Guia de operações do Cisco IQ Link v1.1.1

Introdução

O Cisco IQ™ oferece aos clientes aprimoramentos e recursos projetados para melhorar a visibilidade de ativos, fornecer insights mais inteligentes em seus ambientes e simplificar o gerenciamento de casos. Além disso, os recursos de IA, como o Cisco IQ AI Assistant, otimizam os resultados operacionais e a experiência do usuário do Cisco IQ, fornecendo entendimento contextual que capacita os usuários a tomar decisões proativas e informadas e simplifica os processos para o envolvimento e o sucesso do cliente.

O Cisco IQ Link coleta e transmite com segurança a telemetria de ativos de sua rede local para o Cisco IQ, permitindo insights preditivos baseados em IA que ajudam a melhorar a visibilidade da rede, antecipar problemas e impulsionar a eficiência operacional.

Autenticação Local

Os administradores devem usar as seguintes credenciais para fazer login no Cisco IQ Link:

- Nome de usuário padrão: admin
- Senha padrão: senha que é definida durante o processo de instalação do Cisco IQ Link; consulte o Cisco IQ Link Getting Started Guide para obter mais informações

Após o login, o usuário padrão, "admin", e o nome da conta, "Default-Customer", são exibidos na página inicial.

Definindo a segurança do administrador local

Você pode alterar sua senha e definir perguntas de segurança por meio do menu Segurança do administrador local em Configuração do sistema.

Você tem três (3) tentativas para digitar a senha correta dentro de um período de dez (10) minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 60 minutos para proteger sua segurança.

Não é possível tentar fazer logon durante o período de bloqueio. O sistema exibe a mensagem:

"Conta bloqueada devido a muitas tentativas com falha. Tente novamente mais tarde.", incluindo a hora em que o bloqueio expira.

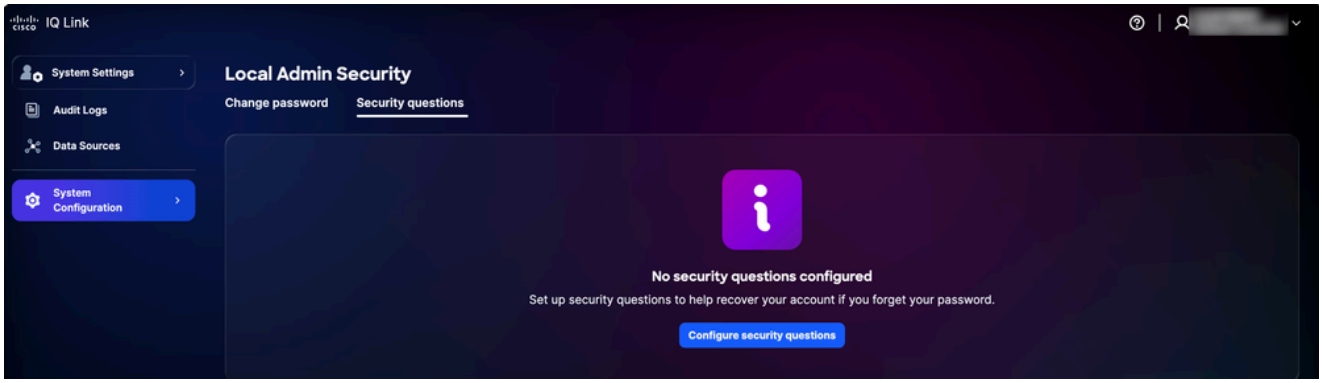
Sua conta é desbloqueada automaticamente após 60 minutos. Nesse momento, você poderá tentar fazer logon ou redefinir sua senha.

Configurando perguntas e respostas de segurança

Perguntas de segurança ajudam a verificar sua identidade se você esquecer sua senha. Os administradores devem configurar as respostas para cinco (5) perguntas de segurança para ativar o recurso de redefinição de senha. Essa é uma configuração única.

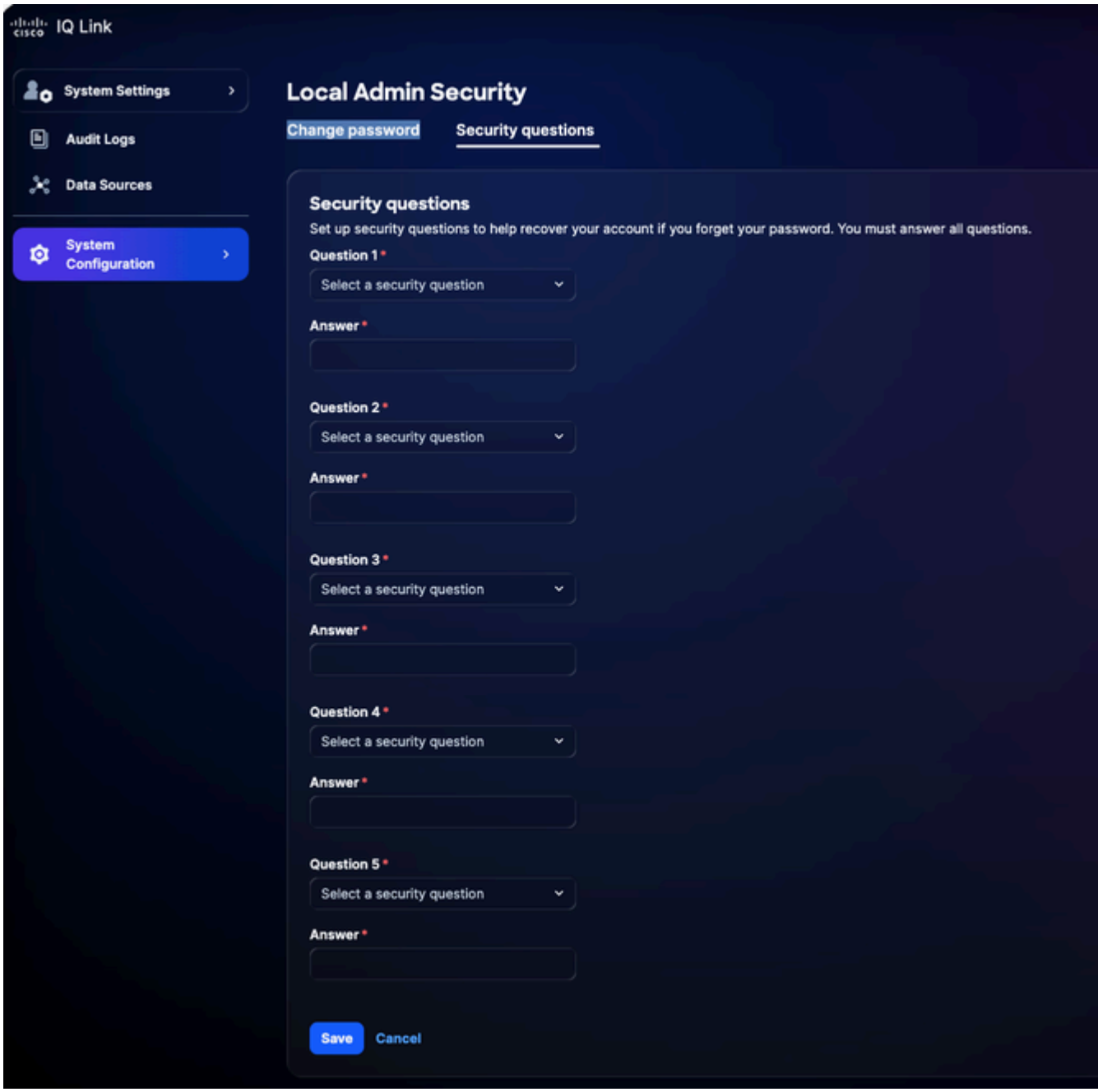
Para configurar perguntas de segurança:

1. Em Configurações do sistema, escolha Configuração do sistema > Segurança do administrador local > Perguntas de segurança.



Perguntas de segurança

2. Clique em Configure security questions.



Perguntas de segurança

3. Escolha qualquer uma das cinco (5) perguntas de segurança nas listas suspensas.

4. Digite sua resposta para cada pergunta.

5. Click Save.

Notas:
· As respostas não diferenciam maiúsculas de minúsculas, por exemplo, "SMITH" e "smith" são considerados iguais
· Espaços extras são ignorados, significando que "Smith" e "Smith" são tratados de forma idêntica

---

Note: Você pode atualizar suas respostas mais tarde, se necessário. Quando você atualiza suas respostas, todas as respostas anteriores são substituídas, portanto, você deve fornecer respostas para todas as cinco (5) perguntas novamente e não apenas aquelas que deseja alterar.

Gerenciamento de senhas

Somente administradores locais podem gerenciar a senha do Cisco IQ.

Pré-requisitos

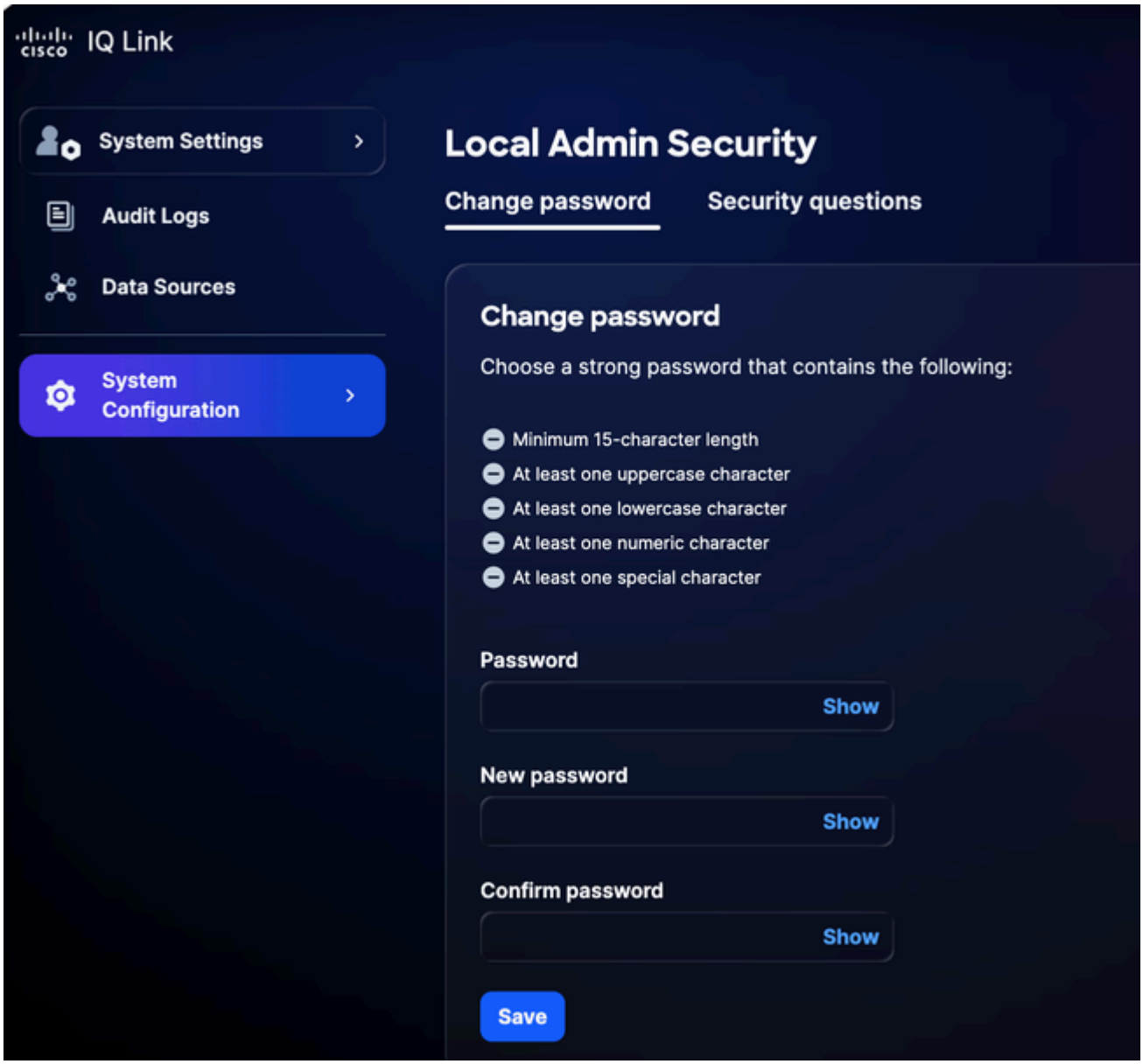
Para gerenciar senhas, as seguintes condições devem ser atendidas:

- Você é um administrador local
- Você está usando uma conta de Administrador local (não SSO (Single Sign-On, login único) ou autenticação externa)
- Você está conectado ao Cisco IQ
- Você conhece a senha atual

Alteração de Senhas

Para alterar a senha:

1. Em Configurações do sistema, navegue para Configuração do sistema > Segurança do administrador local > Alterar senha.



Alterar senha

2. Insira a senha atual.
3. Insira a Nova senha.
4. Digite a nova senha novamente para confirmá-la.
5. Click Save.

A senha é atualizada no sistema Cisco IQ, incluindo a máquina virtual (VM) Cisco IQ.

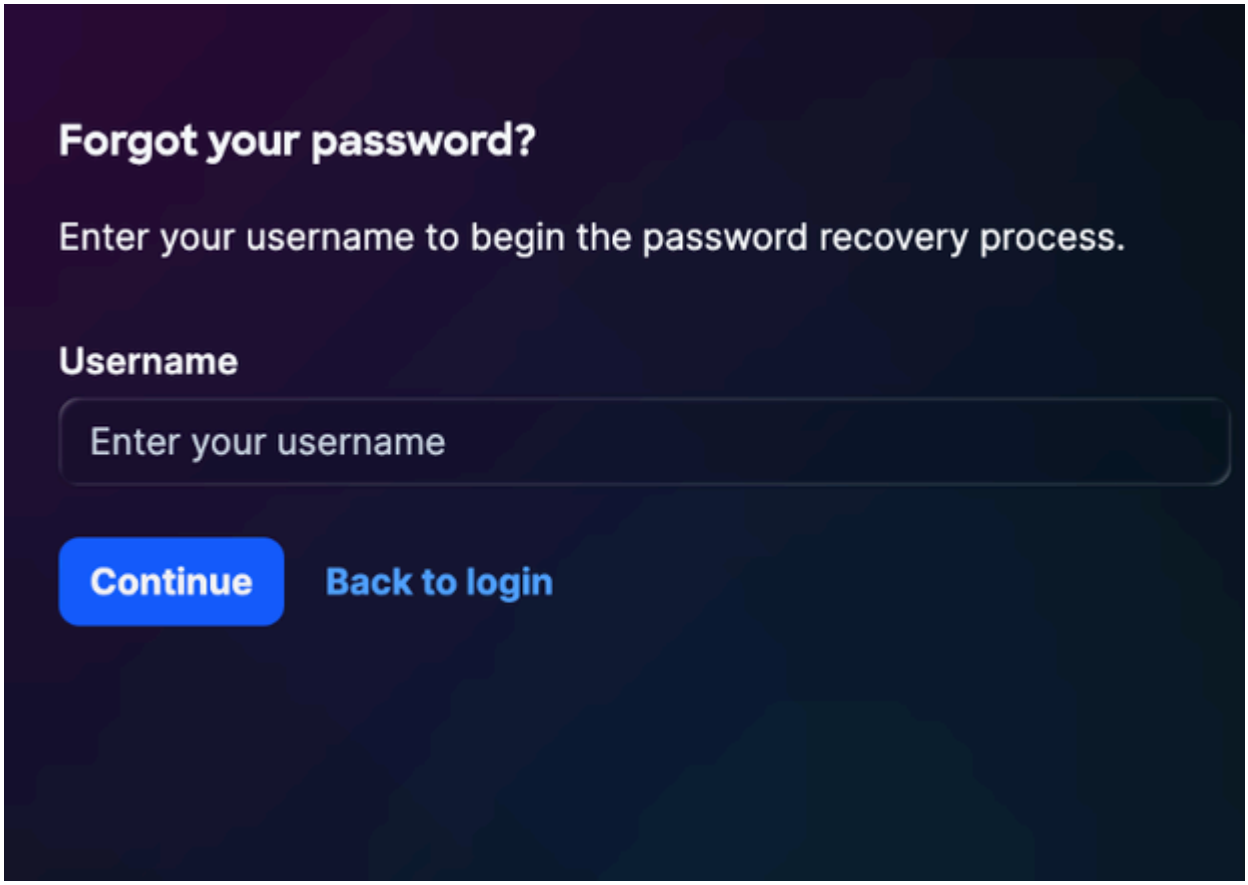
Redefinição de uma senha esquecida

Você pode redefinir uma senha esquecida usando o processo de verificação de pergunta de segurança, se tiver configurado as perguntas de segurança anteriormente. Consulte Configurando

perguntas e respostas de segurança para obter mais detalhes.

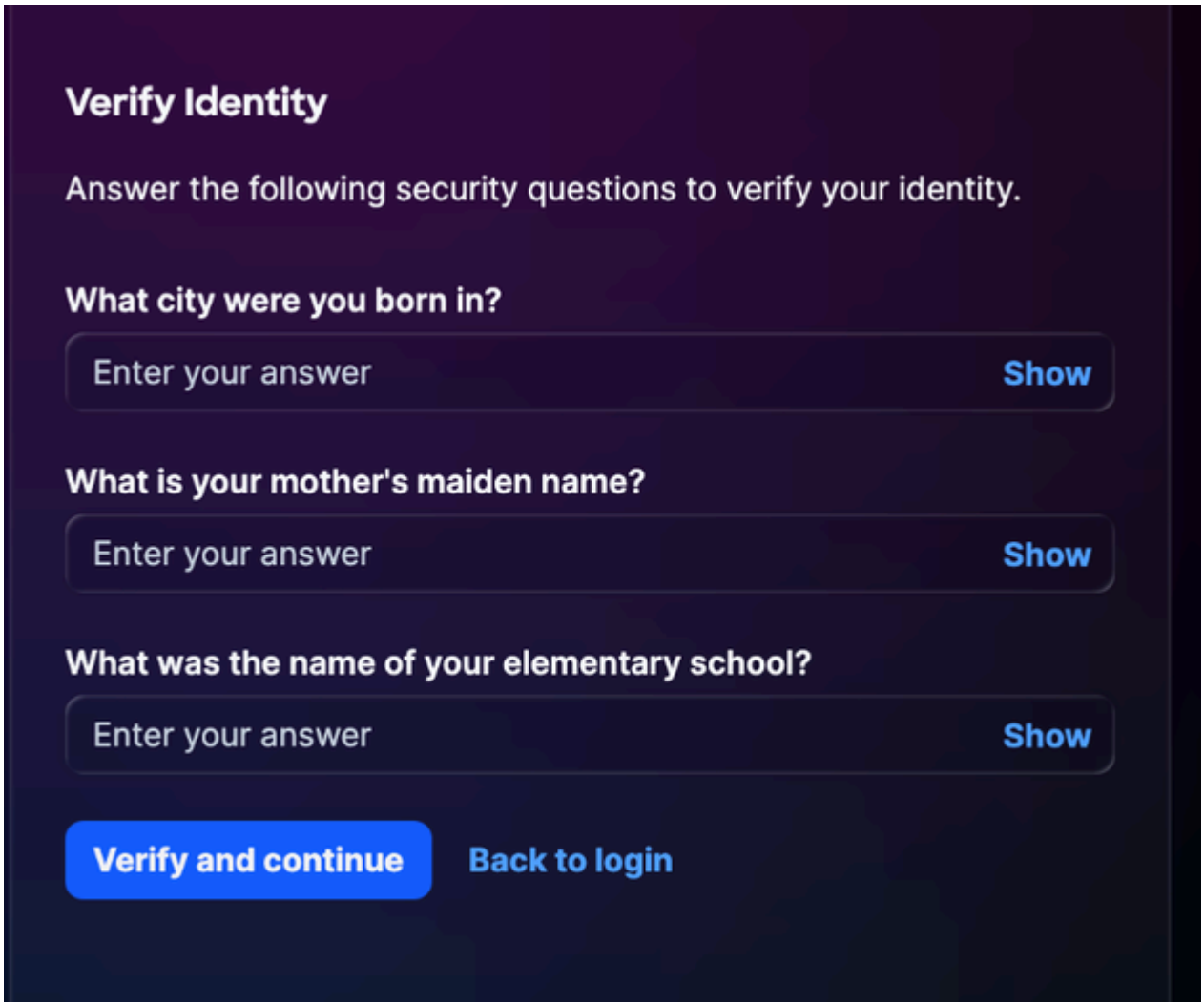
Para redefinir uma senha esquecida:

