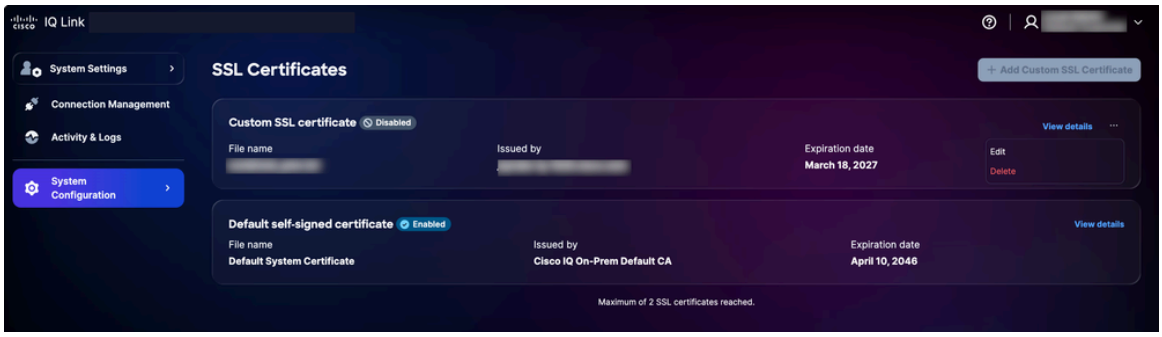
5. Haga clic en Habilitar certificado.
6. Click Save.

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

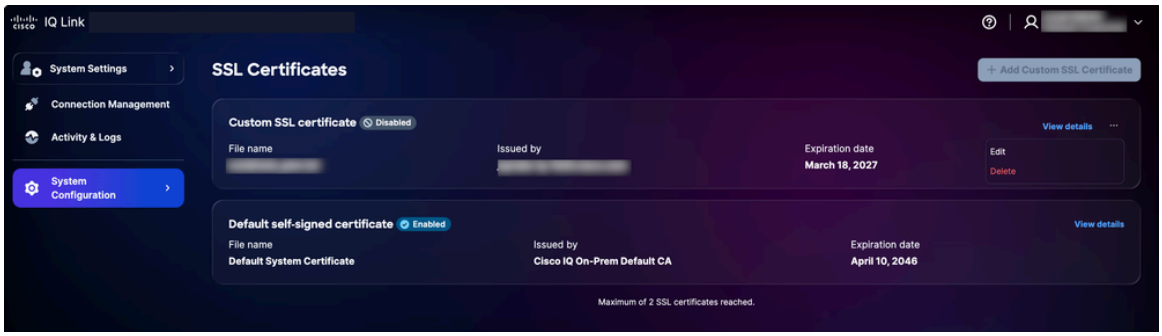
2. Elija el icono Más opciones > Editar. Se muestra la página Editar Certificado SSL.
3. Edite los detalles del certificado según sea necesario.
4. Click Save.

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. Desplácese hasta el certificado SSL personal deseado.



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

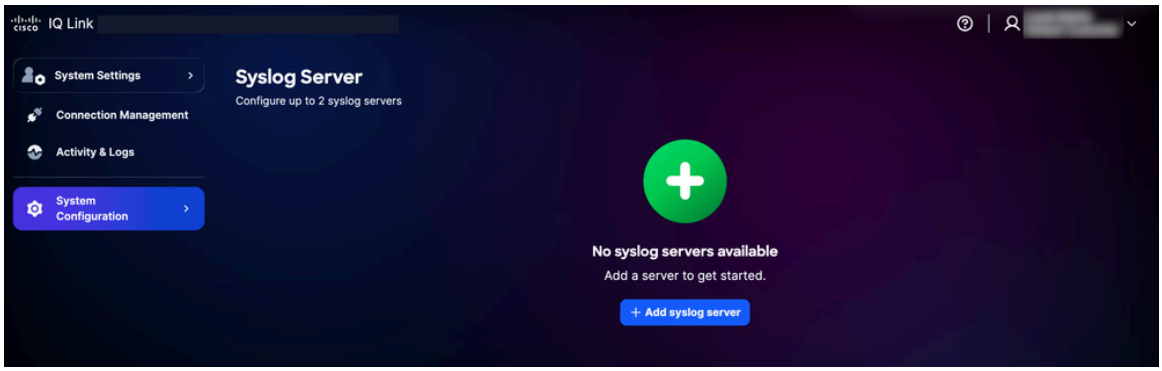
Los usuarios con la función de administrador pueden configurar servidores syslog externos para exportar registros del sistema. Se pueden configurar hasta dos (2) servidores syslog.

Nota: El servidor Syslog debe especificarse como una dirección IP, no como un nombre de dominio completo (FQDN).

Agregar servidores Syslog

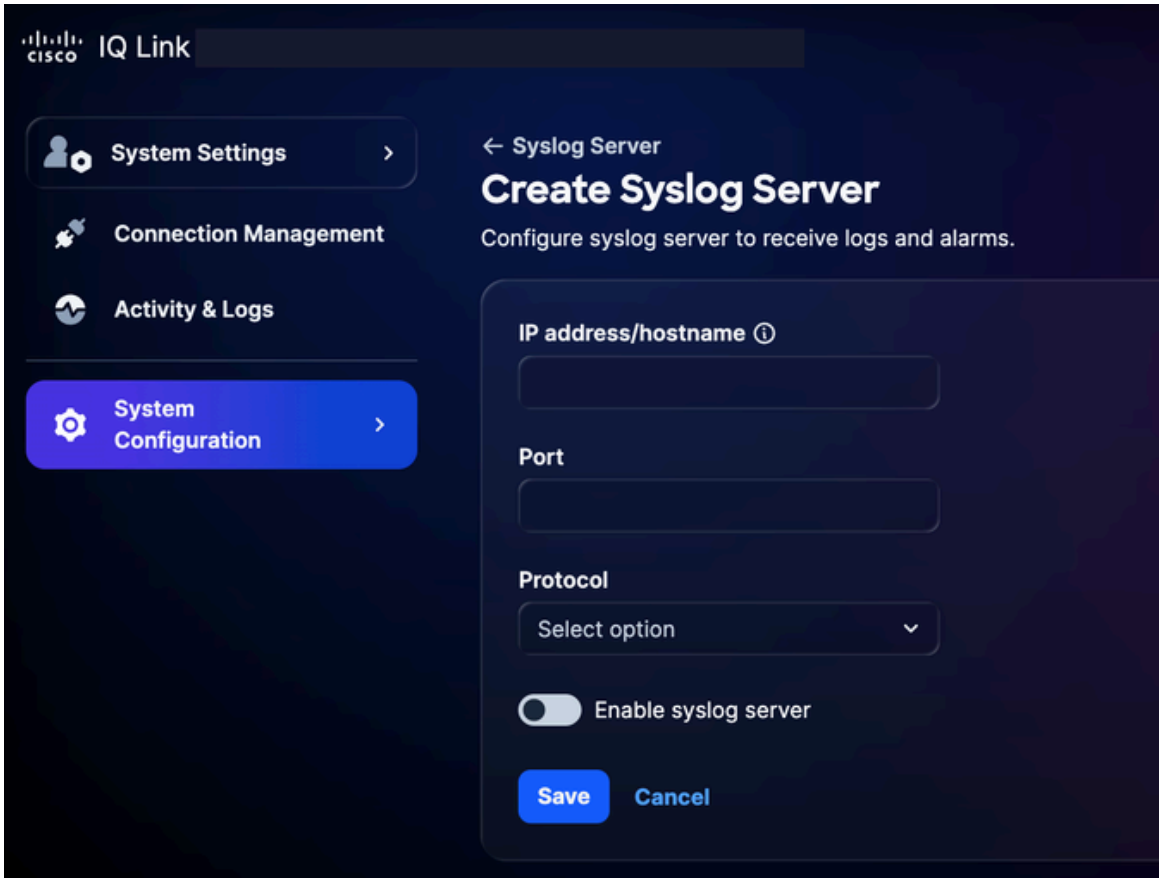
Para agregar un servidor syslog:

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.



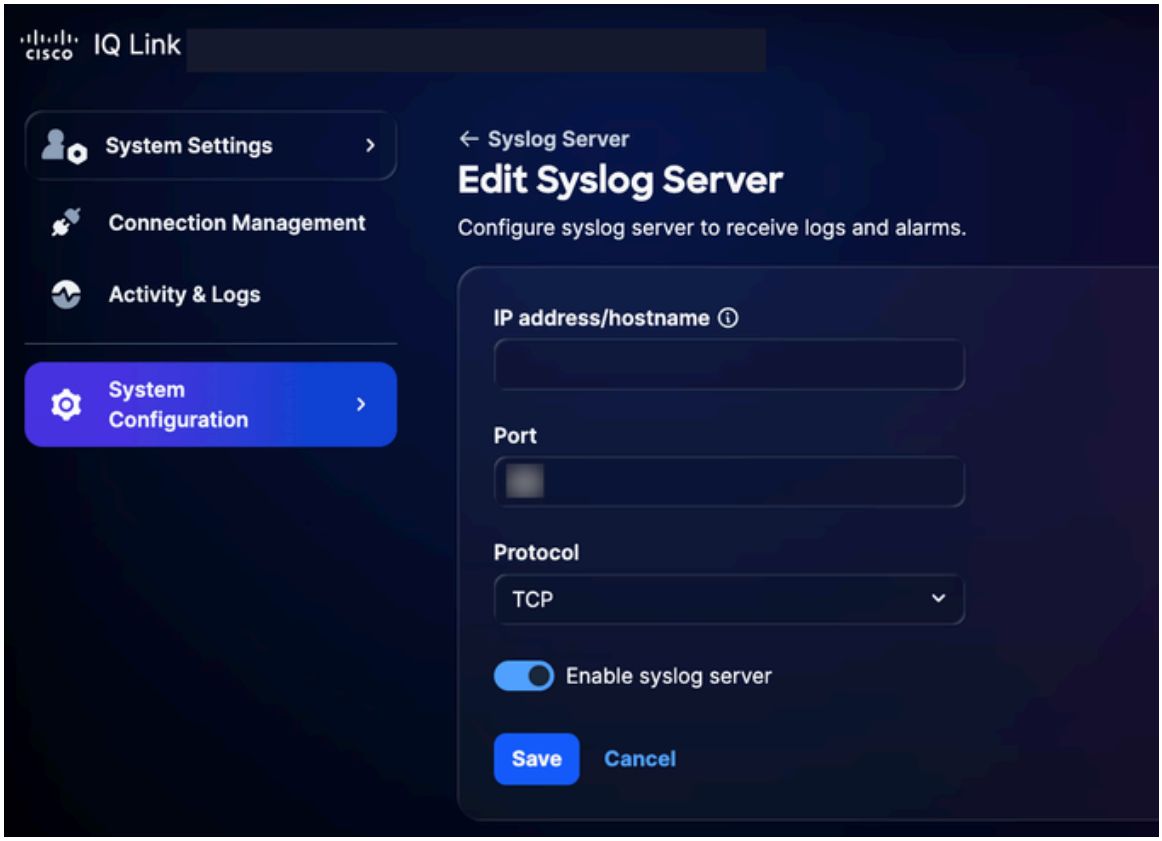
Crear servidor Syslog

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. Aparecerá una confirmación y el servidor syslog recién agregado aparecerá 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.



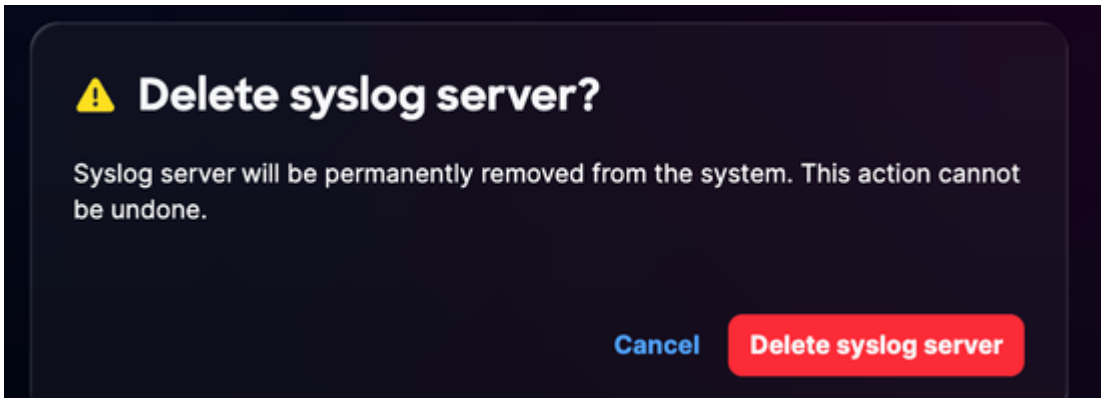
Editar servidor Syslog

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.

