# Guia de operações do Cisco IQ Link v1.2.0

## Introdução

O Cisco IQ™ oferece 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 AI Assistant, otimizam os resultados operacionais e a experiência do usuário do Cisco IQ, fornecendo entendimento contextual que permite que você tome decisões proativas e informadas e simplifique 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 de conta devem usar as seguintes credenciais para fazer login no Cisco IQ Link:

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

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

### Configurando a segurança do administrador local

Você pode alterar sua senha e configurar as perguntas de segurança por meio do menu Perfil de usuário na página inicial.

Configurações de Bloqueio

As seguintes configurações de bloqueio de conta são configuráveis durante a implantação:

- Status do Bloqueio: Ativa ou desativa o recurso de bloqueio de conta.
- Máximo de Tentativas de Login: Define o número máximo de tentativas consecutivas com falha permitido antes que uma conta seja bloqueada (Padrão: 3; Faixa: 0–10).
- Janela Tempo de Rolagem: Define o período de tempo para rastreamento de tentativas com falha (Default: 15 minutos; Faixa: 0-60 minutos).
- Duração: Define a duração pela qual uma conta permanece bloqueada após o número máximo de tentativas ser atingido (Padrão: 30 minutos; Faixa: 0-60 minutos).

---

Note: Você tem três (3) tentativas para inserir a senha correta em um período de 15 minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 30 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 30 minutos. Nesse momento, você poderá tentar fazer logon ou redefinir sua senha.

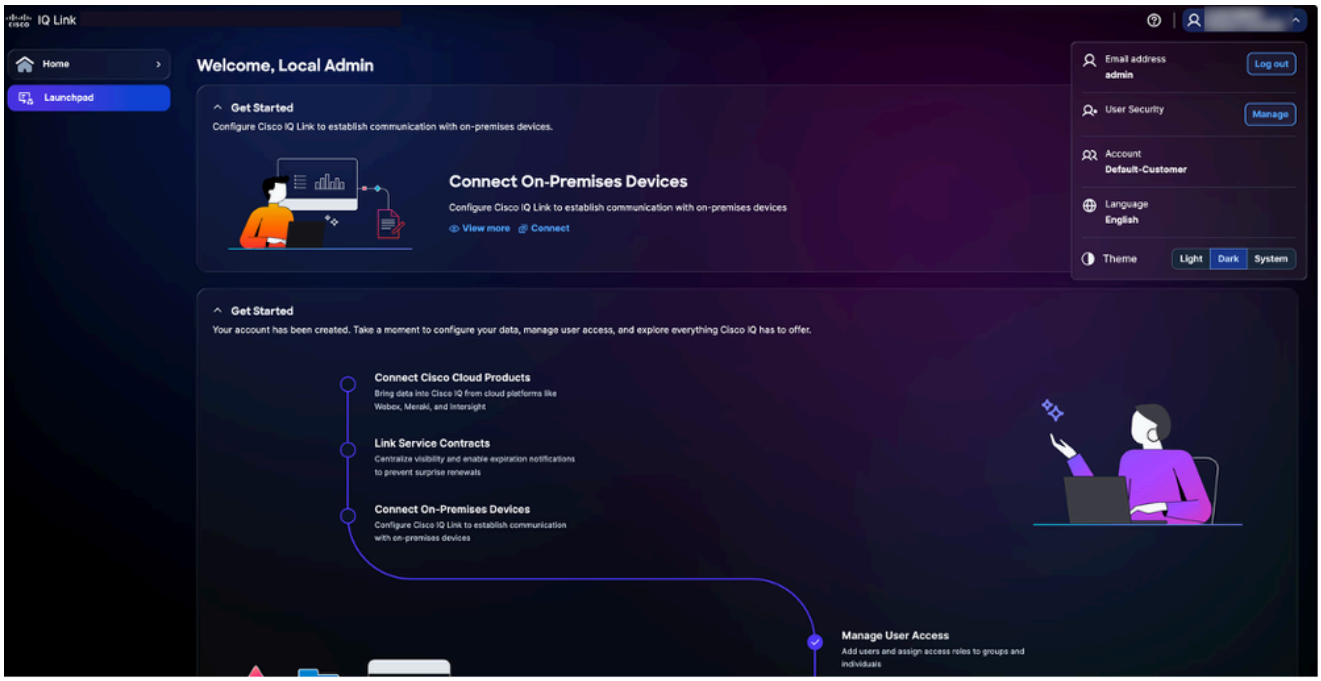
---

Configurando perguntas e respostas de segurança

Perguntas de segurança ajudam a verificar sua identidade se você esquecer sua senha. Os administradores de conta devem configurar 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. Na página inicial, clique no ícone Perfil de usuário. O menu suspenso é aberto.

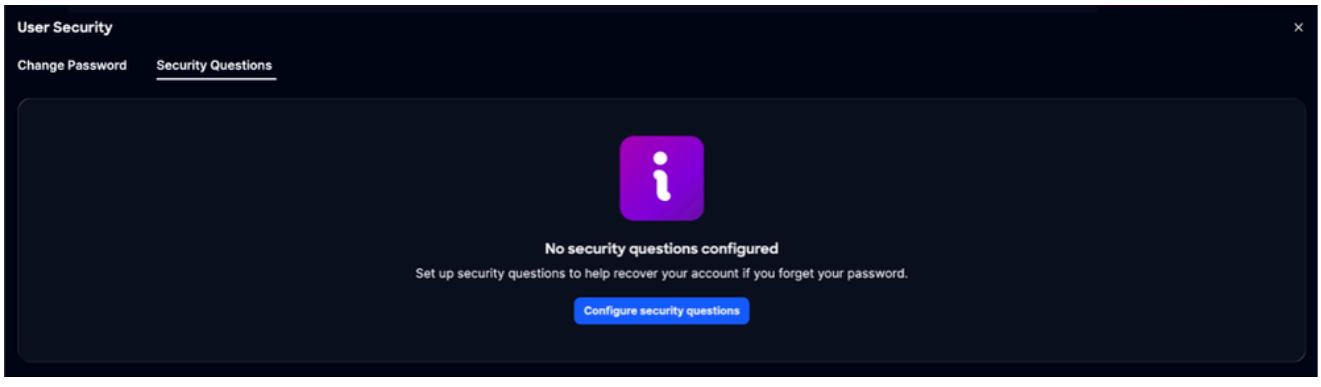



Menu de perfil do usuário

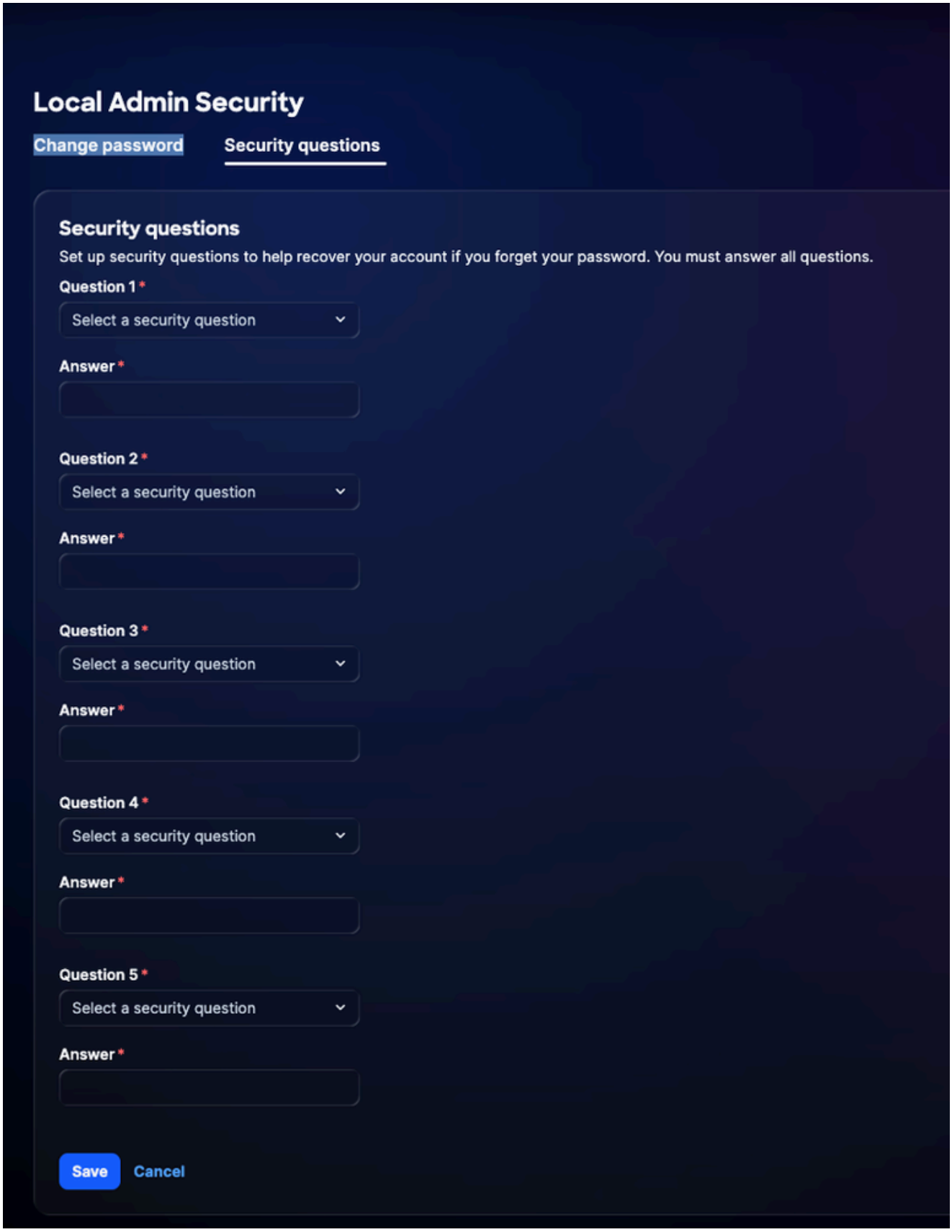
2. Clique em Gerenciar em Segurança do usuário. A página Segurança do usuário é exibida.


Alterar senha

3. Clique em Perguntas de segurança para abrir a guia.



4. Clique em Configure security questions.



5. Escolha qualquer uma das cinco (5) perguntas de segurança nas listas suspensas.
6. Digite sua resposta para cada pergunta.
7. Click Save.

---

Note: As respostas não diferenciam maiúsculas de minúsculas, por exemplo, "SMITH" e "smith" são considerados iguais.
Espaços extras são ignorados, por exemplo, " Smith" e "smith" são considerados iguais.

---

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

Os administradores de conta e os usuários locais podem gerenciar senhas para o Cisco IQ.

Para garantir a segurança de sua conta, as seguintes políticas de senha são aplicadas:

- Restrição de reutilização: sua nova senha não pode corresponder a nenhuma das cinco (5) senhas anteriores. Essa política se aplica aos fluxos Inscrever-se, Esqueci a senha e Alterar a senha.
- Variação de caracteres: ao alterar sua senha enquanto estiver autenticado, pelo menos oito (8) caracteres da senha atual devem ser diferentes da nova senha.
- Intervalo mínimo de alteração: Por padrão, você deve aguardar 24 horas antes de alterar sua senha novamente. Se um intervalo diferente for configurado, você não poderá atualizar sua senha até que esse tempo tenha decorrido.
- Expiração da senha: As senhas expiram a cada 60 dias. Após o primeiro login após a data de expiração, você será solicitado a definir uma nova senha antes de acessar o sistema. (Se configurado como 0, a expiração da senha é desabilitada.)

Pré-requisitos

Para gerenciar senhas, as seguintes condições devem ser atendidas:

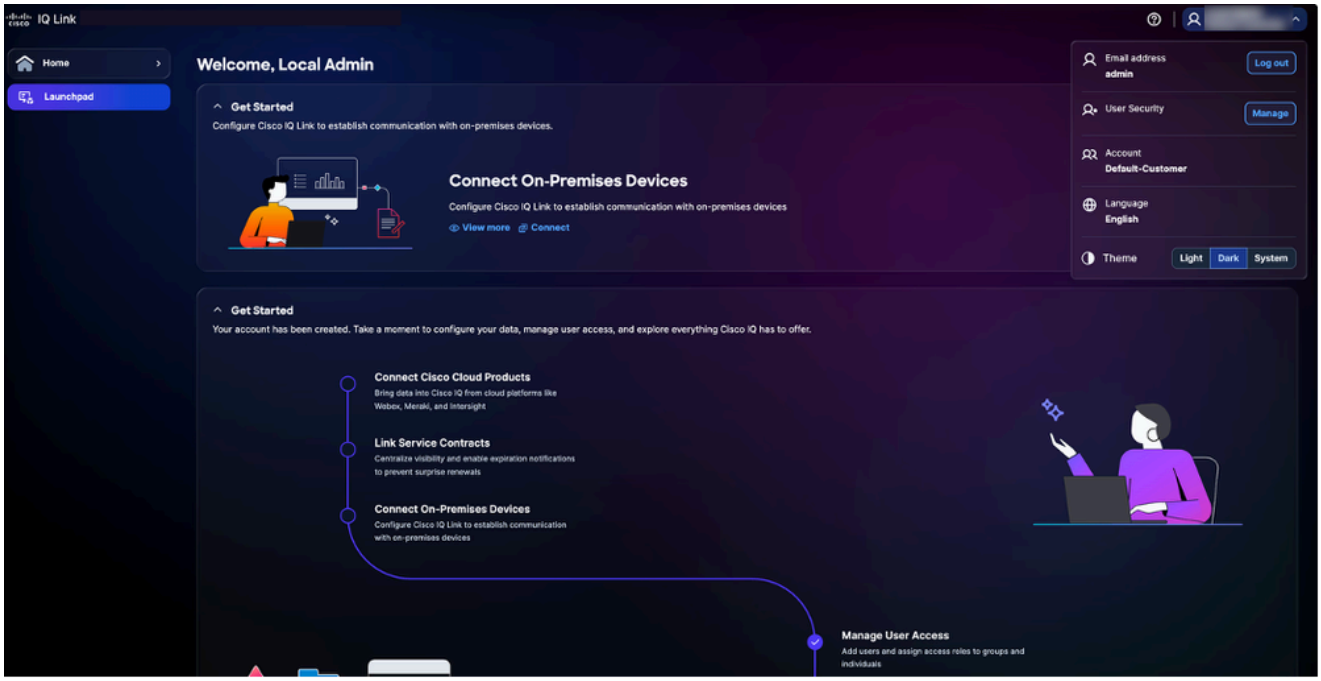
- Você é um administrador ou usuário de conta local

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

Alteração de Senhas

Para alterar uma senha:

1. Na página inicial, clique no ícone Perfil de usuário. O menu suspenso é aberto.




Menu de perfil do usuário

2. Clique em Gerenciar em Segurança do usuário. A página Segurança do usuário é exibida.

Alterar senha

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

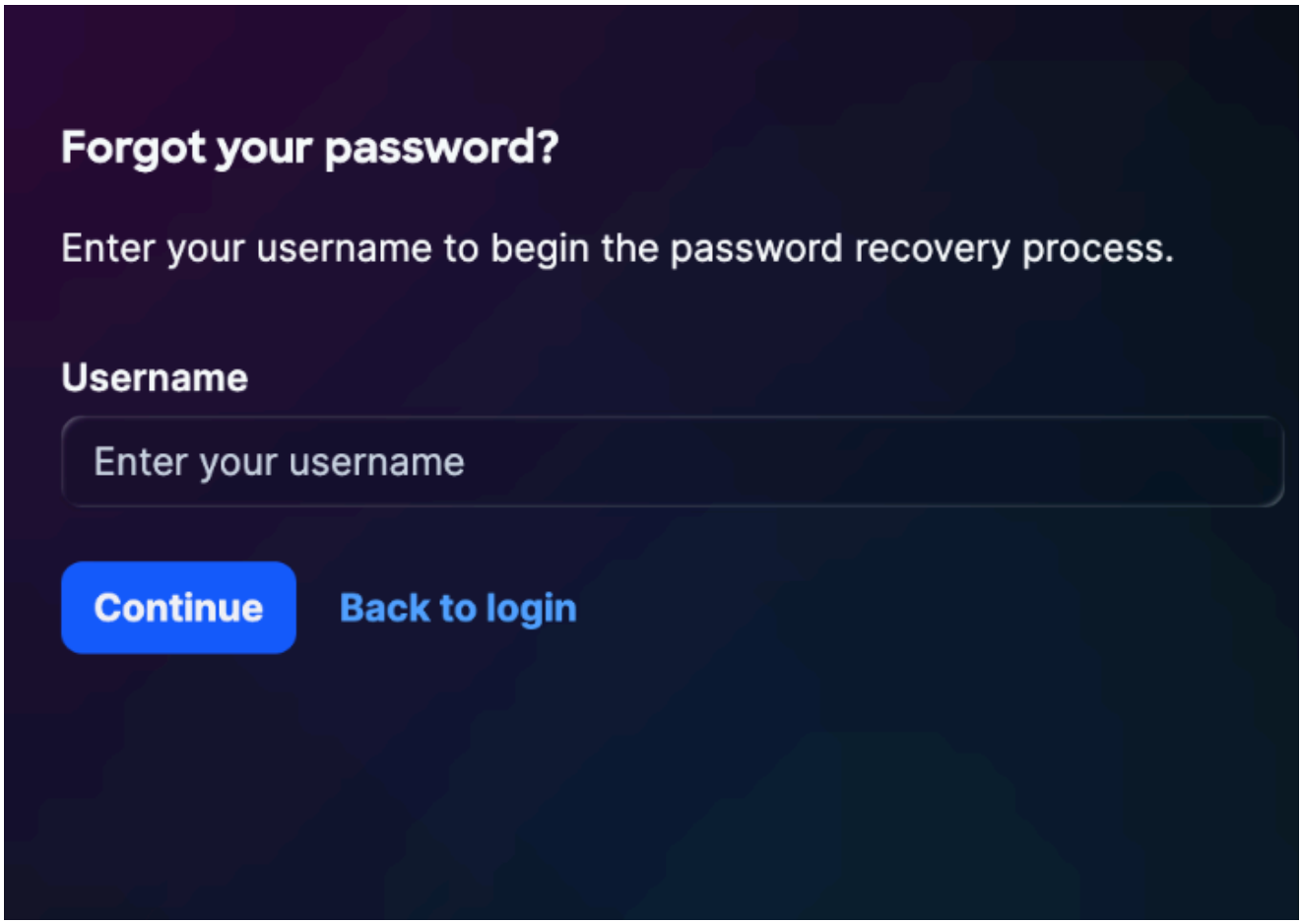
A senha é atualizada no sistema Cisco IQ, incluindo a máquina virtual (VM) Cisco IQ.

### 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.

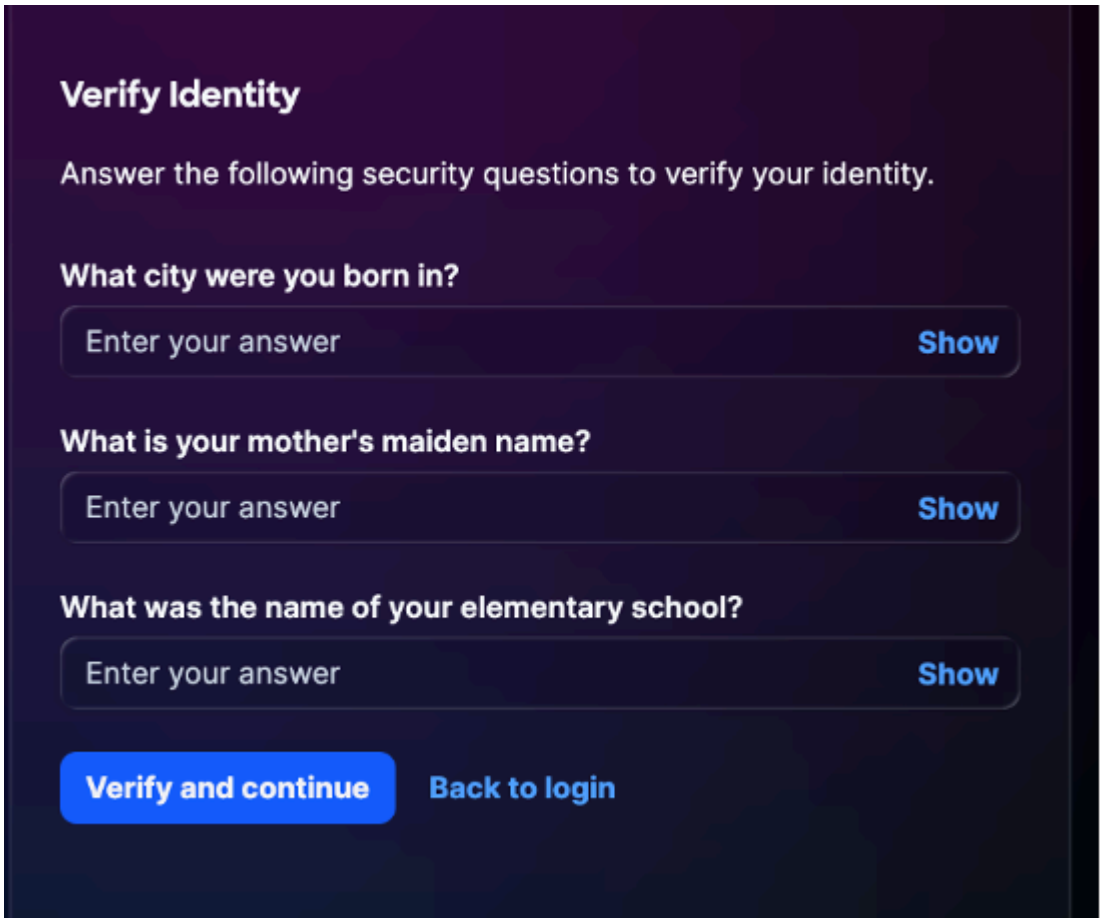
Para redefinir uma senha esquecida:

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

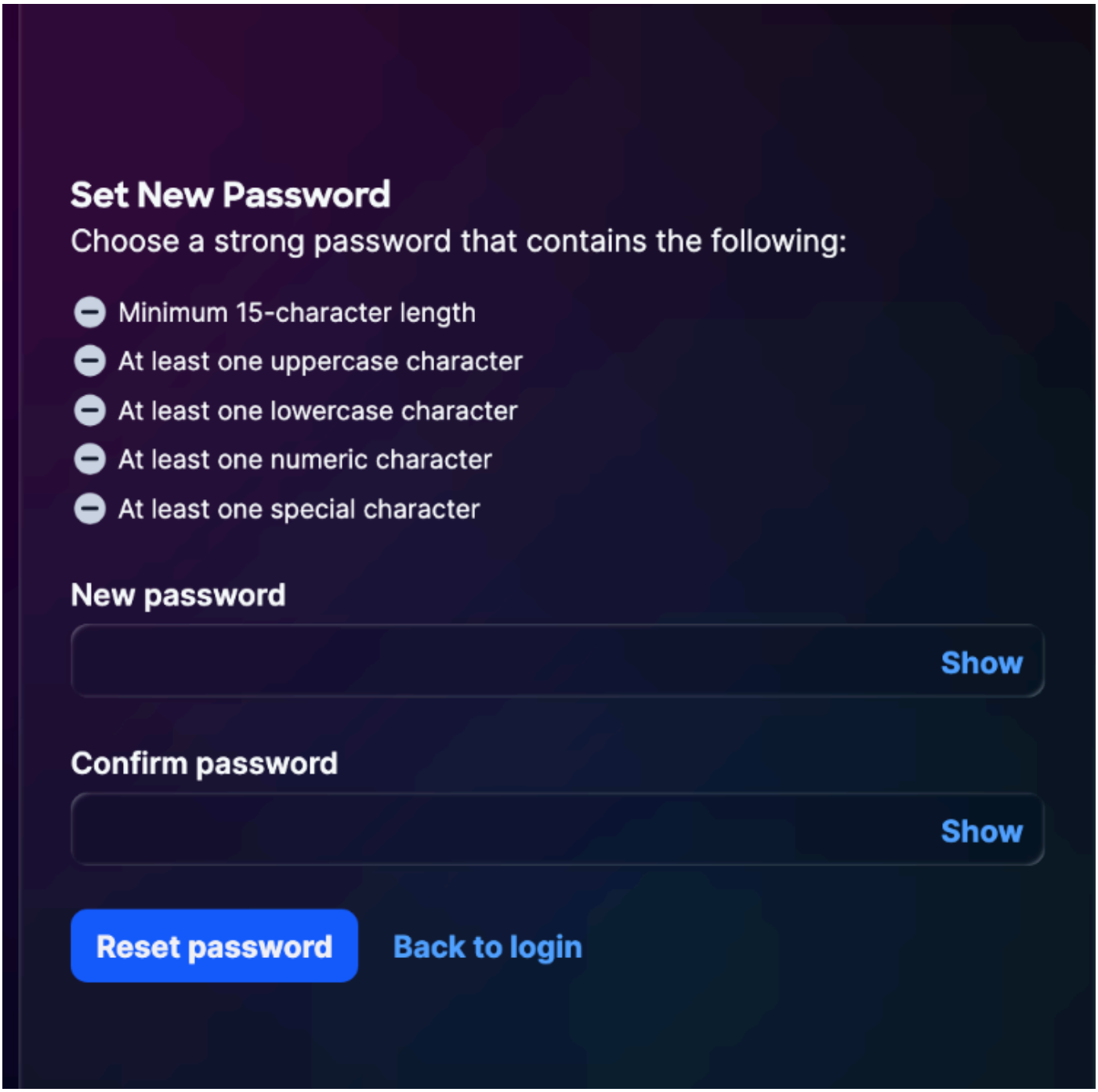
---

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

---

5. Informe as respostas para 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

Você tem três (3) tentativas para responder corretamente às perguntas de segurança em um período de 15 minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 30 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 desbloqueada automaticamente após 30 minutos. Nesse momento, você poderá tentar fazer logon ou redefinir sua senha.

7. Informe a Nova senha.

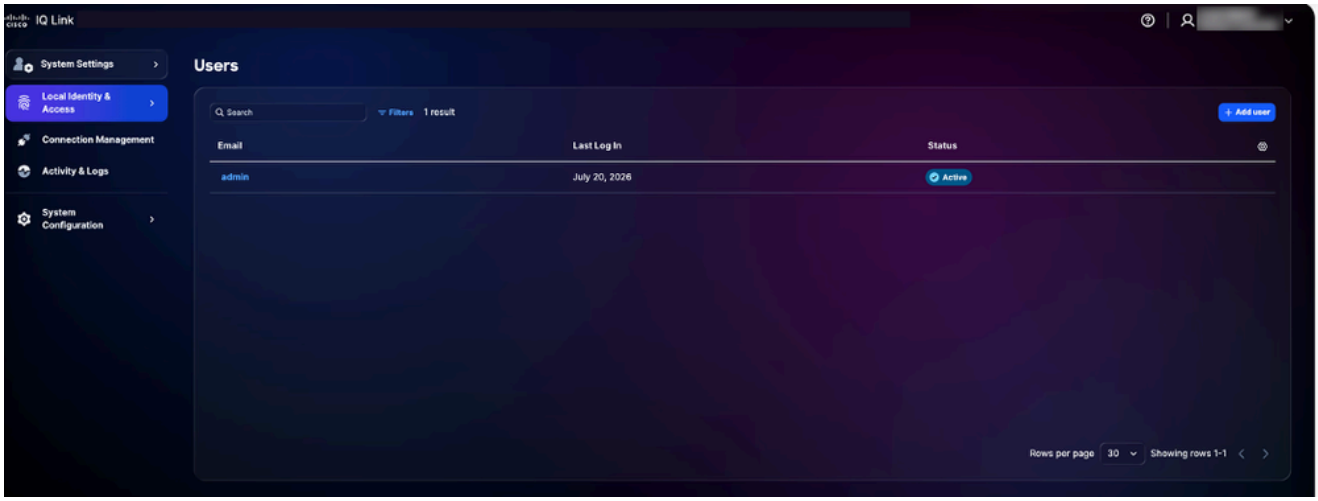
8. Informe a senha novamente para confirmá-la.