1. Navegue até a página de login do Cisco IQ Link.
2. Clique em Esqueci a senha.



Esqueci a senha

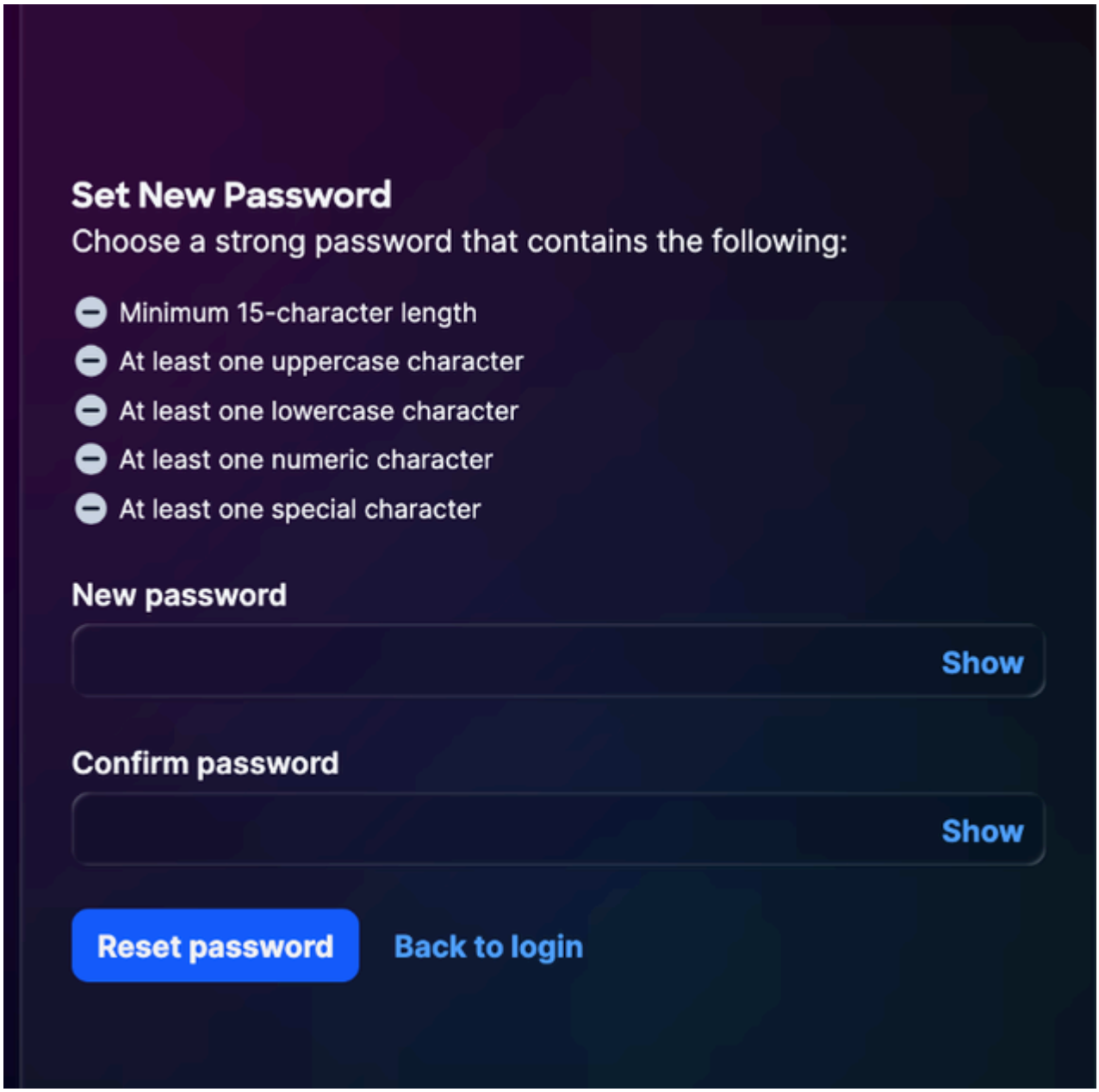
3. Insira o nome de usuário.
4. Clique em Continuar. A página Verificar Identidade exibe três (3) perguntas de segurança aleatórias entre as cinco (5) perguntas que foram configuradas anteriormente.



Verificar identidade

Note: As perguntas de segurança exibidas acima são específicas do usuário e variam de acordo.

5. Insira as respostas para todas as três (3) perguntas exibidas.
6. Clique em Verificar e continue. Se a resposta enviada corresponder às respostas salvas anteriormente, você será solicitado a digitar uma nova senha.



Redefinir senha

Notas:
· Você tem três (3) tentativas para responder corretamente às perguntas de segurança em um período de dez (10) minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 60 minutos para proteger sua segurança.
· Você não pode redefinir sua senha durante o período de bloqueio. O sistema exibe a mensagem: "Conta bloqueada devido a muitas tentativas de verificação com falha. Tente novamente mais tarde.", incluindo a hora em que o bloqueio expira.
· Sua conta é automaticamente desbloqueada após 60 minutos, quando você pode tentar fazer login ou redefinir sua senha.

---

7. Insira a Nova senha.

8. Digite a senha novamente para confirmá-la.

9. Clique em Submit.

Configurando o provedor de identidade

Depois de fazer login no Cisco IQ Link, os administradores podem definir várias configurações. Os administradores podem fazer login no Cisco IQ Link usando a administração local ou a configuração do provedor de identidade (IDP).

Configuração SAML do Okta IDP para SSO

Pré-requisitos para Configurar SAML IDP

- Acesso de administrador local ao Cisco IQ Link
- Acesso ao portal do IDP

Configuração SAML de IDP para SSO

Para configurar a SAML (Security Assertion Markup Language) do IDP para SSO:

1. Navegue até o portal do IDP.
2. Defina os seguintes atributos para a instância do Cisco IQ Link.

Atributos de link do Cisco IQ

Campo	Valor
Nome do aplicativo	<Nome do aplicativo>
Ambiente	Aplicativo empresarial ESP
Grupos de Proprietários de Aplicativos	Proprietário das configurações de IDP
Correio de Equipe	Mala direta para a equipe

Campo	Valor
Público-alvo	Não-força de trabalho
Categoria de integração	Selecione "Nova integração"

Parâmetros de configuração SAML

Parâmetro	Configuração	Exemplo
Audiência (ID da Entidade)	nome FQDN	mymanagementhost.mydomain.com
URL de Logon Único	Ponto de extremidade ACS SAML	https://mymanagementhost.mydomain.com/saml/acs
Formato de ID do Nome	Endereço de e-mail	NA
Nome de usuário do aplicativo	Nome de usuário	NA

3. Configure as seguintes instruções de atributo obrigatórias.

Note: As alterações de atributo de IDP dependem do provedor e da configuração específicos. O Cisco IDP e seus atributos são compartilhados abaixo como um exemplo.

- Primeira entrada
    - Nome: Nome de usuário
    - Valor: user.login
- Segunda entrada
    - Nome: Email principal
    - Valor: usuário.email
- Declarações de Atributos do Grupo

- Nome: grupos
- Filtro: REGEX
- Valor: .*

4. Defina as configurações de Logout único (SLO) no aplicativo.

Definições de configuração do SLO

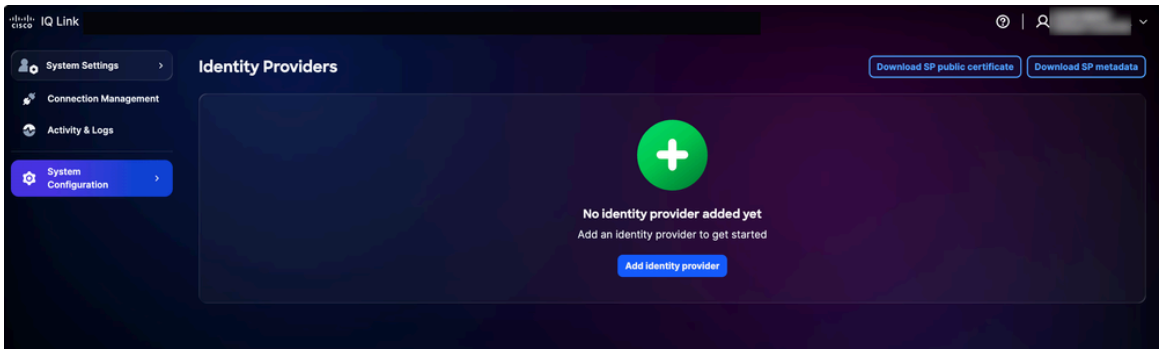
Campo	Valor
Certificado de assinatura	Para o Okta, esse certificado será necessário apenas se você optar por habilitar o SLO. Faça o download do certificado de assinatura usando Download SP Certificate em Identity Providers. Salve o arquivo como sp-public-key.crt. Consulte Configuração de logoff único para obter mais detalhes.
metadados SP	Os metadados da controladora de armazenamento são necessários somente para o ADFS IDP (e não para o Okta).
Deseja habilitar o Logoff Único?	Sim ou Não
URL de logoff único	https://mymanagementhost.mydomain.com/saml/logout
Emissor SP (ID do público/entidade ou URL ACS)	https://mymanagementhost.mydomain.com

5. Clique no ícone Download para fazer o download do arquivo "Metadados SP".
6. Provisione ou crie o aplicativo conforme exigido pelo provedor.

Adicionando IDP

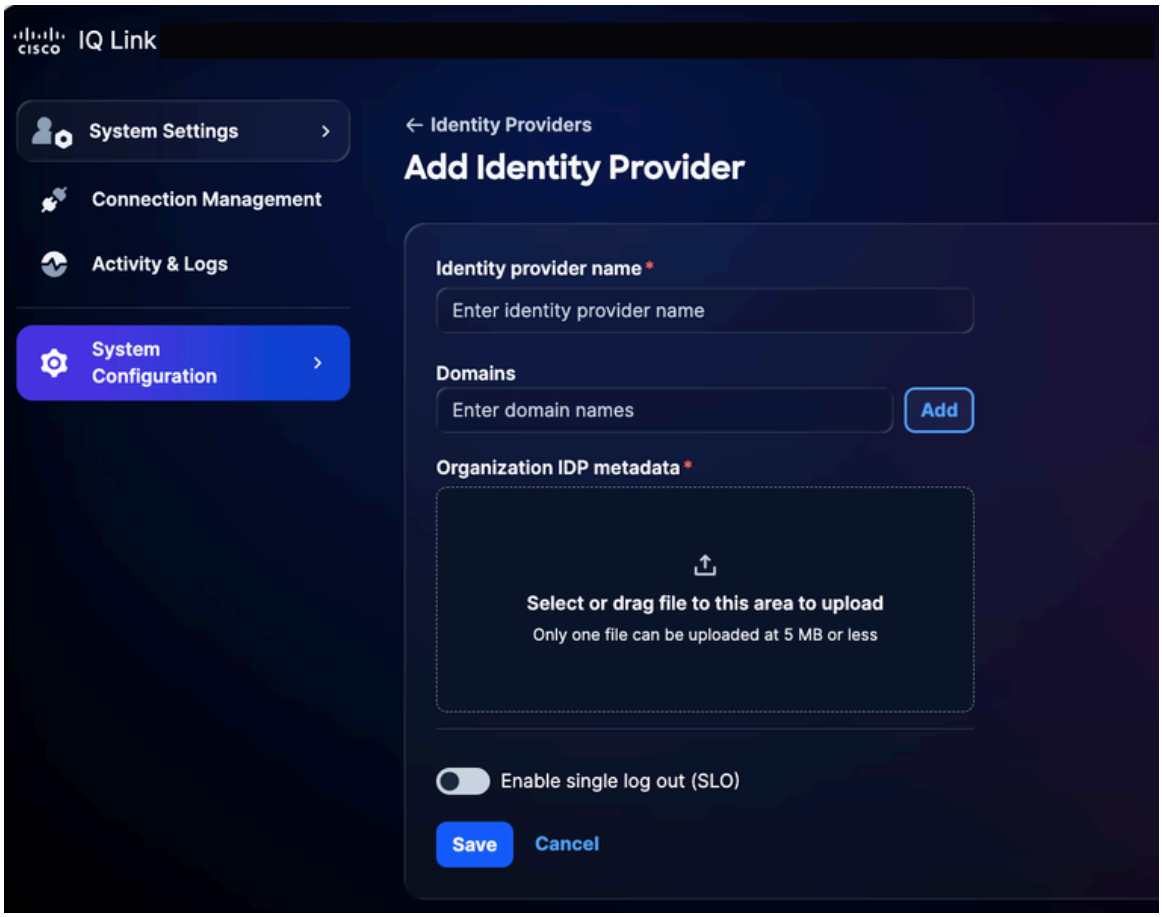
Para adicionar um IDP no Cisco IQ Link:

1. Em Configurações do sistema, escolha Configuração do sistema > Provedores de identidade. A página Provedores de identidade é exibida.



Página inicial do IDP

2. Clique em Adicionar provedor de identidade. A página Adicionar Provedor de Identidade é exibida.



Adicionar provedor de identidade

Note: Apenas um (1) IDP pode ser adicionado em um determinado momento.

3. Insira o nome do provedor de identidade.

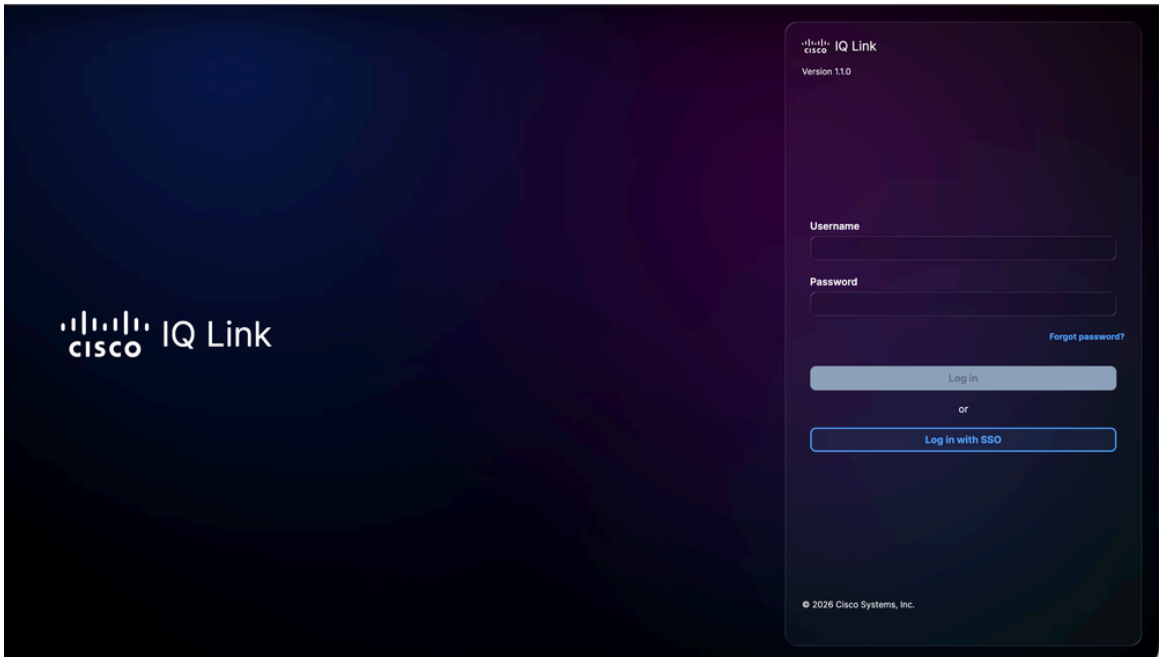
4. Clique em Add para adicionar um nome de domínio configurado do Cisco IQ Link ao campo Domains.

5. Arraste e solte ou carregue o arquivo de metadados SAML obtido do aplicativo IDP no campo Metadados IDP da organização. Este arquivo contém detalhes do certificado e detalhes da entidade do SP (Provedor de Serviços).

6. (Opcionalmente) Ative o botão de alternância Ativar logoff único. Você também pode ativar o SLO posteriormente.

7. Click Save.

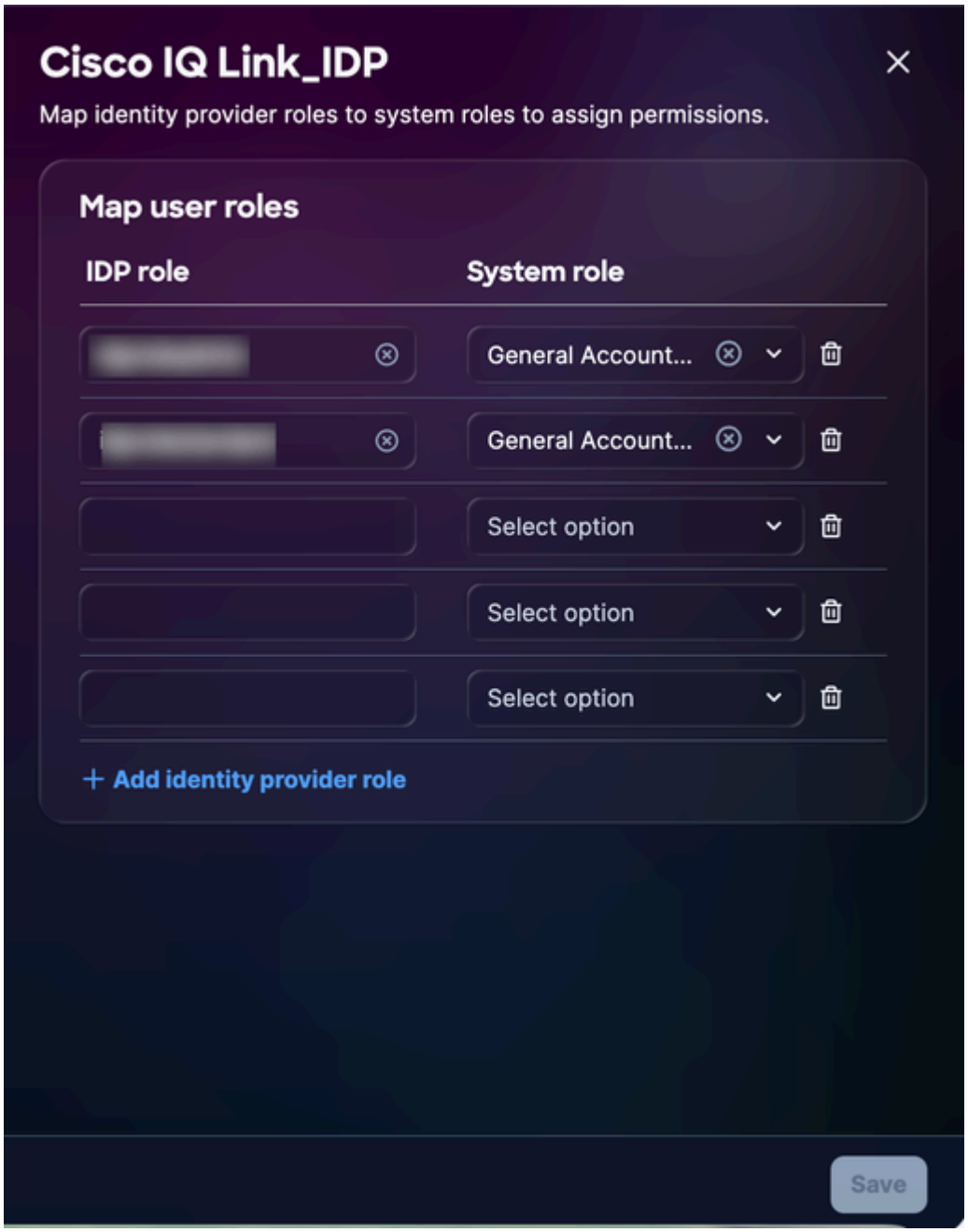
8. Uma vez configurada, a página de login exibe uma opção para efetuar login com o SSO (via IDP).



Login do link do Cisco IQ

Configuração do mapeamento de função

1. No IDP adicionado, selecione o ícone Mais Opções > Mapear Funções. A página Mapear funções de usuário é exibida.



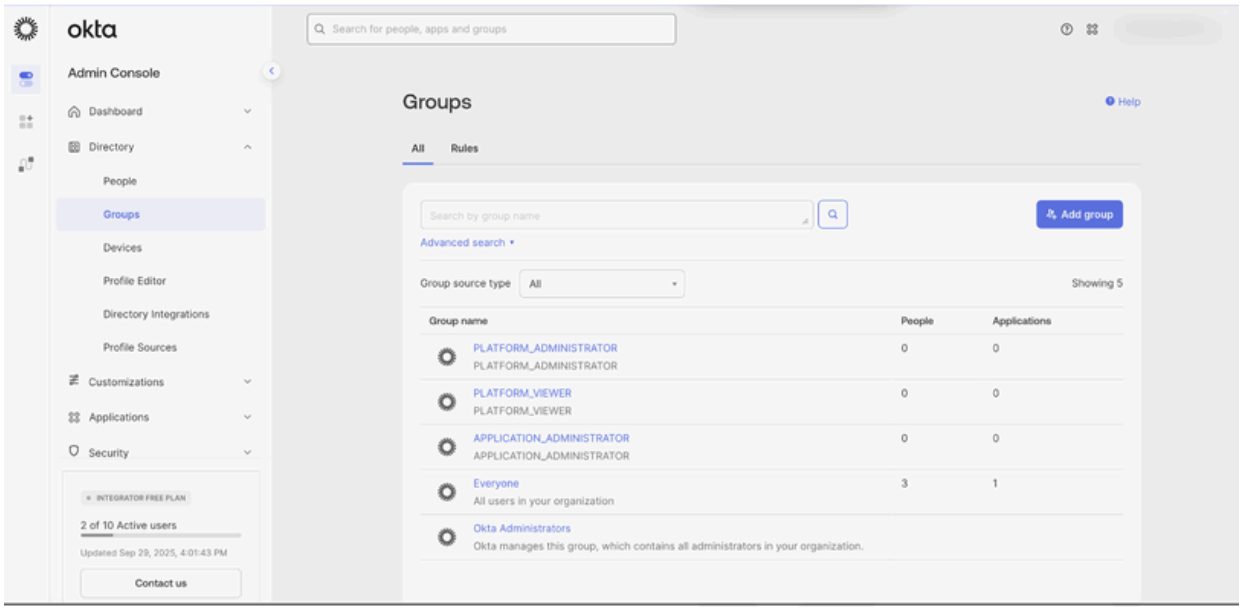
Mapeamento de função de usuário

2. Insira uma função IDP para a função Sistema selecionada. As seguintes funções do sistema são suportadas:

    - general_account _administrator: O administrador da conta geral tem permissões totais para executar todas as ações no produto
    - general_account _viewer: O visualizador de conta geral tem acesso somente leitura

---

Note: A função IDP é um campo de texto aberto. Ele deve corresponder exatamente ao nome do grupo ou função configurado no IDP da sua organização. Um exemplo de grupos Okta é compartilhado abaixo.