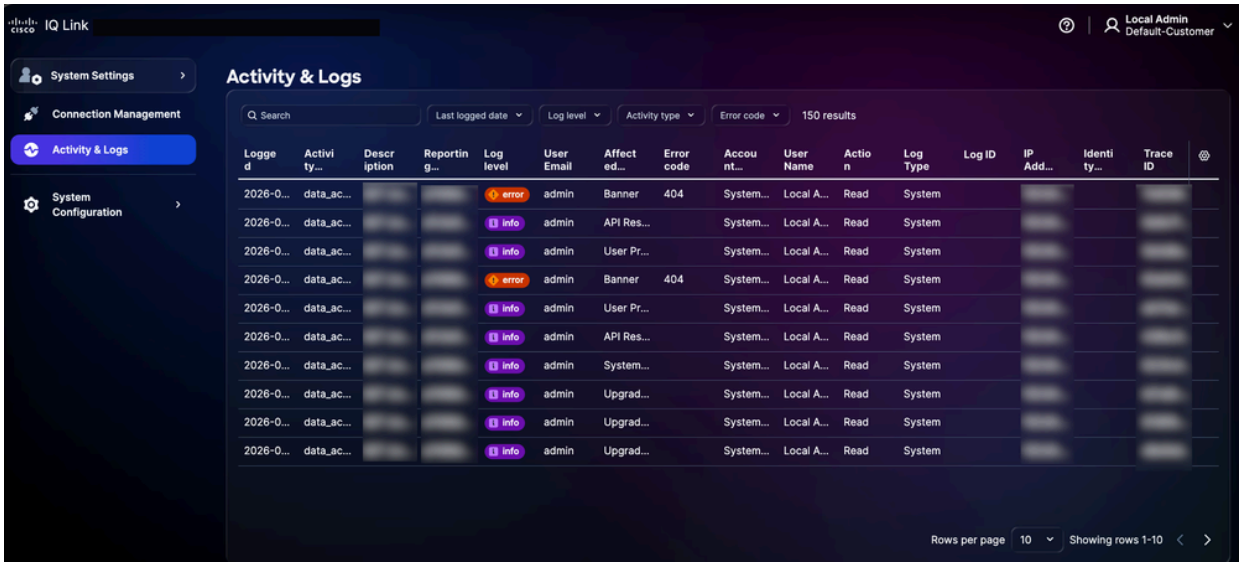


Confirmación

3. Haga clic en Delete syslog server.

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 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:

- Admita filtros, paginación y funciones de búsqueda para encontrar y administrar información con facilidad

- Registre todas las operaciones de la API en el nivel de gateway

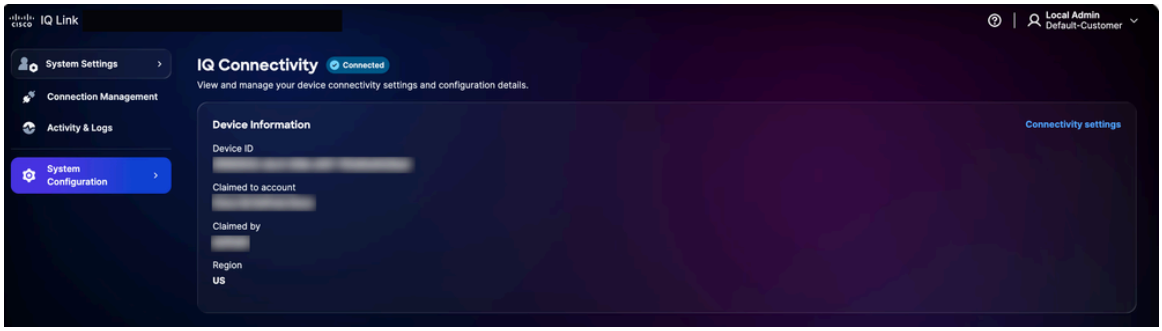
Están disponibles las siguientes opciones de filtro:

- 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

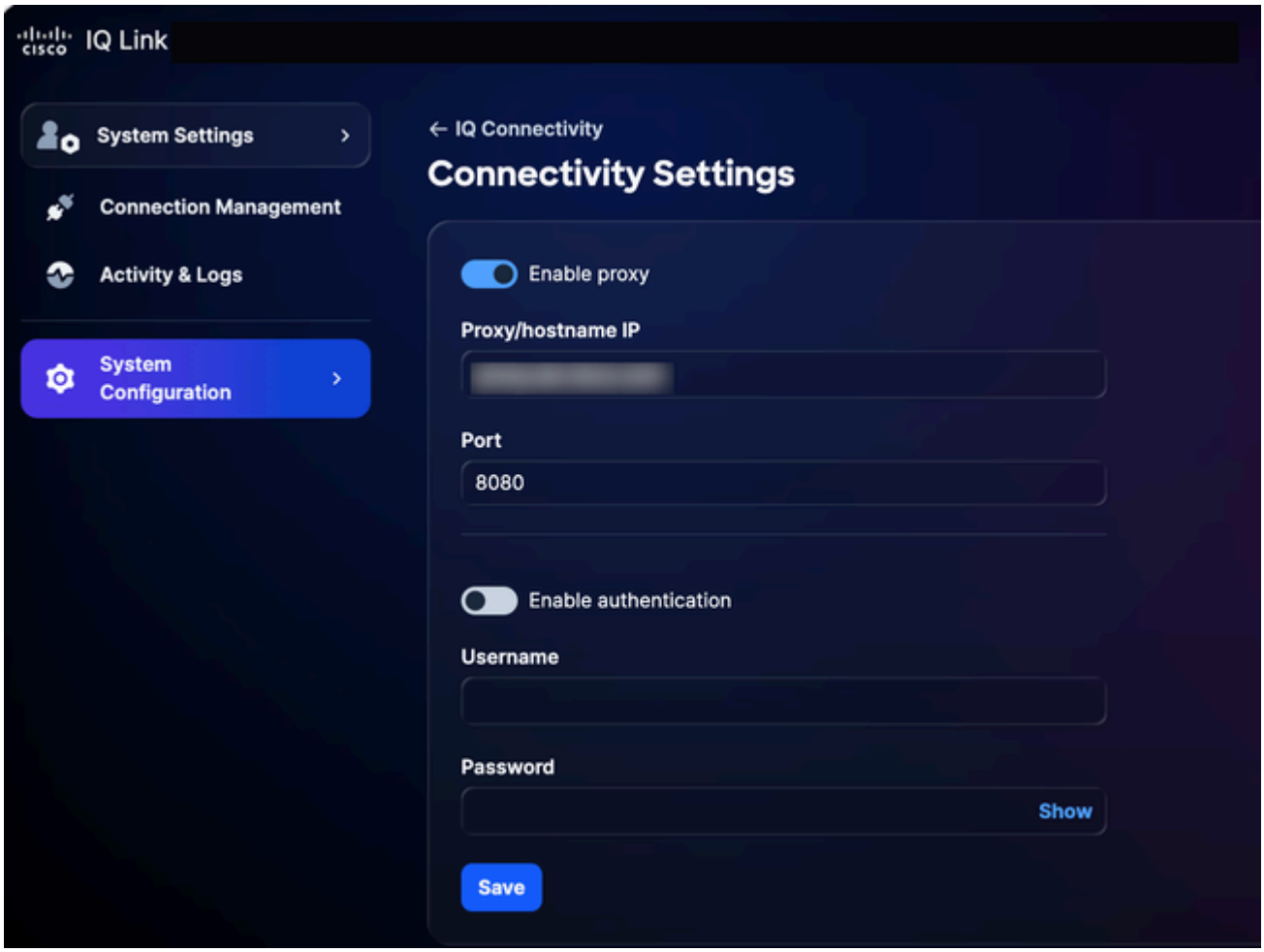
Para ver y administrar los parámetros de conectividad y los detalles de configuración del dispositivo:

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 implementada en las instalaciones para la recopilación de datos de red, diseñada para proporcionar una amplia 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 puede resumir de la siguiente manera:

- Creación de conjuntos de credenciales: Establezca los protocolos de autenticación (por ejemplo, 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.