9. Clique em Submeter.

## Adicionando usuários locais

Os administradores de conta podem adicionar usuários à conta do Cisco IQ. Para adicionar um novo usuário:

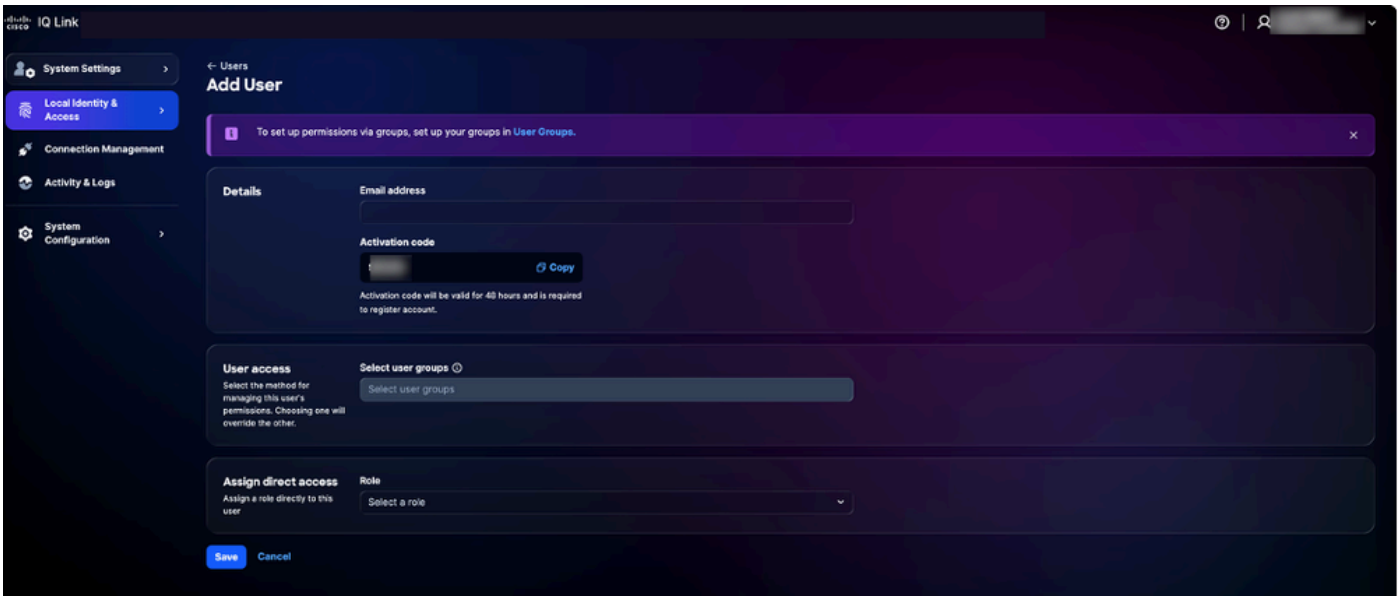
1. Navegue até Configurações do sistema > Identidade local e acesso > Usuários. A página Usuários é exibida. Ela lista todos os usuários locais existentes, juntamente com seus status.




Página Usuários

Note: O ícone Mais Opções não é exibido para Administradores de Contas (como mostrado na imagem acima).

2. Clique em Adicionar usuários. A página Adicionar usuário é exibida.




Adicionar usuário

3. Informe o endereço de e-mail.

4. Informe o Código de Ativação.

---

Note: O código de ativação é exibido por padrão. Compartilhe-o com o usuário, pois ele é necessário para concluir o registro.

---

5. No Acesso de usuário, escolha o grupo de usuários na lista suspensa Selecionar grupos de usuários.

---

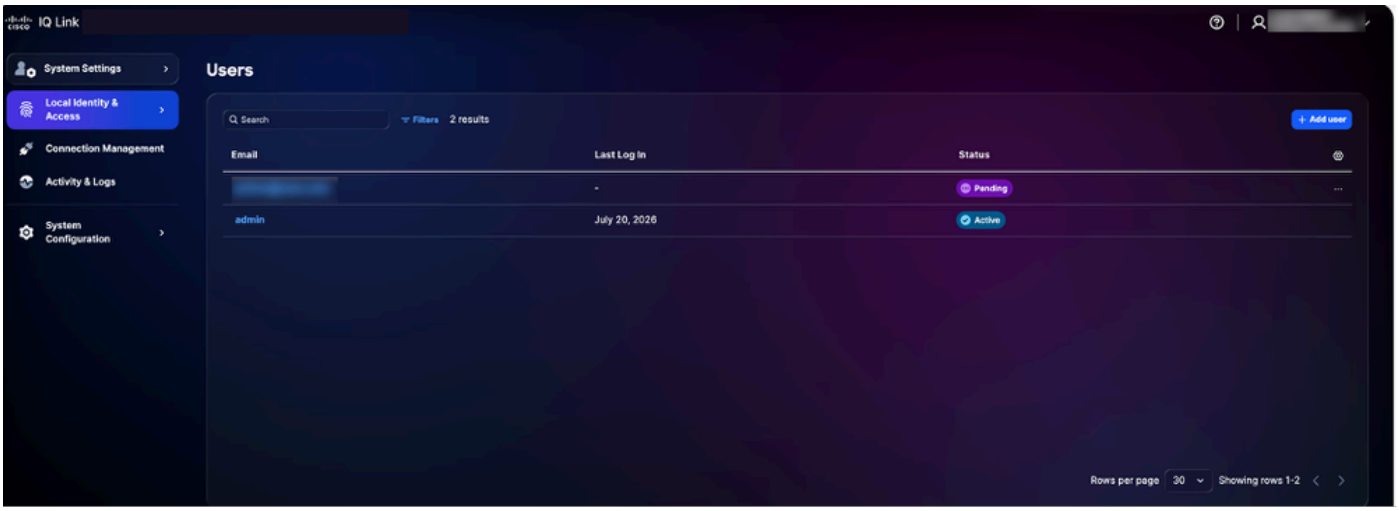
Note: Os usuários herdam o acesso do grupo selecionado.

---

6. Em Atribuir acesso direto, escolha a função na lista drop-down Função. Há duas (2) funções disponíveis:

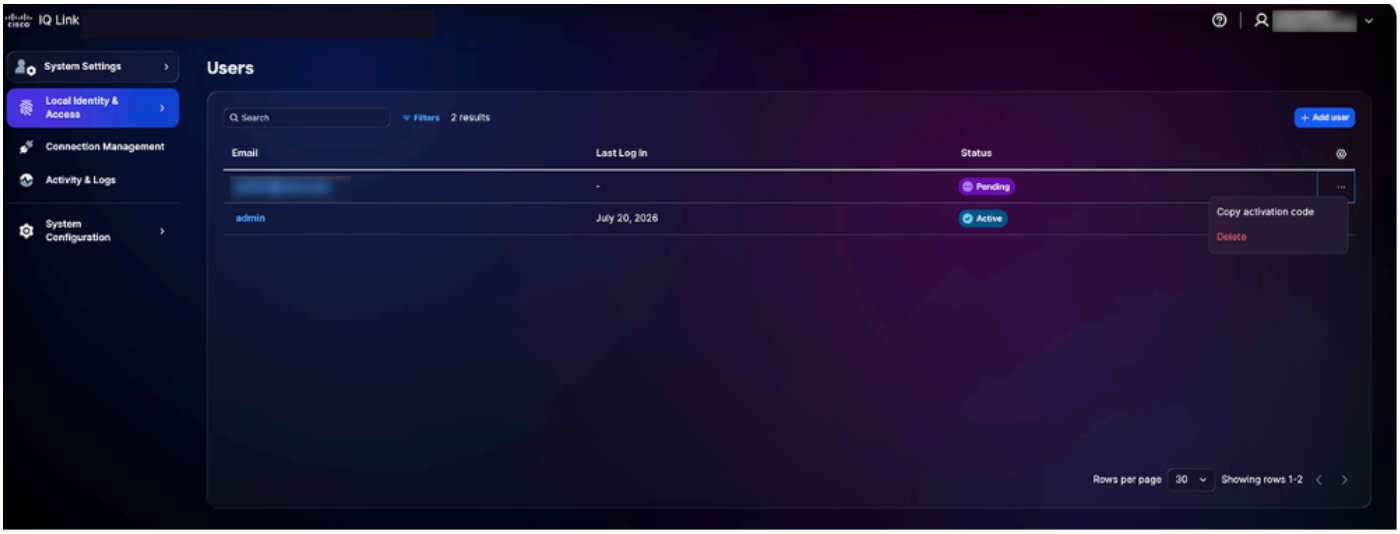
- Visualizador: Exibir e acessar aplicativos
- Administrador: Acessar aplicativos e gerenciar configurações do sistema, exceto Gerenciamento do sistema e IDP

7. Clique em Salvar. O novo usuário é criado e exibido na lista de usuários no estado Pendente. Pendente indica que o usuário ainda não concluiu a autoativação.




Usuário recém-adicionado

8. Localize o usuário recém-criado na lista e confirme se a coluna Status exibe Pendente.




Copiar Código de Ativação

9. Clique no ícone Mais Opções > Copiar código de ativação ao lado do usuário recém-criado. O código de ativação é copiado para a área de transferência.

10. Compartilhe esse código com o usuário de forma segura (por exemplo, através de um canal interno seguro). O código de ativação é para uso único e é necessário para concluir o registro.

Note: Não compartilhe o código de ativação em canais não seguros. Se o código for perdido ou comprometido, use o ícone Menu para gerar novamente um novo código de ativação, que invalida o anterior

Observação: os códigos de ativação são válidos por 48 horas. Se o código expirar, entre em

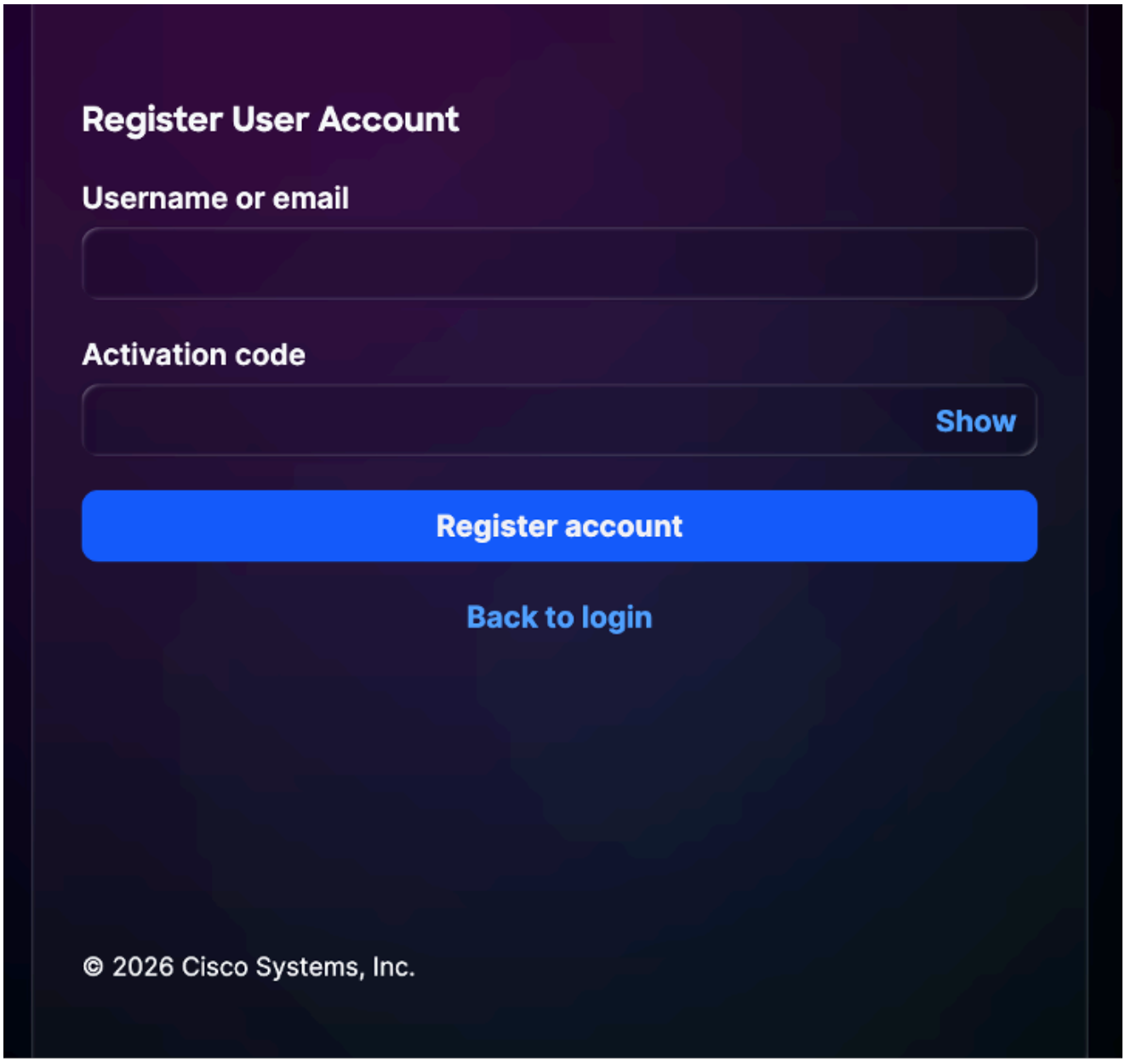
✎ contato com o administrador da conta para solicitar um novo código.

11. Para fazer logoff, clique no ícone Usuário no canto superior direito e selecione Logoff. Você retornará à página de login do Cisco IQ.

Registrando uma nova conta de usuário

Para registrar a nova conta de usuário:

1. Na página de login, clique no link Registrar uma nova conta de usuário.

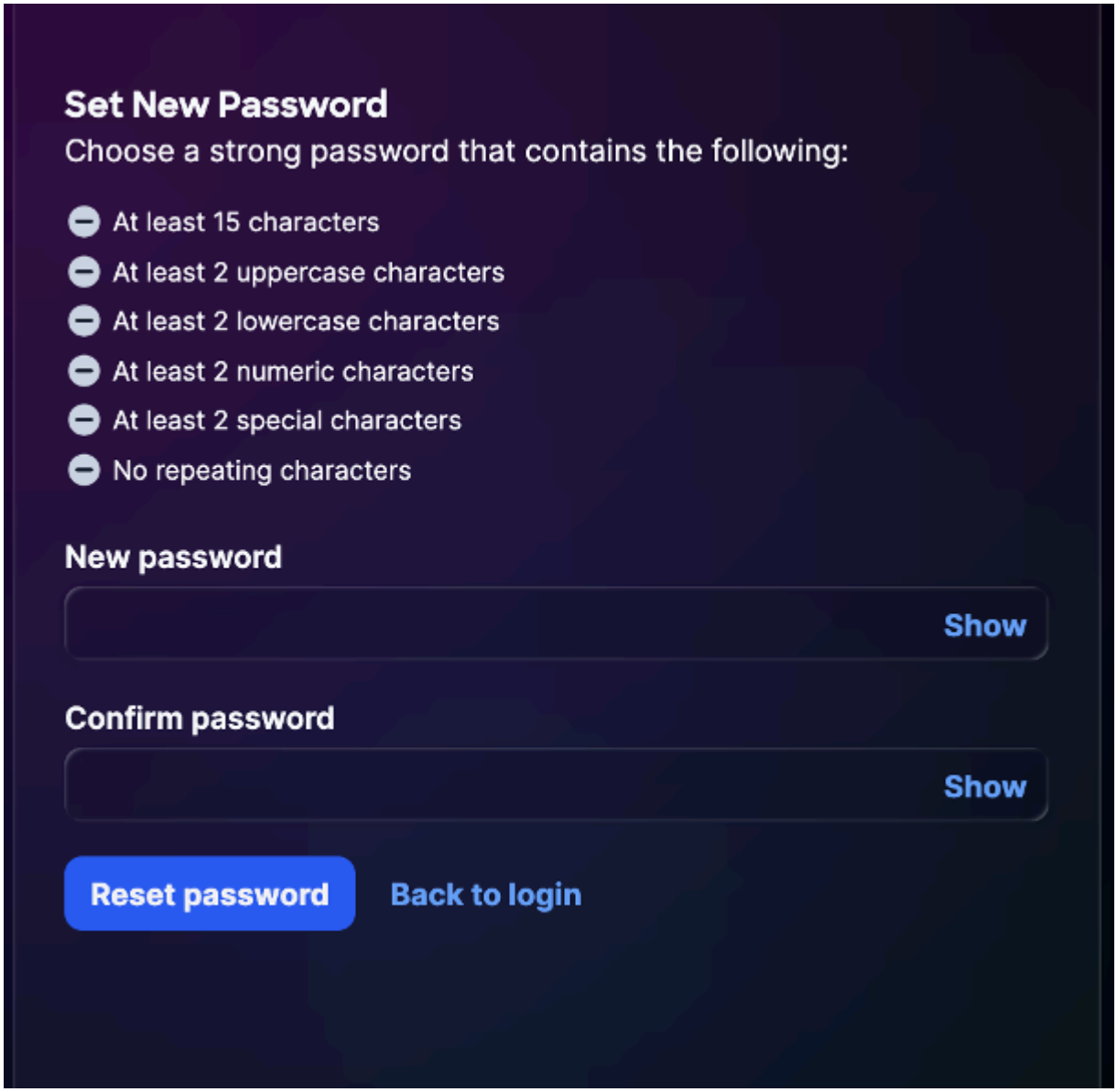



Nova conta de usuário

2. Insira o nome de usuário ou o endereço de e-mail usado quando o usuário foi criado (por

exemplo, user1@abc.com).

3. Insira o código de ativação compartilhado pelo administrador da conta.
4. Clique em Registrar conta. A janela Set New Password é exibida.




Senha da nova conta de usuário

5. Insira uma Nova senha.
6. Digite a senha novamente em Confirmar senha.
7. No primeiro login bem-sucedido, o usuário é solicitado a configurar cinco (5) perguntas de segurança (consulte Configurando perguntas e respostas de segurança para obter mais informações).

## Gerenciamento de grupos de usuários locais

Grupos de usuários permitem que os administradores de conta gerenciem funções para vários usuários locais juntos. Em vez de atribuir uma função a cada usuário individualmente, um administrador de conta pode criar um grupo, anexar uma função e um conjunto de usuários a ele e atualizar a função ou associação em um local. O gerenciamento de todos os grupos de usuários é executado a partir da página Identidade local e acesso.

---

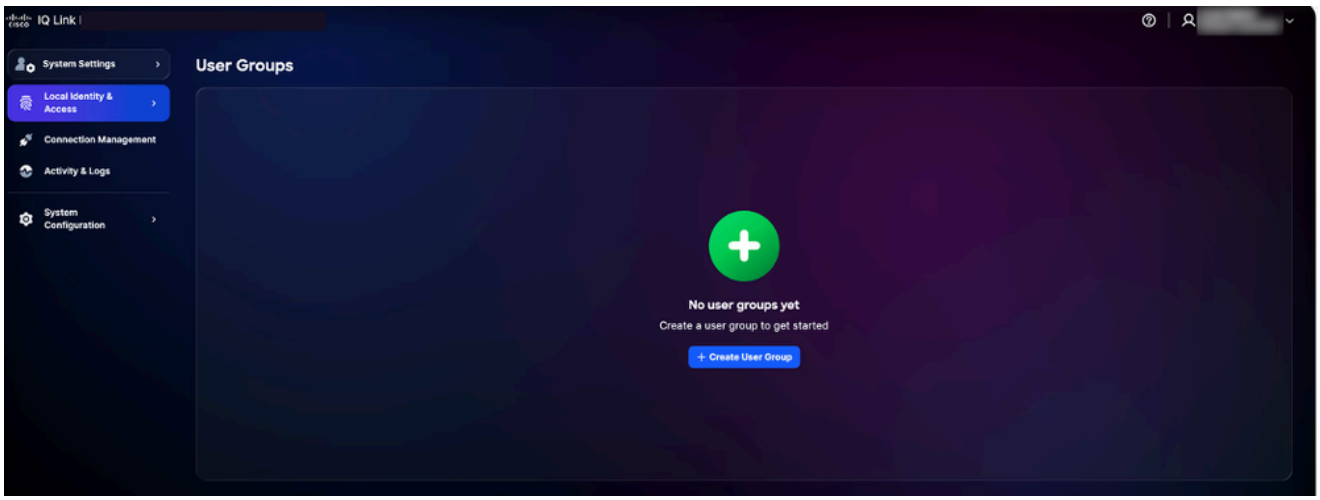
Note: Somente um administrador de conta pode criar, editar ou excluir grupos de usuários. Os grupos são compostos por usuários locais existentes; os usuários devem ser criados antes de serem adicionados a um grupo.

---

Criando um grupo de usuários

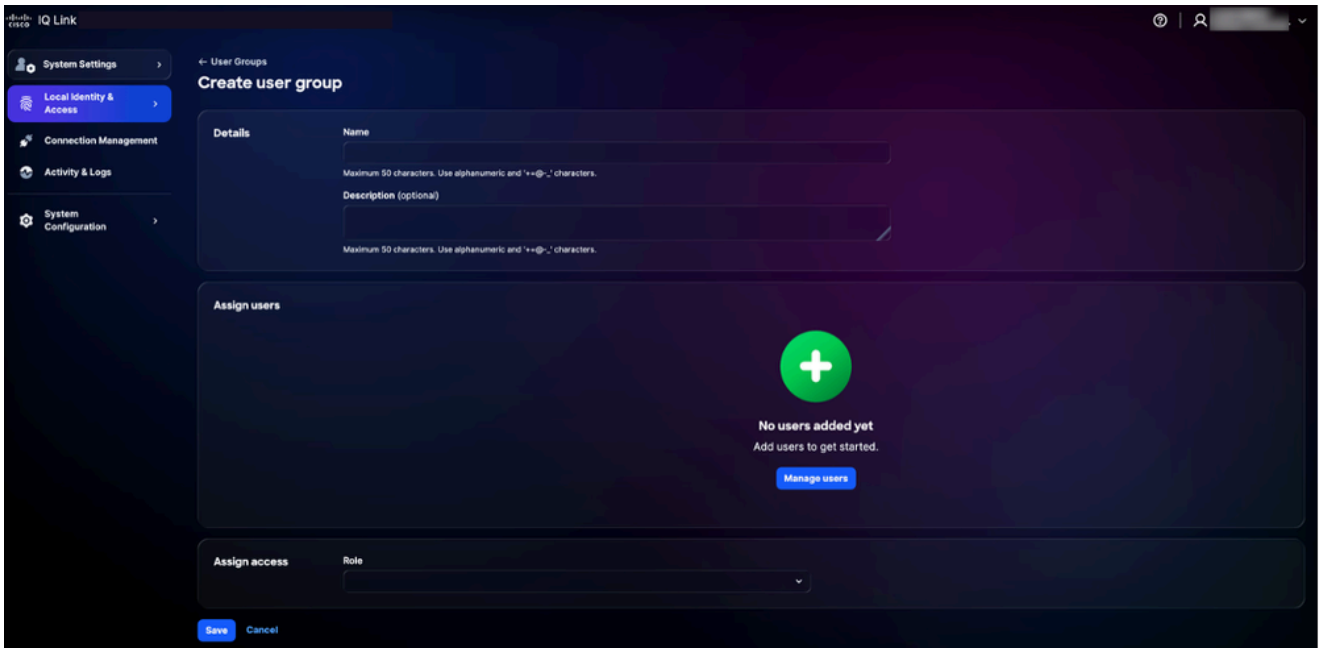
Para criar um grupo de usuários:

1. Em Configurações do sistema, escolha Identidade e acesso local > Grupos de usuários. A página Grupos de usuários é exibida.




Grupos de usuários

2. Clique em Criar grupo de usuários. A página Criar grupo de usuários é exibida.




Criar grupo de usuários

3. Preencha as seguintes seções:

- Detalhes
  - Nome: Informe um nome exclusivo para o grupo (por exemplo, Operadores Somente Leitura)
  - Descrição (opcional): Breve descrição do grupo (máximo 50 caracteres; alfanumérico e + = @ - _ caracteres são permitidos)

- Atribuir usuários

  Procure e selecione um ou mais usuários locais existentes para adicionar ao grupo.

  > Note: Para adicionar usuários que ainda não estão listados, clique em Gerenciar usuários.

- Atribuir acesso

  - Função: Selecione a função do sistema a ser atribuída a todos os membros deste grupo. As seguintes funções estão disponíveis:

    - Visualizador: Exibir e acessar aplicativos (somente leitura)
    - Administrador: Acessar aplicativos e gerenciar configurações do sistema

4. Clique em Salvar.

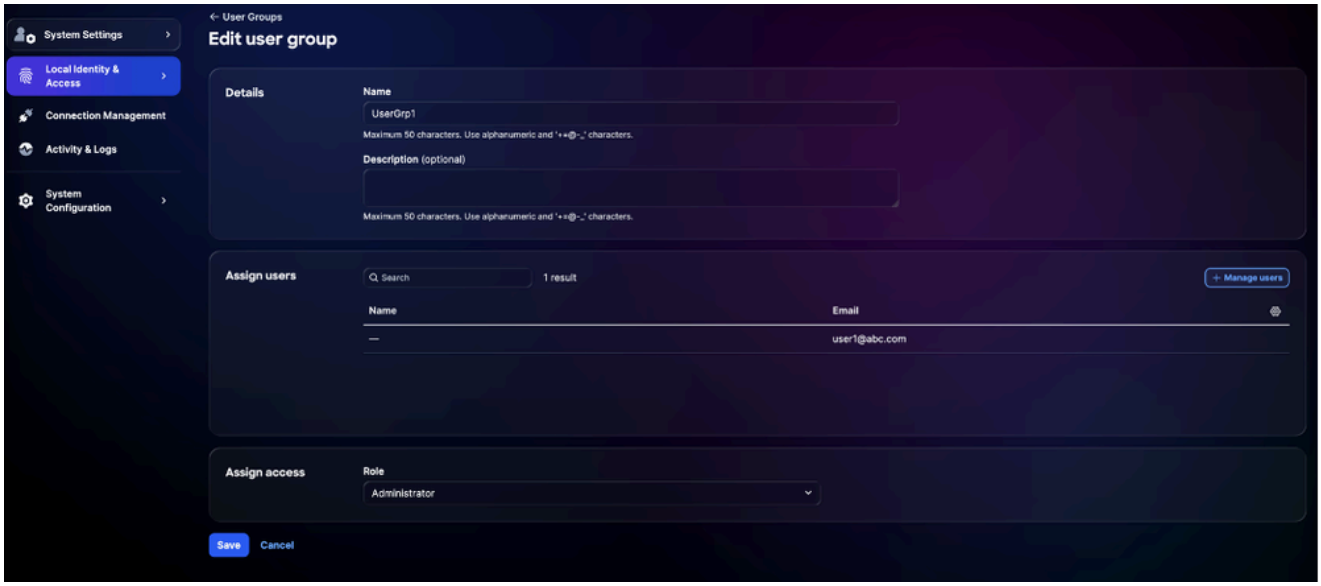
O novo grupo de usuários é exibido na lista Grupos de usuários junto com sua função atribuída e

contagem de membros.