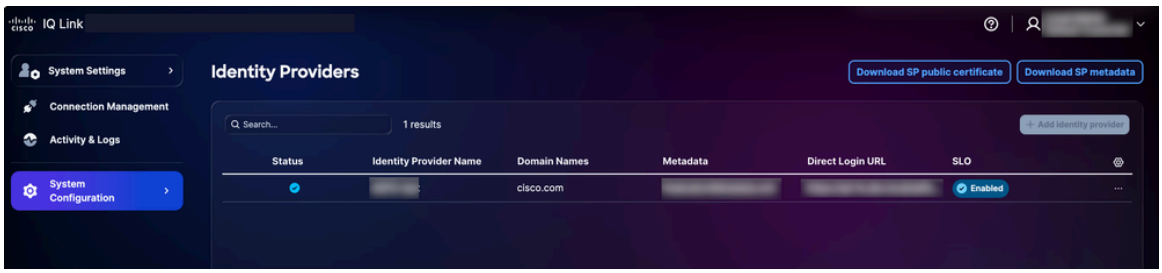
Referência de Mapeamento de Função

3. Mapeie funções adicionais conforme necessário clicando em Adicionar função do provedor de identidade.
4. Click Save.

Configuração de logoff único

Se você optar por habilitar o SLO, deverá carregar metadados que incluam o URL do SLO. Você pode configurar isso editando suas configurações do Provedor de identidade e ativando a opção para Habilitar logoff único. Para concluir a configuração do SLO:

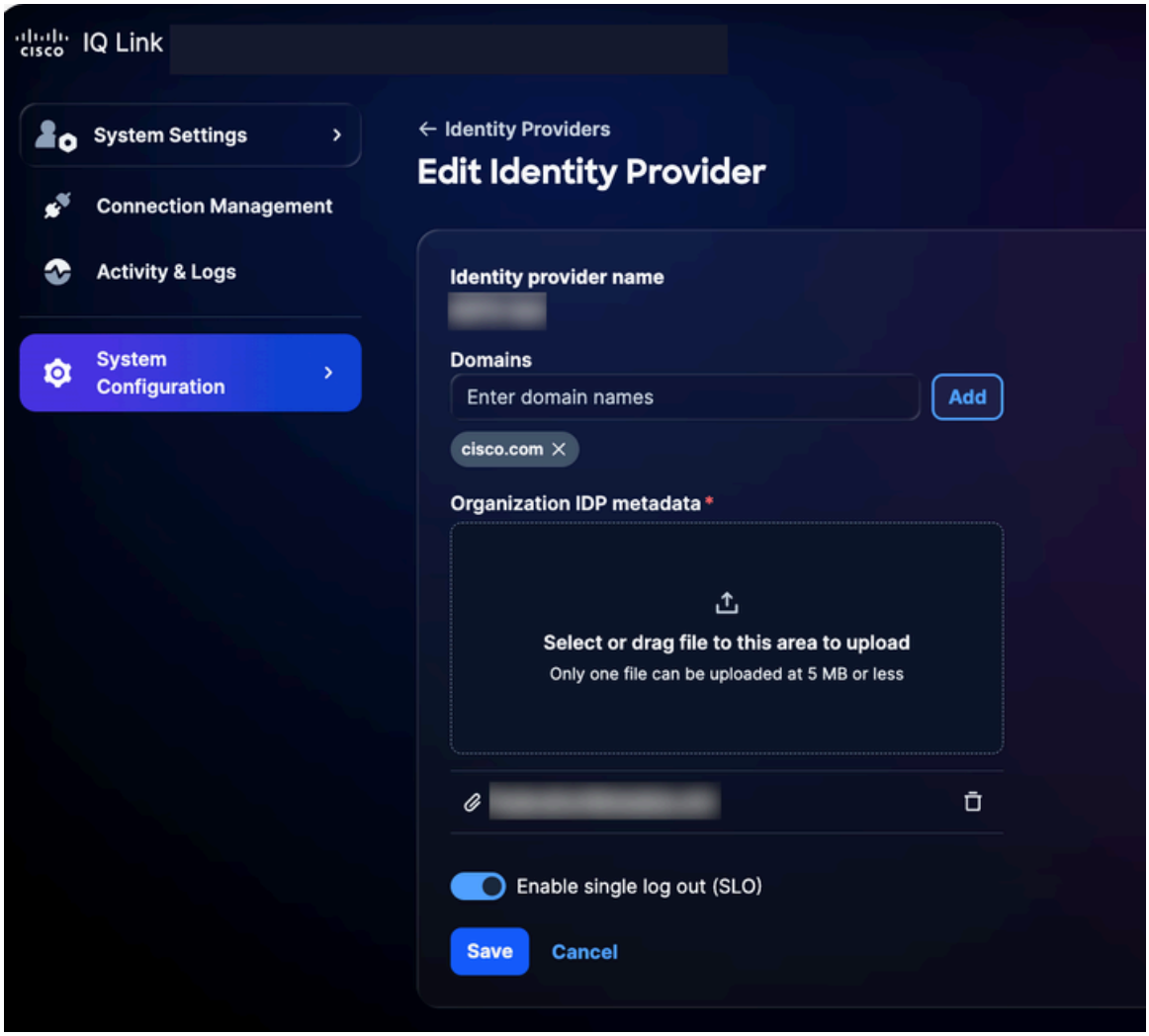
1. Na página Provedores de identidade, clique em Fazer download do certificado público SP.



Fazer download de certificado público

2. Salve o arquivo de download como sp-public-key.crt.
3. Navegue até o portal do IDP.
4. Carregue o arquivo de certificado de assinatura gerado na seção Configuração SAML IDP para SSO.

5. Baixe o arquivo de metadados IDP novamente.
6. Na página Provedores de identidade, escolha o ícone Mais opções do IDP adicionado > Editar.



Editar provedor de identidade

7. Ative o botão de alternância Ativar logoff único (SLO).
8. Carregue o arquivo de metadados recém-baixado.
9. Use a seguinte lista de verificação para verificar a funcionalidade SSO e SLO:

Lista de verificação:

- O login do administrador local foi bem-sucedido
- O portal do IDP está configurado e provisionado
- O IDP é adicionado ao Cisco IQ com status de "Êxito"
- Os mapeamentos de função são configurados e testados

- Os metadados da controladora são baixados e o certificado é extraído
- Se o SLO estiver habilitado, a configuração do SLO será concluída com o certificado de assinatura real
- O fluxo SSO/SLO de ponta a ponta foi testado com êxito

Solução de problemas de IDP

A lista a seguir descreve problemas comuns e possíveis soluções para ajudar a identificar e resolver rapidamente problemas relacionados ao status de IDP, erros de certificado, falhas de login de SSO e configuração de SLO:

Troubleshooting

Problema	Solução
O status de IDP é mostrado como "Incompleto"	Verificar as configurações de mapeamento de função
Erros de certificado	Verificar o formato e a validade do certificado
Falhas de login de SSO	Validar mapeamento de atributo e atribuições de grupo
O SLO não está funcionando conforme esperado	Verifique se o certificado foi carregado corretamente e se as URLs do SLO estão configuradas

Configuração SAML de IDP do ADFS para SSO

Esta seção fornece orientação para configurar o Microsoft Ative Diretory Federation Services (ADFS) como o SAML IDP para o Cisco IQ.

Pré-requisitos para Configurar ADFS IDP SAML para SSO

- O ADFS 6.0+ é recomendado
- Windows Server 2012 R2+
- Integração configurada com o Ative Diretory
- Certificados SSL/TLS no AD FS
- Acesso de administrador ao Cisco IQ
- Acesso administrativo ao servidor ADFS (Windows Server)
- Acesso do PowerShell no servidor ADFS
- Conectividade de rede entre ADFS e Cisco IQ
- Detalhes de configuração do servidor ADFS (conforme listado na tabela abaixo)

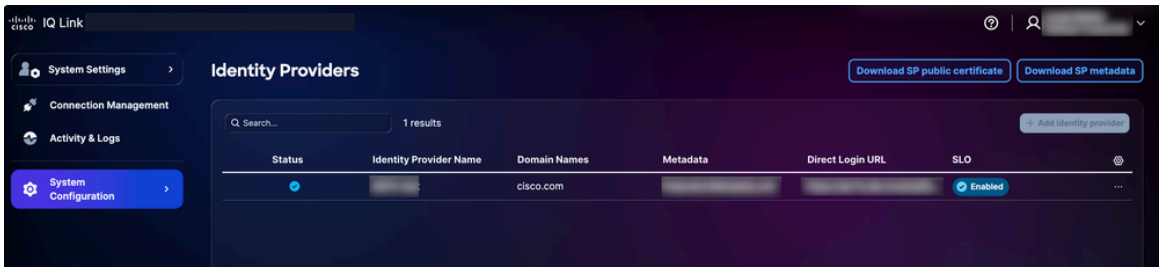
Configuração do Servidor ADFS

Item	Descrição	Exemplo
FQDN do Cisco IQ	Nome de host de implantação de usuário	devxx-23.cx-xxx-xxx.cisco.com
URL do Servidor ADFS	Endereço do servidor ADFS do usuário	https://ad-fs.dev.local
Domínio da empresa	Domínio de e-mail	company.com
Grupos do AD	Nomes de Domínio (DN) do grupo do Ative Diretory	CN=Função - Desenvolvedores do CXIQ

Configurando Servidores ADFS

Para configurar o ADFS:

1. Em Configurações do sistema, escolha Configuração do sistema > Provedores de identidade. A página Provedores de identidade é exibida.



Opções de download

2. Clique em Download SP public certificate e em Download SP metadata para baixar esses arquivos.
3. Copie e salve os arquivos service-provider-metadata.xml e service-provider-certificate.crt no diretório ADFS (por exemplo, C:-certificate.crt).
4. Faça logon no servidor ADFS.
5. No menu Gerenciamento ADFS, clique em Confiança da Terceira Parte Confiável.
6. No menu Trusts da Terceira Parte Confiável, clique em Adicionar Trusts da Terceira Parte Confiável. O novo assistente é aberto.
7. Clique no botão de opção Claims Aware.
8. Clique em Start para continuar com a configuração.
9. Clique em Importar dados sobre a terceira parte confiável de um arquivo.
10. Clique em Procurar para selecionar o arquivo de metadados do provedor de serviços e concluir o upload do arquivo.
11. Clique em Next.
12. Insira um nome de exibição (por exemplo, "CIQ-Stage"), adicione notas relevantes e clique em Avançar.
13. Na página Escolher política de controle de acesso, clique em Permitir todos (ou na política exigida pela configuração de segurança da sua organização).
14. Clique em Avançar nas telas restantes.
15. Clique em Fechar para concluir a configuração da Confiança da Terceira Parte Confiável.

Configurando Regras de Declaração do ADFS

Para configurar as regras de Declaração do ADFS, execute as etapas listadas nas seções a seguir.

Reivindicações obrigatórias

Consulte a tabela a seguir para obter as reivindicações necessárias.

Reivindicações obrigatórias

Reivindicação	Propósito	Fonte
E-mail	Identificador do usuário	E-mail do AD
Nome de exibição	Nome completo do usuário	Nome para Exibição do AD
NameID	assunto SAML	Transformado a partir de email
Grupos	Acesso baseado em função	Associação a um grupo do AD (memberOf)

Aplicando regras de reivindicação

1. Defina o nome do Objeto de Confiança de Terceira Parte Confiável (por exemplo, "Cisco IQ - Stage").

```
$relyingPartyName = “Cisco IQ - Stage”
```

2. Defina regras de reivindicação para enviar informações de usuário e associação de grupo ao 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.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 as regras de reivindicação executando o seguinte comando:

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

Verificando grupos de usuários

1. Defina o nome de usuário para verificar a associação do grupo do usuário.

```
$username = “testuser”
```

2. Execute os seguintes comandos para localizar a conta do usuário:

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

$user = $searcher.FindOne()
```

3. Exibe os grupos aos quais o usuário pertence.

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

Saída de exemplo:

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

Configurar ADFS para Confiar no Certificado de Autenticação da controladora

1. No servidor ADFS, importe o certificado SP para o armazenamento TrustedPeople.

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

2. Escolha uma das seguintes opções:

Note: O certificado SP é emitido por uma Autoridade de Certificação interna que o ADFS não pode validar por meio da cadeia de confiança padrão.

- Desabilitar validação de cadeia globalmente para esta terceira parte confiável

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


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

OU

- Importar o certificado CA que está sendo emitido para o repositório de Autoridades de Certificação de Raiz Confiáveis

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

3. Aplicar as alterações reiniciando o serviço ADFS.

```
Restart-Service adfssrv
```

Exportando Metadados do ADFS

Você pode baixar os metadados do ADFS usando o PowerShell ou o navegador da Web.

PowerShell

Para exportar metadados do ADFS usando o PowerShell:

1. Abra o PowerShell no servidor ADFS.
2. Execute os comandos a seguir para fazer download do arquivo de metadados.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.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
```

Depois de executar os comandos, o arquivo de metadados é salvo em C:-metadata.xml.

Navegador da Web

Para exportar metadados do ADFS usando um navegador da Web:

1. Navegue até https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Substitua <your-adfs-server> pelo nome de host do seu servidor ADFS.
3. Salve o arquivo XML de metadados no computador quando solicitado.

Adicionando ADFS IDP

1. Na página Provedores de identidade, clique em Adicionar provedor de identidade.
2. Insira o nome do provedor de identidade.
3. Insira o(s) domínio(s) (por exemplo, company.com).
4. (Opcionalmente) Ative o botão de alternância Ativar logoff único, se necessário.
5. Arraste e solte ou carregue o arquivo de metadados SAML obtido do aplicativo IDP no campo Carregar metadados IDP.
6. Click Save.

Note: O status é exibido como "Incompleto" até que o mapeamento de funções seja concluído; este é um comportamento esperado.

Configurando o mapeamento de função

Antes de continuar a configurar o mapeamento de função, verifique se você pode localizar grupos do Ative Diretory para uso no mapeamento. Para localizar grupos do Ative Diretory, execute o seguinte comando do 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”] }
```

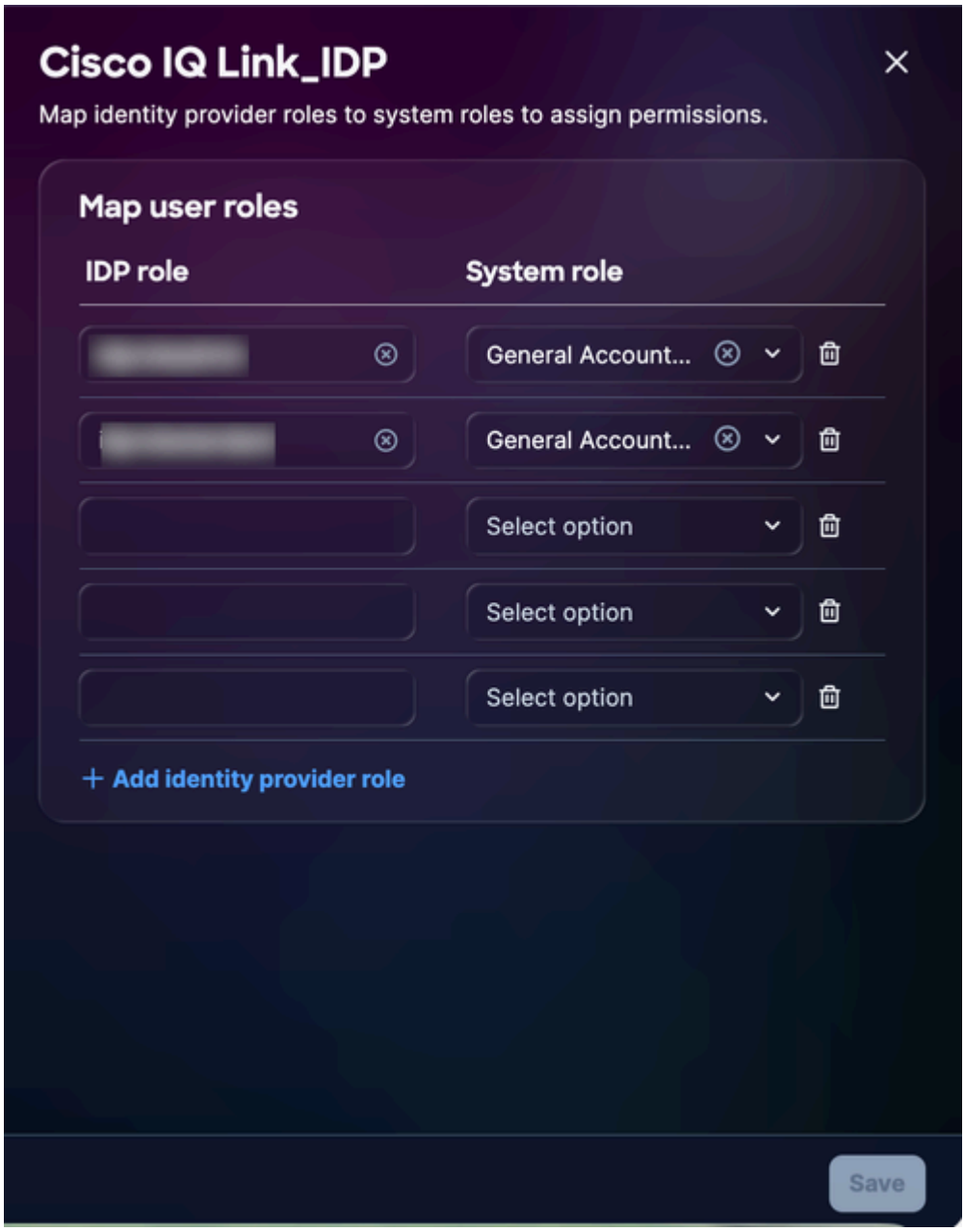
O sistema consulta o Ative Diretory diretamente via LDAP, não exigindo módulos adicionais. As informações do grupo são retornadas no formato DN (Distinguished Name - Nome Distinto) completo, por exemplo:

CN=Função - Desenvolvedores CXIQ,OU=Grupos,DC=dev,DC=example,DC=com CN=Função - Visualizadores CXIQ,OU=Grupos,DC=dev,DC=example,DC=com

Se os grupos necessários não estiverem listados, eles deverão ser criados no Ative Diretory por um Administrador para que você possa concluir o mapeamento de função do ADFS.

Para configurar o mapeamento de função:

1. No IDP adicionado, escolha o ícone Mais Opções > Mapear Funções. A página Mapear funções de usuário é exibida.



Mapeamento de função

2. Insira uma função IDP para a função Sistema selecionada. As seguintes funções do sistema são suportadas:

    - general_account _administrator: O administrador da conta geral tem permissões totais para executar todas as ações no produto. A função IDP (nome analisado) é Administradores CXIQ.
    - general_account__viewer: O visualizador de conta geral tem acesso somente leitura. A função IDP (nome analisado) é Desenvolvedores e Visualizadores CXIQ.

    Note: Use nomes analisados (por exemplo, Desenvolvedores CXIQ) e não nomes de domínio completos.

3. Click Save. O status é atualizado para Sucesso.

Verificação e teste

Testando a autenticação

1. Em um navegador no modo Incognito ou Privado, navegue até https://your-cisco-iq-domain.com/login.
2. Faça login usando suas credenciais do Ative Diretory no formato domínio\nome de usuário ou user@domain.local.
3. Verifique se você foi redirecionado para a página Cisco IQ Home (após a autenticação bem-sucedida).
4. Confirme se as funções atribuídas exibem os nomes de grupos analisados corretamente (por exemplo, Desenvolvedores CXIQ) em seu perfil de usuário.

Testando Logoff

Para testar o logoff, clique em Logoff do Cisco IQ. A mensagem "Logoff, please wait..." (Encerrando a sessão, aguarde...) é exibida e você é redirecionado para a página Cisco IQ Login. O sistema também encerra a sessão ADFS. Se tentar acessar o ADFS diretamente, você será solicitado a fazer logon novamente.

Solução de Problemas do ADFS

A lista a seguir descreve problemas comuns e possíveis soluções para ajudar a identificar e resolver rapidamente problemas relacionados ao status do ADFS, erros de certificado, falhas de login do SSO e configuração do SLO.

Problemas do ADFS

Problema	Sintomas/Descrição	Causas / Verificações / Soluções e Correções
Grupos não extraídos	Nenhuma função após o logon	• Regra de declaração ausente: Execute novamente as instruções em Configuração de Regras de Declaração do ADFS

Problema	Sintomas/Descrição	Causas / Verificações / Soluções e Correções
		• Atributo de grupo incorreto: Deve ser http://schemas.xmlsoap.org/claims/Group • Usuário não está em grupos do AD
Falha na descriptografia	"Falha ao descriptografar a asserção" nos logs	Verificar configuração na configuração de certificado ADFS
Loop de login	Preso na autenticação ou loop de login	• URL ACS inválida: Verifique: https://your-fqdn/saml/acs • Incompatibilidade de cookies: Verificar cookies do navegador para o domínio correto

Comandos de Diagnóstico para Solução de Problemas

Para garantir uma integração bem-sucedida entre o ambiente ADFS e o Cisco IQ, use os seguintes comandos de diagnóstico. Esses comandos ajudam a verificar a acessibilidade de metadados, configurações de certificado e configurações de endpoint.

- Verifique a acessibilidade dos metadados do ADFS: Confirma que os Metadados da Federação ADFS são acessíveis ao público e acessíveis ao público; essa é uma etapa crítica para estabelecer a confiança inicial