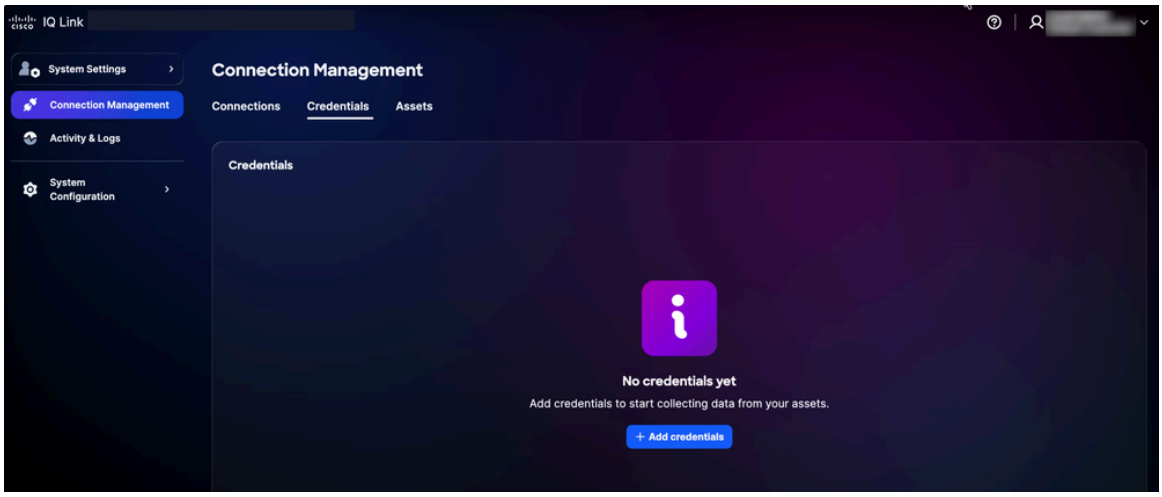
- Asignación de credenciales al inventario: Asigne sus conjuntos de credenciales a los recursos de inventario para automatizar el proceso de autenticación. Al crear reglas que vinculan rangos de IP específicos a conjuntos de credenciales definidos, el sistema aplica automáticamente la autenticación correcta 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

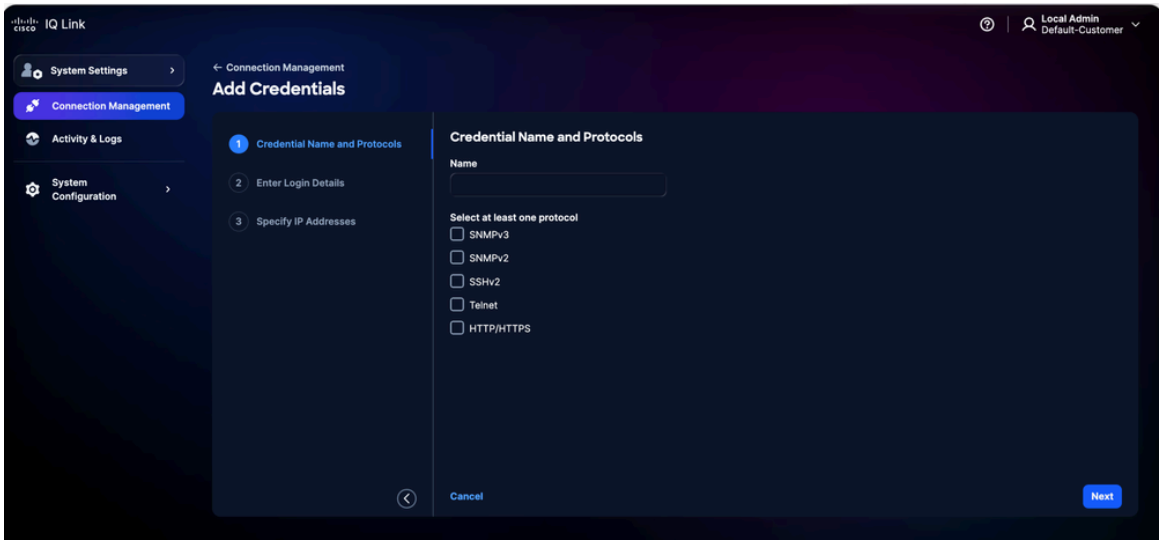
En primer lugar, debe agregar credenciales para realizar la recopilación de datos. Para agregar credenciales:

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



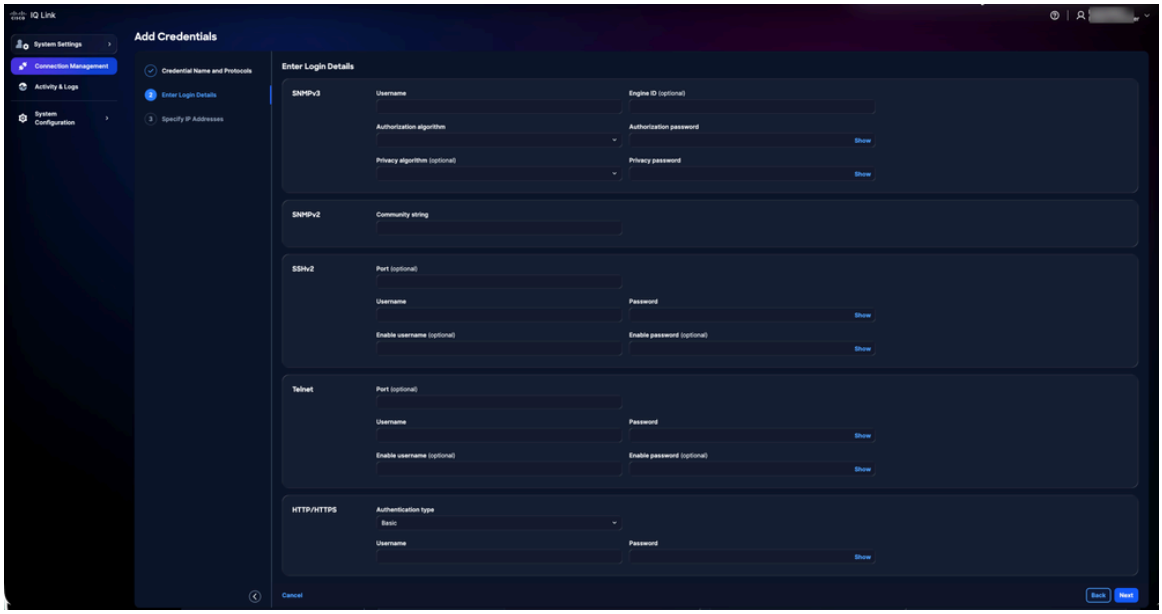
Ficha Credenciales

3. Haga clic en Agregar credenciales.



Agregar credenciales

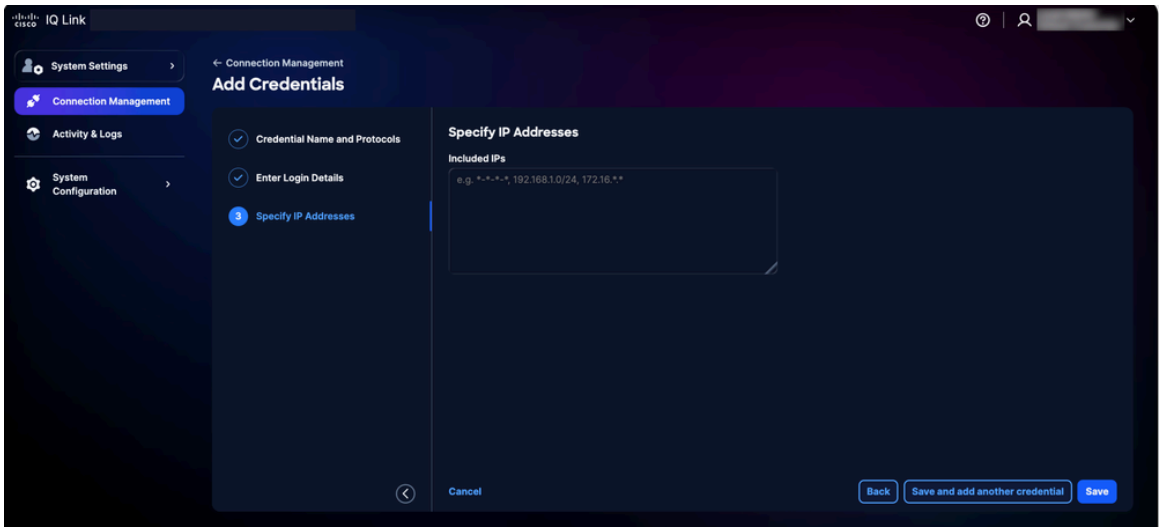
4. Introduzca Nombre.
5. Marque todas las casillas de verificación de protocolo aplicables.
6. Haga clic en Next (Siguiente).



Agregar detalles de credenciales

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

7. Introduzca los detalles de inicio de sesión para cada protocolo seleccionado.
8. Haga clic en Next (Siguiente).



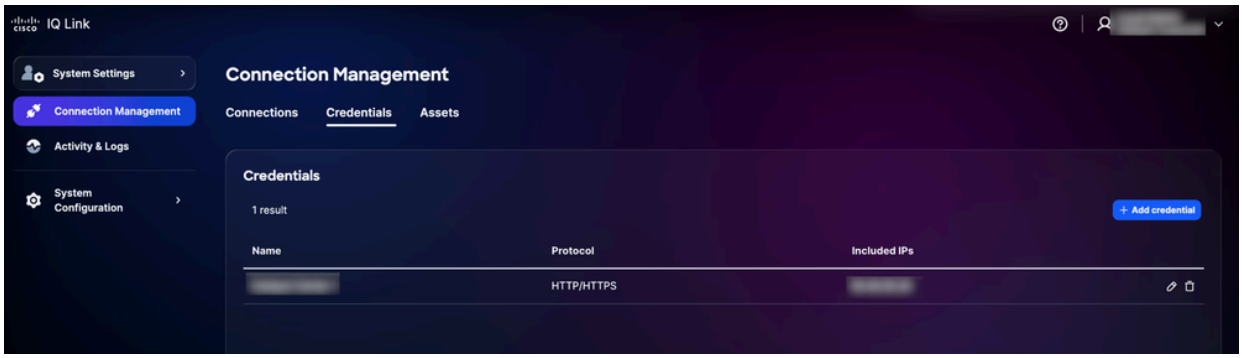
Especificar direcciones IP

9. Ingrese las IPs 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. Click Save. 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.

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,	10.10.1.5 (Coincidencia

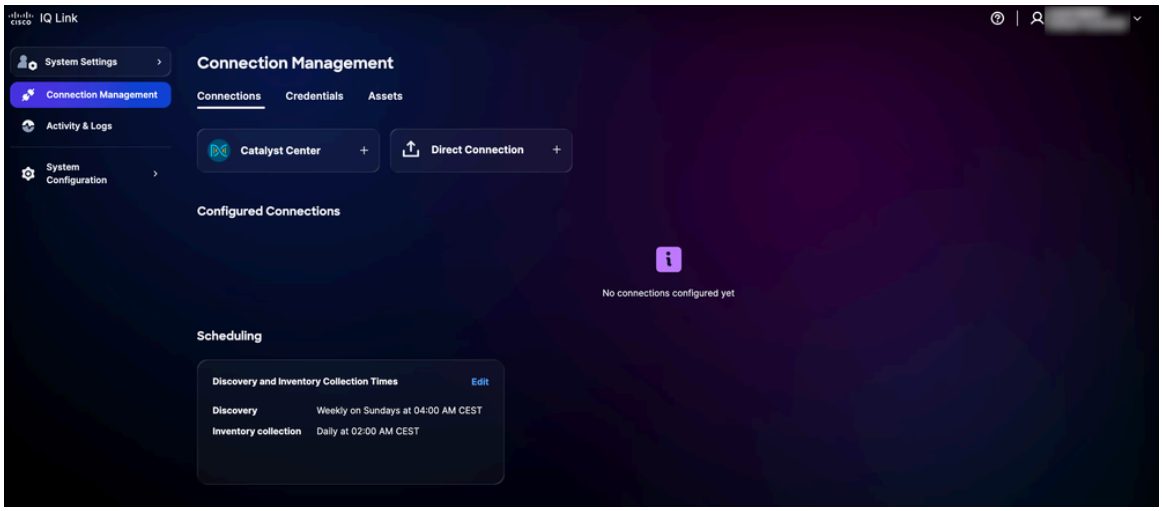
IP del dispositivo	Conjuntos de credenciales disponibles	Conjunto de credenciales seleccionado
	10.10.*	exacta)
10.10.2.15	10.10.2, 10.10.10.*	10.10.2.* (Más específica)
10.10.5.50	10:10 ..., ...	10.10.2010. (Más específica)