Edição de um grupo de usuários

Para editar um grupo de usuários:

1. Na lista Grupos de usuários, localize o grupo que deseja modificar.
2. Clique no ícone Mais ao lado do grupo e escolha Editar. A página Editar grupo de usuários é exibida.




Editar grupo de usuários

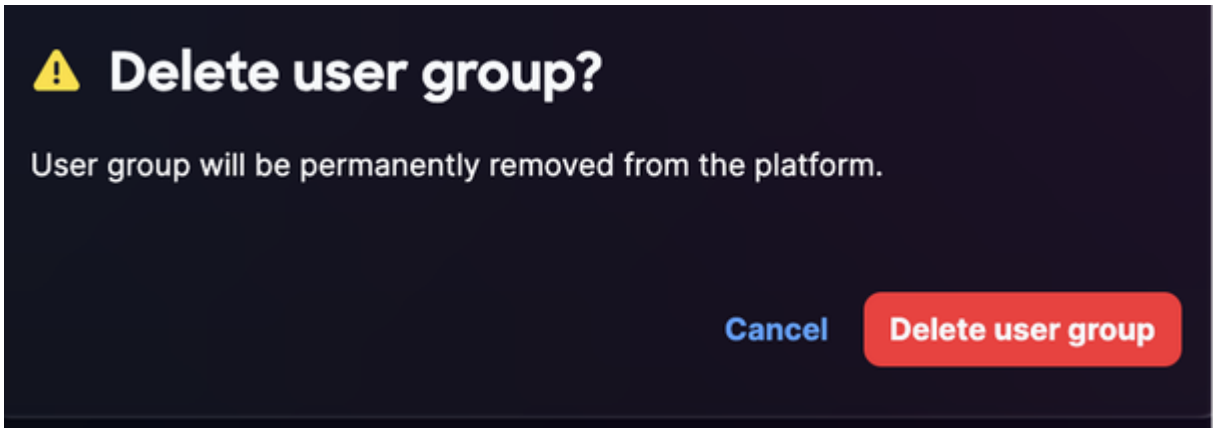
3. Faça as alterações desejadas.
4. Click Save.

O grupo atualizado é exibido na lista Grupos de usuários. A nova função entra em vigor para todos os membros do grupo.

## Exclusão de um grupo de usuários

Para excluir um grupo de usuários:

1. Na lista Grupos de usuários, localize o grupo que deseja excluir.
2. Clique no ícone Mais Opções ao lado do grupo e selecione Excluir.




Excluir grupo de usuários

3. Confirme a exclusão quando solicitado.

O grupo é removido da lista Grupos de usuários.

---

Note: A exclusão de um grupo de usuários remove a atribuição de função baseada em grupo de todos os membros. As contas de usuário individuais não são excluídas.

---

# Configurando o provedor de identidade

Depois de efetuar login no Cisco IQ Link, os administradores de conta podem definir várias configurações. Os administradores de conta 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 do administrador da conta 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.
Tabela 1: 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 |
| Público-alvo | Não-força de trabalho |
| Categoria de integração | Selecione "Nova integração" |

Tabela 2: Parâmetros de configuração SAML

| Parâmetro | Configuração | Exemplo |
|---|---|---|
| Audiência (ID da Entidade) | Nome de domínio totalmente qualificado (FQDN) | mymanagementhost.mydomain.com |
| URL de Logon Único | Ponto de extremidade do SAML Assertion Consumer Service (ACS) | 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 Logoff Único (SLO) no aplicativo.

Tabela 3: 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 |

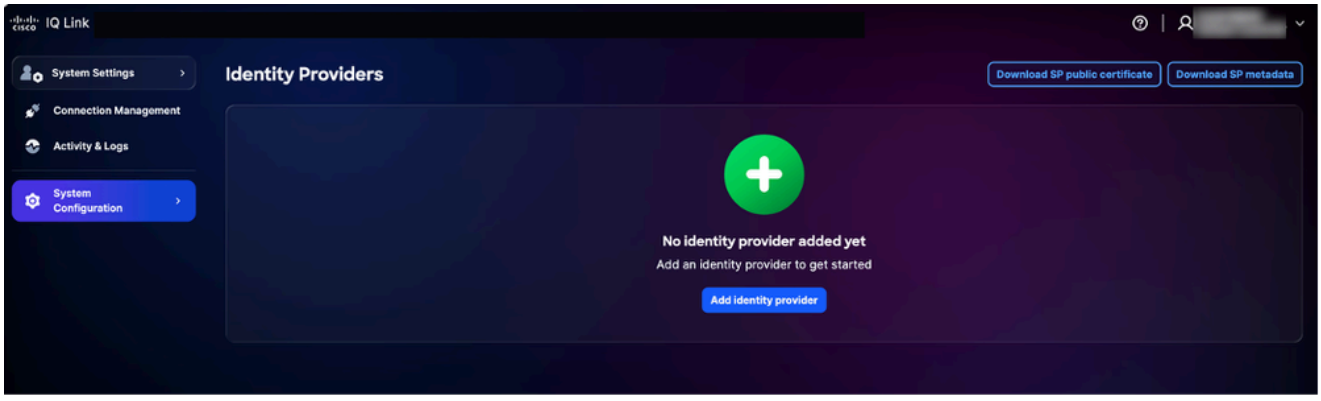
5. Clique no ícone Download para fazer o download do arquivo "Metadados SP".

6. Provisione ou crie o aplicativo conforme exigido pelo provedor.

Adicionando o Okta IDP

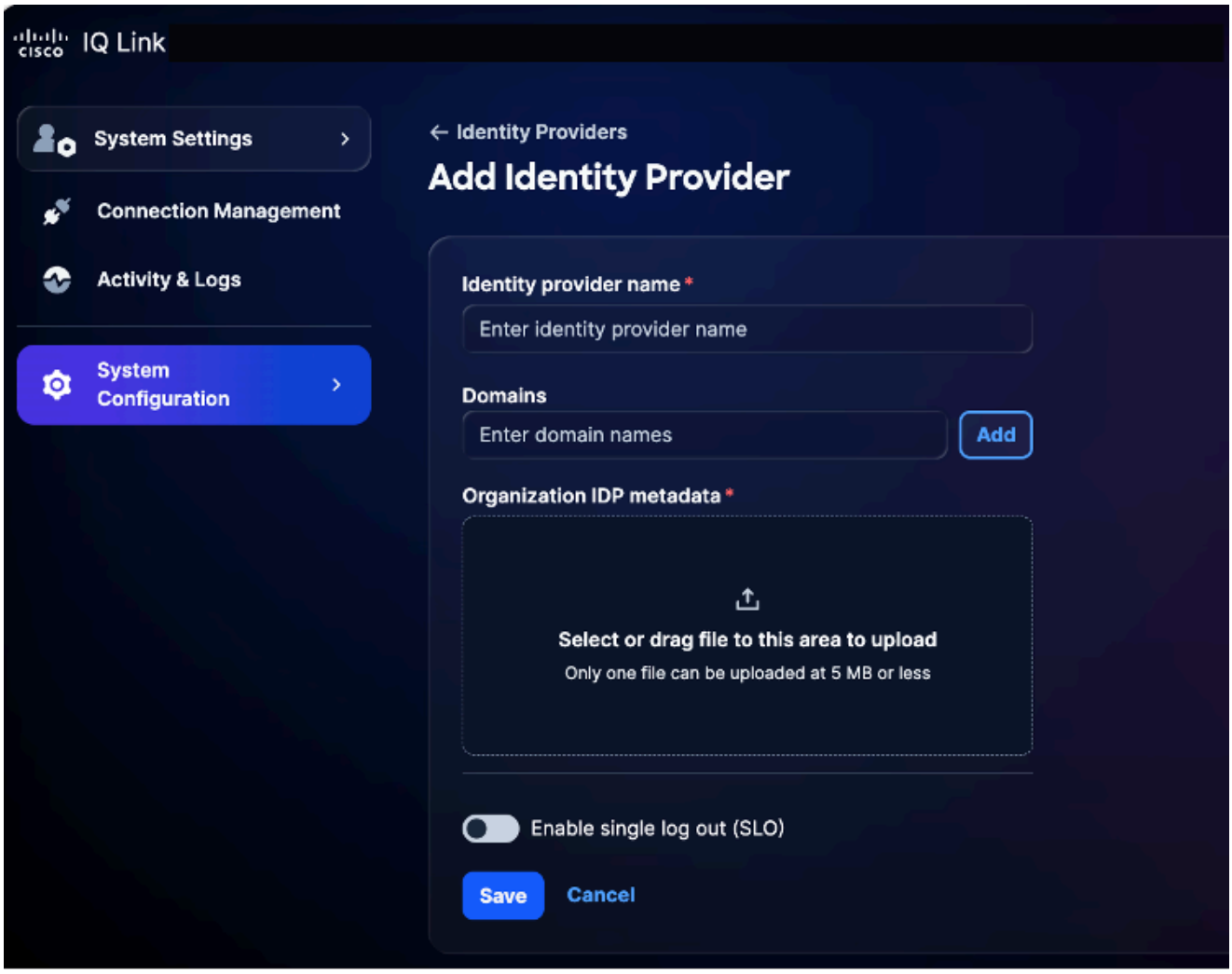
Para adicionar um IDP no Cisco IQ Link:

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. Informe o Nome do provedor de identidade.

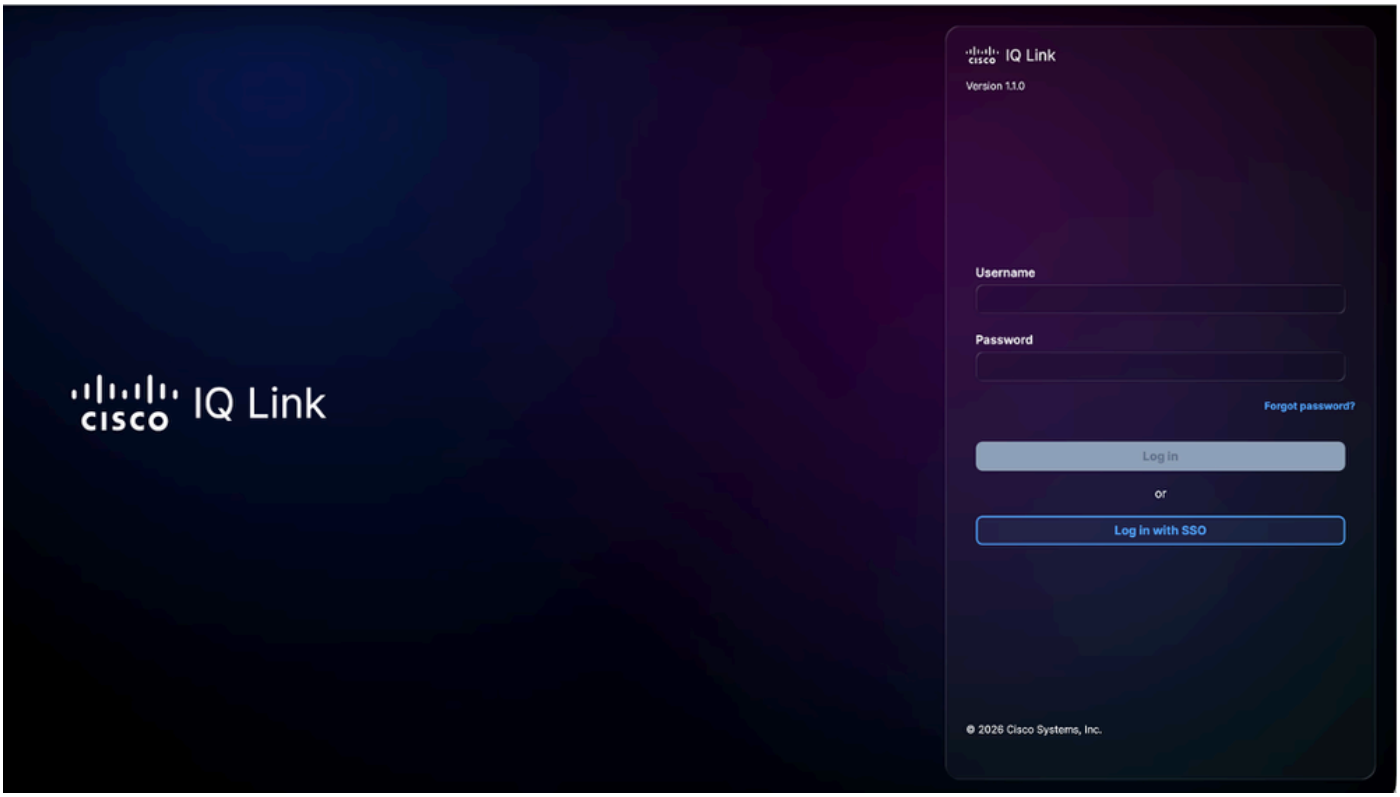
4. Clique em Adicionar para adicionar um nome de domínio configurado do Cisco IQ Link ao campo Domínios.

5. Arraste e solte ou carregue o arquivo de metadados SAML obtido do aplicativo IDP no campo Metadados de 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 logout único. Você também pode ativar o SLO posteriormente.

7. Clique em Salvar.

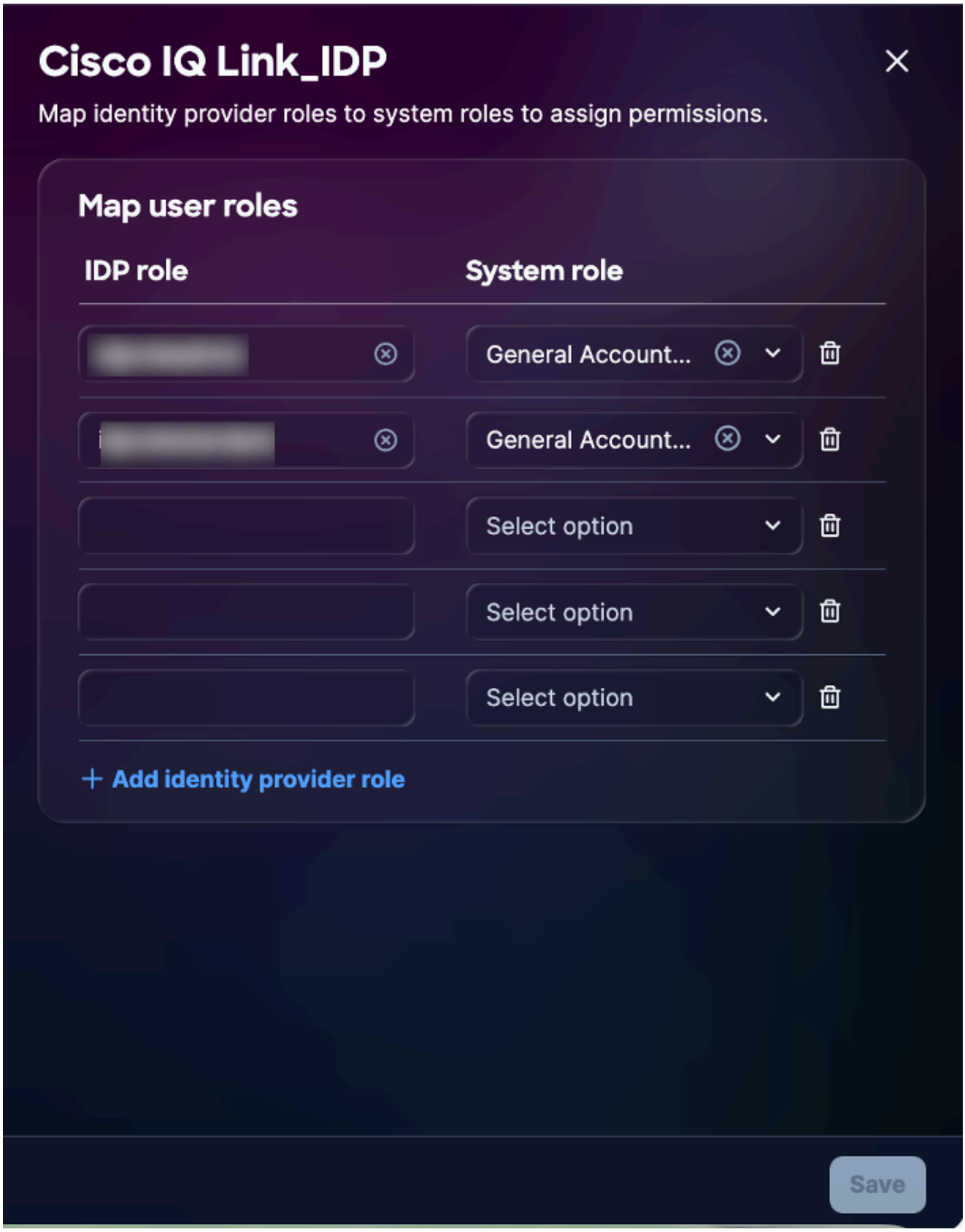
Uma vez configurada, a página de login exibe uma opção para efetuar login com o SSO (via IDP).




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:

- Administrador geral da conta: O Administrador da Conta Geral tem permissões totais para

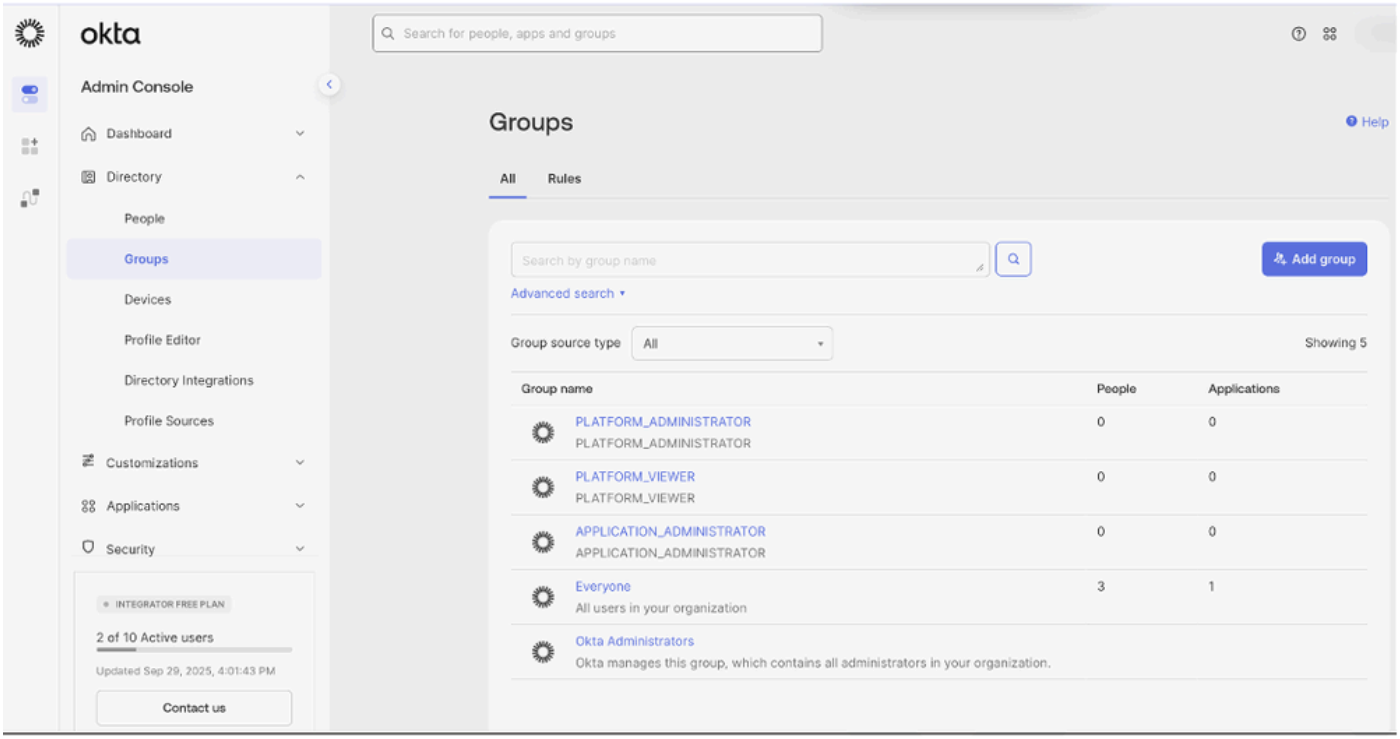
executar todas as ações no produto

- Visualizador de Contas Gerais: O Visualizador de Contas Gerais 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. Clique em Salvar.

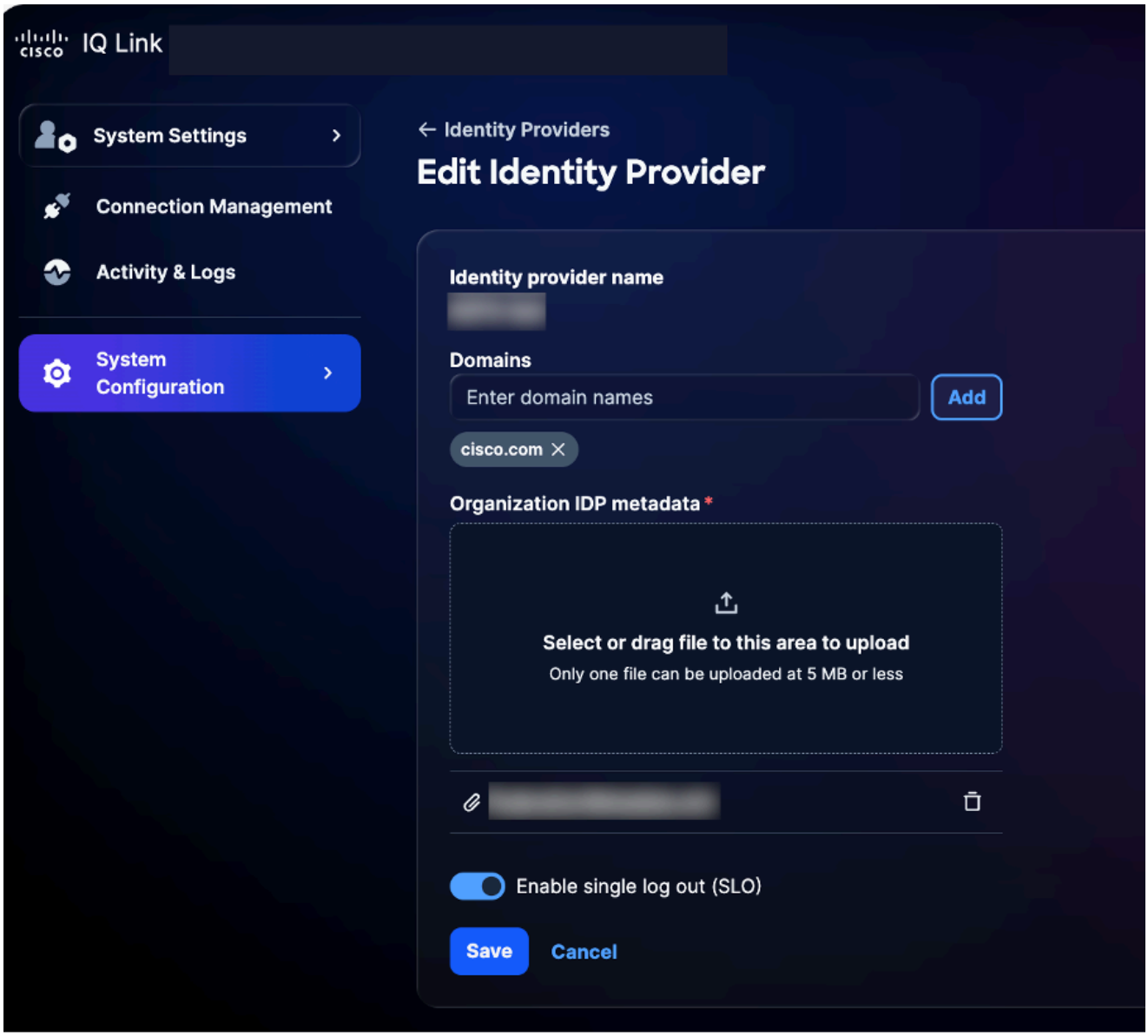
Configuração de logoff único

Se você optar por habilitar a Configuração de Logoff Único (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 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 da conta 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:

Tabela 4: 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 (AD) 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 do AD configurada
- Certificados SSL/TLS no AD FS
- Acesso do administrador da conta 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)

Tabela 5: 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 | DN (Domain Names, nomes de domínio) do grupo AD | 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 para obter detalhes do arquivo que é salvo como parte da etapa 3.
10. Clique em Procurar para selecionar o arquivo de metadados SP 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.

---

Note: Não selecione "Permitir Todos com MFA", a menos que o servidor ADFS tenha um adaptador de Autenticação Multifator (MFA) registrado (por exemplo, Azure MFA ou *Senha Ocasional Baseada em Tempo (TOTP) configurado).
Se esta política for habilitada sem um provedor MFA configurado, o ADFS autenticará o usuário, mas negará a solicitação com o status urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Como a resposta SAML não contém nenhuma asserção, o plug-in falha e relata um erro de "e-mail ausente".

---

Problema: A opção "Permitir todos com MFA" está selecionada.

Solução: No PowerShell, verifique a política atual executando o seguinte comando.

```
Get-AdfsRelyingPartyTrust -Name “

    ”).AccessControlPolicyName
```

Para definir "Permitir todos" (sem requisito de MFA), execute o seguinte comando:

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

Você também pode criar o objeto de confiança de terceira parte confiável por meio do PowerShell:

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

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

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

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.

Tabela 6: 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 |
| UPN | Infraestrutura de Chave Pública (PKI)/autenticação de certificado | O ADFS mapeia o certificado de cliente para um usuário do AD via Nome UPN |
| 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.Iss

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

3. Aplique as regras de reivindicação executando o seguinte comando:

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

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

---

 aviso: Cada conta de usuário do AD deve ter o atributo de email preenchido. Se este atributo estiver ausente, a asserção SAML não conterá uma declaração de email, resultando em uma rejeição de autenticação.

---

Para atualizar o endereço de email de um usuário, execute o seguinte comando do PowerShell:

```
Set-ADUser -Identity “

     ” -EmailAddress “

      ”
```

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. Exiba os grupos aos quais o usuário pertence.

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

Saída de exemplo:

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

Configurando o ADFS para confiar no certificado de assinatura 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 CA (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

- Se o certificado da controladora de armazenamento for emitido por uma CA (não autoassinada), importe o certificado da CA emissora para o armazenamento de certificados raiz:

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

3. Aplique as alterações reiniciando o serviço ADFS.

```
Restart-Service adfssrv
```

Configurando a autenticação de PKI/certificado

Esta seção descreve como adicionar autenticação baseada em certificado (ou seja, cartão inteligente ou certificado de software) ao lado de senhas. Esta seção poderá ser ignorada se a autenticação somente por senha for suficiente.