```
curl -k https://

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

- Validar o certificado de criptografia: Garante que o certificado de criptografia correto esteja associado ao Cisco IQ Relying Party Trust

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

- Revisar Configuração de Ponto de Extremidade SAML: Verifica se os pontos de extremidade SAML para a confiança do Cisco IQ estão configurados corretamente e se as solicitações e asserções de autenticação são roteadas para as URLs esperadas

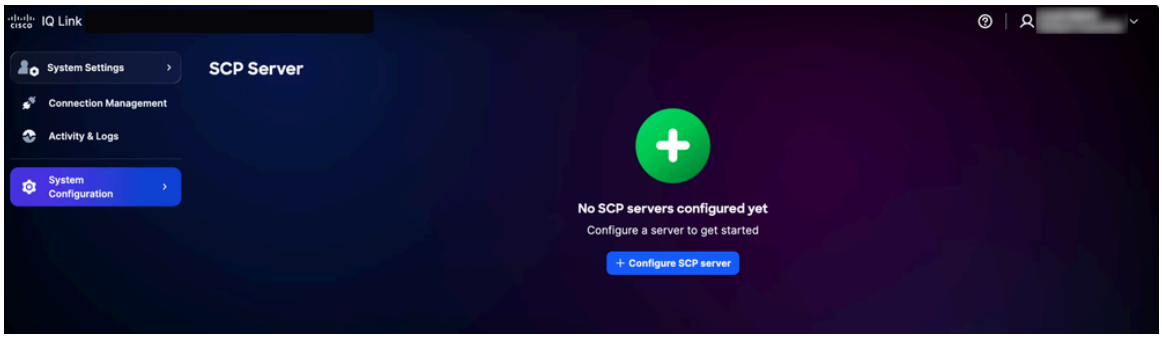
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

Adicionando servidores SCP

Esse servidor SCP (Secure Copy Protocol) é um pré-requisito para importar arquivos de atualização que são essenciais para adicionar, atualizar ou corrigir a instalação do Cisco IQ.

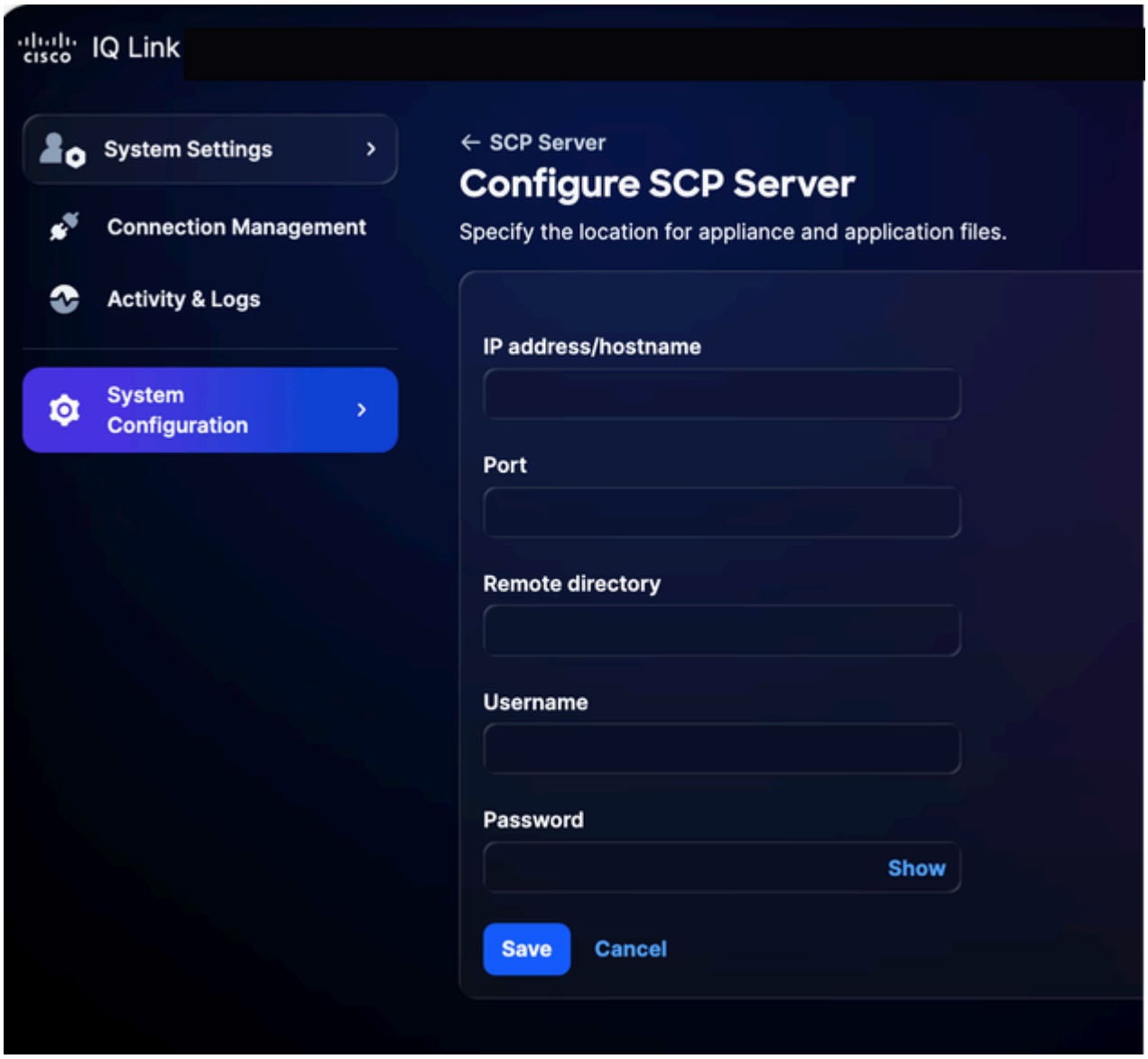
Para adicionar um Servidor SCP:

1. Em Configurações do sistema, escolha Configuração do sistema > Servidor SCP. A página Servidor SCP é exibida.



Home page do Servidor SCP

2. Clique em Configurar Servidor SCP.



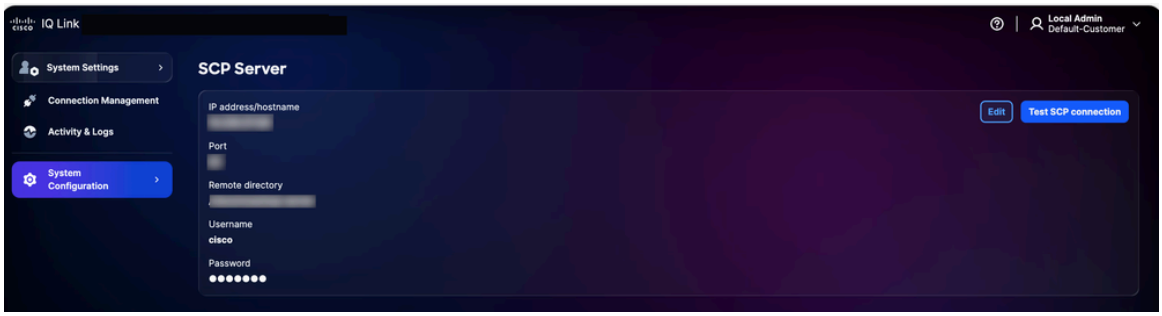
Configurar Servidor SCP

3. Insira o endereço IP/nome do host.
4. Insira um número de porta.
5. Insira o Diretório remoto.
6. Insira um nome de usuário.
7. Digite uma senha.
8. Click Save. Uma confirmação é exibida.

Edição de servidores SCP existentes

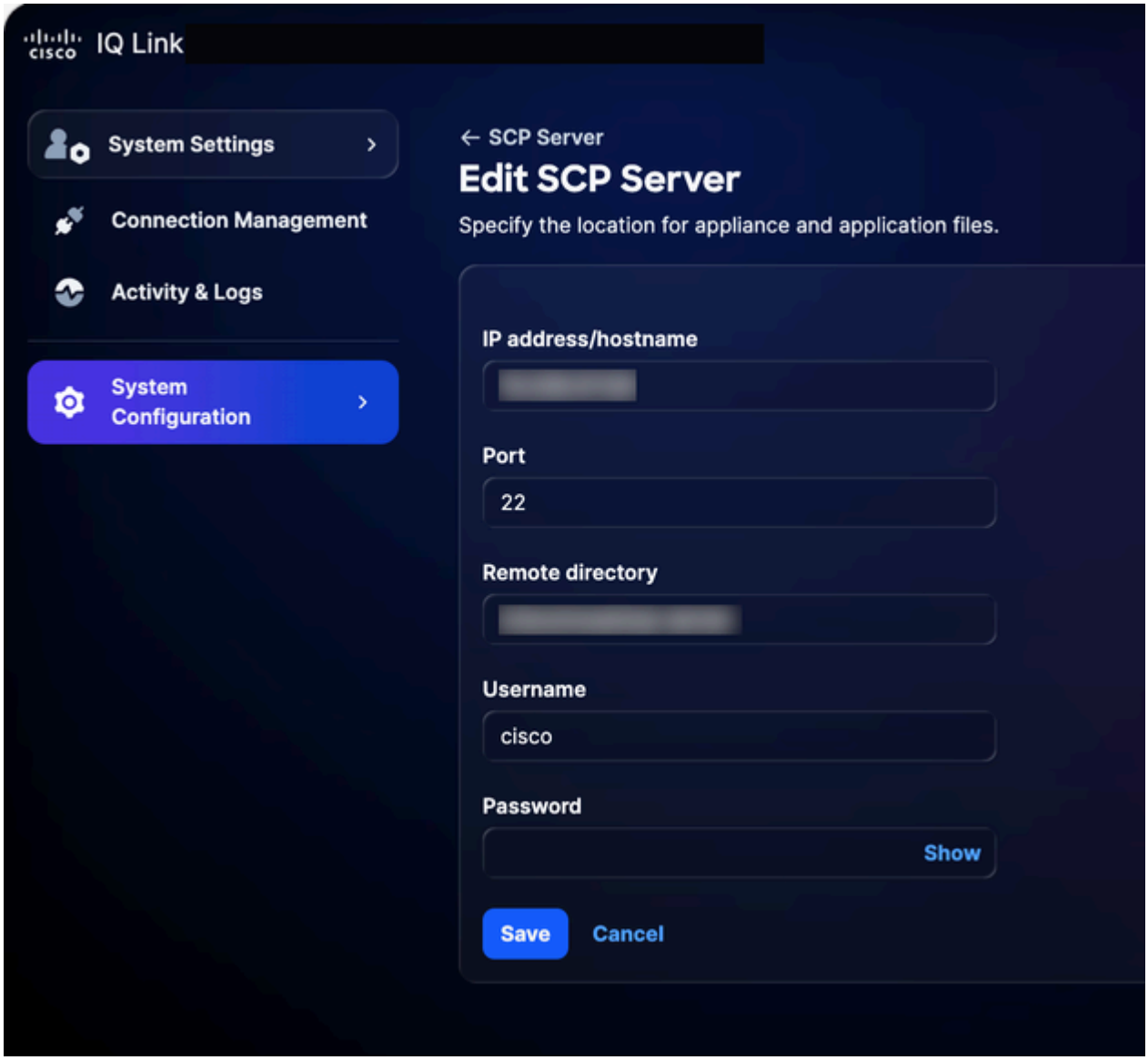
Para editar um servidor SCP existente:

1. Navegue até a página Servidor SCP.



Servidor SCP

2. Clique em Editar para o servidor SCP existente desejado.



Editando o Servidor SCP

3. Modifique os detalhes conforme necessário.

4. Click Save.

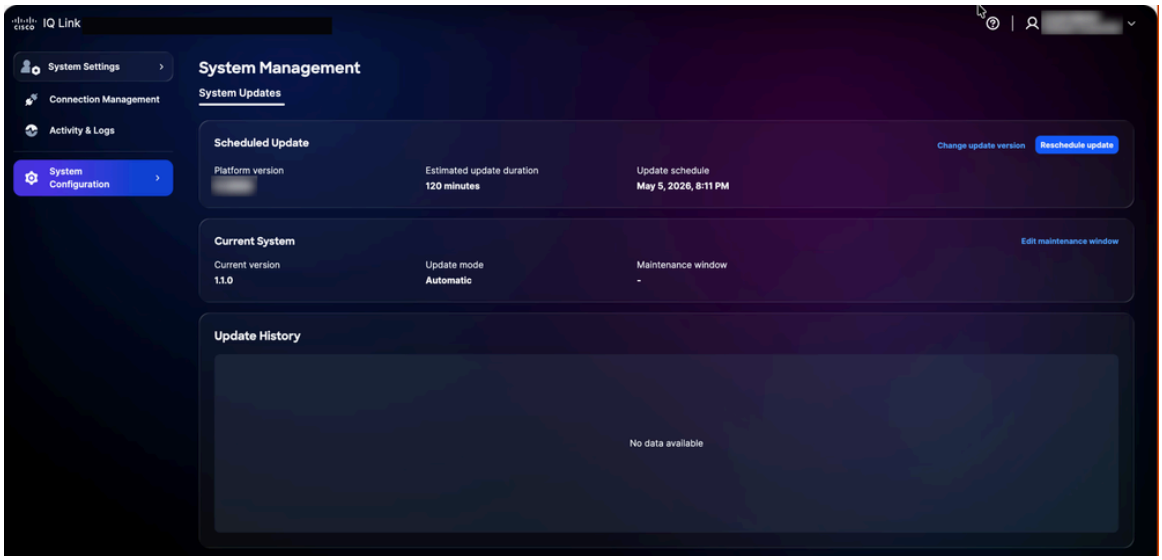
Atualização do gerenciamento do sistema

Os clientes podem atualizar para a versão mais recente do Cisco IQ Link através da interface do usuário. Você também pode verificar na página Cisco IQ Data Connectors.

Reprogramando sistema

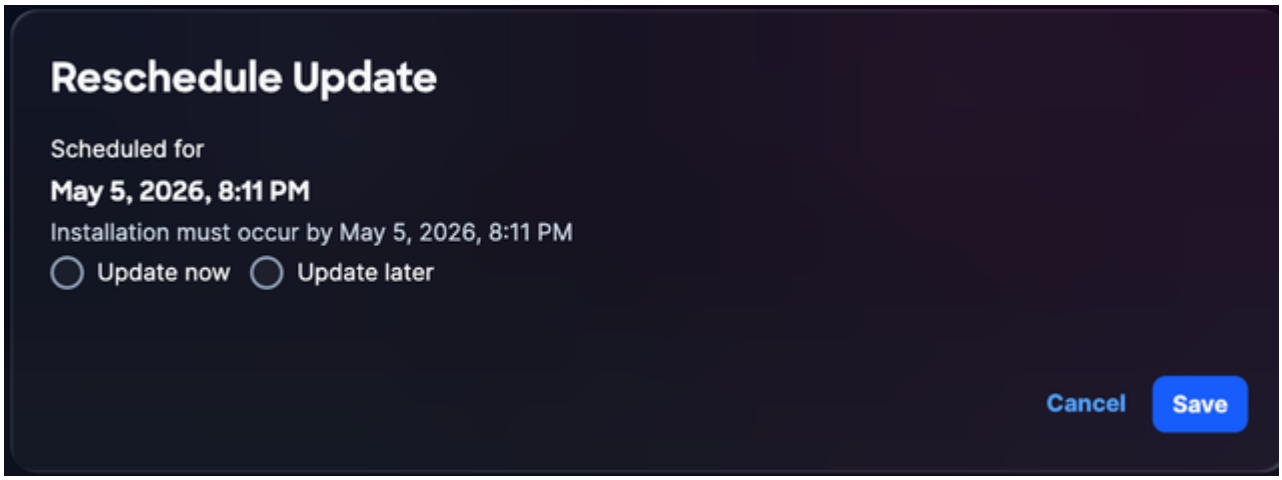
Para reprogramar a atualização do sistema:

1. Em Administração, escolha Configuração do Sistema > Gerenciamento do Sistema. A página Gerenciamento do sistema é exibida. Esta página exibe a versão do sistema que está em execução no momento; se nenhuma atualização tiver sido configurada, a seção Update History estará vazia.



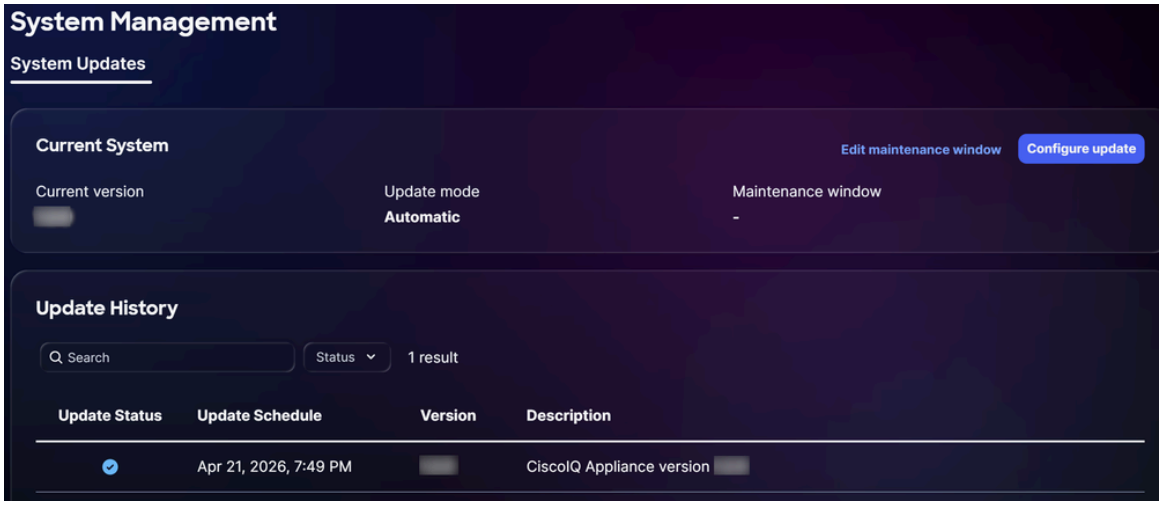
Atualização do sistema

2. Clique em Reagendar atualização.



Reagendar Atualização

3. Clique em Atualizar agora para reagendamento imediato ou em Atualizar mais tarde para agendar outro horário.
4. Click Save. Uma confirmação será exibida e você será redirecionado para a página inicial de atualização do sistema.