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

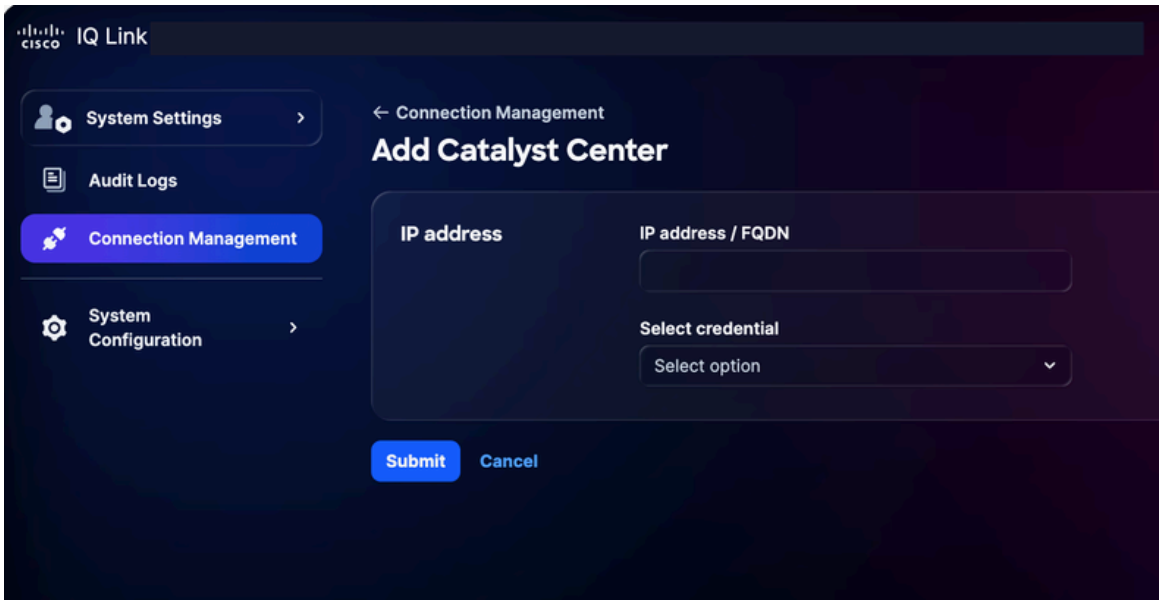
Para la recopilación de datos mediante Catalyst Center:

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



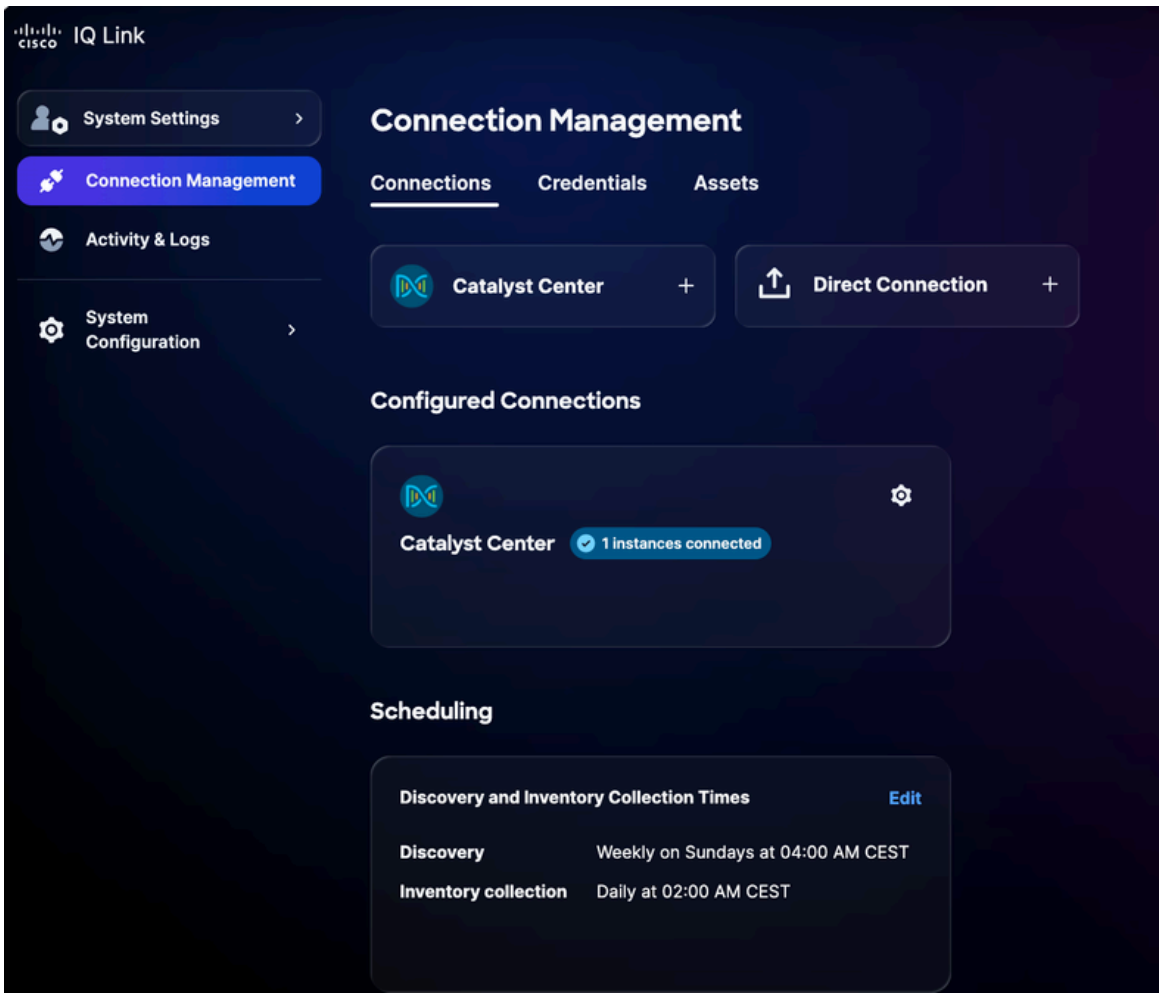
Administración de conexiones

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

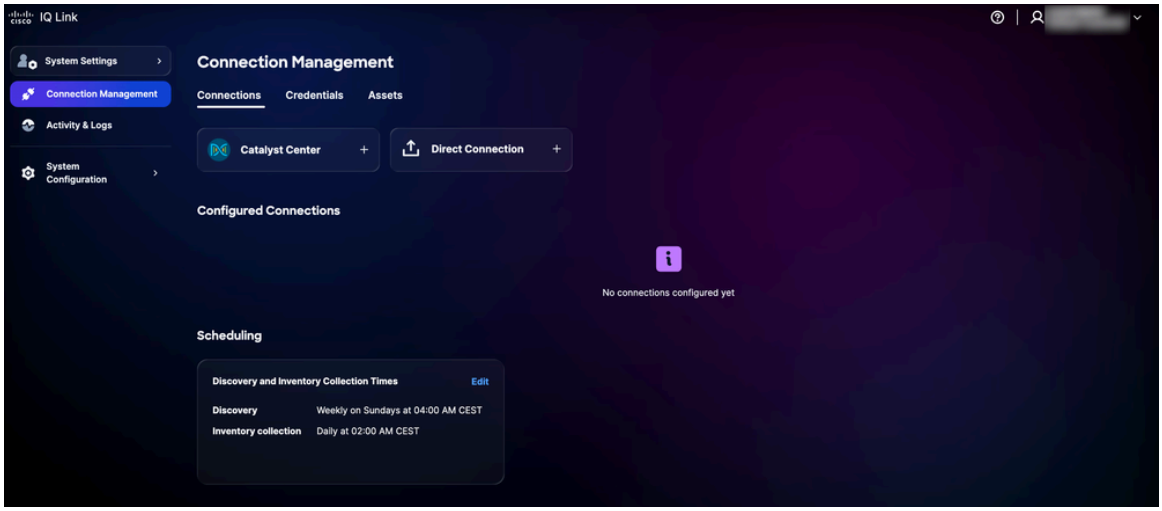
6. Programe una recopilación. Consulte Programación para obtener más detalles.

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

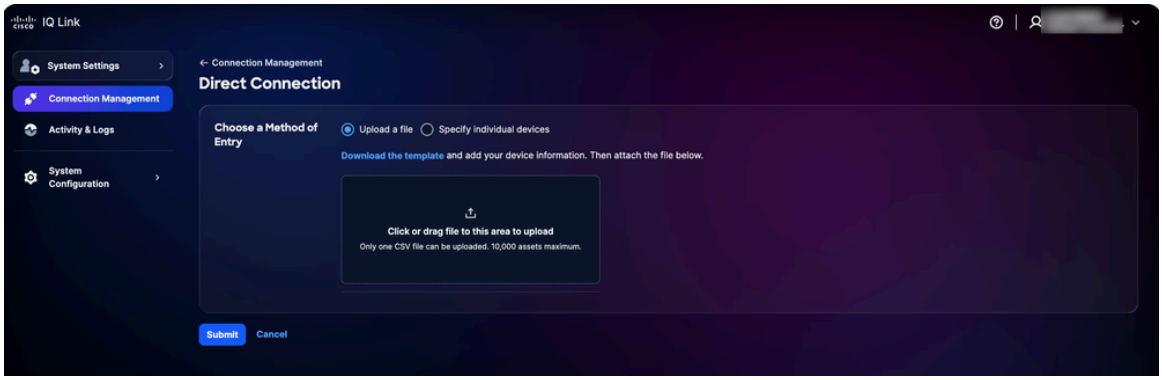
Para agregar dispositivos para la conexión directa:

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



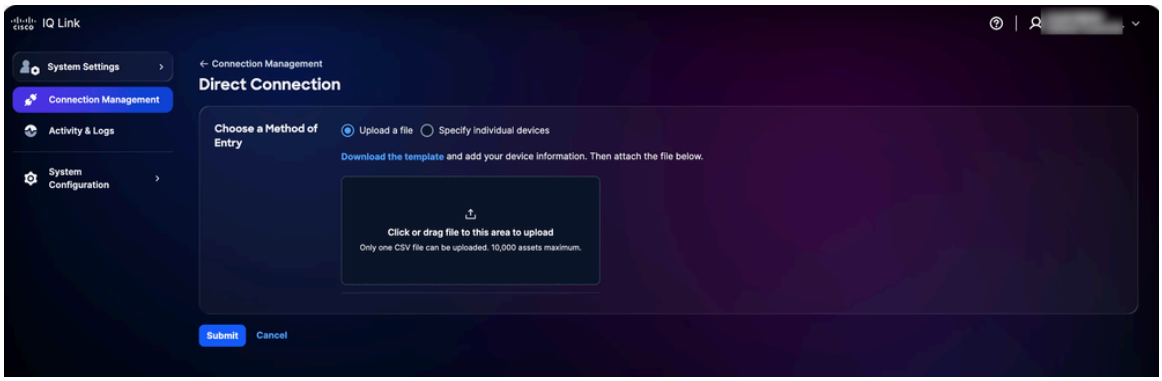
Administración de conexiones

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



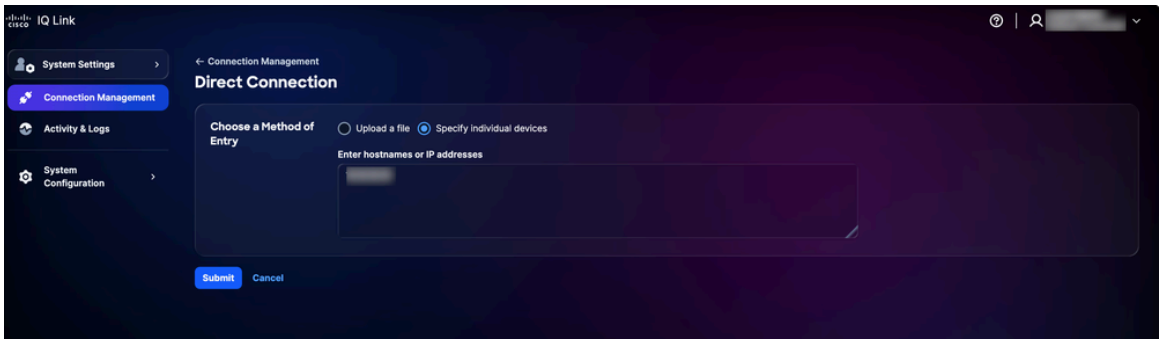
Cargar archivo

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.

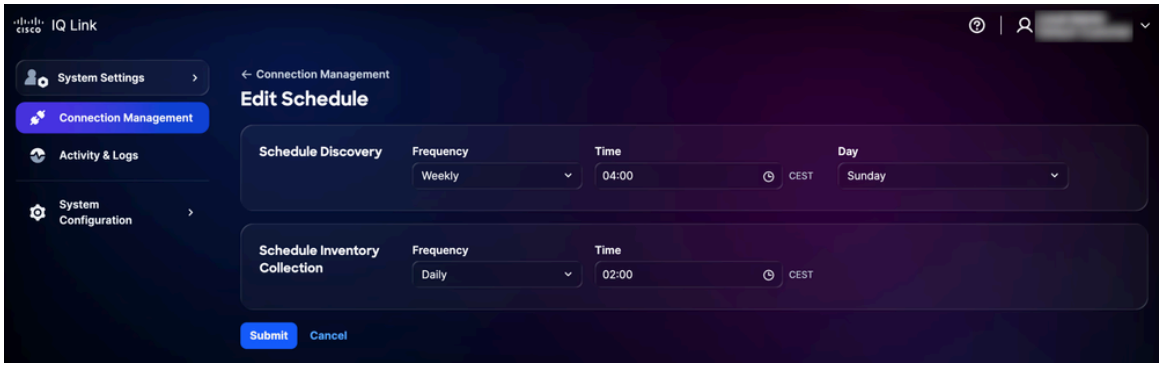
Nota: Cisco IQ Link está preconfigurado con una configuración de programación automatizada y el sistema inicia una programación de recopilación automatizada predeterminada. Se recomienda encarecidamente que edite la programación para ajustarla a los requisitos y ventanas de mantenimiento de su organización.