Instalando a Função de AC do AD CS

Para instalar a função de CA do CS (Serviços de Certificados) do AD:

1. Verifique se já existe uma autoridade de certificação empresarial no seu domínio executando o seguinte comando:

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

Se o comando retornar uma resposta válida, você poderá ignorar o restante desta seção. Seu ambiente já está configurado. Se o comando indicar que nenhuma CA foi encontrada, vá para a etapa 2.

2. Instale a função de CA executando o seguinte comando:

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

3. Configure a função de CA executando o seguinte comando:

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

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

4. Instalação executando o seguinte comando:

```
certutil -ca
```

5. Confirme se o serviço está ativo e acessível executando o seguinte comando:

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

Configurando um modelo de certificado

Para configurar um modelo de certificado com EKU (Uso Avançado de Chave) de Autenticação de Cliente:

1. Abra certsrv.msc e expanda o nó CA.
2. Clique com o botão direito do mouse em Modelos de certificado > Gerenciar.
3. Duplicar o modelo do usuário.

---

Note: O modelo de Usuário interno será funcional ou válido somente se o certificado emitido a partir dele incluir o EKU de Autenticação de Cliente.

---

4. Defina as configurações nas seguintes guias:

- General: Digite "CIQ User Authentication" no campo Name com um período de validade de um (1) ano
- Tratamento de Solicitações: Selecione Signature and encryption na lista suspensa Purpose e marque a caixa de seleção Allow private key to be export

- Nome do assunto: Selecione Build from Ative Diretory Information e inclua um email nos campos Subject e SAN

---

aviso: Os campos Assunto e SAN devem conter um UPN do usuário ou um email que corresponda a uma conta do AD. O ADFS mapeia o certificado para um usuário do AD usando esses campos.

---

- Extensões: Certifique-se de que as políticas de aplicativos incluam "autenticação de cliente (1.3.6.1.5.5.7.3.2)"
- Segurança: Adicione usuários de domínio e conceda a eles permissões de Leitura e Registro

5. Publique o modelo usando o seguinte comando:

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

Registrando um certificado do usuário

1. Efetue login como o usuário de destino.
2. Registre o certificado executando o seguinte comando:

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

3. Verifique a instalação do certificado executando o seguinte comando:

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

Exportação de um certificado de usuário do Windows e instalação no cliente (Mac)

Para exportar um certificado do usuário do Windows para o Mac:

1. Exporte o certificado do Windows como um arquivo PFX executando os seguintes

comandos:

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

     *” }
$password = ConvertTo-SecureString -String “

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

2. Transfira o arquivo user-cert.pfx para o seu dispositivo Mac.

3. Importe o certificado para o Mac Keychain executando o seguinte comando:

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

     ”
```

Note: Depois de importar o certificado, o navegador deve ser fechado e reaberto para que seja reconhecido.

4. Confie no CA no Mac executando:

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

Habilitando Pontos de Extremidade de Autenticação de Certificado ADFS

Para habilitar pontos de extremidade de autenticação de certificado ADFS:

1. Habilite os pontos de extremidade de certificado ADFS necessários executando os seguintes comandos:

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

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

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

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

2. Verifique se todos os pontos finais estão habilitados executando o seguinte comando:

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

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

Como habilitar a autenticação de certificado como principal

Para ativar a Autenticação de certificado como principal:

1. Configure os provedores de autenticação primária para acesso à intranet e à extranet usando o seguinte comando:

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

2. Verifique se ambas as listas incluem CertificateAuthentication e FormsAuthentication usando os seguintes comandos:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Verifique a configuração atual da porta do cliente TLS, usando o seguinte comando:

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

4. Se TlsClientPort não estiver 49443, atualize a porta e reinicie o serviço ADFS usando os seguintes comandos:

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

Correções SChannel/TLS (CRÍTICAS para PKI)

As etapas nas seções a seguir resolvem os erros CERT_E_UNTRUSTEDROOT (0x800B0109), que impedem o funcionamento da autenticação de certificado.

Vinculando certificados SSL na porta 49443

Para vincular certificados SSL na Porta 49443:

1. Remova qualquer associação de certificado SSL existente na porta 49443 usando o seguinte comando:

```
netsh http delete sslcert hostnameport=

     :49443
```

2. Crie uma nova vinculação com a negociação de certificado de cliente ativada usando o seguinte comando:

```
netsh http add sslcert hostnameport=

     :49443 `
    certhash=
```

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

3. Verifique se a negociação de certificado de cliente está ativada, usando o seguinte comando:

```
netsh http show sslcert hostnameport=

     :49443
```

Limpando o Repositório de Certificados (CRÍTICO)

Para limpar o armazenamento de certificados:

---

aviso: O Windows SChannel rejeitará todos os certificados de cliente se houver certificados não autoassinados no repositório Raiz Confiável. Essa é a principal causa de falhas de PKI.

---

1. Identifique certificados não autoassinados no repositório Raiz Confiável executando o seguinte comando:

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

2. Mova esses certificados para o repositório intermediário de CA executando o seguinte comando:

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

3. Verifique se nenhum certificado não autoassinado permanece no armazenamento Raiz, executando o seguinte comando:

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

Correções de registro de canal SC (CRÍTICO)

Para definir as configurações do Registro SChannel para garantir a autenticação de certificado adequada:

1. Defina a variável de caminho do Registro usando o seguinte comando:

```
$regPath = “HKLM:”
```

2. Aplique as configurações de registro definidas na tabela abaixo usando os seguintes comandos:

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

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

Tabela 7: Configurações De Registro Do Schannel

| Configuração | Valor | Propósito |
|---|---|---|
| ClientAuthTrustMode | 2 | Habilita a confiança exclusiva de CA para corrigir o caminho de validação padrão. |
| EnviarListaDeEmissoresConfiáveis | 0 | Impede que o servidor envie a lista completa de emissores confiáveis durante o handshake TLS. |

Verificando o Armazenamento de Certificados de Autoridade de Certificação

Para verificar o armazenamento de certificados da autoridade de certificação:

---

Note: O certificado CA que emite certificados de usuário deve estar no repositório SystemCertificatesstore para garantir que ele seja reconhecido corretamente.

---

1. Defina a impressão digital do seu certificado CA usando o seguinte comando:

```
$caThumbprint = “

    ”
```

2. Verifique se o certificado CA já está presente no LocalMachinestore usando o seguinte comando:

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

Se o certificado não for encontrado, importe-o para o LocalMachinestore:

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

Reinicializando o Servidor ADFS (OBRIGATÓRIO)

Reinicie o servidor ADFS usando o seguinte comando:

```
Restart-Computer -Force
```

Note: A alteração do Registro ClientAuthTrustMode somente entrará em vigor depois que o servidor for reiniciado.

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.

Configuração no Cisco IQ

Para configurar no Cisco IQ:

1. Transfira o adfs-metadata.xml para sua estação de trabalho.
2. No Cisco IQ, navegue para Configurações do sistema > Configuração do sistema > Provedores de identidade.
3. Carregue o arquivo de metadados do ADFS para extrair automaticamente o certificado IDP, a ID da entidade e a URL do SSO.
4. Salve a configuração.

Note: Se o ADFS executar uma substituição automática de certificado de assinatura de token, você deverá exportar novamente o arquivo de metadados e carregá-lo no Cisco IQ para garantir a autenticação contínua.

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 AD para usar no mapeamento. Para localizar grupos do AD, execute o seguinte comando do PowerShell.

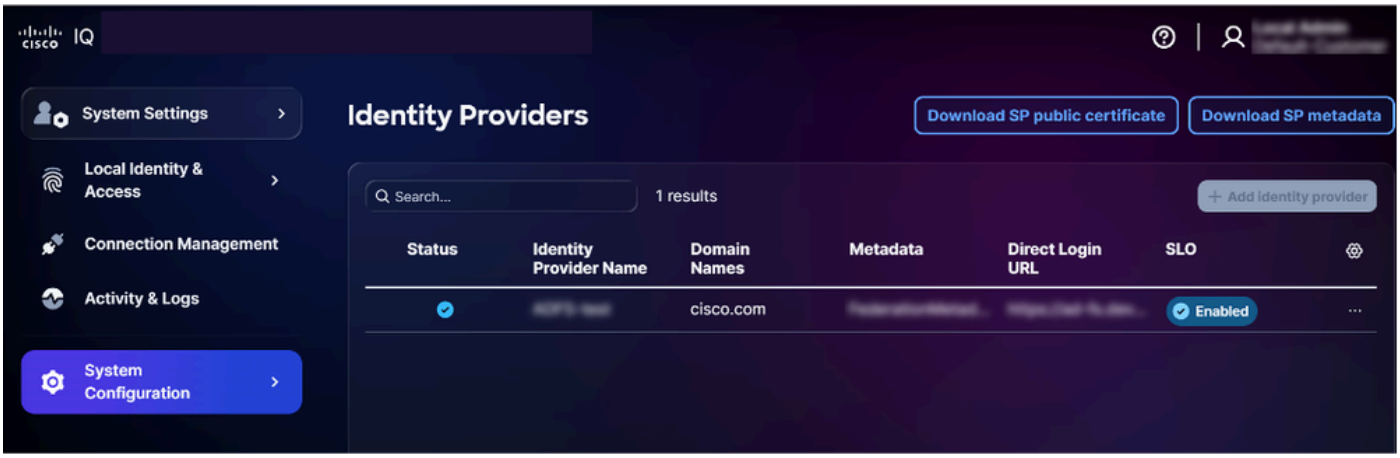
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

O sistema consulta o AD diretamente via LDAP (Lightweight Diretory Access Protocol), não exigindo módulos adicionais. As informações do grupo são retornadas em formato de 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

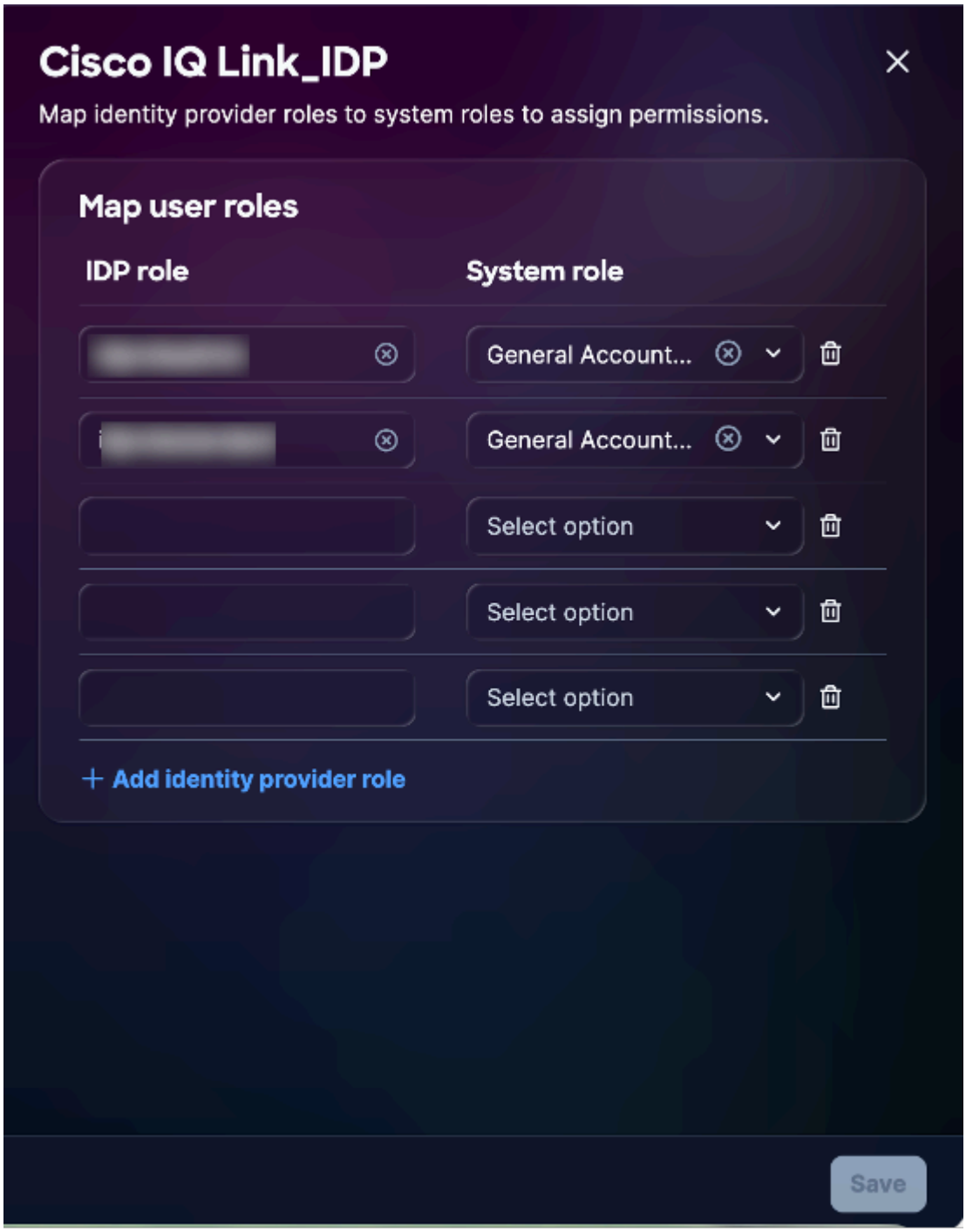
Se os grupos necessários não estiverem listados, eles deverão ser criados no AD por um Administrador de Conta para que você possa concluir o mapeamento de função do ADFS.

Para configurar o mapeamento de função:




Mapear Funções

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 selecionado. As seguintes funções do sistema são suportadas:

- Administrador geral da conta: O Administrador da Conta Geral tem permissões totais para executar todas as ações no produto. A função IDP (nome analisado) é Administradores CXIQ.
- Visualizador de Contas Gerais: O Visualizador de Contas Gerais 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. Clique em Salvar. O status é atualizado para Sucesso.

Teste de Certificação de Cliente SChannel

Para verificar se o SChannel está configurado corretamente para aceitar certificados de cliente, abra uma nova janela do PowerShell e execute o seguinte comando:

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


     :49443/adfs/ls/”
```

A saída esperada é uma resposta HTTP (por exemplo, um redirecionamento ou a página ADFS). Se ocorrer um erro de handshake TLS, a conexão falhou.

Teste completo do navegador para o fluxo de PKI

Antes de iniciar o teste de navegador de ponta a ponta para o fluxo de PKI, verifique se o certificado do usuário está instalado no conjunto de chaves do macOS (consulte Importação do certificado do usuário na máquina cliente (macOS) emConfiguração da autenticação baseada em certificado para obter mais informações).

Para testar:

1. Navegue até o URL de login do SAML do aplicativo. O ADFS apresenta opções de certificado e senha.
2. Escolha Certificate Authentication. O navegador solicita o certificado.
3. Carregue o certificado. O ADFS autentica o usuário, redireciona a solicitação com uma resposta SAML e estabelece uma nova sessão.

Teste de Navegador de Ponta a Ponta para Fluxo de Senha

Antes de iniciar o teste de fluxo de senha do navegador de ponta a ponta:

1. Navegue até o URL de login do SAML do aplicativo. O ADFS apresenta opções de certificado e senha.
2. Selecione Autenticação de Senha/Formulários.
3. Digite Username.
4. Digite a senha.
5. Verifique se o login foi bem-sucedido.

---

Note: Ambos os fluxos devem funcionar simultaneamente.

---

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.

Tabela 8: 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<br>• Atributo de grupo incorreto: Deve ser http://schemas.xmlsoap.org/cla ims/Group<br>• O 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 do ACS inválida: Verifique: https://your-fqdn/saml/acs<br>• Incompatibilidade de cookies: Verificar |

| Problema | Sintomas/Descrição | Causas / Verificações / Soluções e Correções |
| --- | --- | --- |
| | | 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
```

## Configuração de SAML do Microsoft Entra ID para SSO

Esta seção fornece orientação para configurar o Microsoft Entra ID (Entra ID) como o SAML IDP para o Cisco IQ, suportando a autenticação baseada em senha e a autenticação baseada em

PKI/certificado (CBA).

Pré-requisitos para Configurar o Entra ID SAML para SSO

- Locatário do Microsoft Entra ID (por exemplo, "ciqtestdev.onmicrosoft.com")
- Acesso à função de Administrador global ou Administrador de aplicativos do Cisco IQ
- Conectividade entre Entra ID (nuvem) e Cisco IQ
- Autoridade de certificação corporativa instalada ou acessível (necessário apenas para PKI)
- Ponto de Distribuição de Lista de Revogação de Certificados (CRL) acessível da Internet (necessário apenas para PKI)

Tabela 9: Configuração do servidor de ID Entra

| Item | Descrição | Exemplo |
|---|---|---|
| ID do Locatário | Identificador de locatário do Entra ID | 37352d8f-0ebe-4762-8161-8775ffe897cb |
| FQDN do Cisco IQ | Nome de host de implantação | <SEU-CIQ-FQDN> |
| ID da entidade IDP | URL do emissor da ID de entrada | https://sts.windows.net/<TENANT-ID>/ |
| URL SSO IDP | Ponto de extremidade de logon SAML | https://login.microsoftonline.com/<TENANT-ID>/saml2 |
| Domínio da empresa | Domínio de e-mail para usuários | <SEU-DOMÍNIO> |

Configurando o aplicativo Entra ID SAML

Criando uma aplicação empresarial

1. Entre no centro de administração do Microsoft Entra.
2. Navegue até Identity > Applications > Enterprise applications.
3. Clique em Novo aplicativo > Criar seu próprio aplicativo.

4. Insira o nome (por exemplo, "Cisco IQ").
5. Escolha Integrar qualquer outro aplicativo que não esteja na galeria (Não-galeria).
6. Clique em Criar.

Configurando o Logon Único do SAML

Para configurar o logon único SAML, você deve carregar o arquivo de metadados SP. Você pode obtê-lo executando as seguintes etapas do Virtual Appliance (VA):

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 metadata para fazer o download. Este arquivo de metadados SP baixado é carregado para concluir a configuração de logon único SAML.
3. Clique no botão Upload Metadata file para carregar o arquivo de metadados SP. Os dados do arquivo de metadados SP serão preenchidos automaticamente na tela Logon único baseado em SAML após o upload bem-sucedido.

Você também pode optar por inserir manualmente esses detalhes para definir as configurações de logon único. Para configurar manualmente o Logon único SAML:

1. No aplicativo empresarial, navegue para Logon único e escolha SAML.
2. Na seção Configuração SAML Básica, clique em Editar e insira o seguinte:
    a. Identificador (ID da entidade): <SEU-CIQ-FQDN>
    b. URL de resposta (URL ACS): https://<YOUR-CIQ-FQDN>/saml/acs
    c. URL de Logon: https://<YOUR-CIQ-FQDN>/saml/login
    d. URL de logoff: https://<YOUR-CIQ-FQDN>/saml/logout

3. Click Save.

Note: A ID da entidade deve corresponder exatamente ao que o Cisco IQ usa como sua ID de entidade SP. Normalmente, é o FQDN da implantação.

4. Para configurar Atributos SAML e declarações, na seção Atributos e Declarações, clique em Editar.

5. Configure as seguintes declarações:

Tabela 10: Reivindicações SAML necessárias

| Reivindicação | Atributo de Origem | Espaço de nomes |
|---|---|---|
| Identificador de Usuário Exclusivo (NameID) | user.userprincipalname | (padrão) |
| endereço de e-mail | user.mail | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| nome dado | user.givenname | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| sobrenome | user.surname | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| nome | user.userprincipalname | http://schemas.xmlsoap.org/ws/2005/05/identity/claims |
| grupos | user.assignedroles | (VAZIO — limpar o namespace) |

Note: Para a alegação dos grupos:
- Use user.assignedroles como origem - não user.groups
O campo Namespace deve estar vazio. Isso garante que o nome do atributo na asserção SAML seja simplesmente grupos, em vez de um Uniform Resource Identifier (URI) completo
- Não adicione uma declaração de grupo duplicada com user.groups, pois isso causa conflitos

Configurando funções de aplicativo

As funções de aplicativo são configuradas no registro de aplicativo (não no aplicativo empresarial); para configurar Funções de Aplicativo:

1. Navegue até Identidade > Aplicativos > Registros de aplicativo.
2. Localize e escolha seu aplicativo.
3. Vá para Funções de aplicativo > Criar função de aplicativo.
4. Para cada função necessária, configure o seguinte:

- Nome de exibição: Por exemplo, Cisco IQ Admins
- Tipos de membro permitidos: Usuários/Grupos
- Valor: Por exemplo, Cisco IQ Admins
- Descrição: Por exemplo, Cisco IQ Administrators

5. Clique em Aplicar.

---

Note: Crie funções que correspondam aos seus requisitos de mapeamento de funções do Cisco IQ (por exemplo, Administradores CXIQ, Desenvolvedores CXIQ, Visualizadores CXIQ).

---

As funções de aplicativo são usadas em vez de declarações de grupo pelos seguintes motivos:

- Os locatários somente em nuvem não podem enviar nomes para exibição de grupo sem uma licença P1 ou P2
- sAMAccountName só funciona para grupos sincronizados do AD local
- A origem da ID de grupo envia Universally Unique Identifiers (UUIDs), que são difíceis de mapear
- As funções de aplicativo enviam valores de string exatos que correspondem às expectativas da função do Cisco IQ

Atribuição de Usuários a Funções de Aplicativo

Para atribuir usuários a funções de aplicativo:

1. Volte para Aplicativo Empresarial > Usuários e grupos.
2. Clique em Adicionar usuário/grupo.
3. Escolha o(s) usuário(s) e atribua a Função de Aplicativo apropriada.
4. Clique em Atribuir. Os valores de função são exibidos como strings legíveis no atributo de grupos de asserção SAML.

Download de metadados e certificados IDP

Para fazer download de metadados e certificados IDP:

1. No aplicativo empresarial, vá para a seção Logon único > Certificado de assinatura SAML.
2. Faça download do XML de Metadados de Federação (salve como entra-id-metadata.xml).

   Ou

   Fazer download de certificado (Base64) para entrada de certificado manual.
3. Anote os seguintes valores na seção Configuração:

- URL de logon (URL SSO do IDP)
- Identificador do Azure AD (ID da Entidade do IDP)
- URL de logoff (URL do SLO do IDP)

---

Note: Como a ID Entra gira certificados de assinatura periodicamente, você deve baixar novamente os metadados e carregá-los no VA sempre que o certificado ativo for alterado para garantir serviço SSO ininterrupto.

---

Adicionando ID do Entra IDP

---

Note: As rotas APISIX para SAML são criadas automaticamente quando um IDP é adicionado ao Cisco IQ, eliminando a necessidade de configuração de rota manual.

---

Para adicionar Entra ID IDP:

1. Faça login no VA como um administrador de conta.
2. Navegue até Configurações do sistema > Configuração do sistema > Provedores de identidade.
3. Clique em Adicionar provedor de identidade.
4. Insira o Nome do IDP (por exemplo, "ID Entra").
5. Insira o(s) Domínio(s) (por exemplo, "ciqtestdev.onmicrosoft.com" ou o domínio da sua empresa).
6. (Opcionalmente) Ative o botão de alternância Ativar logoff único, se necessário.
7. Arraste e solte ou carregue o arquivo entra-id-metadata.xml obtido do Entra ID no campo Upload IDP Metadata.
8. Click Save.

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

Configurando o mapeamento de função

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.
2. Insira uma função de IDP para cada função do sistema. As seguintes funções do sistema são suportadas:

Tabela 11: Funções do sistema

| Função do sistema | Função IDP (Valor da Função do Aplicativo) | Descrição |
|---|---|---|
| Administrador geral da conta | Administradores do CXIQ | Permissões totais para todas as ações |
| Visualizador de Contas Gerais | Desenvolvedores do CXIQ | Acesso somente leitura |
| Visualizador de Contas Gerais | Visualizadores CXIQ | Acesso somente leitura |

Note: Use as strings de Valor da Função de Aplicativo exatamente como configuradas no ID do Entra (consulte Configurando Funções de Aplicativo em Configurando o Aplicativo SAML do ID do Entra para obter mais detalhes).

3. Clique em Salvar. O status é atualizado para Sucesso.

Verificando o fluxo SAML (autenticação de senha)

Para verificar o fluxo SAML:

1. Abra um navegador no modo Incognito ou Privado.
2. Navegue até https://<YOUR-CIQ-FQDN>/saml/login.
3. Verifique se você foi redirecionado para a página de login da Microsoft.
4. Autentique com suas credenciais (e MFA, se configurado).

5. Após a autenticação, verifique se você foi redirecionado de volta para /saml/acs e se o aplicativo Cisco IQ é exibido.
6. Verifique a extração do grupo executando o seguinte comando:

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

Saída esperada

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

## Configurando a autenticação baseada em certificado

Esta seção descreve como adicionar CBA ao lado de senhas. Esta seção poderá ser ignorada se a autenticação somente por senha for suficiente.

### Pré-requisitos para CBA

- Windows Server com Serviços de Certificados do AD (CS) com CA Corporativa configurada (por exemplo, "DEV-ADCS-CA")
- Acesso de administrador do PowerShell no servidor de autoridade de certificação
- O certificado UPN deve corresponder à ID de entrada userPrincipalName
- O Ponto de Distribuição de CRL deve estar acessível na Internet

### Criando um Modelo de Certificado no AD CS

1. Abra certtmpl.msc no servidor de autoridade de certificação.
2. Duplicar o modelo do usuário e nomeá-lo como "EntraUserCert".
3. Configure o modelo:

- General: Nome para exibição EntraUserCert, validade de 1 a 2 anos

- Tratamento de Solicitações: Finalidade = Assinatura e criptografia
- Nome do assunto: Selecionar Suprimento na solicitação
- Extensões: As políticas de aplicativos devem incluir a autenticação do cliente (1.3.6.1.5.5.7.3.2)
- Segurança: Conceder permissões de leitura e registro a usuários autenticados

4. Publique o modelo usando o seguinte comando:

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

Solicitando e emitindo um certificado do usuário

1. Crie um arquivo de Configuração de Certificado (INF) (por exemplo, C:-cert.inf) usando o seguinte script do PowerShell:

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

[NewRequest]
Subject = “CN=



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

[RequestAttributes]
CertificateTemplate = EntraUserCert

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2

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



      &”
_continue_ = “email=
```

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

2. Substitua <USER-UPN> pelo seu Entra ID UPN (por exemplo, user@ciqtestdev.onmicrosoft.com).

3. Para gerar o certificado, execute o seguinte comando:

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

4. Para enviar a solicitação à CA, execute o seguinte comando:

```
certreq -submit -config “

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

5. Para instalar o certificado na CA, execute o seguinte comando:

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

Exportando certificados

- Para exportar o certificado do usuário como um arquivo PFX (para o cliente), execute o seguinte script:

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

```
     *" }
$password = ConvertTo-SecureString -String "


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

- Para exportar o certificado CA Root (para Entra ID), execute o seguinte script:

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


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

Importando o certificado do usuário na máquina cliente (macOS)

- Para importar o certificado do usuário (PFX), execute o seguinte comando:

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


     "
```

- Para importar o certificado raiz da CA, execute o seguinte comando:

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

- Para definir o certificado CA como Sempre Confiar no Acesso ao Conjunto de Chaves:
    1. Abra o Keychain Access (Acesso ao conjunto de chaves).

2. Localize o certificado CA e clique em Obter informações.

3. Em Confiança, defina como "Sempre Confiar".

---

Note: Após importar, saia e reabra o navegador para que o certificado seja reconhecido.

---

Carregando o Certificado Raiz da CA para a ID do Entra

1. Entre no centro de administração do Microsoft Entra.
2. Navegue até Proteção > Segurança > Autoridades de certificado.
3. Clique em Upload e selecione o arquivo ca-root.cer.
4. Marcá-lo como um certificado CA raiz.
5. Insira a URL do Ponto de Distribuição da CRL (deve estar publicamente acessível).

Ativando o CBA nos métodos de autenticação da Entra ID

1. Navegue até Protection > Authentication methods > Policies.
2. Clique em Autenticação baseada em certificado para configurar.
3. Ative o CBA e adicione os usuários ou grupos-alvo.
4. Em Configure, defina o nível de proteção como Single-fator authentication.

Configurando a vinculação de nome de usuário

Na configuração do CBA, vá até a guia Associação de nome de usuário e defina a seguinte associação:

- Campo do certificado: NomePrincipal
- Atributo do usuário: userPrincipalName

Isso mapeia o UPN no Nome Alternativo do Assunto do certificado para o usuário da ID Entra.

Verificando o fluxo do CBA

1. Abra um navegador no modo Incognito ou Privado.
2. Navegue até https://<YOUR-CIQ-FQDN>/saml/login.
3. Na página de login da Microsoft, digite o e-mail do usuário e clique em Avançar.
4. Selecione Use a certificate or smart card (ou ele pode solicitar automaticamente).
5. Escolha o certificado de usuário aplicável quando o navegador solicitar a seleção do certificado.
6. Verifique se a ID da Entra valida o certificado, redireciona com uma resposta SAML e cria uma sessão.

---

Note: Certifique-se de selecionar o certificado de cliente correto. A seleção de um certificado incorreto (por exemplo, um certificado de usuário diferente ou um certificado expirado) causa uma falha de autenticação.

---

Troubleshooting de Problemas de Entra ID

A lista a seguir descreve problemas comuns e possíveis soluções para ajudar a identificar e resolver rapidamente problemas relacionados à configuração do Entra ID SAML.

Tabela 12: Troubleshooting

| Problema | Causa | Reparar |
|---|---|---|
| Resposta SAML inválida - email ausente | A asserção SAML não tem atributo NameID ou email | Verifique a configuração de declarações de ID Entra (consulte Configuração de Logon Único SAML em Configuração de Aplicativo SAML de ID Entra para obter mais detalhes). Verifique se o usuário tem o atributo de e-mail preenchido. |
| Total de grupos extraídos: 0 | Declarações de grupo não configuradas ou origem incorreta | Use user.assignedroles como a origem. Certifique-se de que o usuário esteja atribuído a uma Função de Aplicativo (consulte Atribuindo Usuários a Funções de Aplicativo em Configurando o Aplicativo SAML Entra ID para obter mais detalhes). |
| Declarações de grupo duplicadas | user.groups e user.assignedroles ativos | Remova a declaração user.groups. Manter apenas user.assignedroles. |
| Grupos exibidos como UUIDs | O atributo de origem é "ID do grupo" | Use a abordagem Funções de Aplicativo (consulte Configurando Funções de Aplicativo em Configurando o Aplicativo SAML Entra ID para obter mais detalhes). |

| Problema | Causa | Reparar |
|---|---|---|
| Nome do Atributo mostra URI longo | O campo Namespace não está vazio | Limpe o campo Namespace nas configurações de declaração de grupos. |
| Assinatura SAML inválida | Certificado IdP girado ou incompatível | Baixe novamente os metadados da ID do Entra e carregue novamente no Cisco IQ. |
| AADSTS500191 | CRL não alcançável pela Internet | Publique a CRL em uma URL publicamente acessível ou use uma abordagem de CA autoassinada (consulte Solução alternativa da CRL para ambientes de laboratório para obter mais detalhes). |
| Certificado não solicitado | O certificado não está no conjunto de chaves, a autoridade de certificação não é confiável no cliente ou o CBA não está ativado | Verifique se o certificado do usuário é importado no MacOS Keychain Access (consulte Importação do certificado do usuário na máquina cliente (MacOS) emConfiguração da autenticação baseada em certificado para obter mais detalhes), o CBA é habilitado no Entra ID com as configurações necessárias (consulte Habilitação do CBA em Métodos de autenticação de ID do Entra em Configuração da autenticação baseada em certificado para obter mais detalhes) e o Chrome é reiniciado para aplicar as alterações. |
| Asserção SAML expirada | Desvio de relógio entre sistemas | Aumente clock_skew_seconds na configuração do plugin (padrão 300, use 30000 para laboratório). |
| Status "Incompleto" em VA | Mapeamento de função ainda não configurado | Conclua o mapeamento de funções (consulte Configuração do Mapeamento de Funções para obter mais detalhes). |

Solução alternativa de CRL para problemas de acessibilidade

Se o Ponto de Distribuição de CRL de sua CA não estiver acessível pela Internet (comum em configurações de laboratório), use uma CA autoassinada sem requisitos de CRL:

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

# Create user cert signed by the CA
```

```
$userCert = New-SelfSignedCertificate `
    -Subject “CN=


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


      &email=


       ”
)
```

Carregue somente o certificado CA raiz para a ID do Entra. Como é autoassinado sem CDP, o Entra ID não tenta a validação de CRL.

## Lista de verificação de instalação completa

Esta seção descreve uma lista de verificação de configuração completa para configurar o VA com o Microsoft Entra ID SAML Application e o CBA opcional.

### Configuração do Aplicativo SAML do Entra ID

- Criar Aplicativo Empresarial (Não galeria) na ID do Entra
- Configurar a configuração SAML básica inserindo manualmente os metadados SP
- Configurar atributos e reivindicações (incluindo email, nome e grupos com user.assignedroles)
- Criar Funções de Aplicativo no Registro do Aplicativo
- Atribuir usuários a funções de aplicativo

- Baixar XML de Metadados de Federação

Configuração do Cisco IQ

- Adicione o provedor de identidade no Cisco IQ carregando metadados de ID do Entra
- Configure o Mapeamento de Função para mapear valores de Função de Aplicativo para funções do sistema Cisco IQ
- Verificar se o login baseado em senha funciona de ponta a ponta
- Verificar se os grupos foram extraídos corretamente nos logs

Autenticação Baseada em Certificado (opcional)

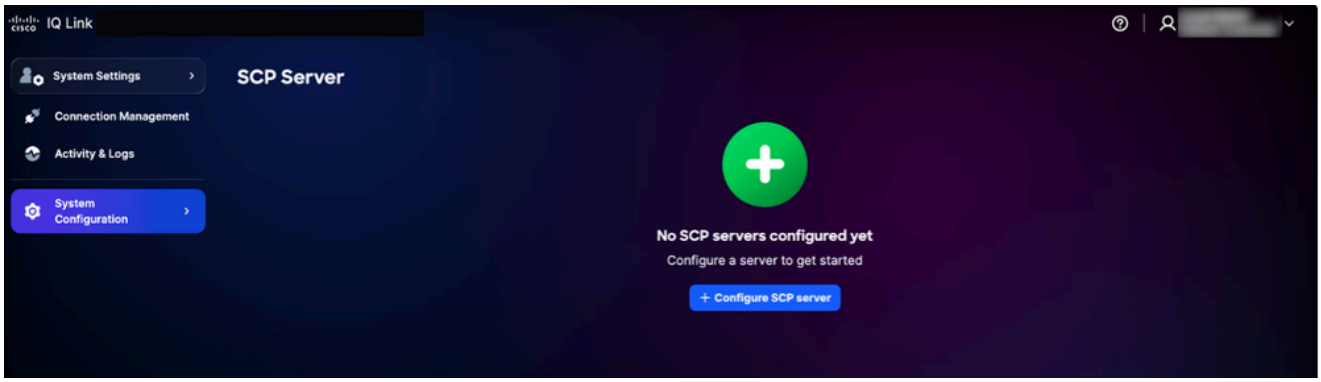
- Criar modelo de certificado no AD CS com EKU de Autenticação de Cliente
- Emitir certificado de usuário com UPN correspondente ao usuário da ID Entra
- Exportar certificado do usuário como PFX e instalar no computador cliente
- Confiar no certificado CA no computador cliente
- Carregue o certificado raiz de CA para o ID da Entra em Protection > Certificate authorities
- Ativar o CBA nos métodos de autenticação
- Configurar associação de nome de usuário (PrincipalName e userPrincipalName)
- Verificar se o login do CBA funciona de ponta a ponta

# 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.

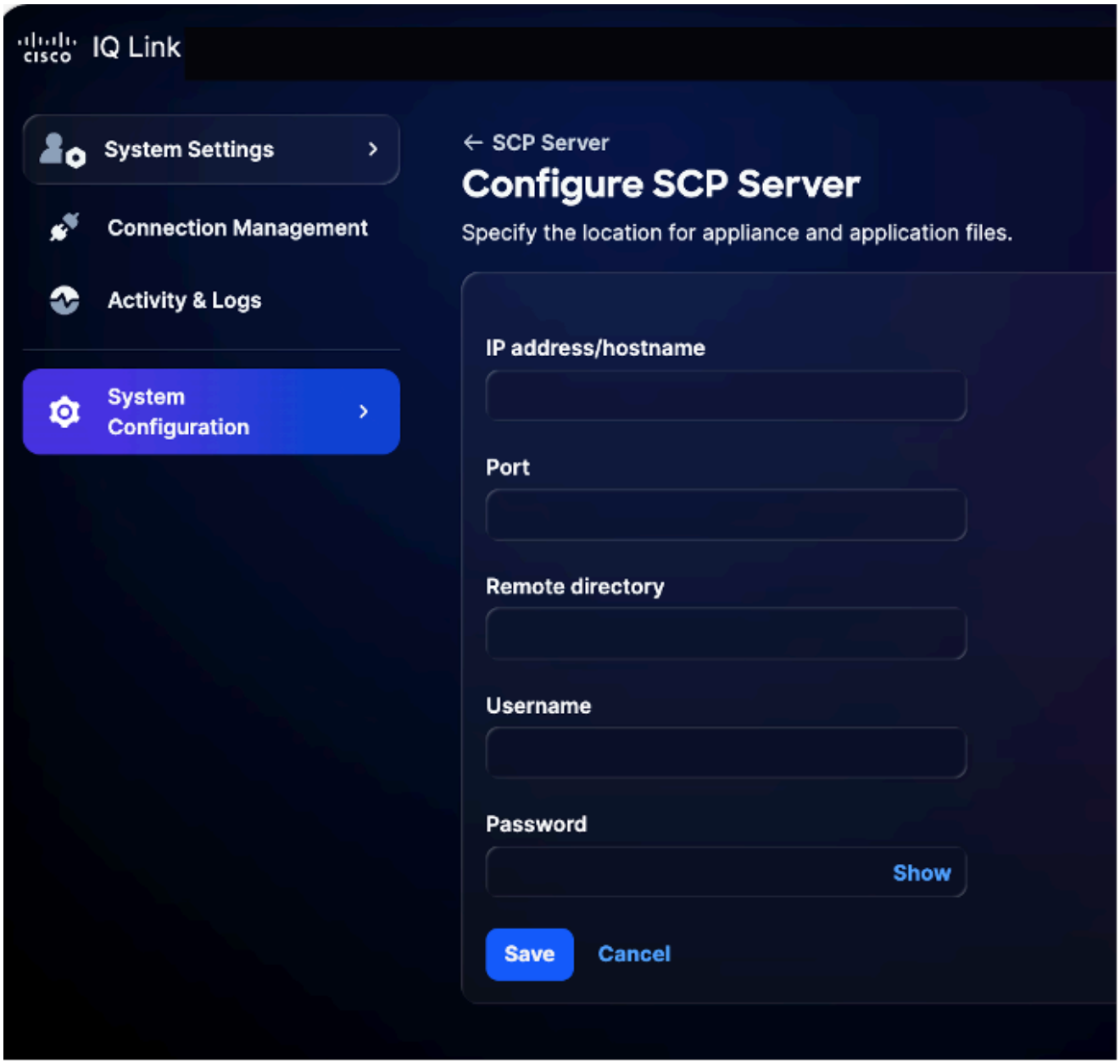
Para adicionar um Servidor SCP:

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.

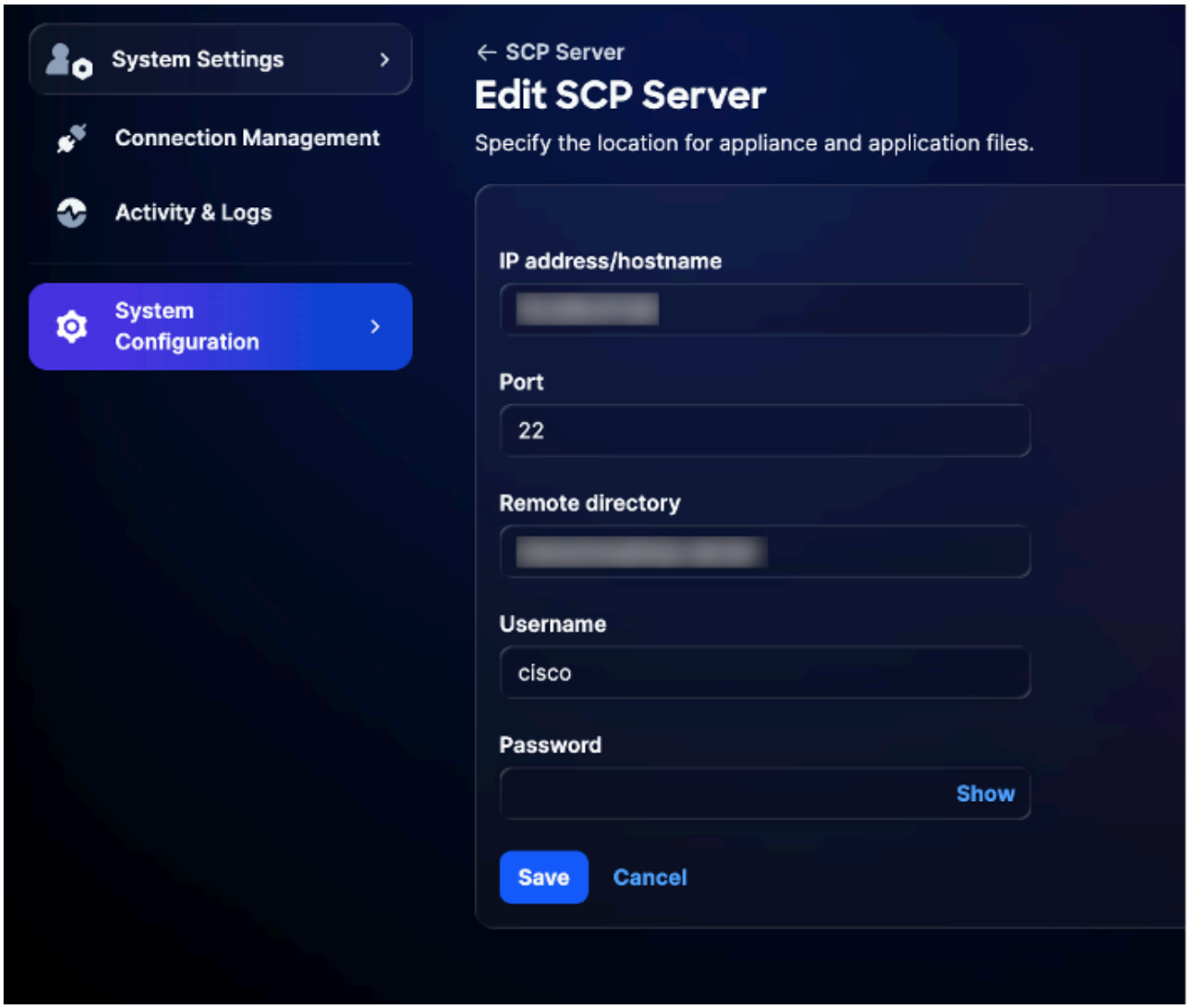
## Edição de servidores SCP existentes

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.

# Gerenciamento do sistema

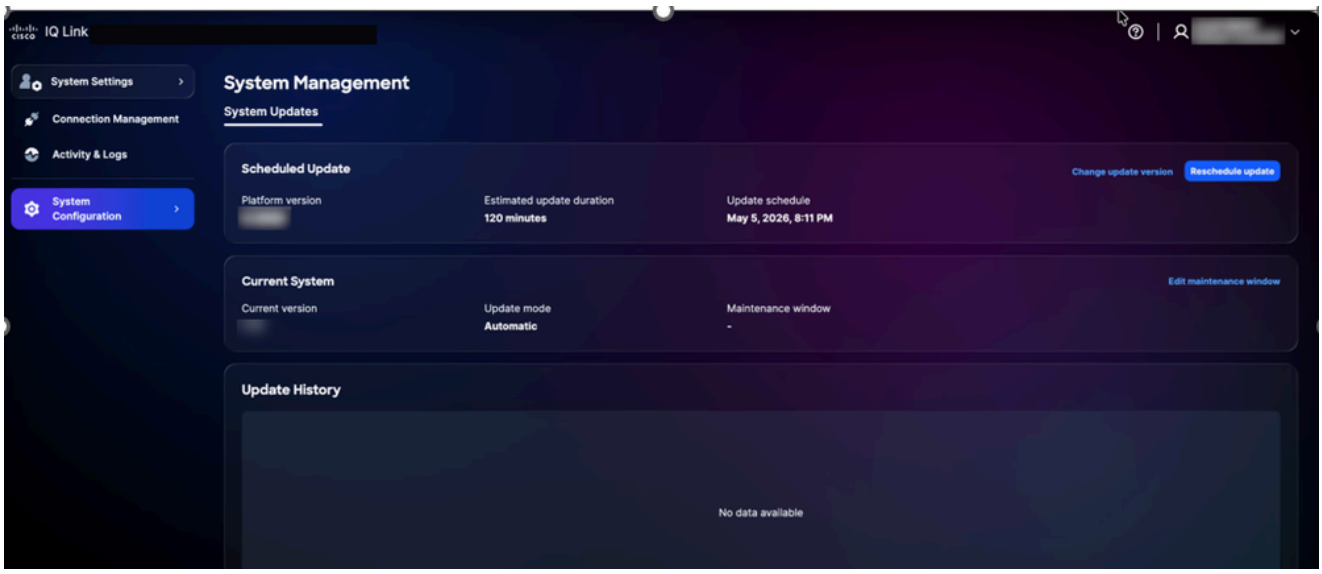
Você pode atualizar para a versão mais recente do Cisco IQ Link através da interface do usuário. Você também pode verificar na página Cisco IQ Data Connectors.

## Reagendando a atualização do sistema

Para reprogramar a atualização do sistema:

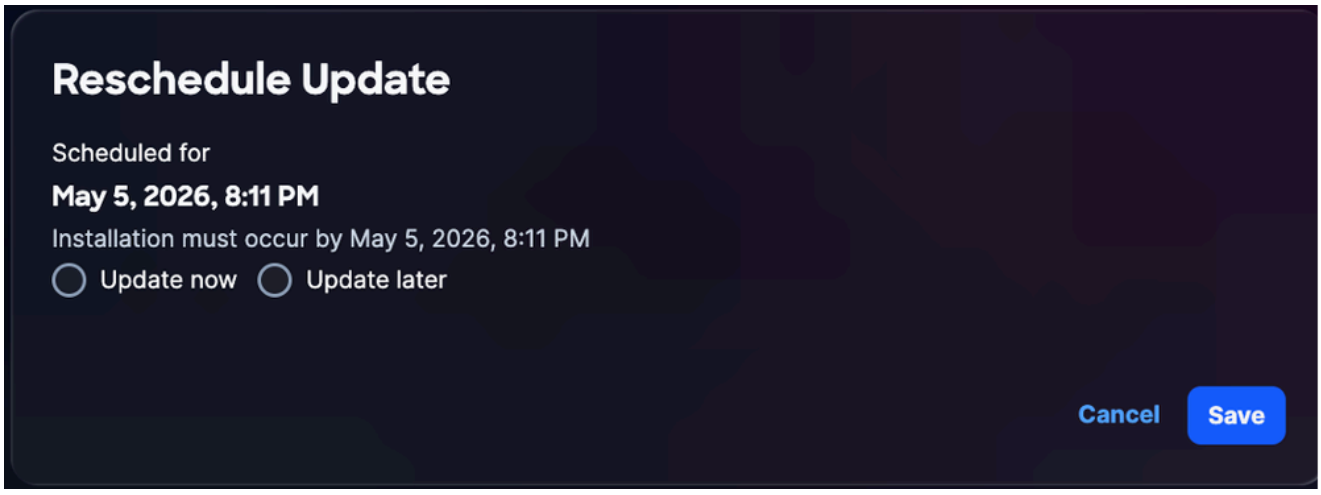
1. Em Administração, escolha Configuração do Sistema > Gerenciamento do Sistema. A

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

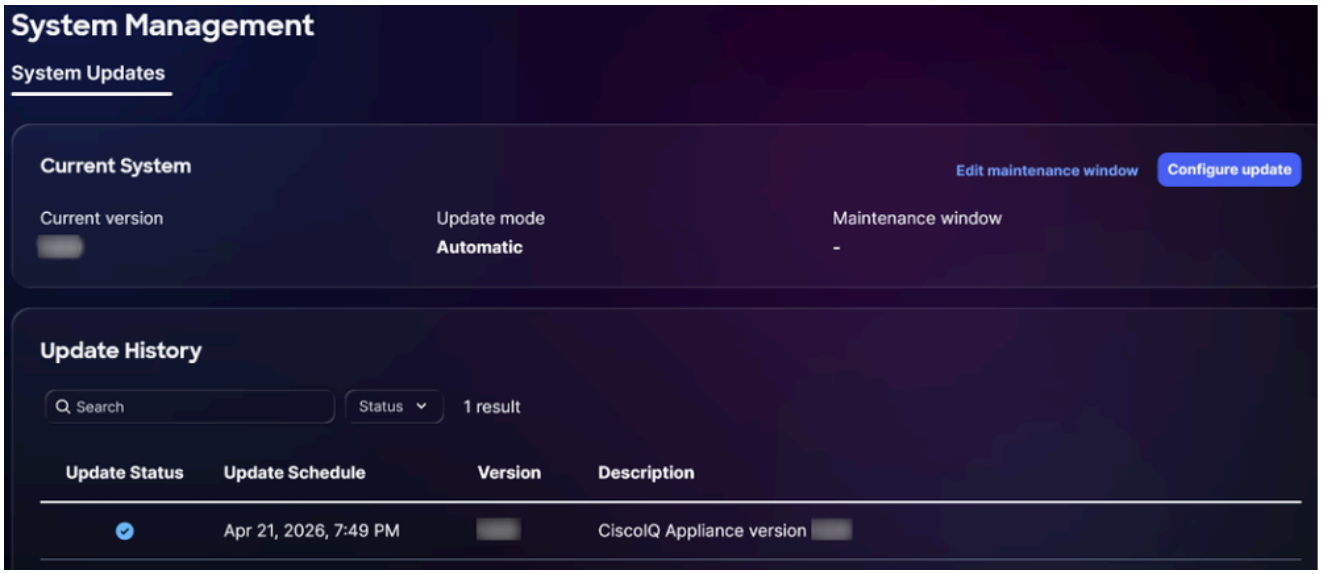
2. Clique em Reagendar atualização.




Reagendar Atualização

3. Escolha o botão de opção Atualizar Agora para reprogramação imediata ou o botão de opção Atualizar Depois para programar outro horário.

4. Click Save. Uma confirmação é exibida e você é redirecionado para a página inicial da Atualização do sistema.

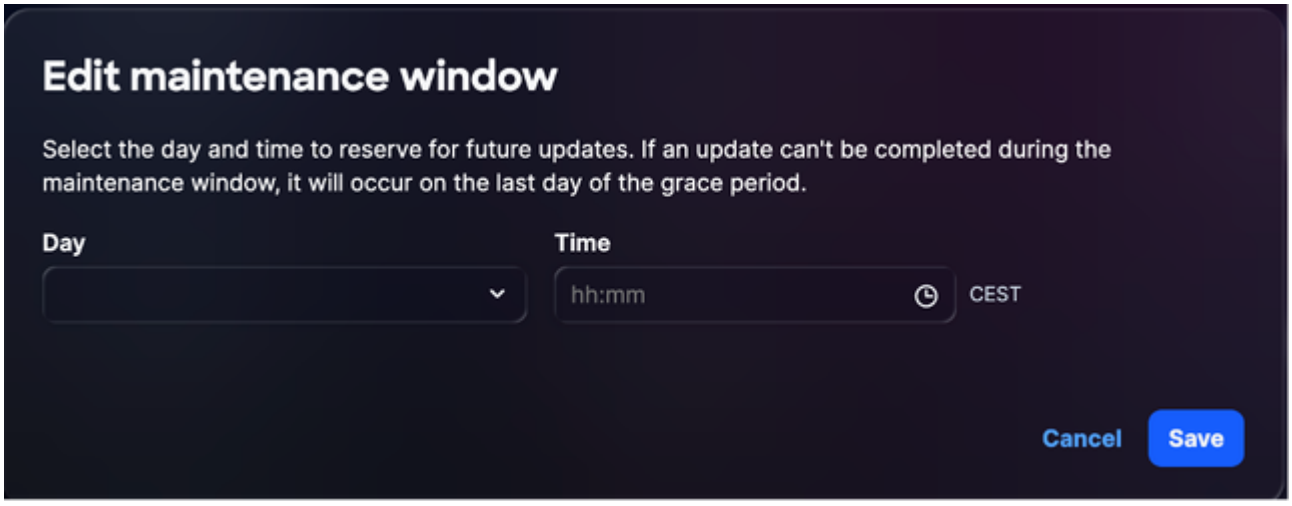



Atualização bem-sucedida

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

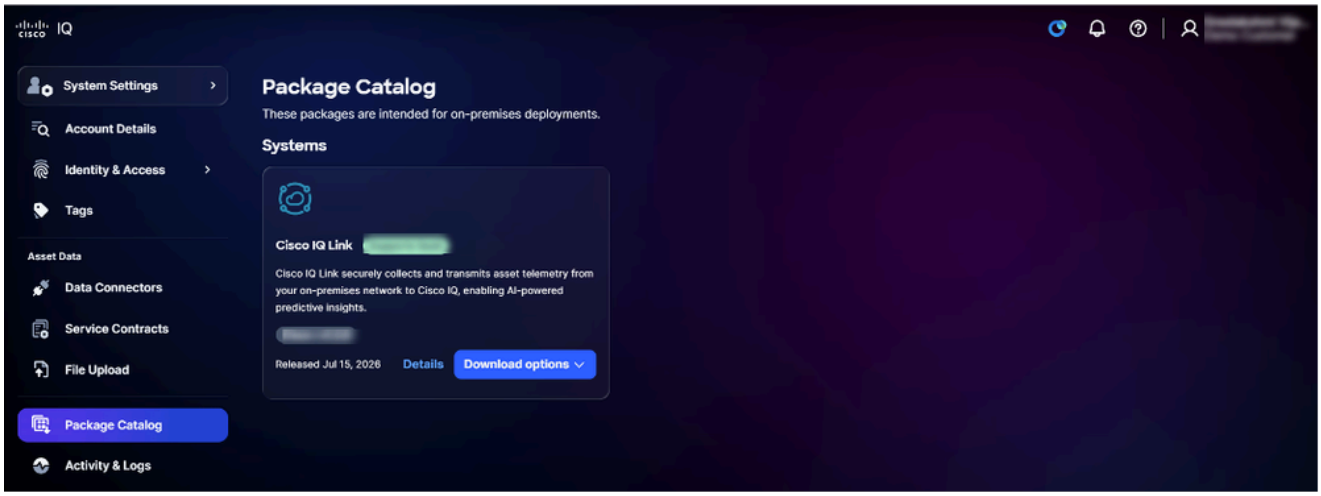
2. Escolha uma opção nas listas suspensas Dia e Hora.
3. Clique em Salvar. A janela de manutenção foi programada com êxito. A atualização é acionada de acordo com a programação exibida.