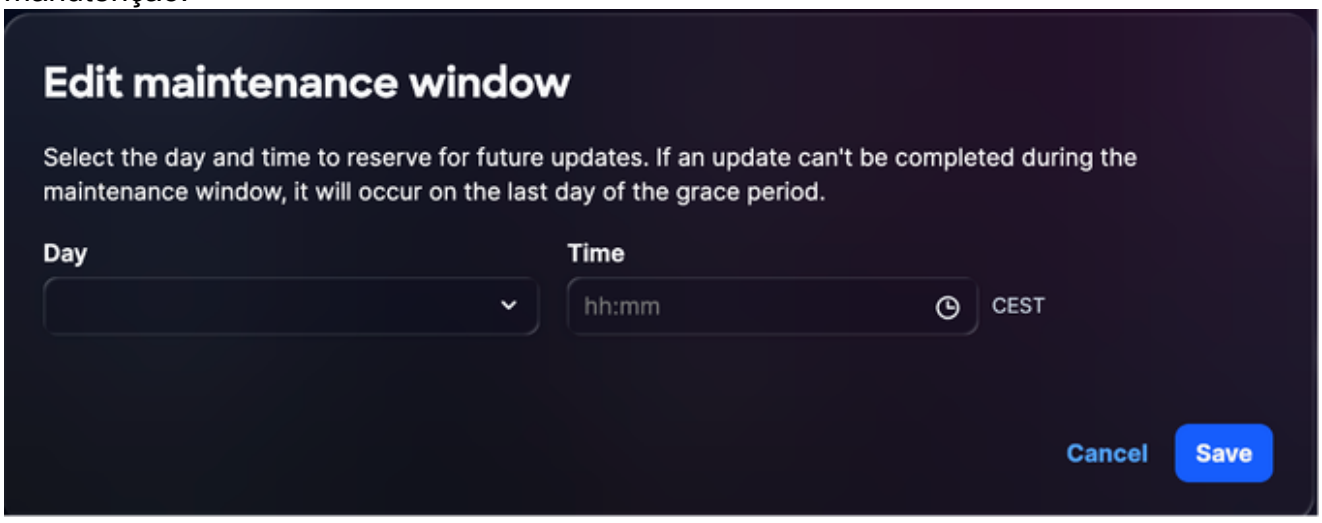
Atualização bem-sucedida

Editando Programações de Atualização do Sistema

Você pode criar um agendamento personalizado para atualizações do sistema. Se um agendamento personalizado for configurado, as atualizações ocorrerão em datas definidas pelo usuário, desde que elas permaneçam dentro do período de cortesia máximo.

Para criar um agendamento de atualização do sistema:

1. Na seção Sistema Atual da página Gerenciamento do Sistema, clique em Editar janela de manutenção.



Editar janela de manutenção

2. Escolha uma opção nas listas suspensas Dia e Hora.
3. Clique em Salvar. A janela de manutenção foi agendada com êxito. A atualização é acionada de acordo com a programação exibida.

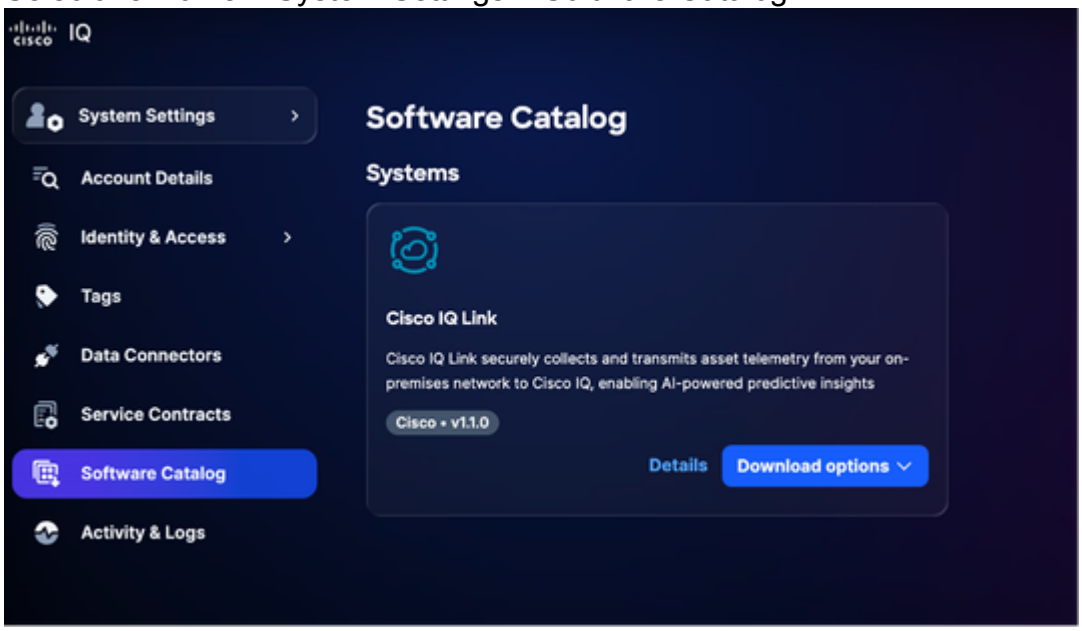
Notas:
· Se nenhuma programação de upgrade estiver configurada, o sistema assumirá como padrão períodos de carência de duas (2) semanas para upgrades sem reinicialização e de quatro (4) semanas para upgrades que exigem uma reinicialização. Após esses períodos de tolerância, as atualizações devem ser executadas manualmente.
· Em caso de falha de atualização, o sistema executa até duas (2) tentativas automáticas. Uma terceira tentativa está agendada, mas requer iniciação manual.

Atualizando manualmente o sistema

Em cenários onde a distribuição automática do Cisco IQ SaaS está indisponível ou atrasada, você pode executar manualmente uma atualização do sistema fazendo o download do pacote de atualização diretamente do Cisco IQ SaaS.

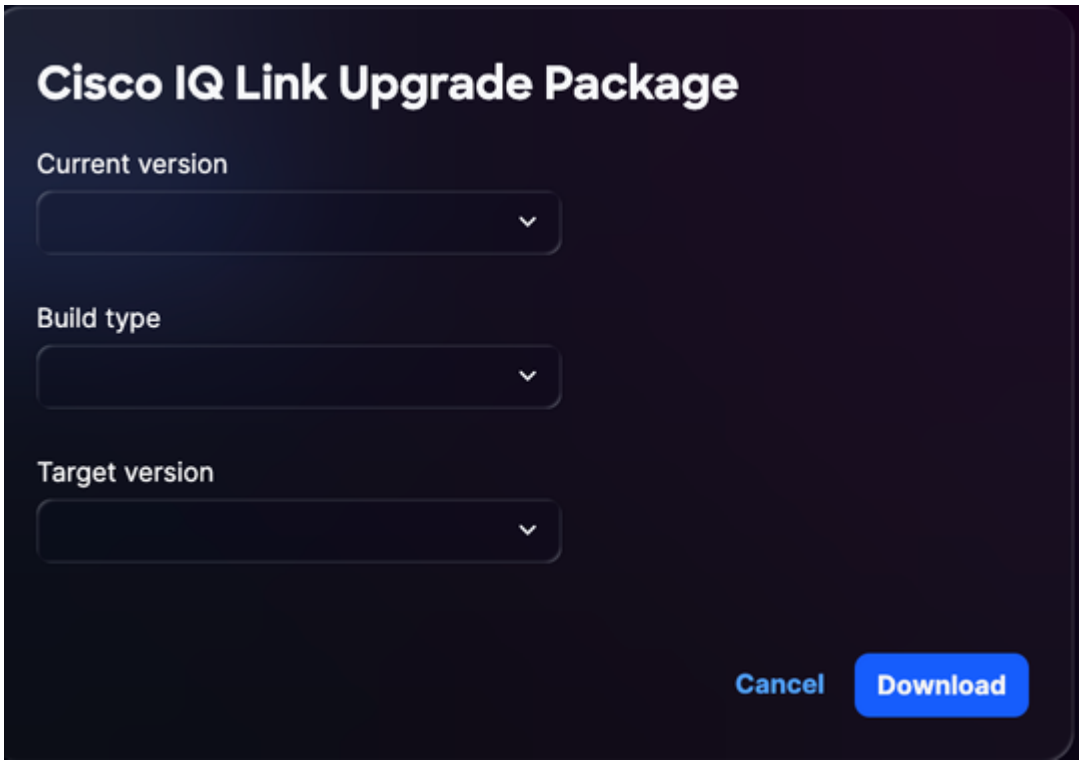
Para atualizar manualmente o sistema:

1. Faça login no Cisco IQ SaaS.
2. Selecione Home > System Settings > Software Catalog.



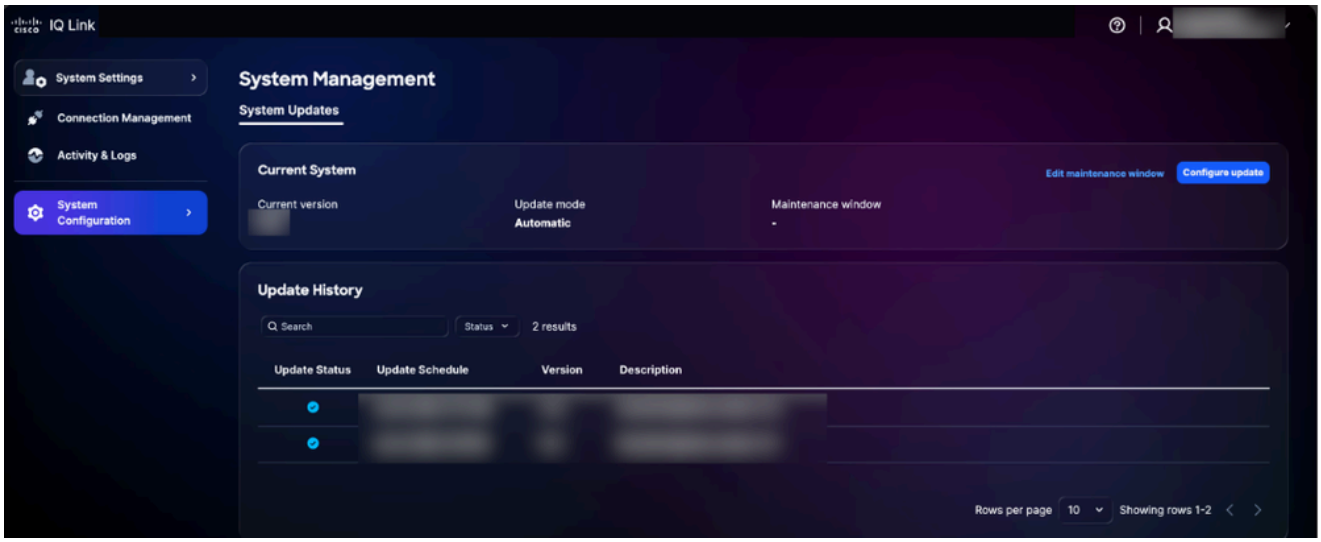
Catálogo de software

3. Na seção Cisco IQ Link, clique em Download options > Upgrade packages.



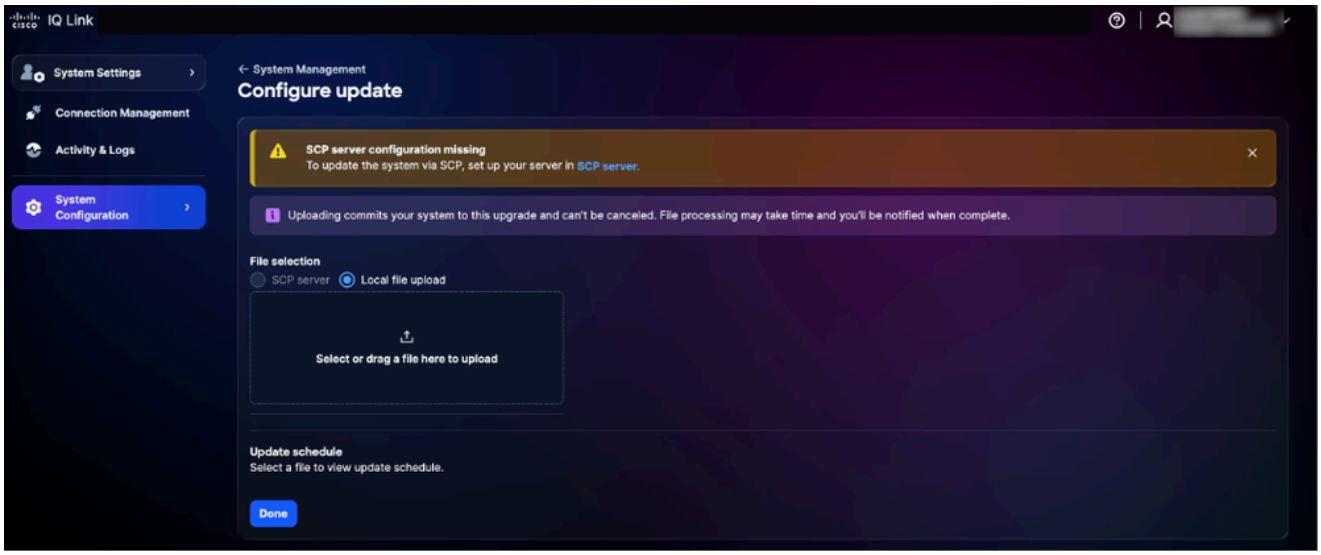
Pacote de atualização

4. Escolha a Versão atual na lista suspensa.
5. Escolha o Tipo de construção na lista suspensa.
6. Escolha a versão de Destino na lista suspensa.
7. Clique em Download. O pacote de atualização é baixado.
8. Navegue até Cisco IQ Link.
9. Em Configurações do sistema, escolha Configuração do sistema > Gerenciamento do sistema.



Configurar atualização

10. Clique em Configure update.



Carregamento de arquivo local

11. Clique no botão de opção Local file upload.
12. Selecione ou arraste o arquivo do pacote de atualização baixado para o campo de carregamento.
13. Clique em Concluído. Uma mensagem de confirmação é exibida depois que o sistema é atualizado com êxito.

Configuração de Certificados SSL

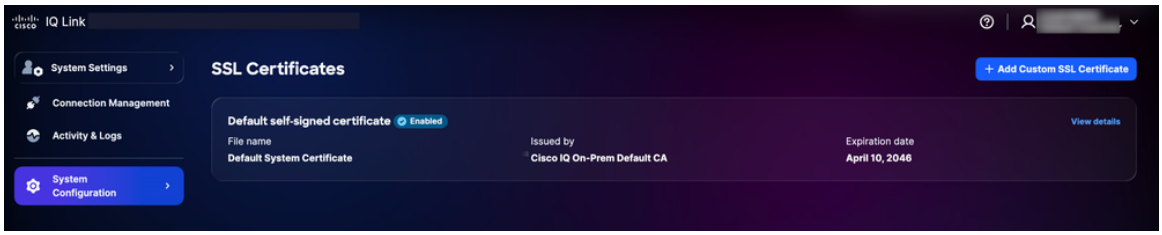
Um certificado autoassinado padrão é pré-instalado e habilitado no Cisco IQ, mas os usuários podem carregar certificados SSL personalizados. Quando um certificado SSL personalizado é habilitado, ele é usado para conexões HTTPS; se o certificado for desativado ou excluído, o sistema reverterá automaticamente para o certificado padrão.

Note: O certificado deve ter pelo menos 90 dias de validade. Um certificado é considerado "prestes a expirar" quando tem menos de 90 dias até a expiração. Após adicionar, editar ou excluir um certificado SSL, o cliente deve carregar o novo SSL conforme descrito na seção Concluindo a configuração do SLO para o IDP do Okta ou o IDP do ADFS.

Adicionando certificado SSL personalizado

Para adicionar um certificado SSL personalizado:

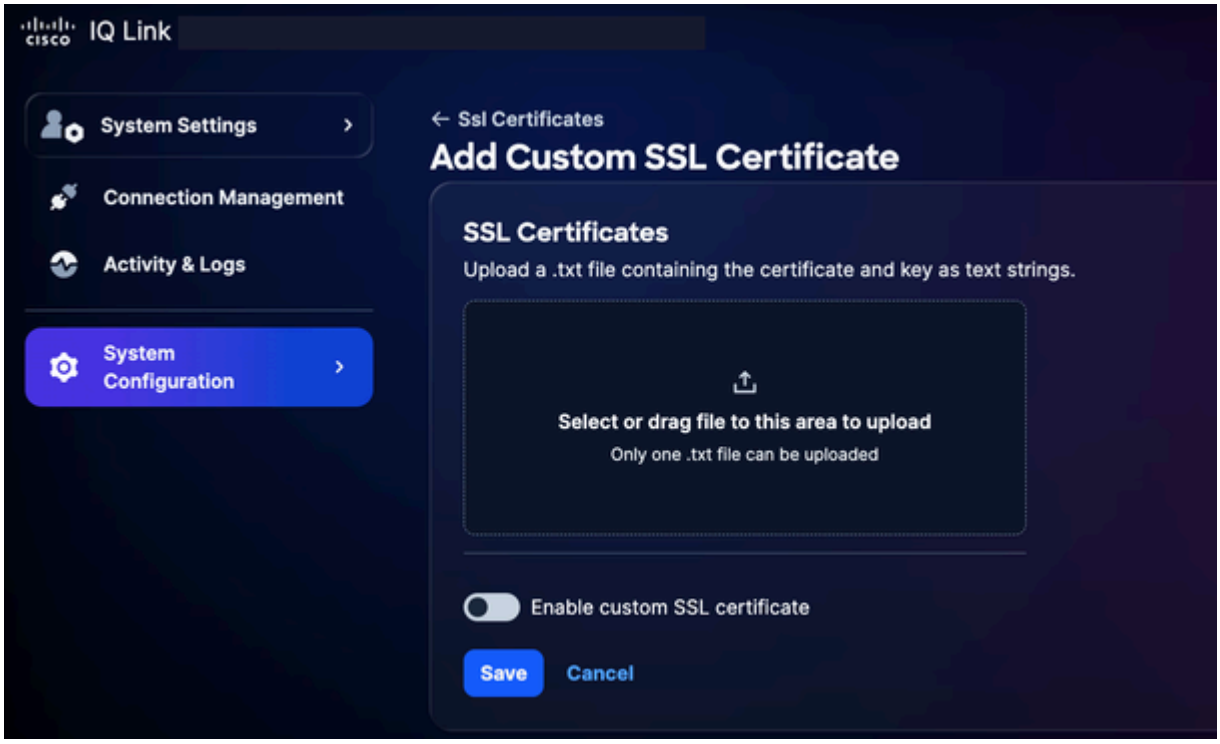
1. Em Configurações do sistema, escolha Configuração do sistema > Certificados SSL. A página Certificados SSL é exibida, listando todos os certificados SSL do seu sistema.



Adicionando Certificado SSL

2. Clique em Adicionar certificado SSL personalizado.

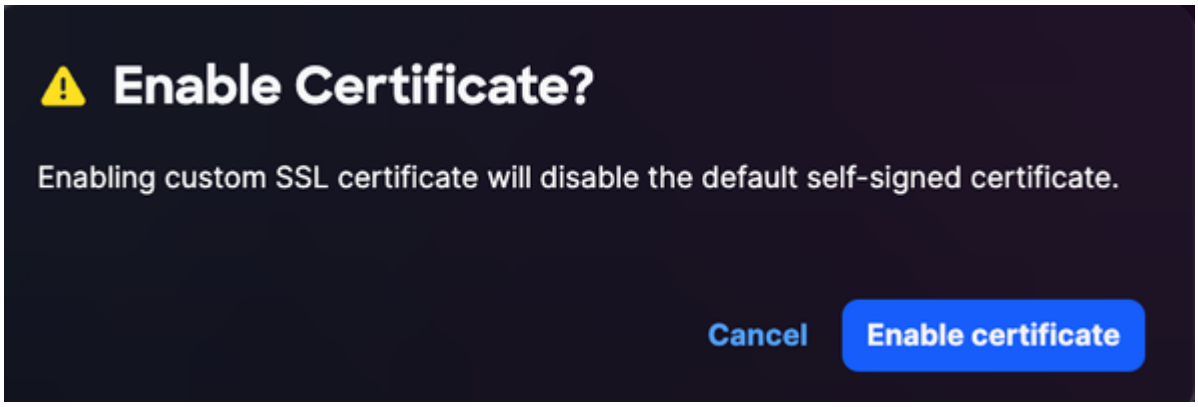
Notas:
· Carregue um arquivo .txt que inclua o certificado e a chave codificados no Privacy-Enhanced Mail como strings de texto
· Somente um arquivo .txt pode ser carregado por vez
· O arquivo deve conter o certificado e a chave privada



Carregar Certificados SSL

3. Arraste e solte ou carregue o certificado SSL personalizado no campo Certificado SSL.

4. Ative o botão de alternância Habilitar certificado SSL personalizado.



Habilitar certificado

Note: Mantenha a tecla de alternância DESATIVADA se desejar carregar o certificado sem ativá-lo imediatamente.

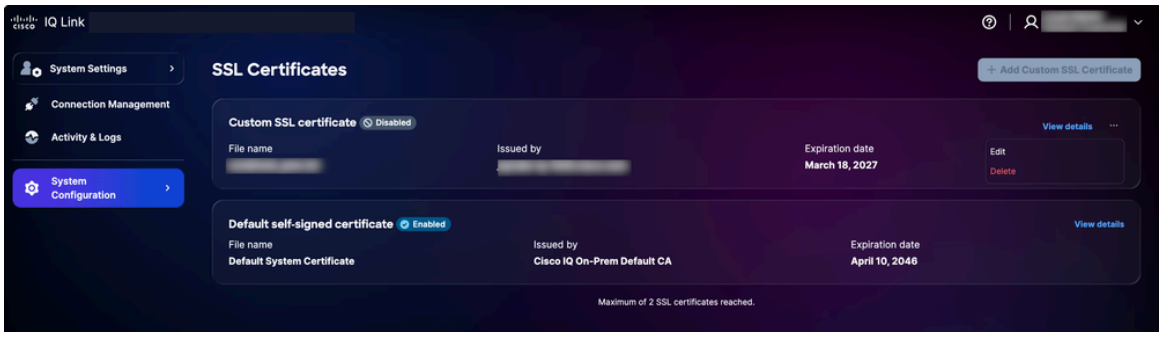
5. Clique em Ativar certificado.
6. Click Save.