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 pueden configurar banners personalizados que se muestran en toda la aplicación.

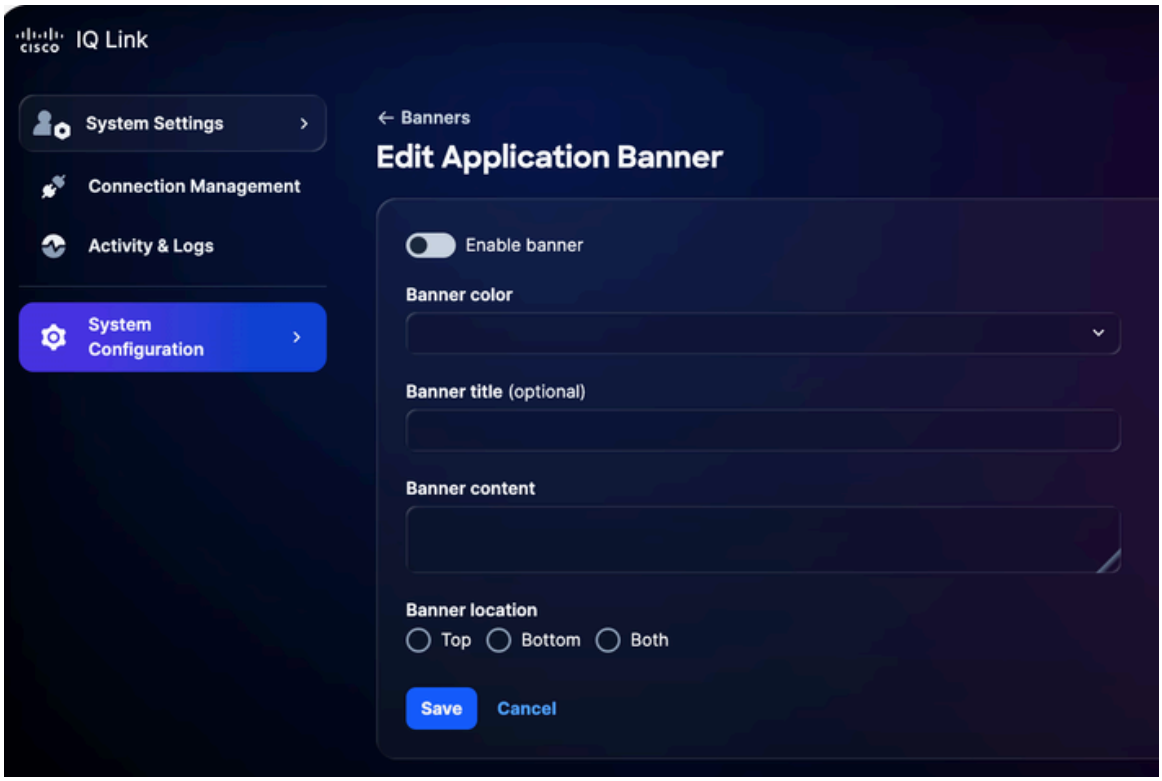
Configuración de Banners

Para configurar un banner:

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

Banner de configuración

2. Haga clic en Configure (Configurar). 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.

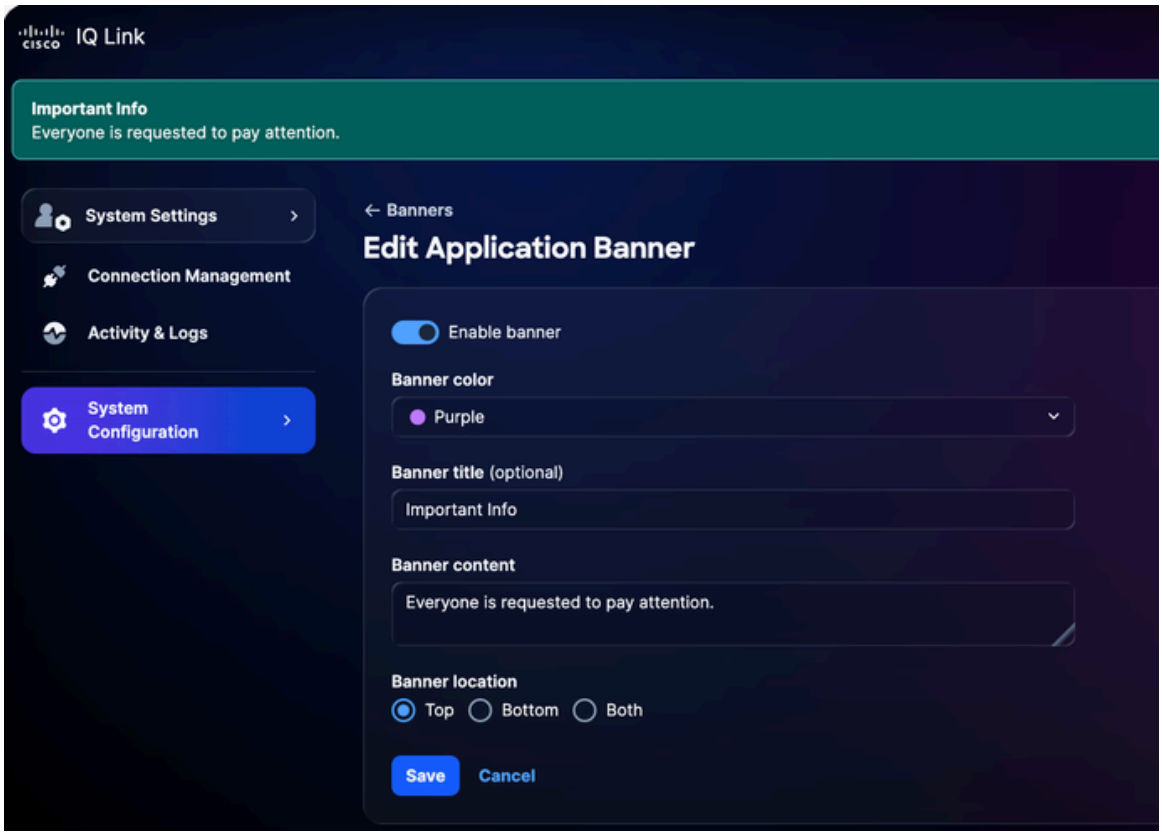
Edición de banners

Para editar un banner:

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

Editar banners

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

Los clientes pueden 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.

Funcionamiento de diagnóstico del sistema Funcionamiento de diagnóstico del coSistema completo

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).