Note:
- Se nenhum agendamento de upgrade estiver configurado, 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

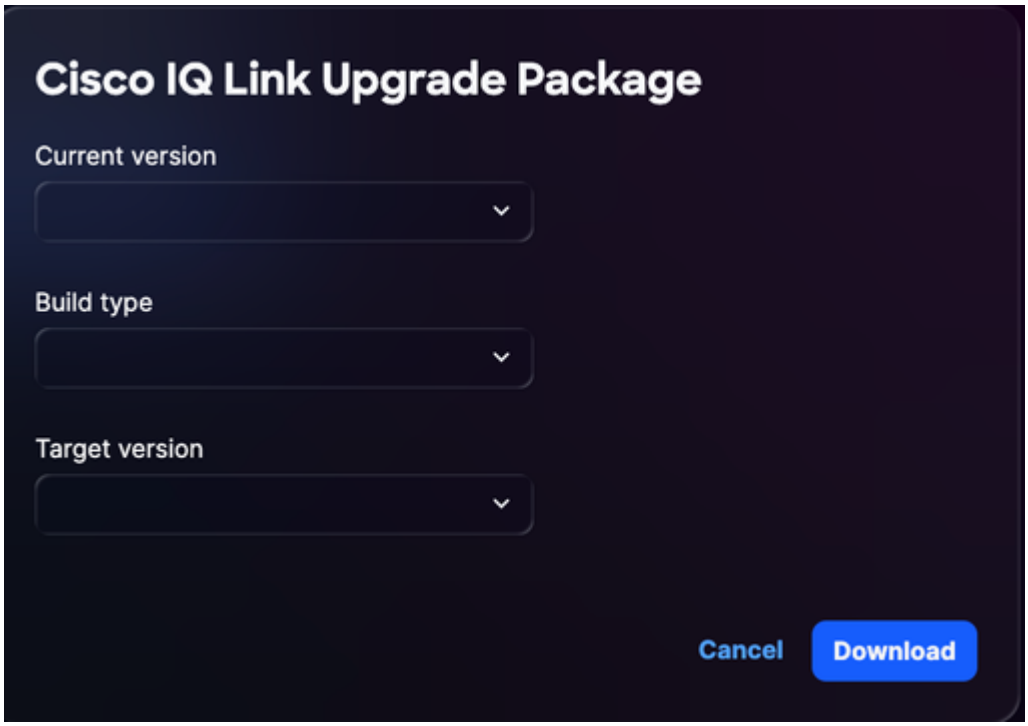
Em cenários onde a distribuição automática do Cisco IQ SaaS está indisponível ou atrasada, você pode executar manualmente uma atualização do sistema fazendo o download do pacote de atualização diretamente do Cisco IQ SaaS. Para atualizar manualmente o sistema:

1. Faça login no Cisco IQ SaaS escolha Home > Configurações do sistema > Catálogo de pacotes.



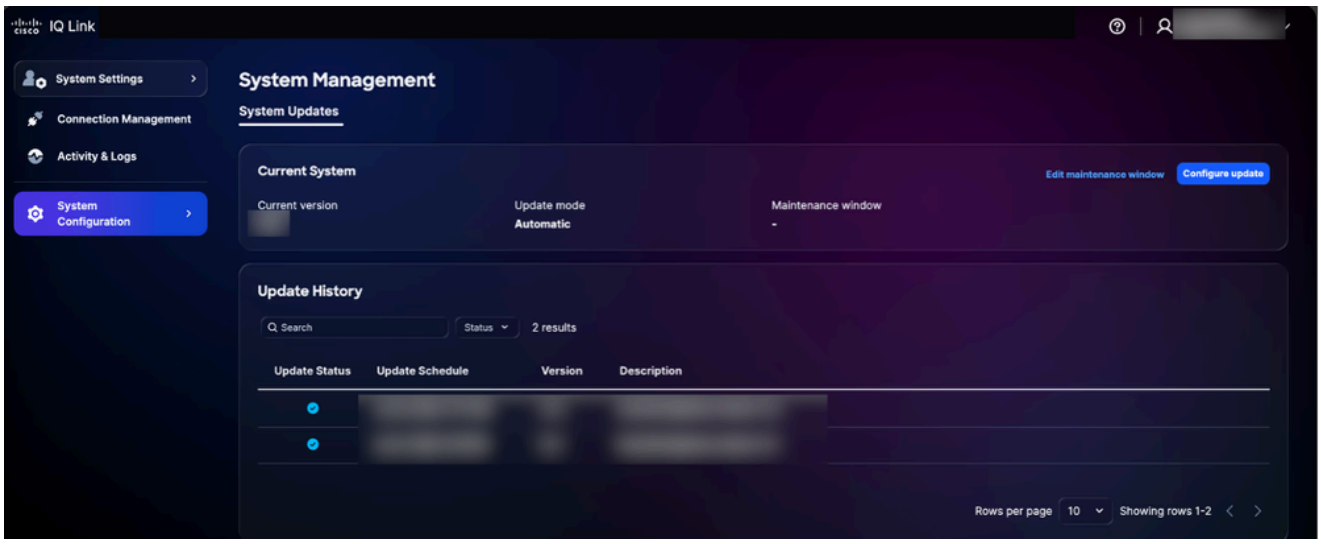

Catálogo de Pacotes

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



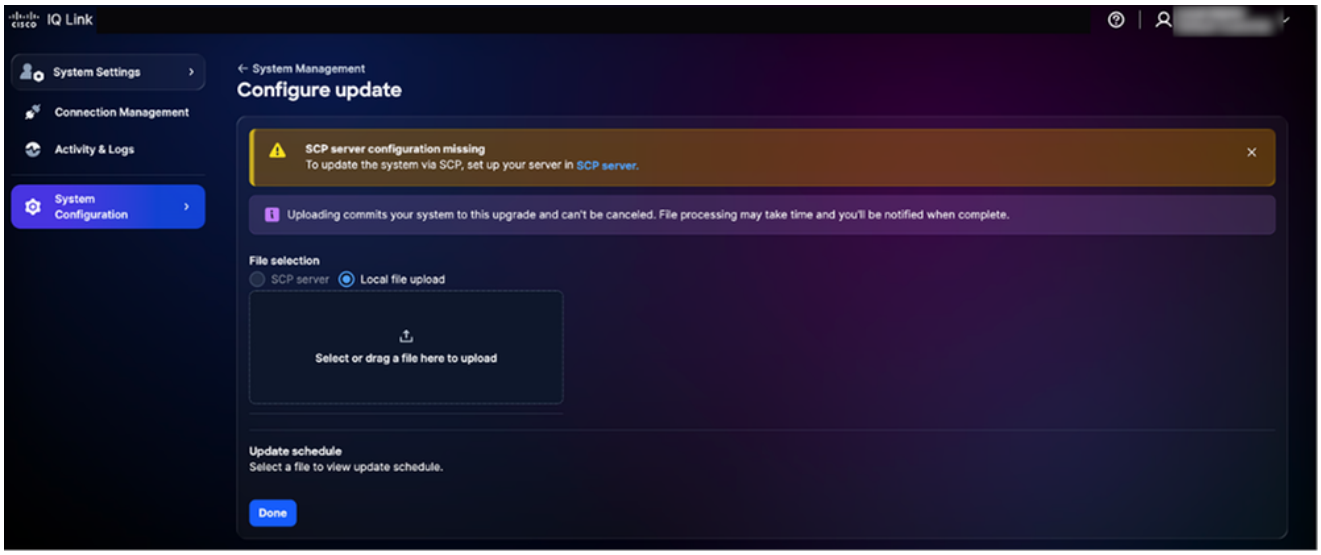

Pacote de atualização

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




Configurar atualização

9. Clique em Configure update.




Carregamento de arquivo local

10. Clique no botão de opção Local file upload.

11. Selecione ou arraste o arquivo do pacote de atualização baixado para o campo de carregamento.
12. 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 você pode 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.

O certificado SSL padrão não pode ser editado ou excluído.

---

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.

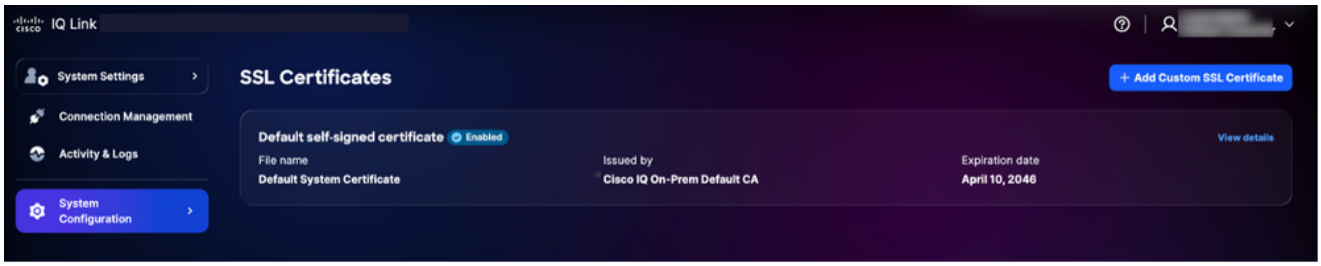
---

Após adicionar, editar ou excluir um certificado SSL, você deve carregar o novo certificado SSL conforme descrito em Configuração de Logoff Único 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.



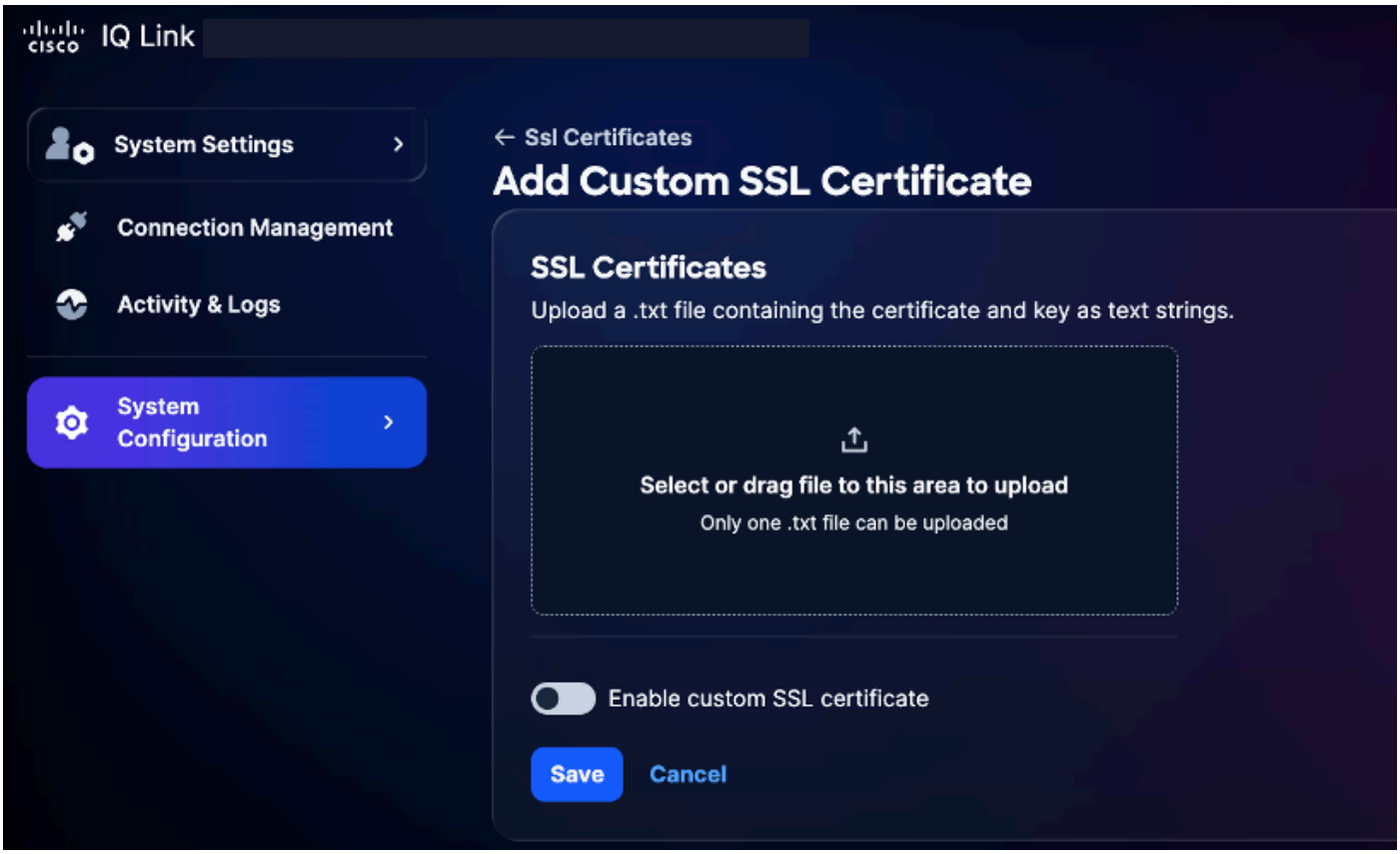

Adicionando Certificado SSL

2. Clique em Adicionar certificado SSL personalizado.

---

Notas:
- Carregue um arquivo .txt que inclua o certificado e a chave codificados por Privacy-Enhanced Mail como sequências de texto
- Somente um arquivo .txt pode ser carregado por vez
- O arquivo deve conter o certificado e a chave privada

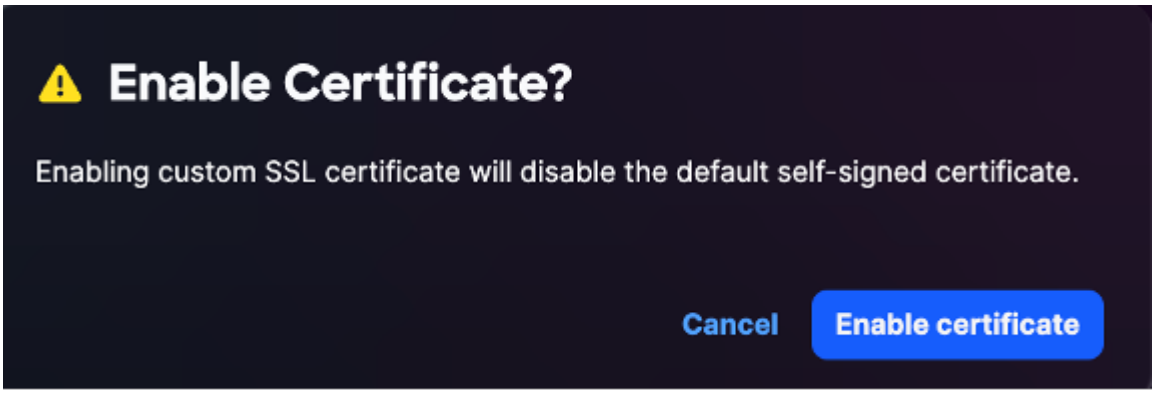
---




Carregar Certificado SSL

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

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




Editar Certificado SSL

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

5. Clique em Ativar certificado.

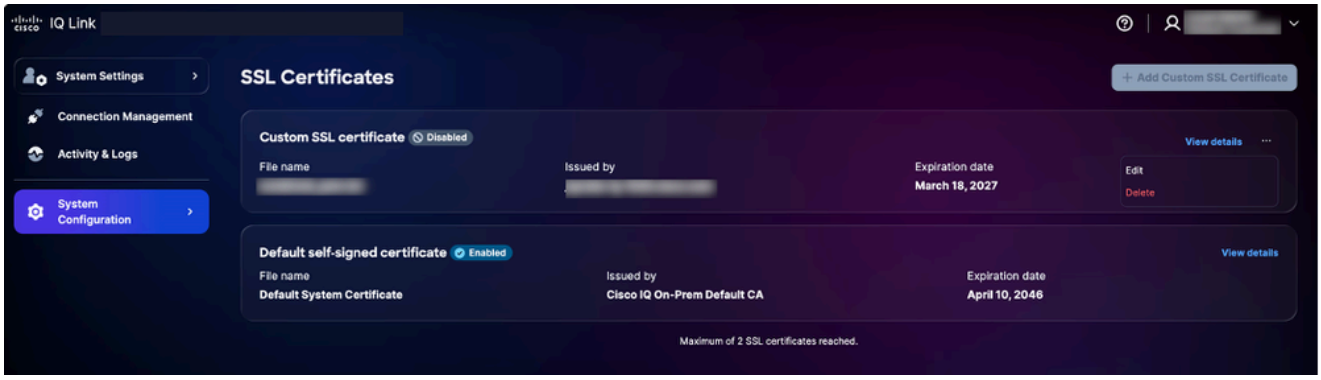
6. Clique em Salvar.

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

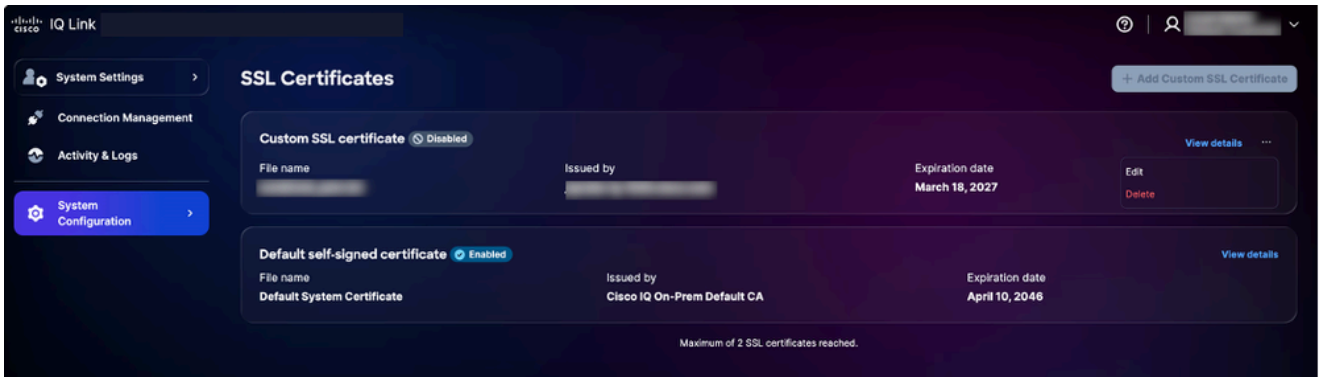
2. Escolha o ícone Mais Opções > Editar. A página Editar Certificado SSL é exibida.
3. Edite os detalhes do certificado conforme necessário.
4. Click Save.

### 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 personalizado 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

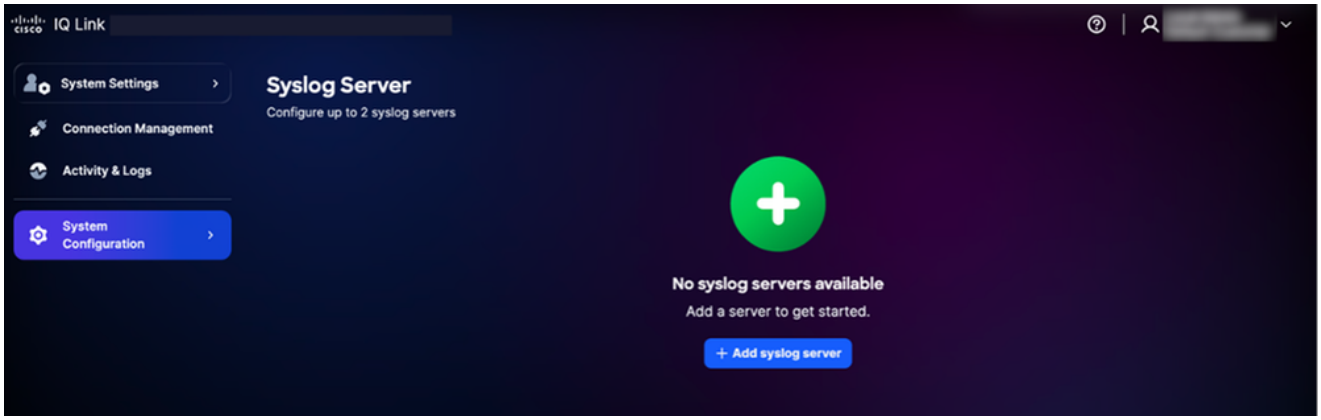
Os usuários com a função Administrador de conta podem configurar servidores syslog externos para exportar logs do sistema. Até 2 (dois) servidores syslog podem ser configurados.

Note: O servidor Syslog deve ser especificado como um endereço IP, não um FQDN.

### Adicionando servidores Syslog

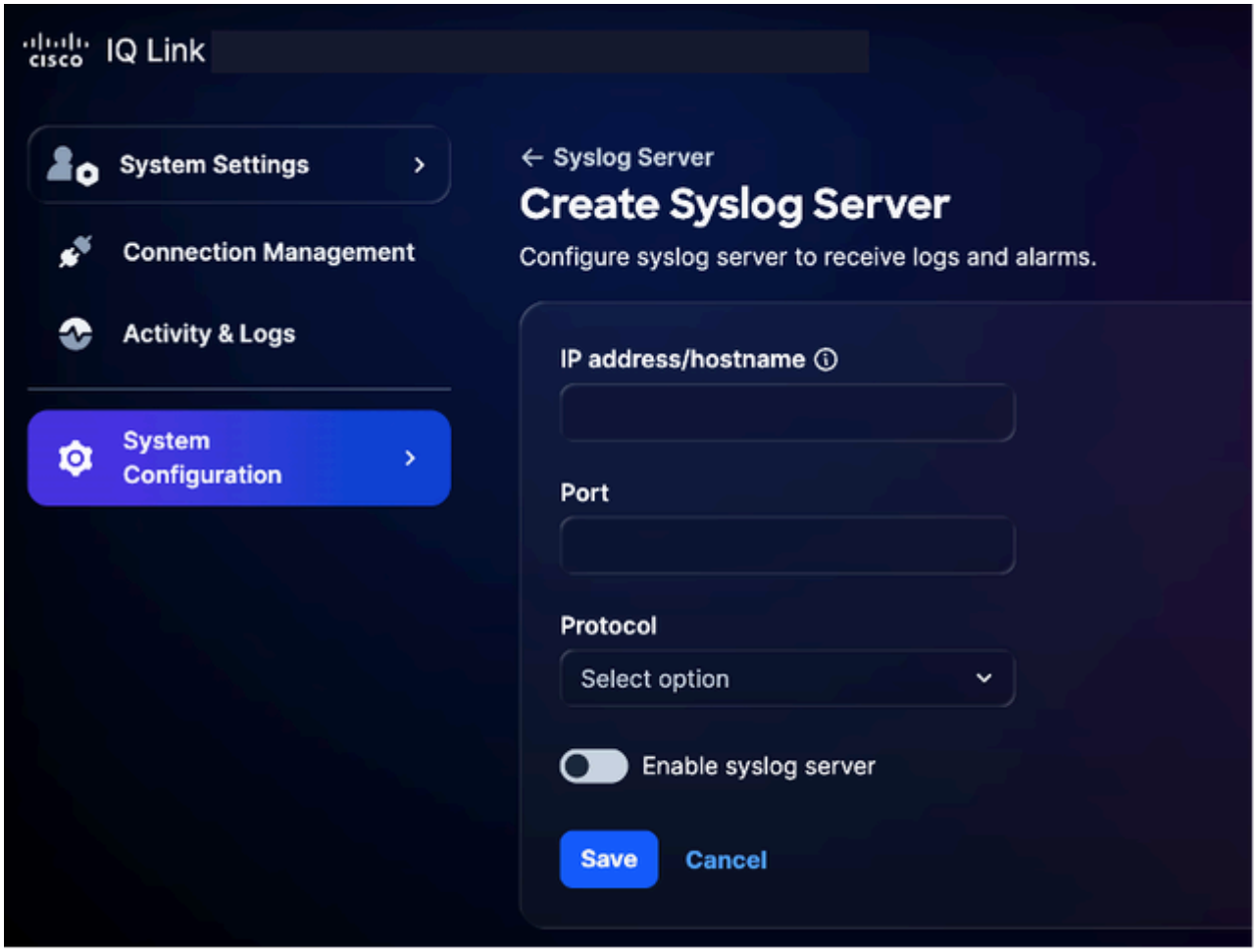
Para adicionar um Servidor syslog:

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

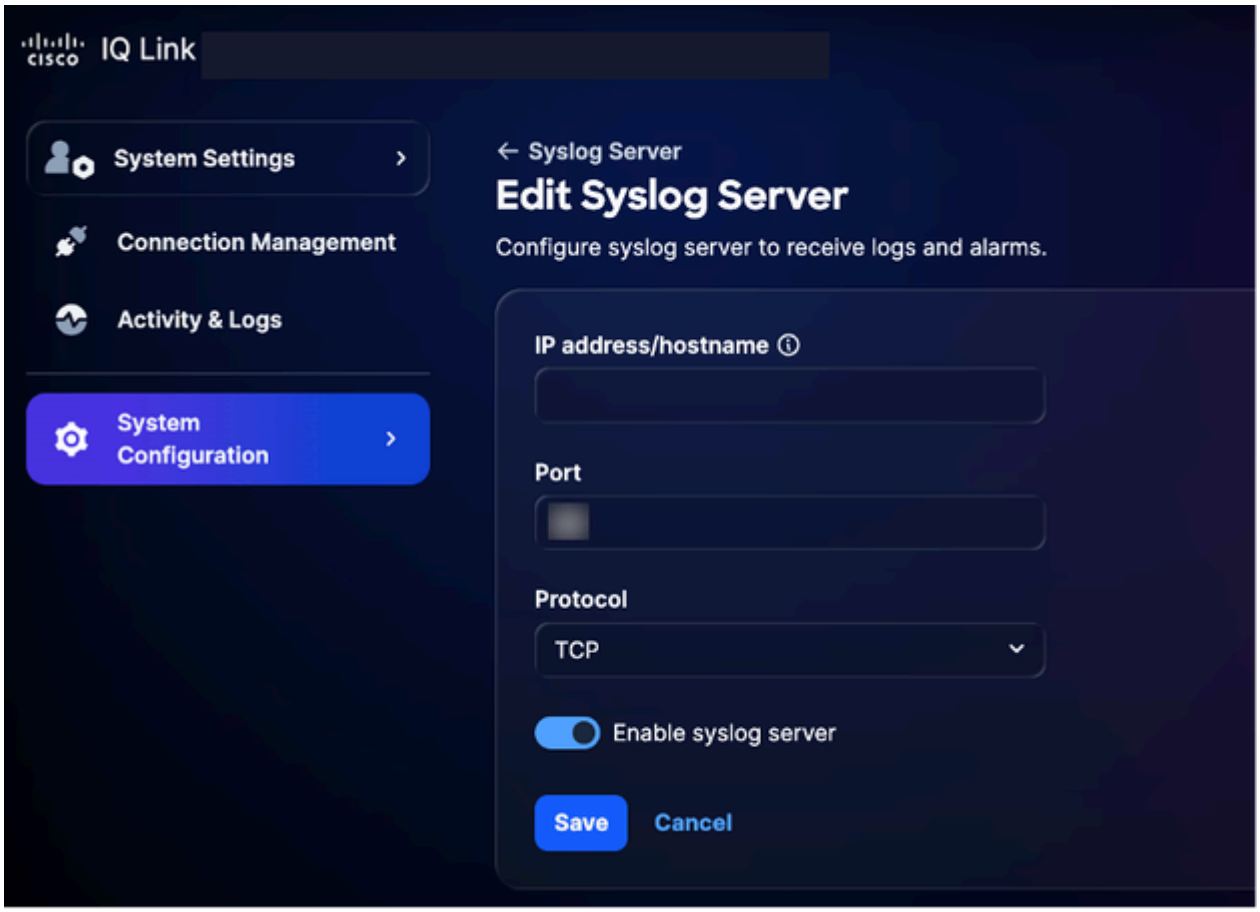
3. Insira o endereço IP/nome do host.