O certificado SSL personalizado está habilitado e ativo. O certificado padrão do sistema é desativado automaticamente.

Edição de certificados SSL personalizados

Você pode editar o certificado SSL personalizado para carregar um novo certificado ou desabilitar o certificado habilitado no momento. Para editar:

1. Navegue até o certificado SSL personalizado desejado.



Editar Certificado SSL

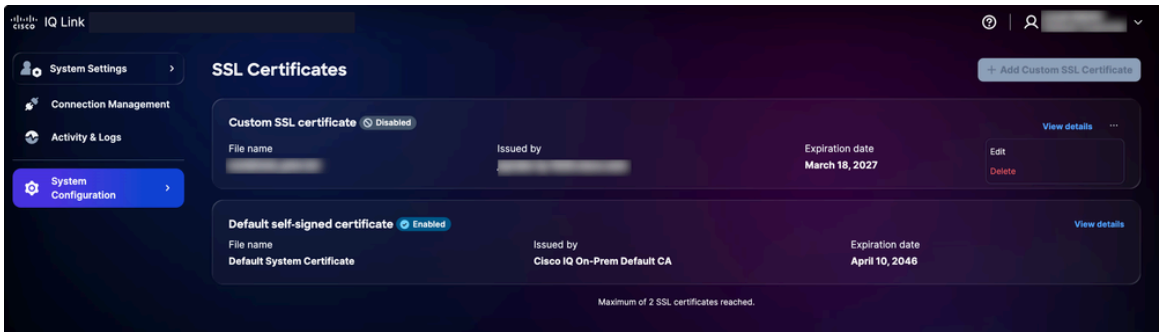
2. Escolha o ícone Mais Opções > Editar. A página Editar Certificado SSL é exibida.
3. Edite os detalhes do certificado conforme necessário.
4. Click Save.

Excluindo certificados SSL personalizados

aviso: Um certificado SSL personalizado pode ser excluído a qualquer momento, mas é uma ação irreversível; você pode carregar um novo certificado personalizado a qualquer momento após a exclusão.

Para excluir:

1. Navegue até o certificado SSL pessoal desejado.



Excluir Certificado SSL

2. Escolha o ícone Mais Opções > Excluir.
3. Clique em Excluir certificado. O certificado personalizado é excluído e o certificado padrão é reativado automaticamente.

Configuração do Servidor Syslog

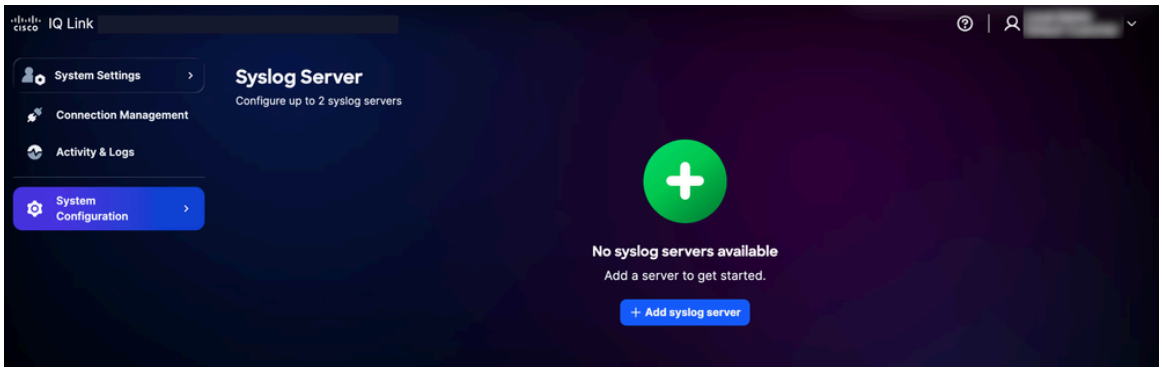
Os usuários com a função Administrador podem configurar servidores syslog externos para exportar logs do sistema. Até 2 (dois) servidores syslog podem ser configurados.

Note: O servidor Syslog deve ser especificado como um endereço IP, não como um FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado).

Adicionando servidores Syslog

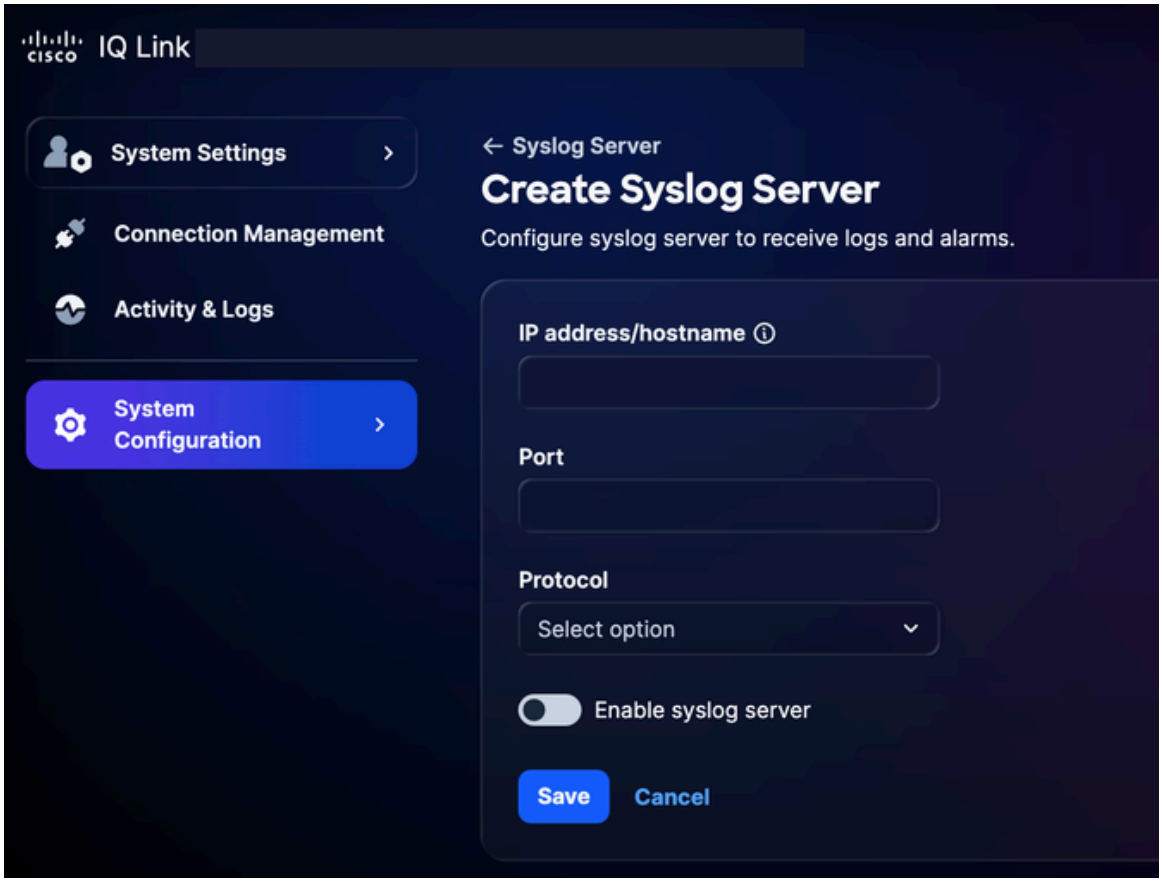
Para adicionar um Servidor syslog:

1. Em Configurações do sistema, escolha Configuração do sistema > Servidor Syslog. A página Servidor Syslog é exibida.



Adicionar Servidor Syslog

2. Clique em Add syslog server. A página Criar Servidor Syslog é exibida.



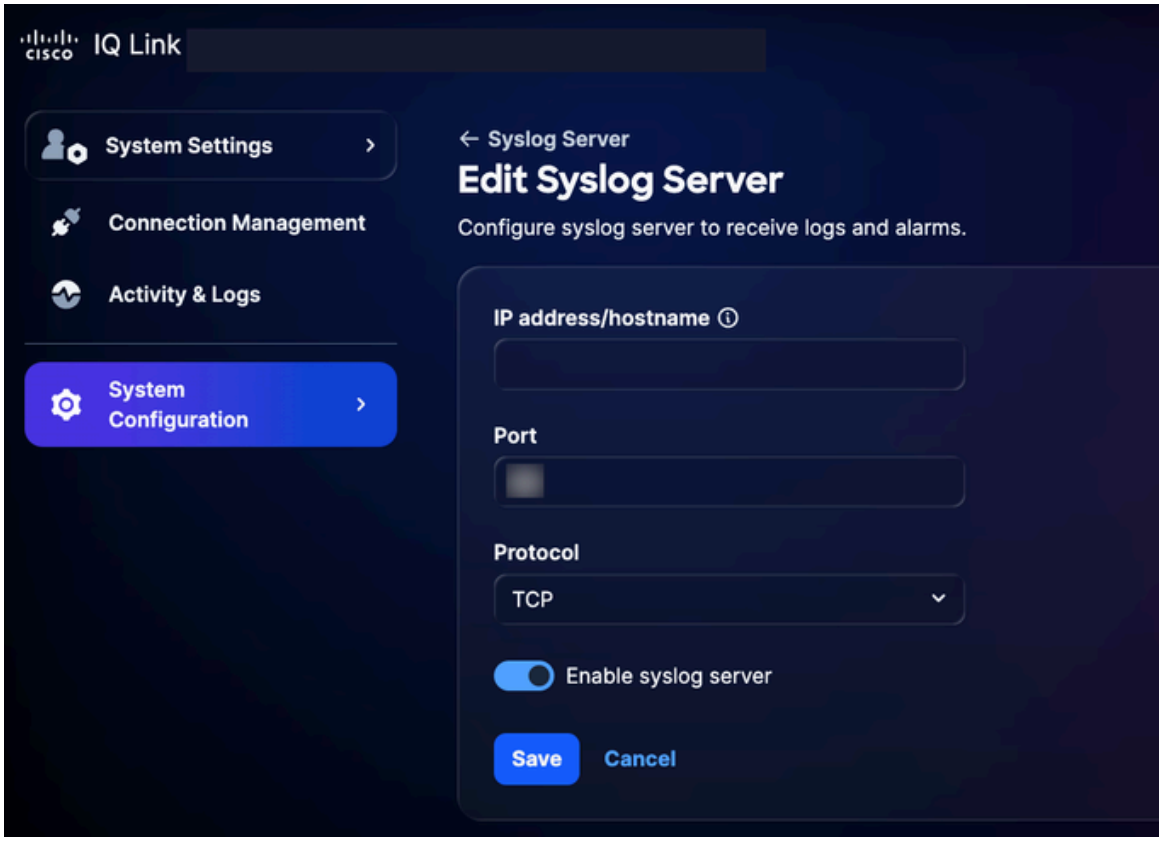
Criar Servidor Syslog

3. Insira o endereço IP/nome do host.
4. Insira um número de porta.
5. Selecione o protocolo aplicável na lista suspensa Protocolo (por exemplo, UDP ou TCP).
6. Ative o botão de alternância Enable syslog server.
7. Click Save. Uma confirmação é exibida e o Servidor syslog recém-adicionado é exibido na página inicial do Servidor Syslog.

Editando servidores Syslog configurados

Para editar um servidor syslog configurado:

1. Navegue até o Servidor syslog desejado.
2. Escolha o ícone Mais Opções > Editar. A página Edit Syslog Server é exibida.



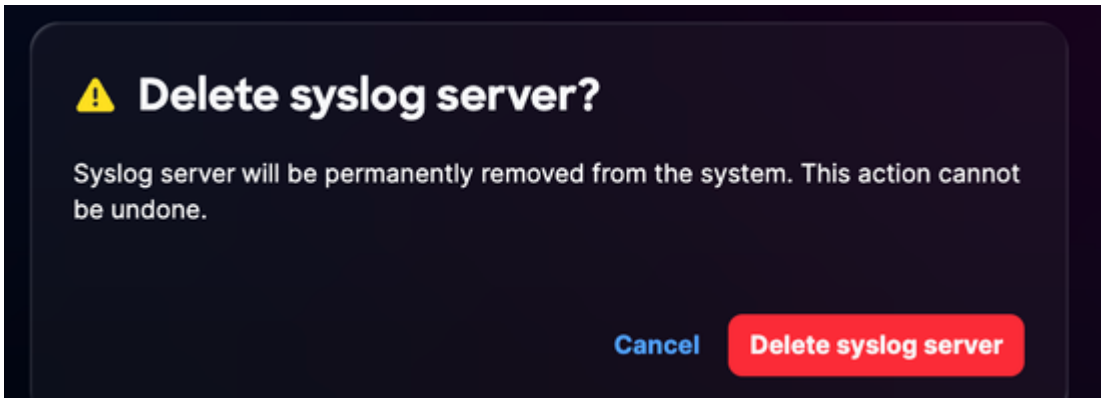
Editar Servidor Syslog

3. Edite os detalhes ou desative a alternância Enable syslog server, conforme necessário.
4. Click Save.

Excluindo servidores Syslog configurados

Para excluir um servidor syslog configurado:

1. Navegue até o Servidor syslog desejado.
2. Escolha o ícone Mais Opções > Excluir. Uma confirmação é exibida.

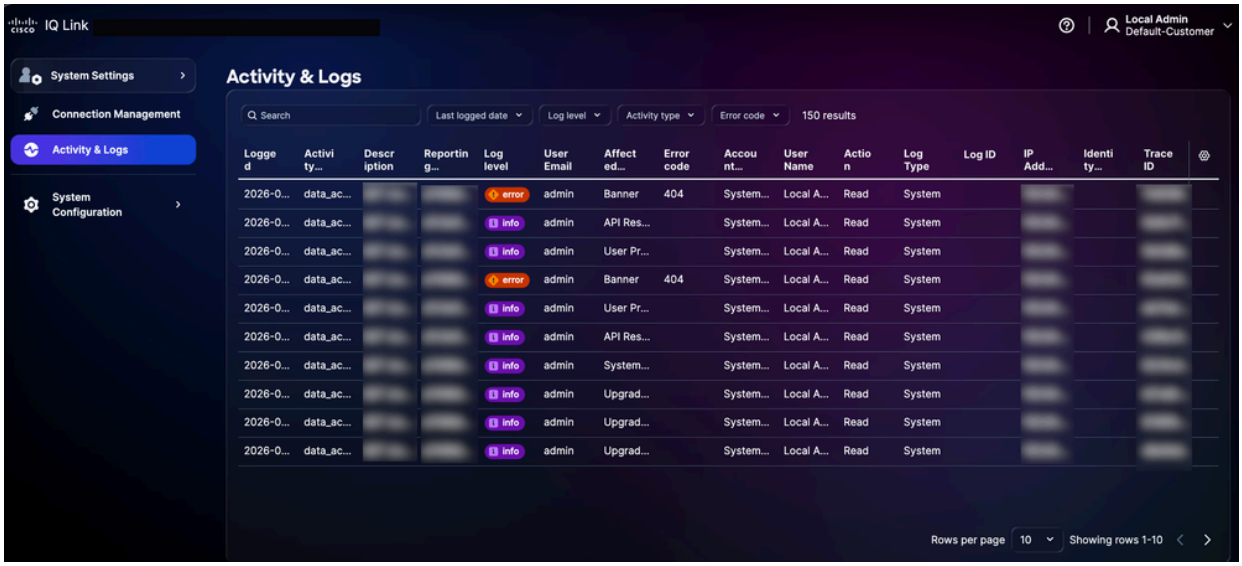


Confirmação

3. Clique em Excluir Servidor syslog.

Atividade e registros

Atividade e registros fornecem um registro detalhado das ações e alterações do usuário no Cisco IQ, permitindo que os administradores controlem as atividades do usuário e mantenham a transparência.



Atividade e registros

Para exibir atividades e logs, selecione Activity & Logs no menu System Settings.

Atividade e registros:

- Suporte a filtros, paginação e recursos de pesquisa para ajudar a localizar e gerenciar informações com facilidade

- Registrar todas as operações de API no nível do gateway

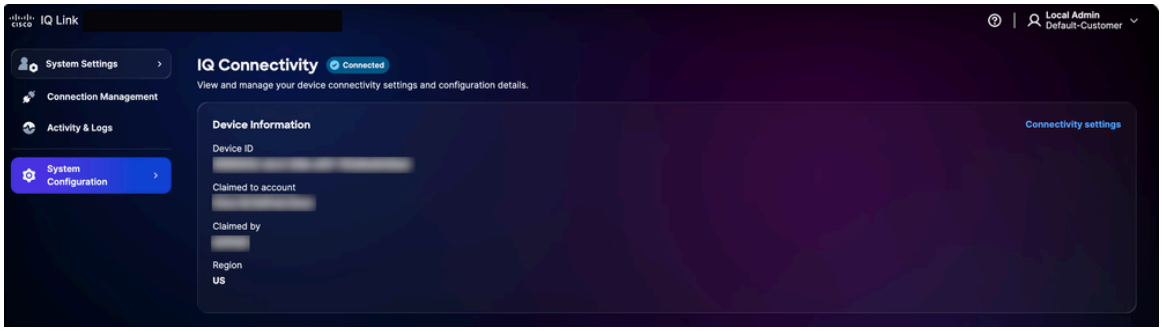
As seguintes opções de filtro estão disponíveis:

- Data: Filtra logs para um intervalo de tempo específico
- Nível de log: Filtra logs por gravidade (por exemplo, erro, aviso e informações)
- Tipo de atividade: Filtra logs pelo tipo de atividade do sistema
- Código de erro: Filtra logs para um código de erro específico

Conectividade IQ

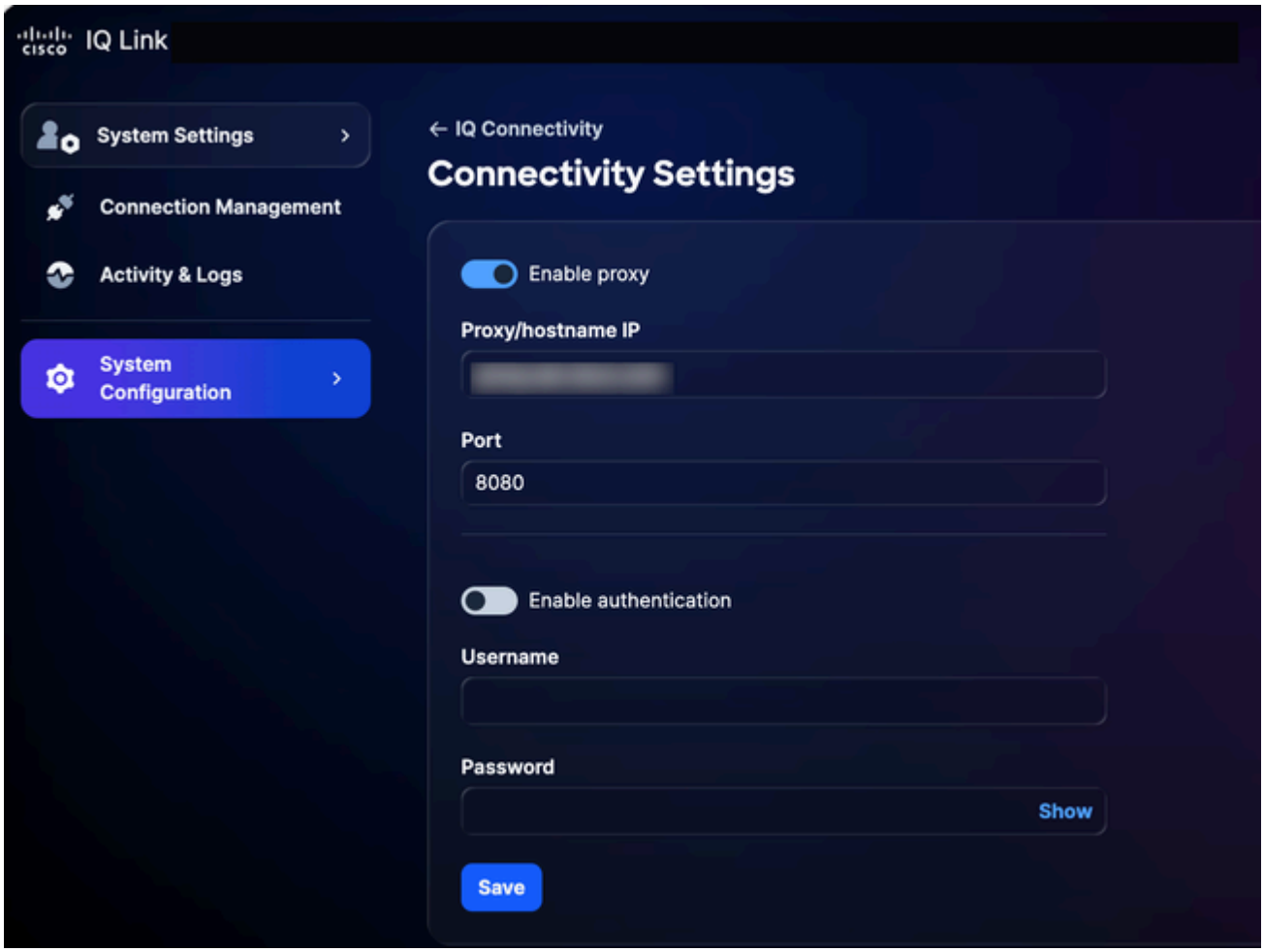
Para exibir e gerenciar as definições de conectividade do dispositivo e os detalhes de configuração:

1. Em Configurações do sistema, escolha Configuração do sistema > Conectividade IQ. A página IQ Connectivity é exibida.



Conectividade IQ

2. Clique em Configurações de conectividade.



Configurações de conectividade

3. Atualize os detalhes conforme necessário.
4. Click Save.

Gerenciamento de Conexões (Coleta de Dados)

O Cisco IQ Link é uma solução implantada no local para coleta de dados de rede, projetada para fornecer visibilidade profunda em sua infraestrutura. Ele coleta dados através do Catalyst Center e do Direct Connection. Ele simplifica a forma como você gerencia a autenticação de rede e a descoberta de dispositivos. A configuração da coleta de dados pode ser resumida como compartilhada abaixo:

- Criando conjuntos de credenciais: Estabeleça os protocolos de autenticação (por exemplo, SNMP v1/v2c/v3) para se comunicar com seus dispositivos de rede. A centralização de credenciais por zona de segurança ou local (por exemplo, "SanJose-SNMPv3") permite que você atualize senhas em um local, com alterações que se propagam automaticamente para todos os dispositivos associados.

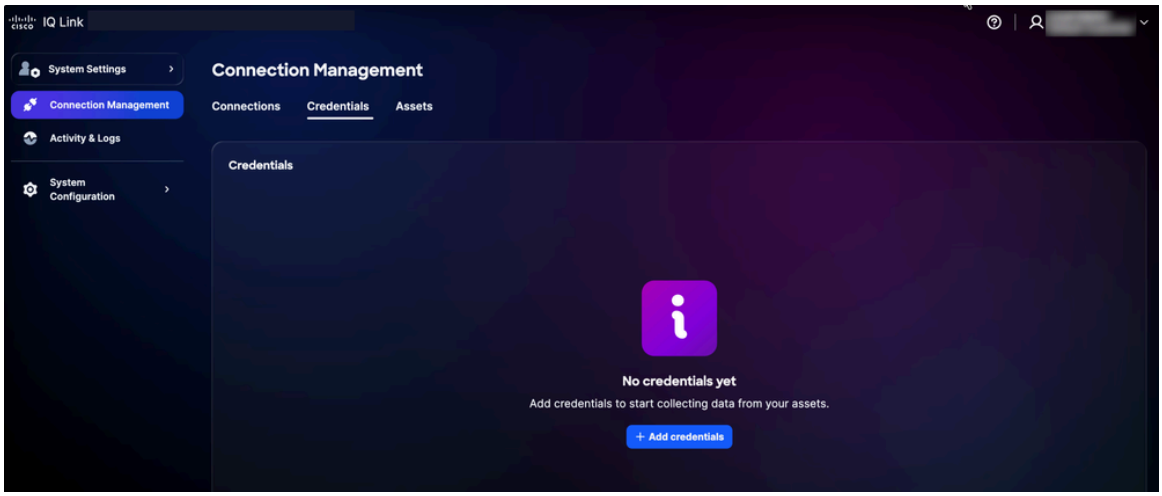
- Mapeando credenciais para Inventário: Mapeie seus conjuntos de credenciais com os ativos de inventário para automatizar o processo de autenticação. Criando regras que vinculam intervalos de IP específicos a Conjuntos de Credenciais definidos, o sistema aplica automaticamente a autenticação correta durante a coleta de dados. Isso elimina erros de entrada manual e garante que sua configuração permaneça precisa à medida que a rede cresce.

Note: O SNMPv2c/SNMPv3 e o SSH são necessários para a descoberta de dispositivos e as credenciais HTTP/HTTPS devem ser fornecidas antes da configuração do Catalyst Center.

Adicionando credenciais

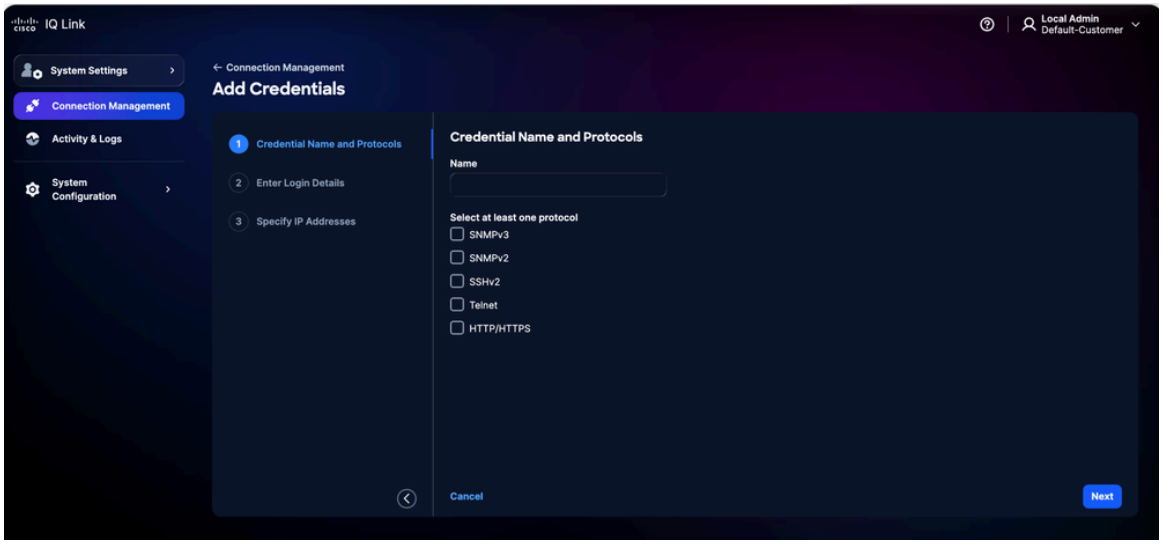
Primeiro você deve adicionar credenciais para executar a coleta de dados. Para adicionar credenciais:

1. Em Configurações do Sistema, escolha Gerenciamento de Conexões. A página Gerenciamento de conexões é exibida.
2. Clique na guia Credenciais.



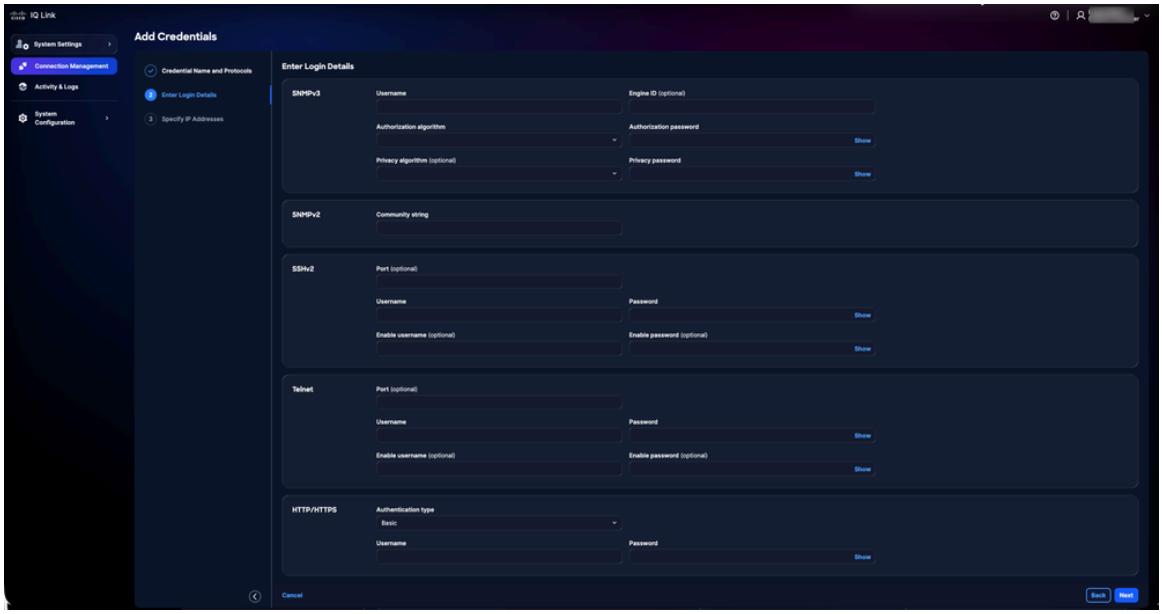
Guia Credenciais

3. Clique em Adicionar credenciais.



Adicionar Credenciais

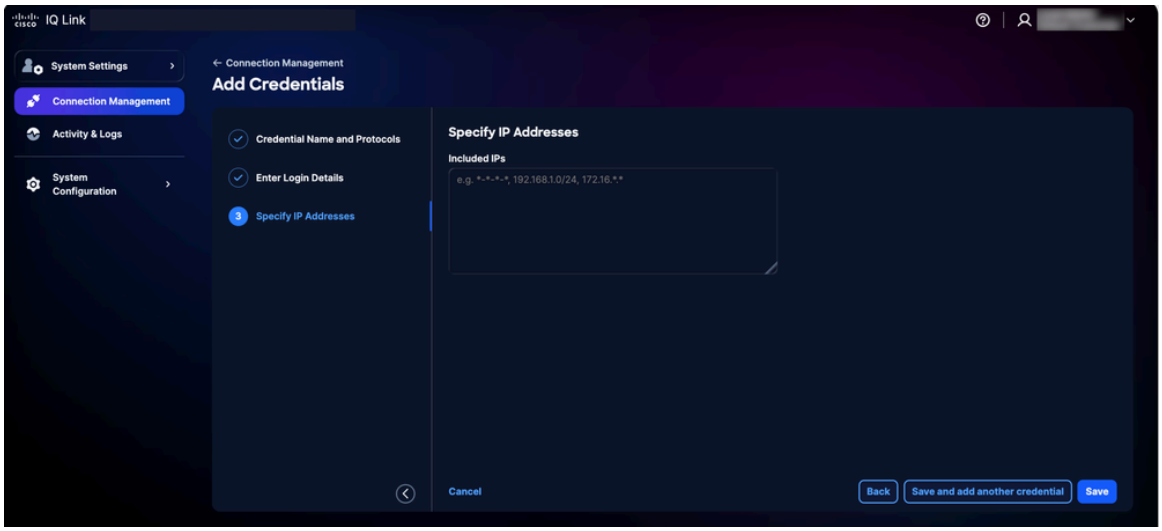
4. Insira Name.
5. Marque todas as caixas de seleção de protocolo aplicáveis.
6. Clique em Next.



Adicionar detalhes de credenciais

Note: Para a imagem acima, ilustramos a visualização quando todos os protocolos são selecionados na etapa anterior. Sua interface exibirá apenas os protocolos específicos que você escolheu.

7. Insira os detalhes de logon para cada protocolo selecionado.
8. Clique em Next.



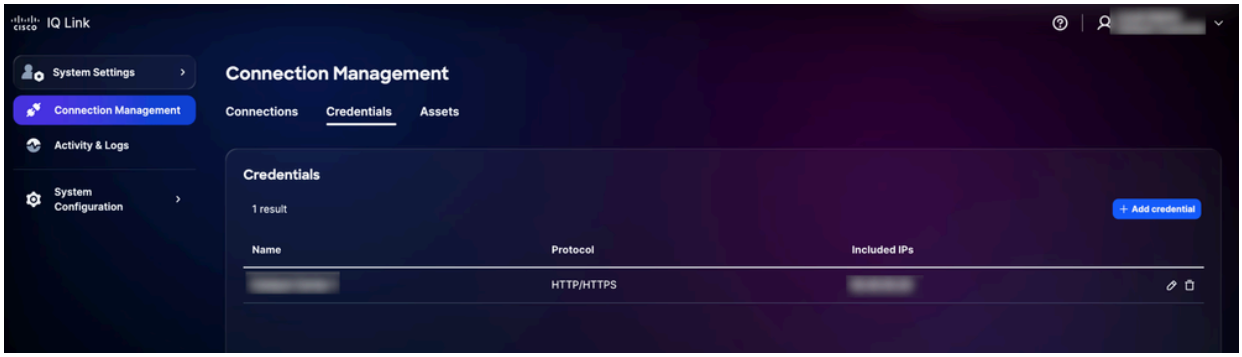
Especificar Endereços IP

9. Insira os IPs incluídos.

Note: Esse campo define os endereços IP ou intervalos de IP em que as credenciais podem ser usadas para estabelecer uma conexão. Ele suporta uma combinação de IPs e máscaras IP (usando notação curinga). Para obter detalhes sobre formatos suportados, consulte Seleção de Credencial e Lógica de Correspondência.

---

10. Click Save. Uma confirmação é exibida e você é redirecionado para a guia Credenciais.



Credenciais Adicionadas

Você pode editar as credenciais clicando no ícone Editar e excluí-las clicando no ícone Excluir.

Seleção de Credencial e Lógica de Correspondência

O mecanismo de telemetria emprega uma lógica de correspondência baseada em prioridade para determinar quais credenciais aplicar durante a descoberta e a coleta. Entender essa hierarquia garante que as credenciais corretas sejam usadas para os dispositivos pretendidos.

- Classificação de prioridade: Quando vários conjuntos de credenciais se aplicam a um dispositivo, o Cisco IQ os avalia com base em como eles correspondem especificamente ao dispositivo; o sistema aplica a seguinte prioridade, com correspondências mais específicas tendo precedência:
    - Correspondência de IP exata: Prioridade mais alta
    - Correspondência Curinga à Direita:** **A prioridade depende do número de estrelas à direita; menos estrelas indicam uma correspondência mais específica e, portanto, maior prioridade
- Regras de Formatação Curinga: Caracteres curinga (*) são suportados apenas como caracteres à direita em um endereço IP; elas devem ser aplicadas da direita para a esquerda.
    - Formatos suportados:

      1.2.3.* (prioridade mais alta entre os curingas)

      1.2.*.*

      1.**.*

      ..*.* (Prioridade mais baixa)
    - Formatos sem suporte:

      Curingas à esquerda (por exemplo, *.1.2.3)

      Caracteres curinga entre octetos (por exemplo, 10.10.*.20)

      Uso de traços ou outros delimitadores não padrão

Exemplo de Seleção de Credencial:

A tabela a seguir ilustra como o mecanismo de telemetria seleciona o conjunto de credenciais mais apropriado quando um dispositivo corresponde a vários padrões definidos.

Exemplo de Seleção de Credencial

IP do dispositivo	Conjuntos de credenciais disponíveis	Conjunto de Credenciais Selecionado
10.10.1.5	10.10.1.5, 10.10.1., 10.10.*	10.10.1.5 (Correspondência exata)

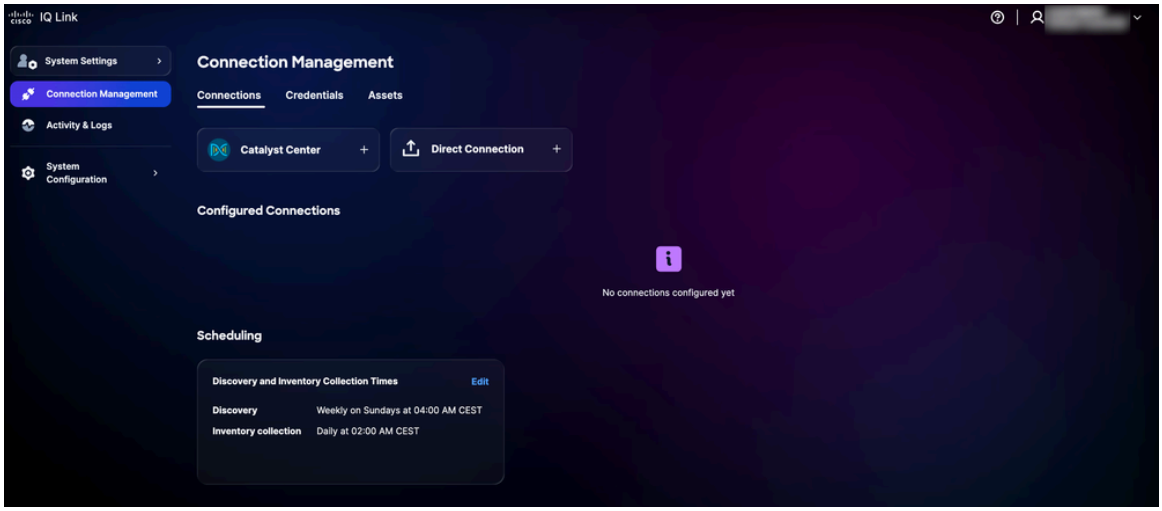
IP do dispositivo	Conjuntos de credenciais disponíveis	Conjunto de Credenciais Selecionado
10.10.2.15	10.10.2., 10.10.*	10.10.2.* (Mais específico)
10.10.5.50	10.10..., ...	10.10.. (Mais específico)

Note: Se um dispositivo se enquadra em várias categorias sobrepostas, o sistema sempre seleciona o conjunto de credenciais com a especificidade mais alta (em outras palavras, o menor número de curingas à direita).

Coleta de dados usando o Catalyst Center

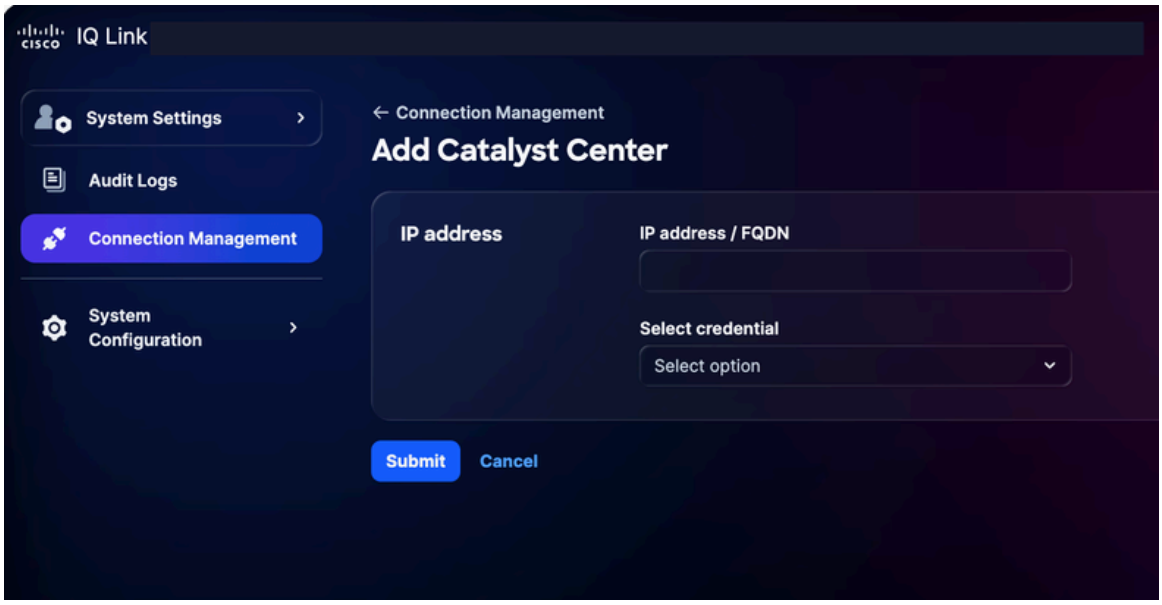
Para coleta de dados usando o Catalyst Center:

1. Em Configurações do Sistema, escolha Gerenciamento de Conexões. A página Gerenciamento de conexões é exibida.



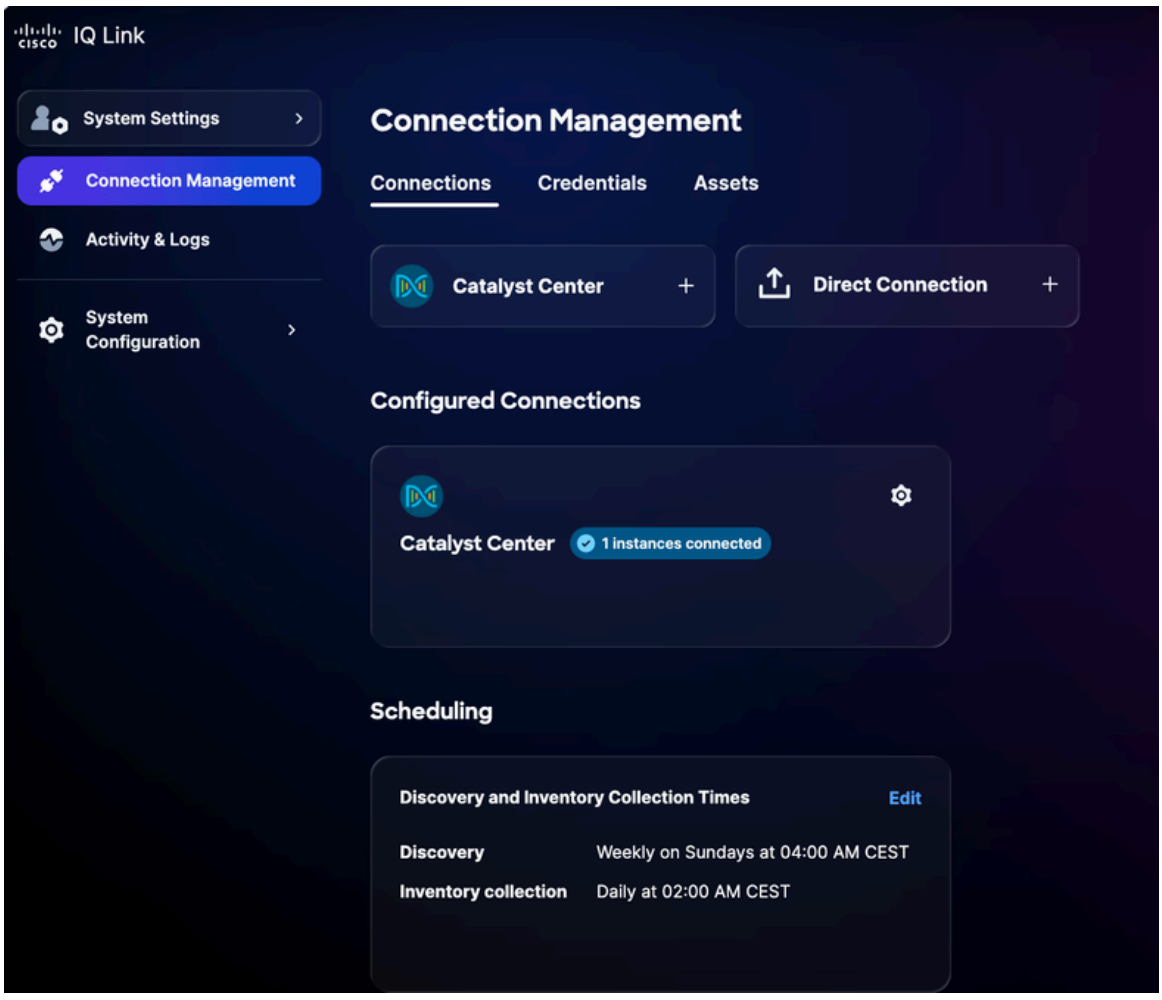
Gerenciamento de conexões

2. Clique na opção Catalyst Center.



Adicionar Catalyst Center

3. Insira o endereço IP ou o FQDN.
4. Escolha uma credencial HTTP/HTTPS configurada na lista suspensa.
5. Clique em Submit. Uma confirmação é exibida (pode levar até 75 minutos). Você pode visualizar o Catalyst Center recém-adicionado em Conexões Configuradas.