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.



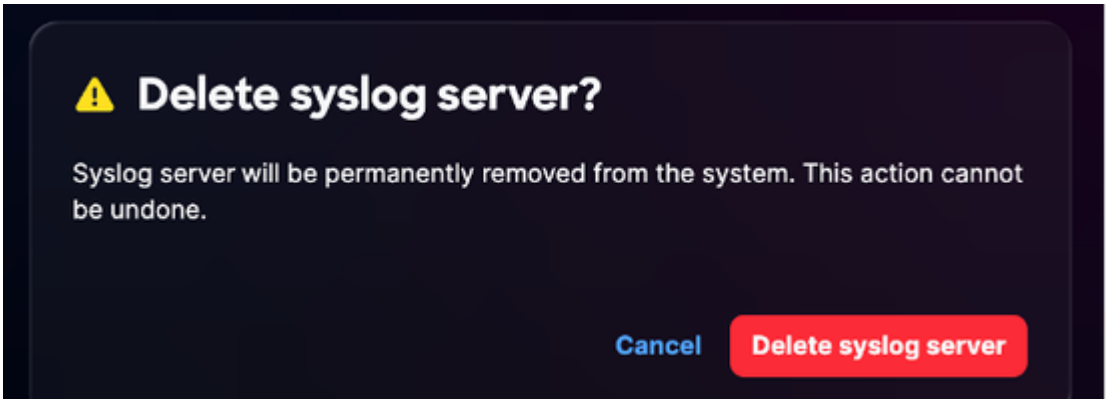

Editar Servidor Syslog

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.

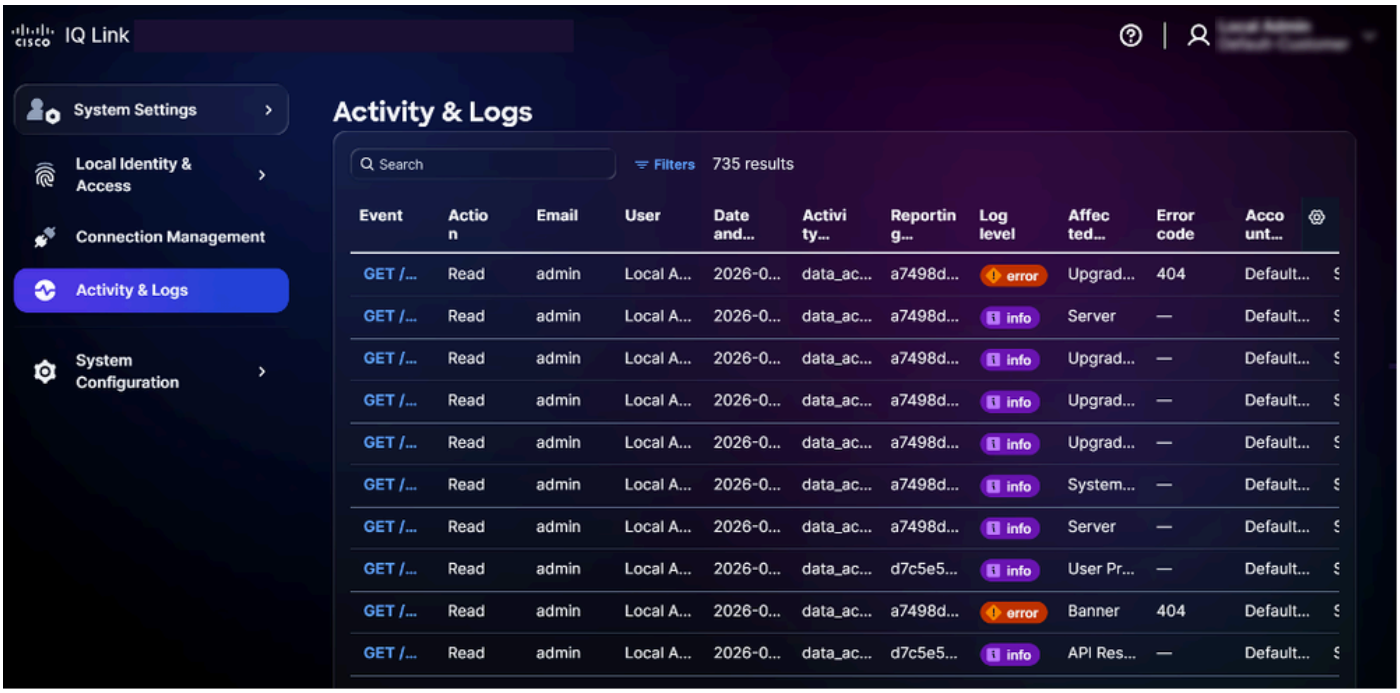



Confirmação

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 de conta 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:

- Oferece suporte a filtros, paginação e recursos de pesquisa para ajudar a localizar e gerenciar informações com facilidade
- Registra todas as operações de API no nível do gateway

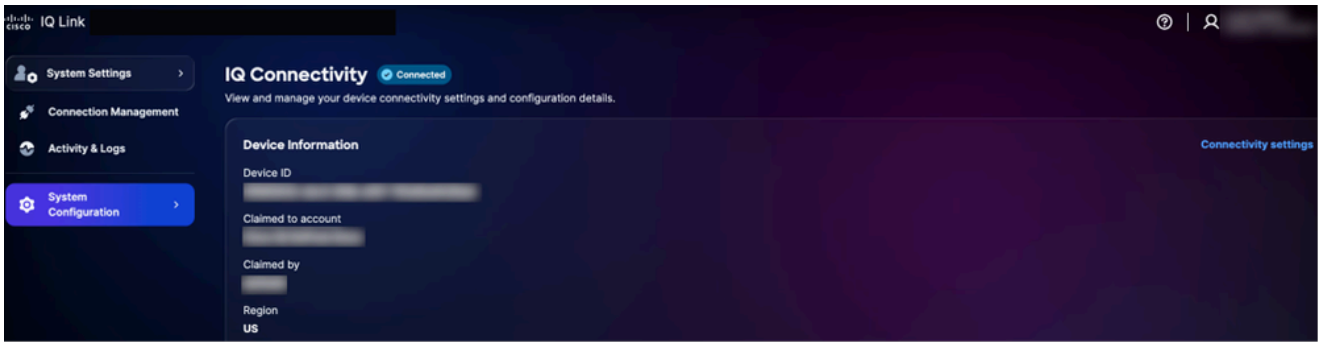
As seguintes opções de filtro estão disponíveis:

- 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

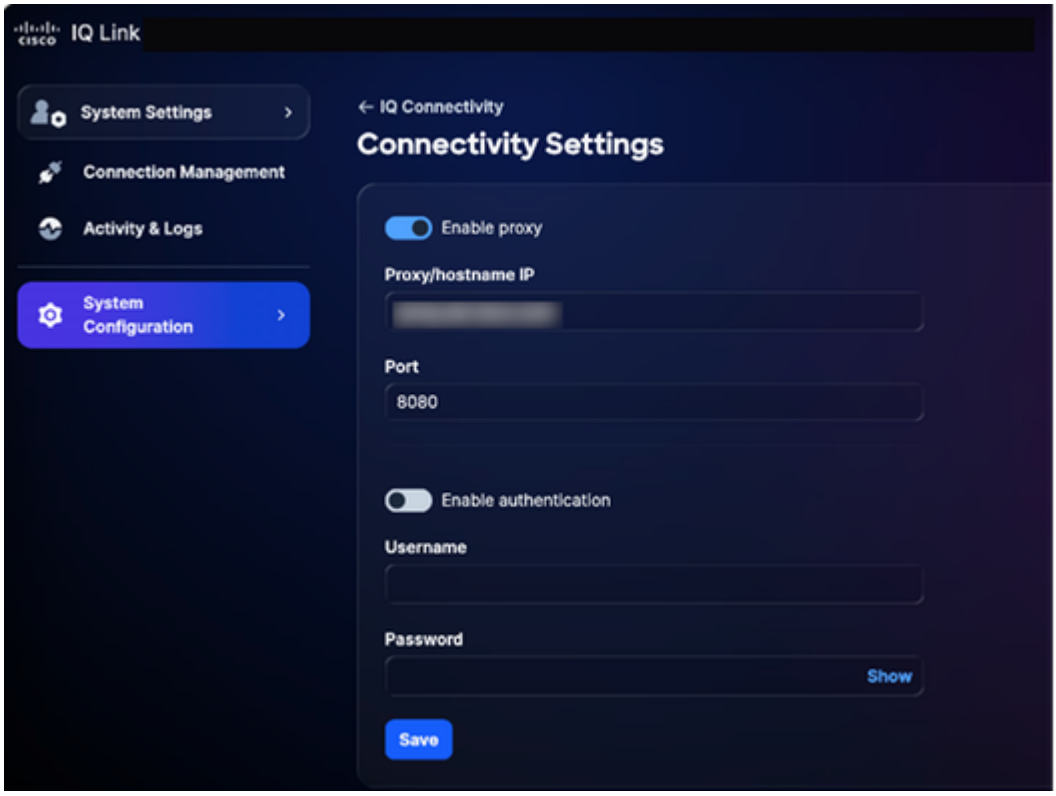
Para exibir e gerenciar as definições de conectividade do dispositivo e os detalhes de configuração:

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 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 está resumida abaixo:

- Criando conjuntos de credenciais: Estabeleça os protocolos de autenticação (por exemplo, SNMP (Simple Network Management Protocol) 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.

---

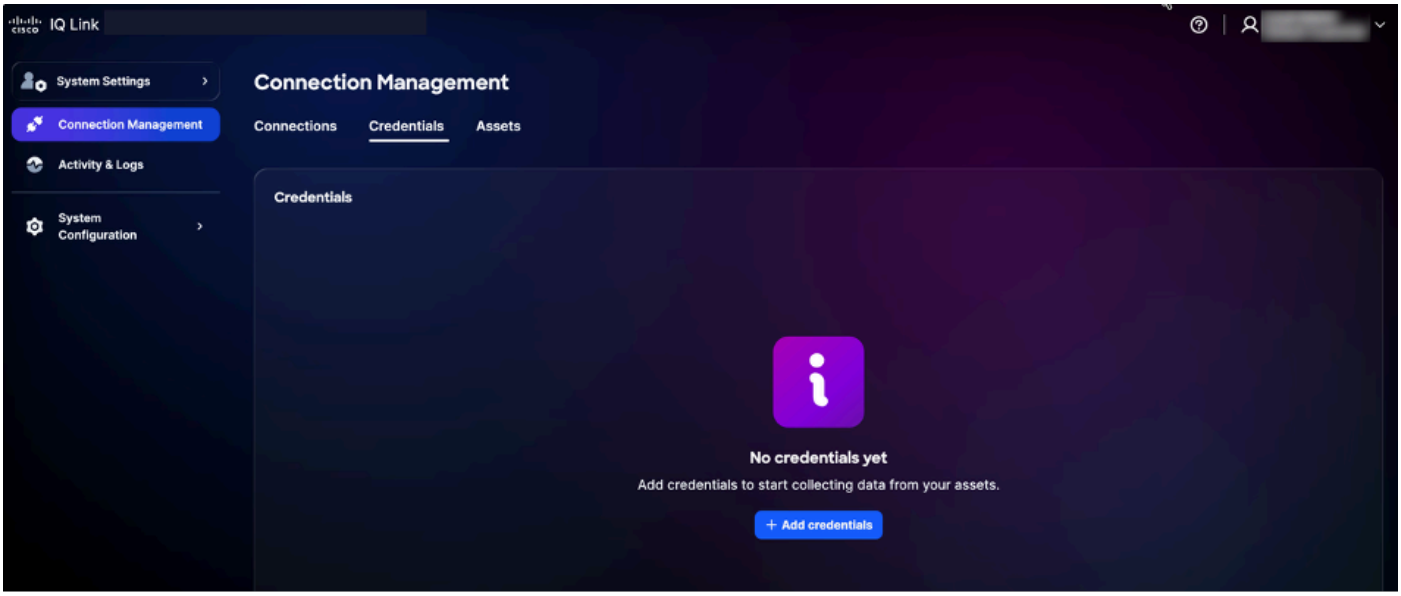
Note: O SNMPv2c/SNMPv3 e o SSH são necessários para a descoberta de dispositivos, e as credenciais HTTP/HTTPS devem ser fornecidas antes da configuração do Catalyst Center.

---

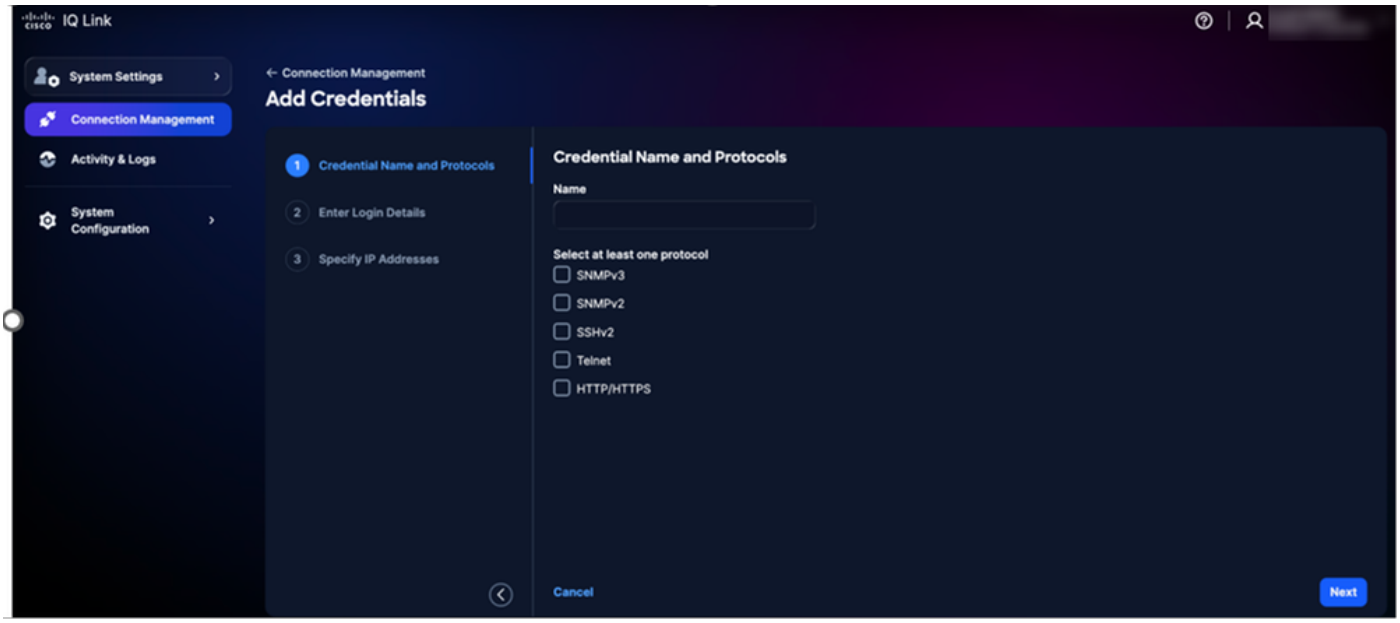
## Adicionando credenciais

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.



3. Clique em Adicionar credenciais.

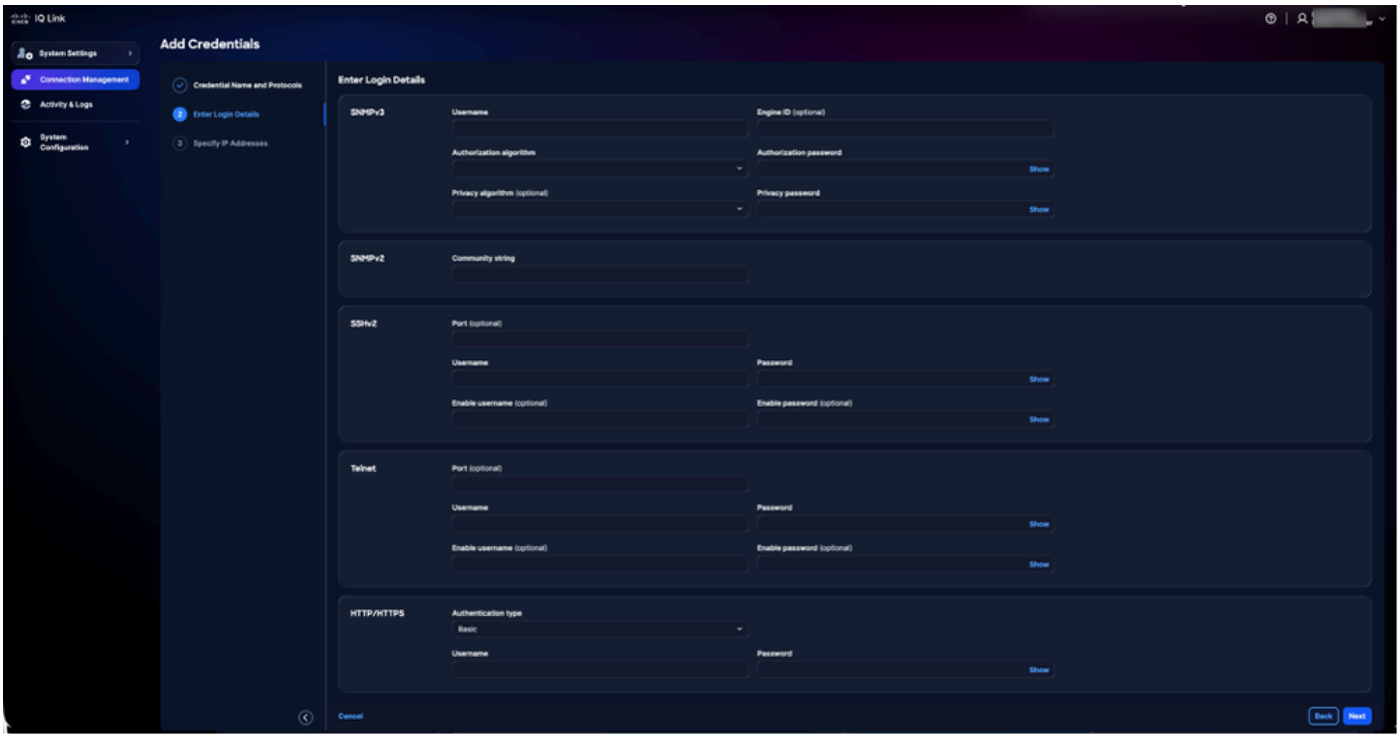



Adicionar Credenciais

4. Informe Nome.

5. Marque todas as caixas de seleção de protocolo aplicáveis.

6. Clique em Próximo.

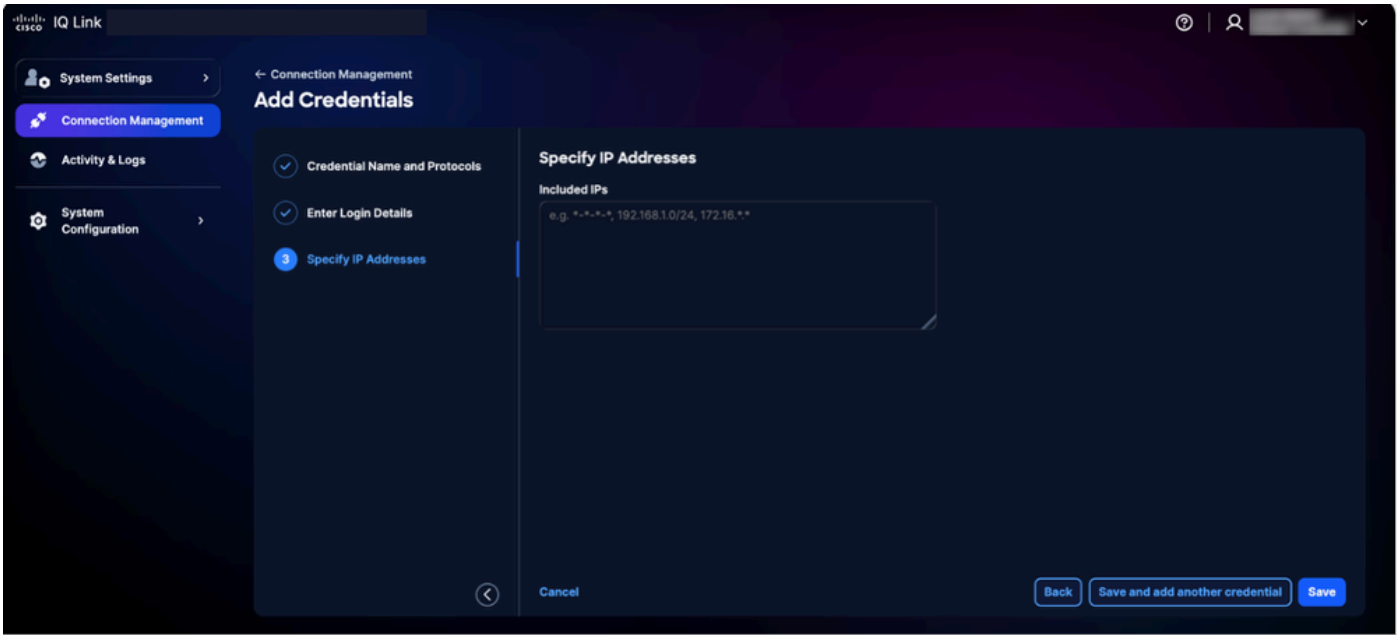



Adicionar detalhes de credenciais

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

7. Informe os detalhes de login para cada protocolo selecionado.

8. Clique em Próximo.

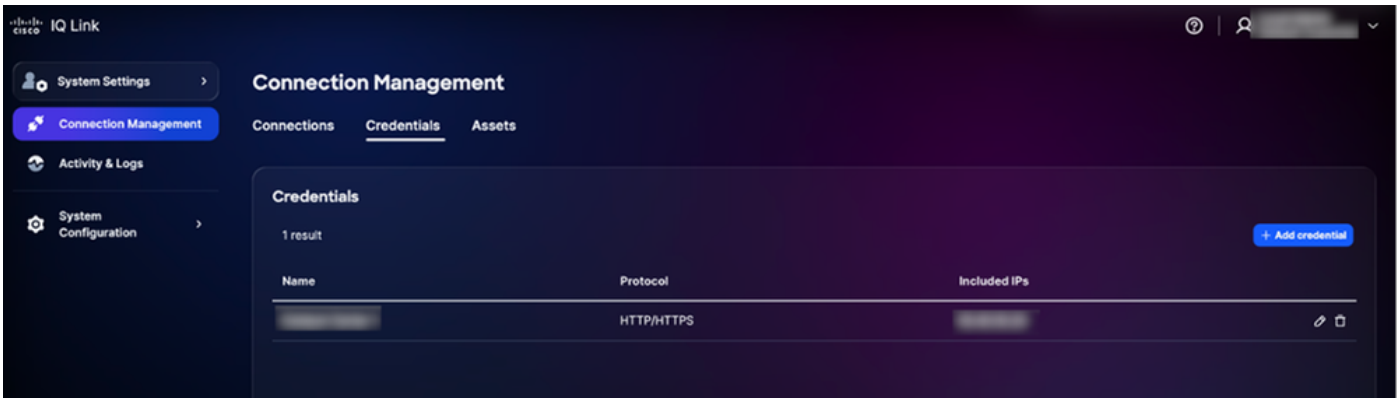



Especificar Endereços IP

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. Clique em Salvar. 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)

  Curingas 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.

Tabela 13: 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) |
| 10.10.2.15 | 10.10.2., 10.10.* | 10.10.2.* (Mais específico) |
| 10.10.5.50 | 10.10..., ... | 10.10.. (Mais específico) |

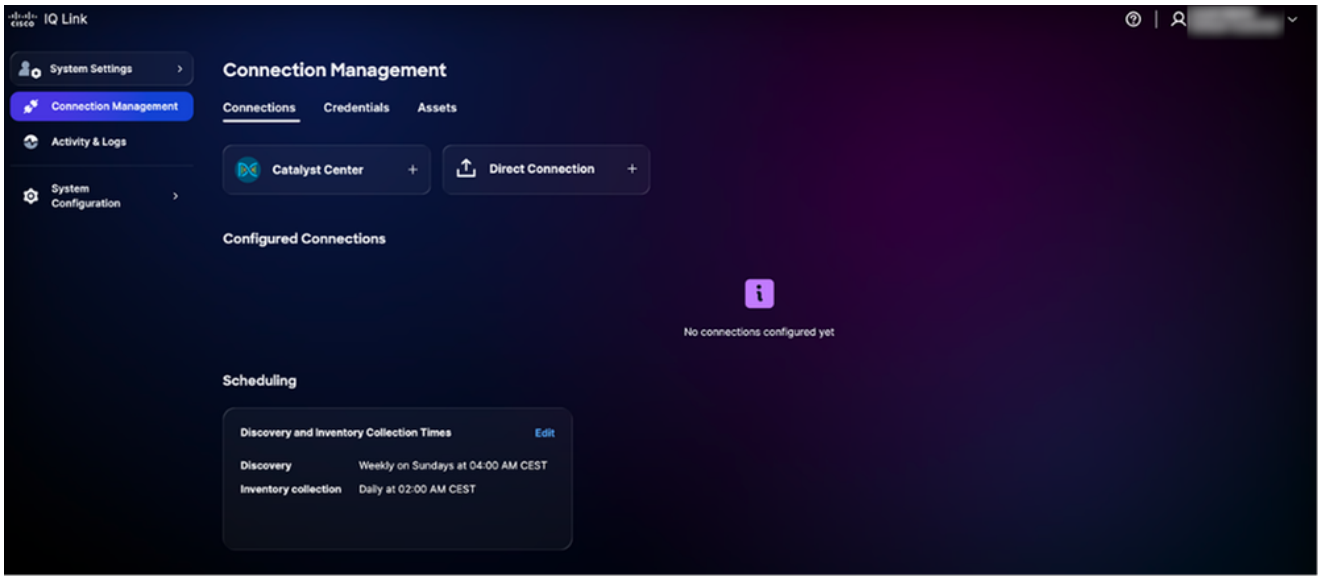
Note: Se um dispositivo se enquadra em várias categorias sobrepostas, o sistema sempre seleciona o conjunto de credenciais com a especificidade mais alta (em outras palavras, o menor número de curingas à direita).

## Coleta de dados usando o Catalyst Center

Você pode conectar até 20 Centros Catalyst (não cluster) para cada instância do Cisco IQ Link.