Catalyst Center Adicionado com Êxito

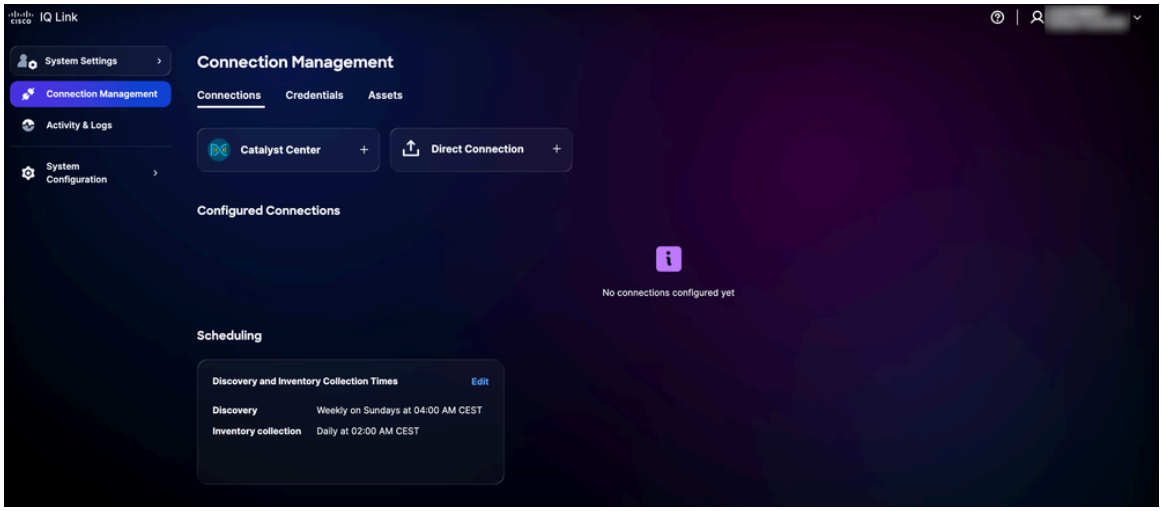
6. Programar uma coleta. Consulte Agendamento para obter mais detalhes.

Note: O Cisco IQ Link é pré-configurado com uma configuração de programação automatizada e o sistema inicia uma programação de coleta automatizada padrão. É altamente recomendável que você edite o agendamento para alinhá-lo aos requisitos e janelas de manutenção da sua organização.

Conexão direta

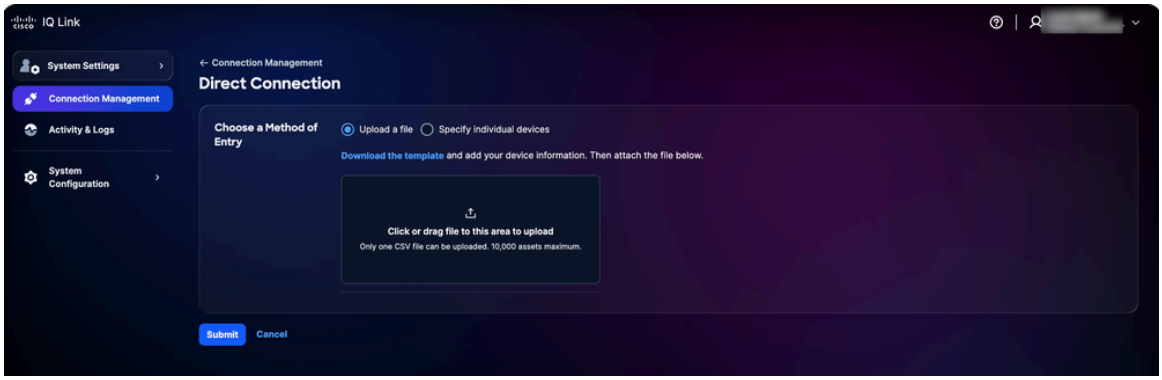
Para adicionar dispositivos para conexão direta:

1. Em Configurações do Sistema, escolha Gerenciamento de Conexões. A página Gerenciamento de conexões é exibida.



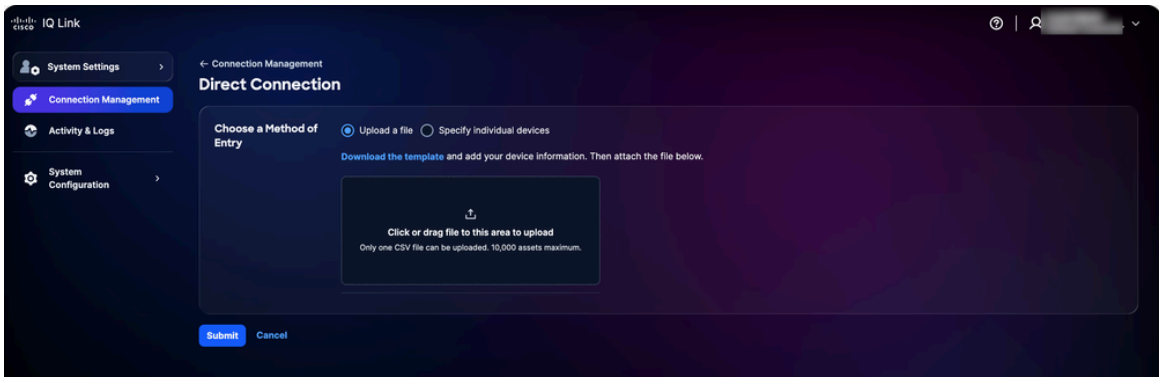
Gerenciamento de conexões

2. Clique em Direct Connection. A página Conexão direta é exibida com duas (2) opções para coletar dados.



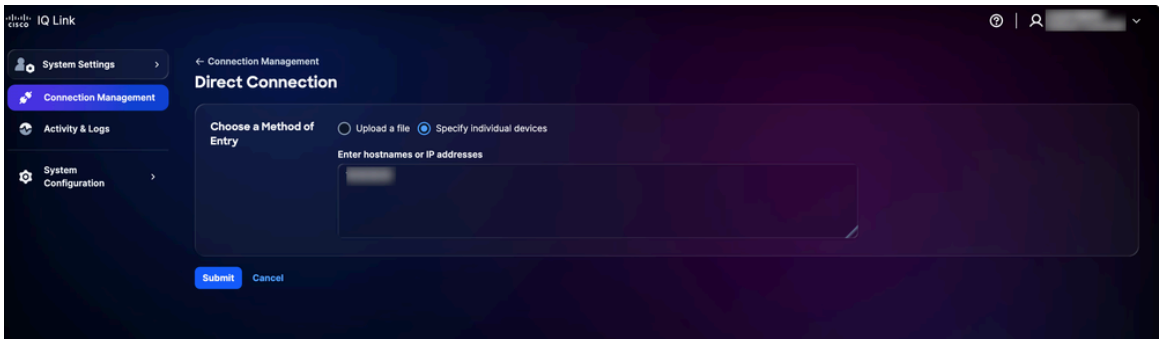
Carregar arquivo

3. Clique na opção preferida para Escolher um método de entrada e envie seus dispositivos usando um dos seguintes métodos:



Carregar um arquivo

- Carregar um arquivo: Clique ou arraste e solte o arquivo e clique em Enviar



Especificar dispositivos individuais

- Especifique dispositivos individuais: Insira um único nome de host, endereços IP ou uma lista separada por vírgulas de nomes de host e/ou endereços IP e clique em Enviar

Você será redirecionado para a guia Ativos após o envio bem-sucedido.

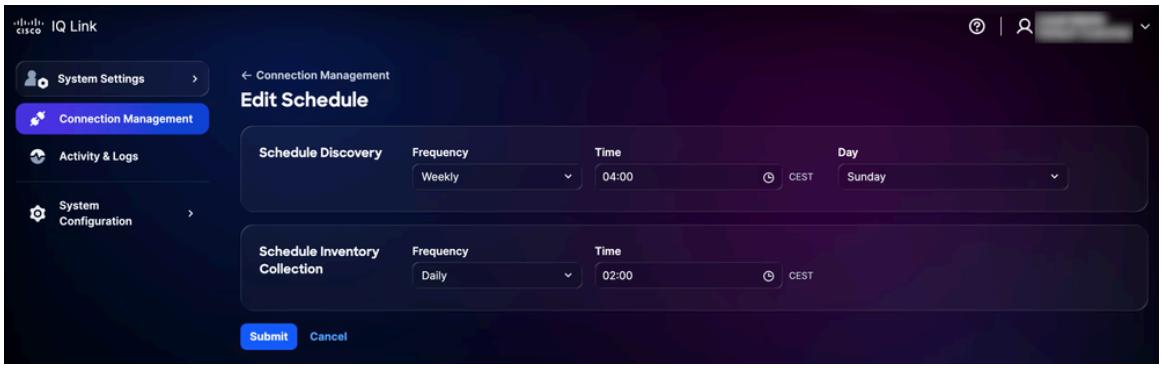
4. Programar uma coleta. Consulte Agendamento para obter mais detalhes.

Note: O Cisco IQ Link é pré-configurado com uma configuração de programação automatizada e o sistema inicia uma programação de coleta automatizada padrão. É altamente recomendável que você edite o agendamento para alinhá-lo aos requisitos e janelas de manutenção da sua organização.

Programação

O Agendamento permite que você defina quando o Cisco IQ Link executa a coleta automatizada de dados. Para agendar a coleta:

1. Na seção Programação da página Gerenciamento de conexões, clique em Editar para a programação que você deseja modificar. A página Editar Programação é exibida.



Editar Agenda

2. Na seção Schedule Discovery, escolha sua Frequência e Dia preferidos nas listas suspensas e digite sua Hora de início desejada.
3. Na seção Agendar coleta de inventário, escolha sua frequência preferida nas listas suspensas e digite a hora de início desejada.
4. Clique em Submit.

Note: Aguarde de 5 a 10 minutos para que todas as alterações feitas nas programações de descoberta ou coleta sejam sincronizadas e refletidas com precisão no Cisco IQ Link.

Banners

Os administradores podem configurar banners personalizados que são exibidos em todo o aplicativo.

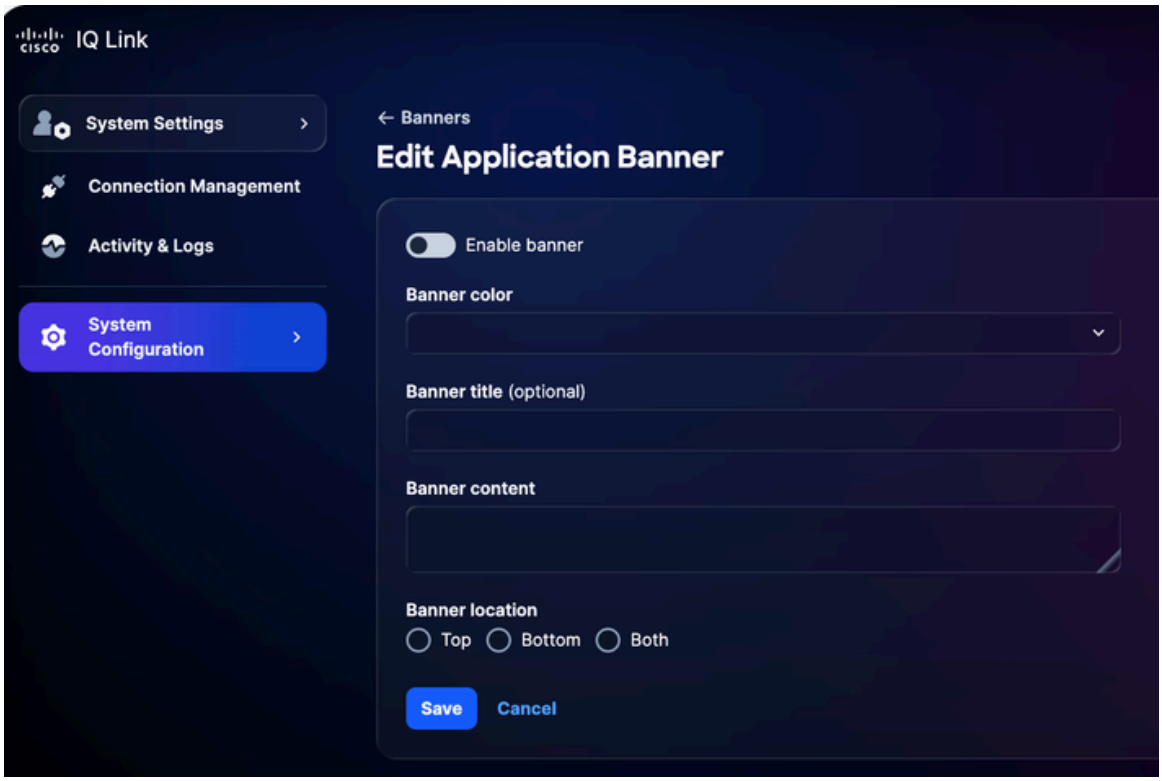
Configurando banners

Para configurar um banner:

1. Em Configurações do sistema, escolha Configuração do sistema > Banners. A página Banners é exibida.

Configurar banner

2. Clique em Configurar. A página Editar banner do aplicativo é exibida.



Editar banner do aplicativo

3. Clique no botão de alternância para ativar ou desativar o banner.
4. Selecione uma cor de banner.
5. Insira o título do banner.
6. Insira o conteúdo do banner.
7. Selecione um local de banner.
8. Click Save. O banner é exibido no aplicativo.

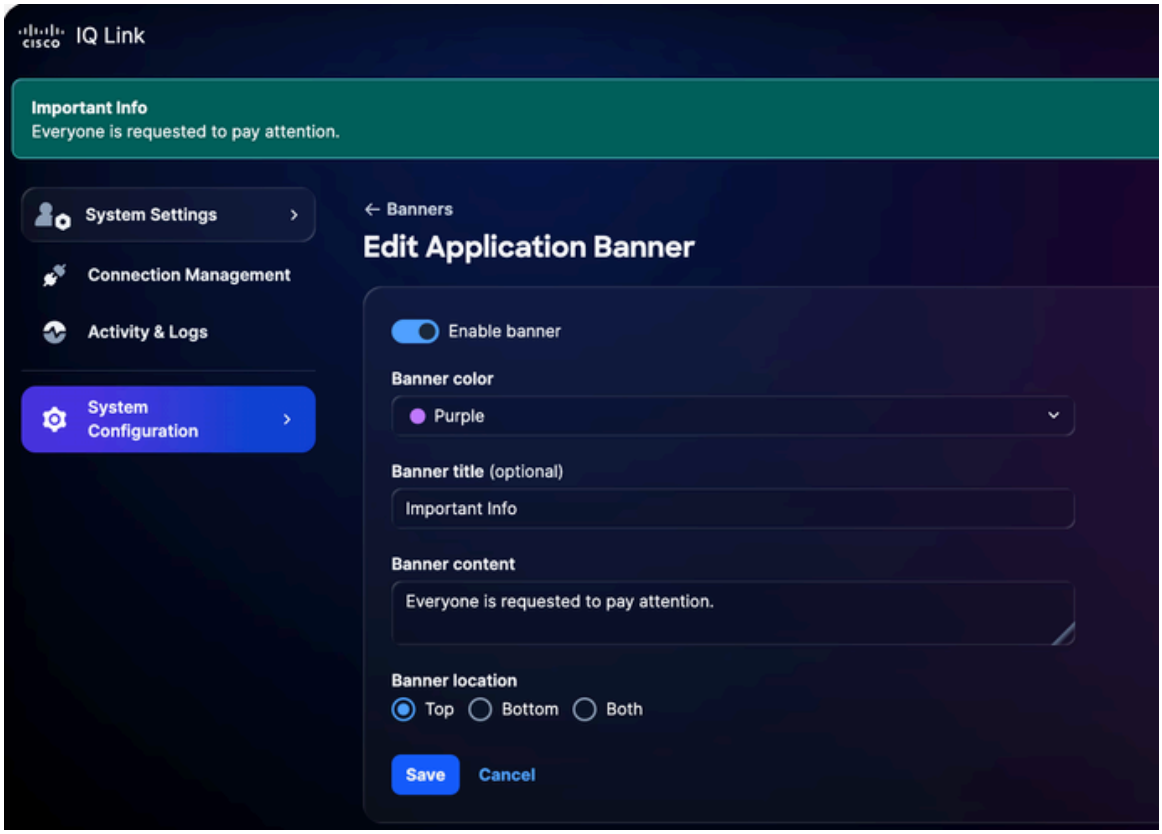
Editando banners

Para editar um banner:

1. Em Configurações do sistema, escolha Configuração do sistema > Banners. A página Banners é exibida.

Editar banners

2. Clique em Editar. A página Editar banner do aplicativo é exibida.



Editar banner do aplicativo

3. Edite os detalhes desejados.
4. Clique no botão de alternância para ativar ou desativar o banner.
5. Click Save.

Troubleshooting

Os clientes podem coletar arquivos de diagnóstico e de registro do sistema Cisco IQ e transferi-los com segurança para um servidor SCP. Esses arquivos podem ser compartilhados com a equipe de suporte ao relatar problemas para fornecer contexto valioso e ajudar na solução de problemas.

Para coletar arquivos de diagnóstico e de log:

1. Faça login no Cisco IQ.

Menu principal

2. No Cisco IQ Main Menu, digite "3" e pressione Enter para selecionar System Diagnostics.

Diagnóstico do sistema

3. Insira o endereço do servidor SCP/SFTP.
4. Insira a Porta do servidor SCP/SFTP.
5. Insira o caminho do servidor SCP/SFTP.
6. Selecione um protocolo.
7. Insira o nome de usuário.
8. Digite a senha.
9. Digite "C" e pressione Enter para continuar com o diagnóstico do sistema.

Operação de Diagnóstico do Sistema Operação de Diagnóstico do CoSistema Concluída Modelo

O sistema inicia o processo de diagnóstico e executa as seguintes ações:

- Verificando a acessibilidade
- Coletando informações do sistema
- Coletando informações do Kubernetes
- Coletando logs
- Preparando o pacote de diagnósticos do sistema
- Carregando pacote de diagnóstico do sistema

Uma vez concluído, uma mensagem de confirmação é exibida indicando o nome do pacote gerado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.