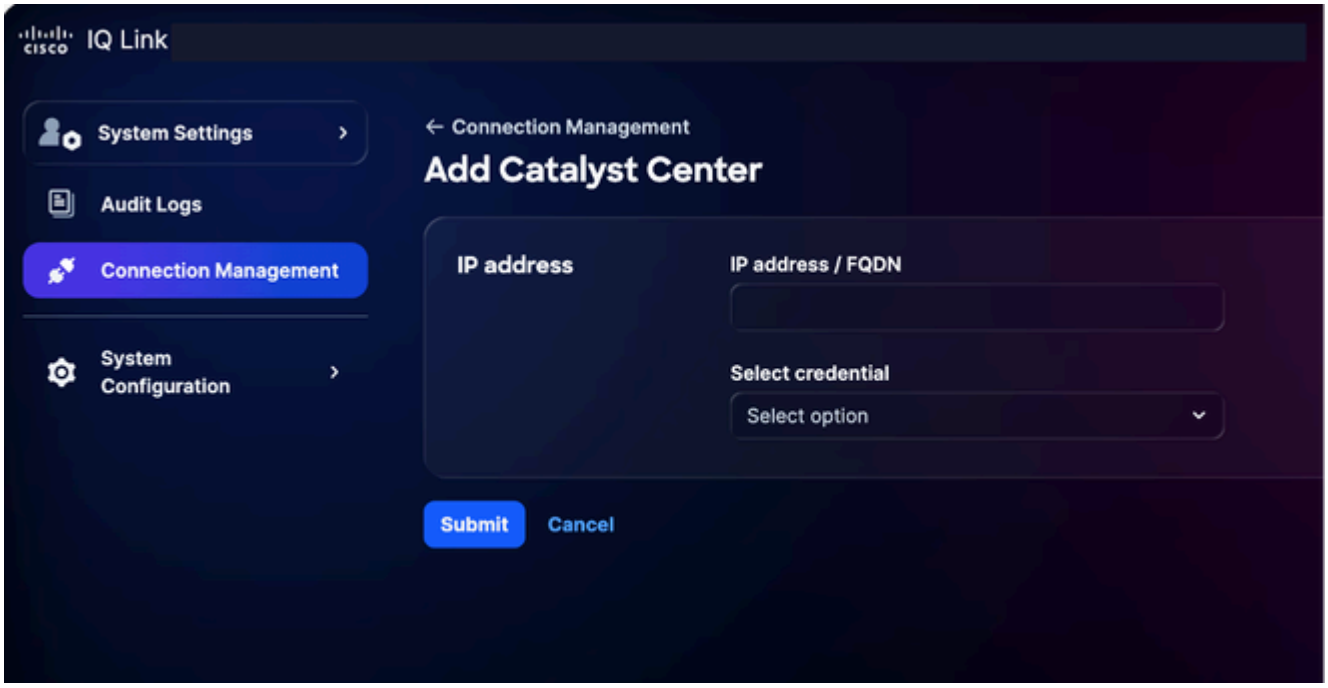
Para coleta de dados usando o Catalyst Center:

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



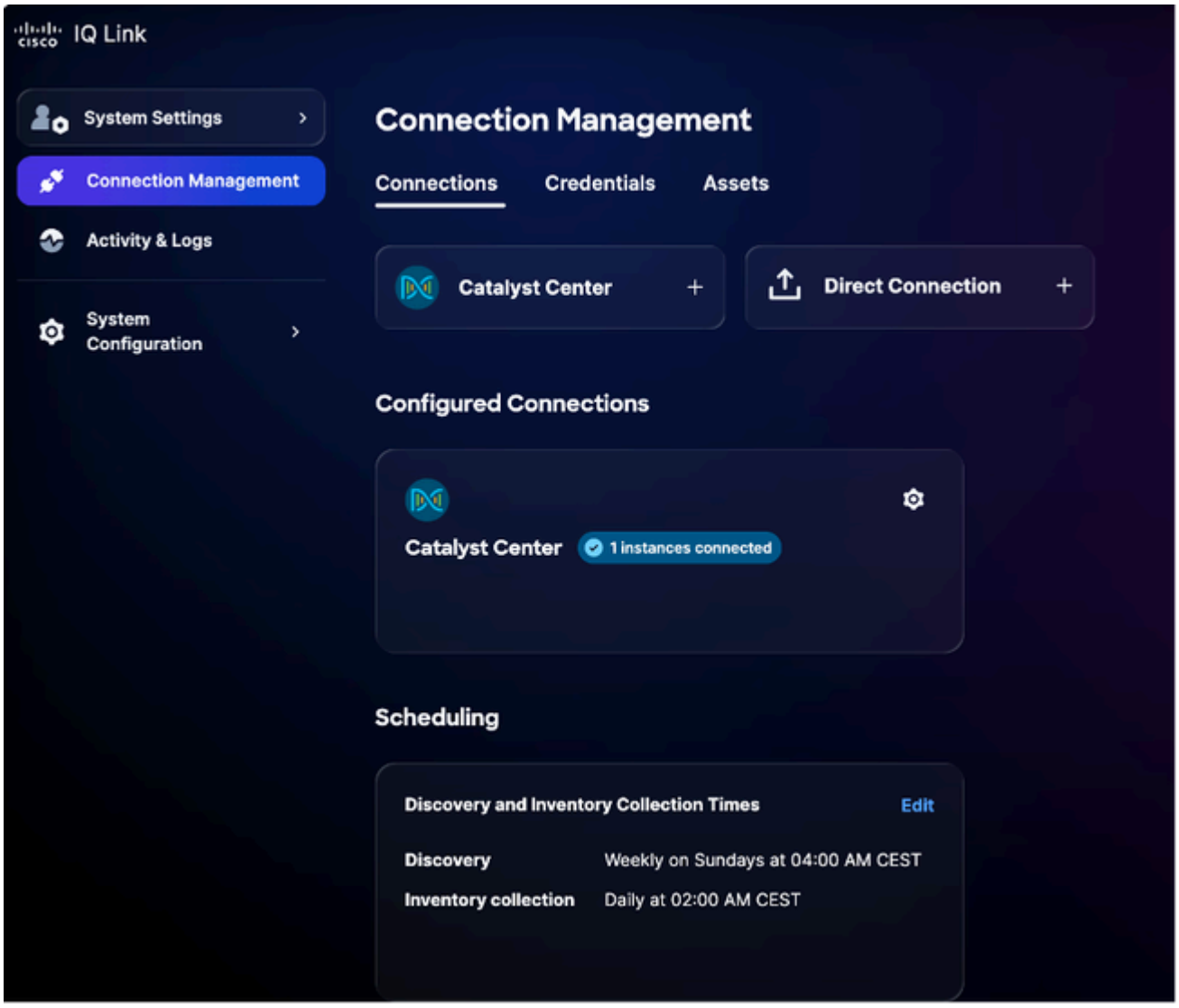

Gerenciamento de conexões

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.

---

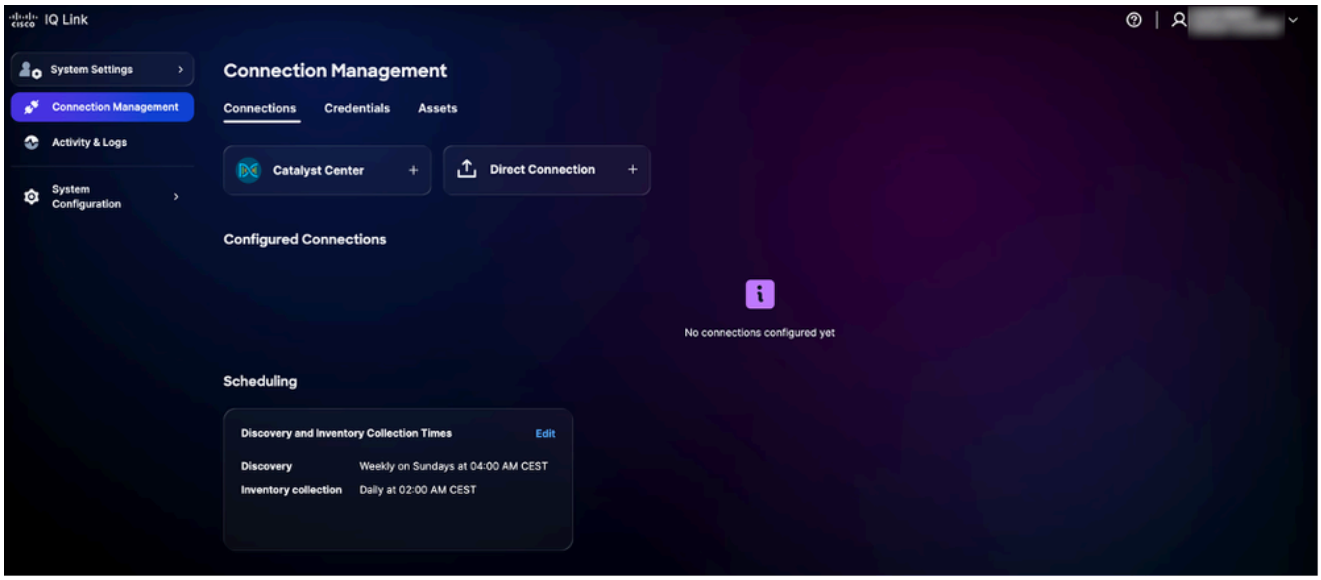
Note: O Cisco IQ Link é pré-configurado com uma configuração de programação automatizada e o sistema inicia uma programação de coleta automatizada padrão. É altamente recomendável que você edite o agendamento para alinhá-lo aos requisitos e janelas de manutenção da sua organização.

---

## Conexão direta

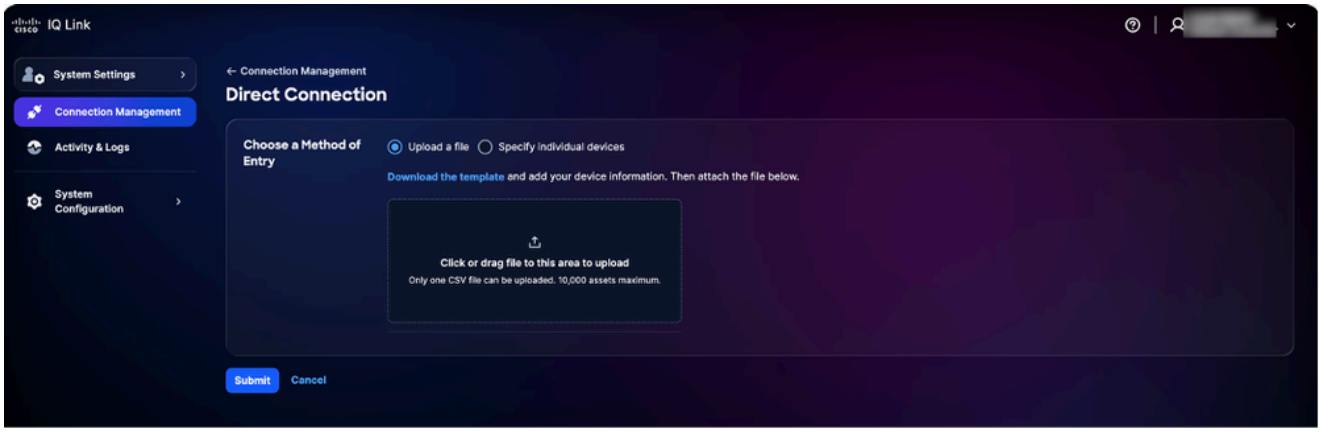
Para adicionar dispositivos para conexão direta:

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



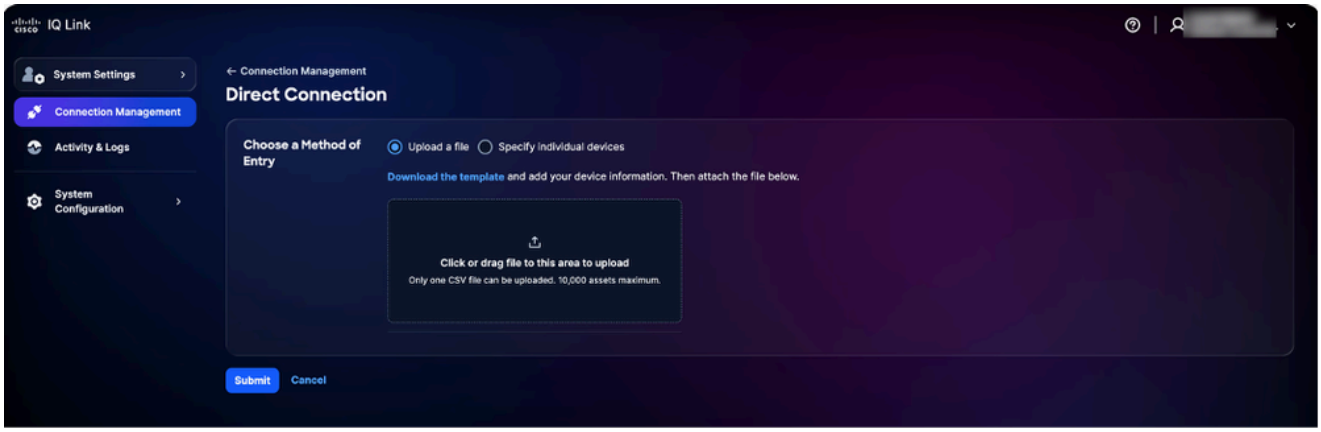

Gerenciamento de conexões

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



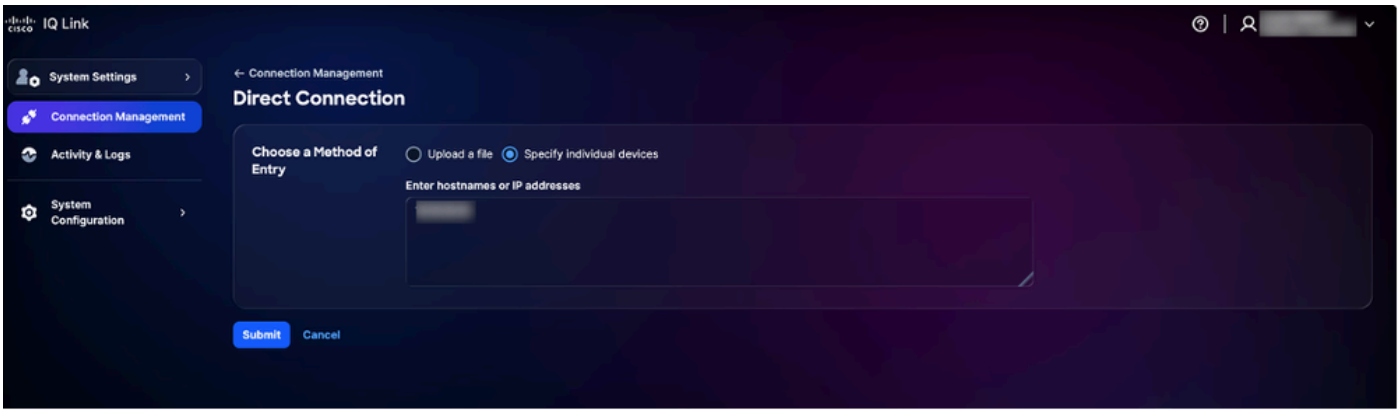

Carregar arquivo

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. Programe uma coleta. Consulte Agendamento para obter mais detalhes.

---

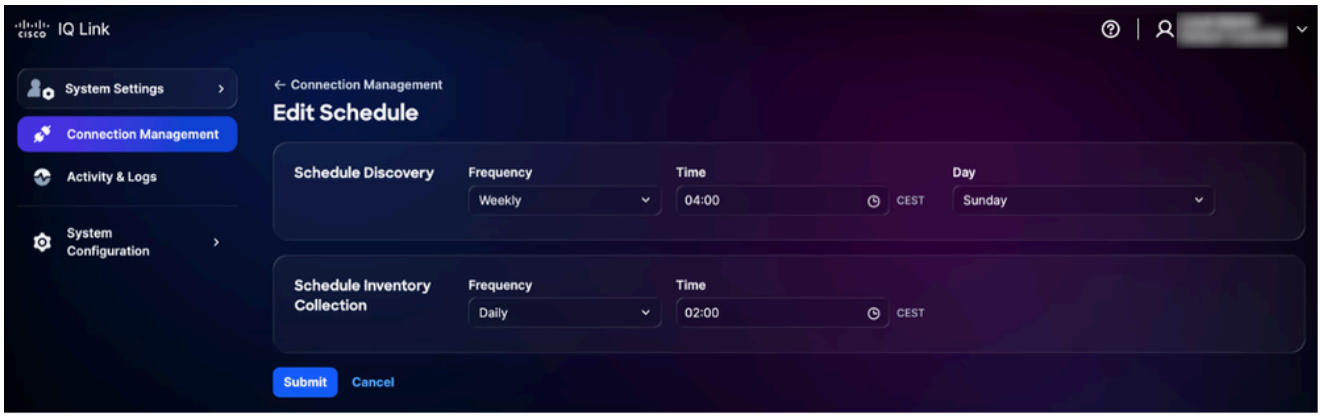
Note: O Cisco IQ Link é pré-configurado com uma configuração de programação automatizada e o sistema inicia uma programação de coleta automatizada padrão. É altamente recomendável que você edite o agendamento para alinhá-lo aos requisitos e janelas de manutenção da sua organização.

---

## 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

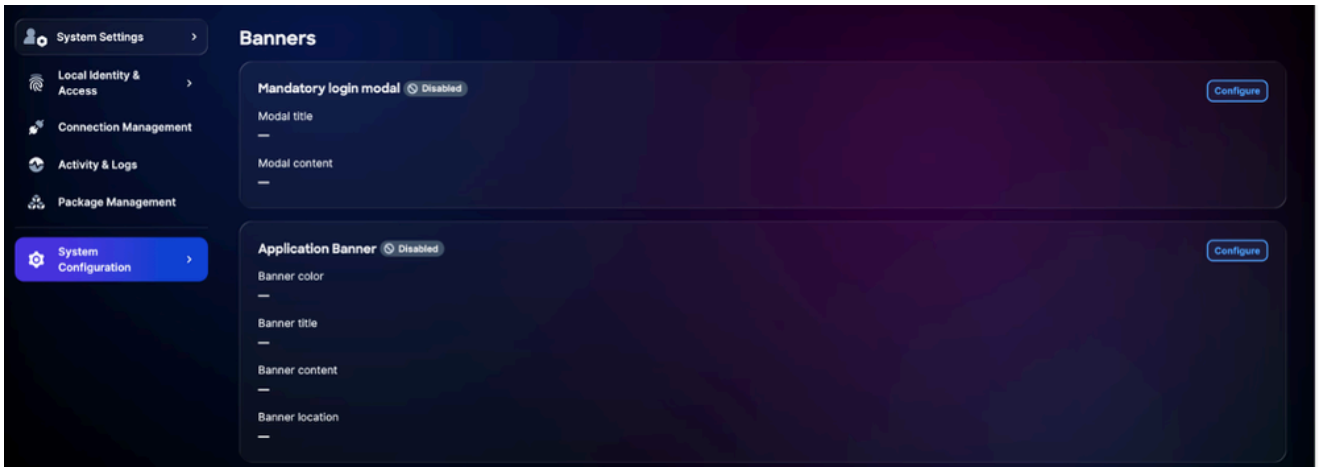
Os administradores de conta podem configurar banners de todo o sistema para atender aos padrões de segurança e conformidade.

- Login obrigatório modal: Você deve confirmar o banner obrigatório antes de prosseguir para a tela de login.
- Banners de aplicativos: São banners personalizados que são exibidos no aplicativo após a autenticação bem-sucedida.

## Configurando banners modais de login obrigatórios

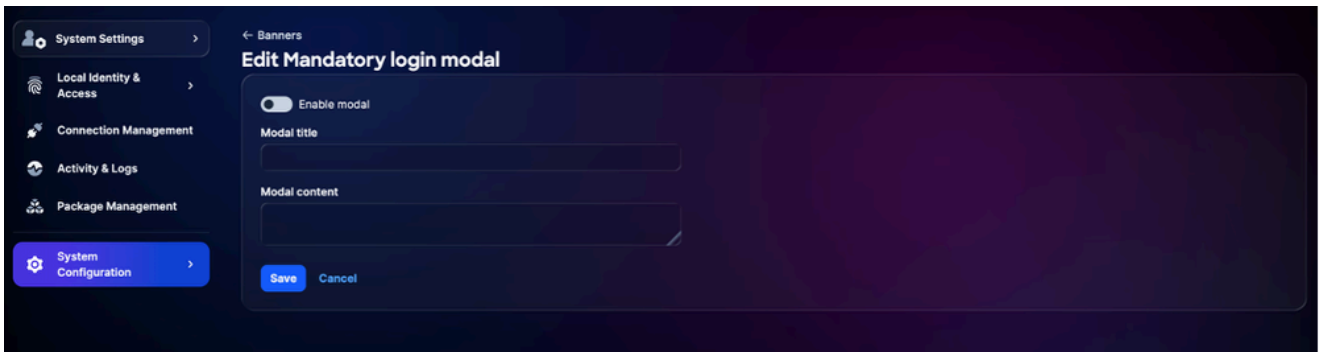
Para configurar um banner obrigatório:

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




Configurar banner obrigatório

2. Clique em Configurar no modal de login obrigatório. A página Editar modal de login obrigatório é exibida.



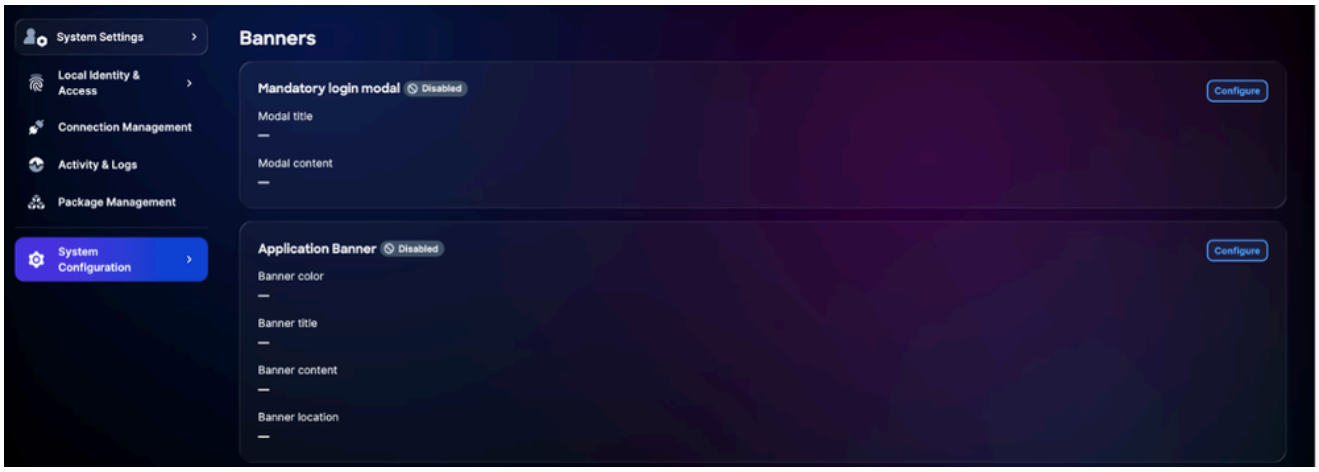

Editar banner modal de login obrigatório

3. Clique no botão de alternância para ativar ou desativar o banner.
4. Insira o título Modal.
5. Insira o conteúdo Modal.
6. Click Save. O modal de login obrigatório é salvo.

## Configurando banners de aplicativos

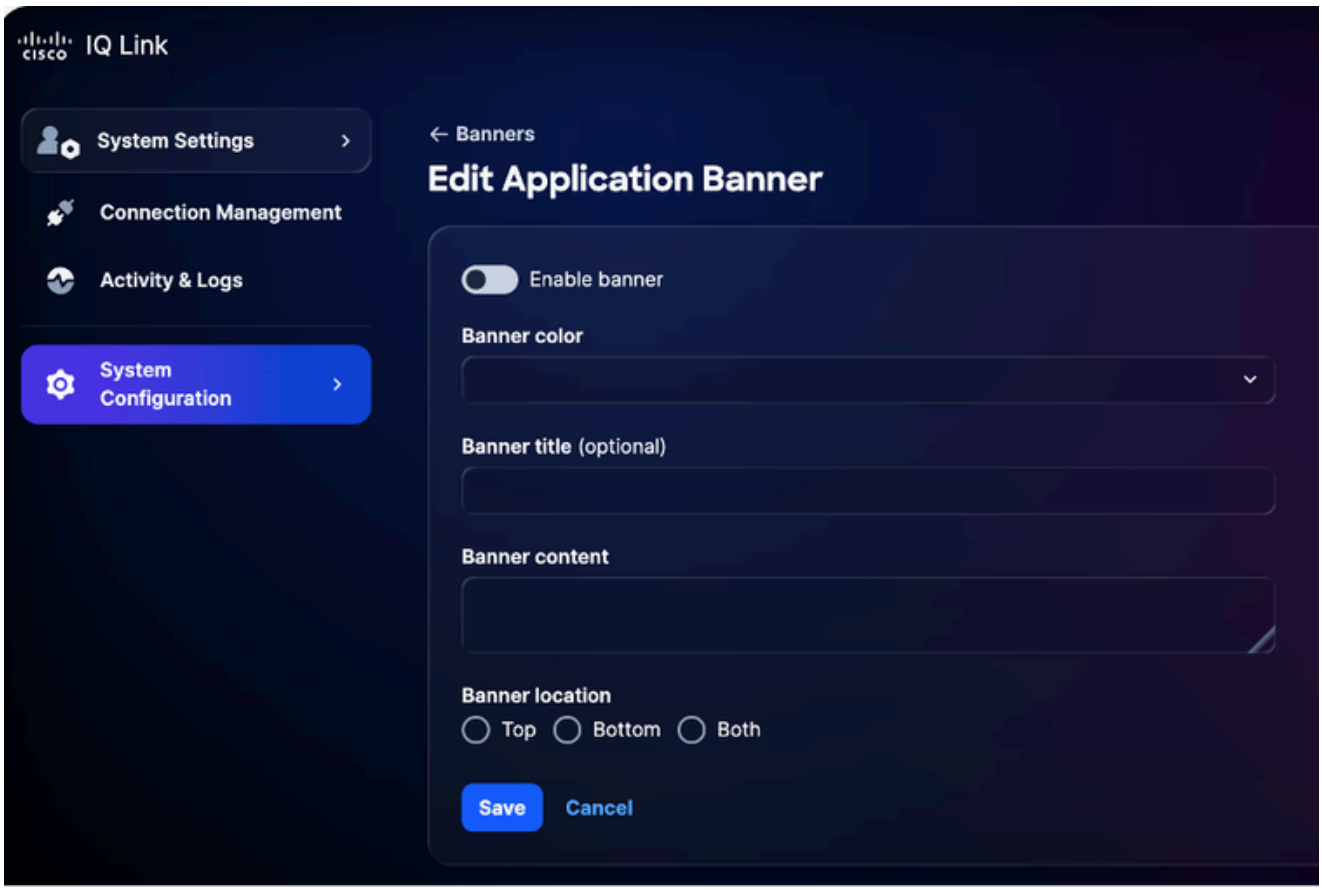
Para configurar um banner de aplicativo:

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




Configurar banner

2. Clique em Configurar no banner do aplicativo. 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.

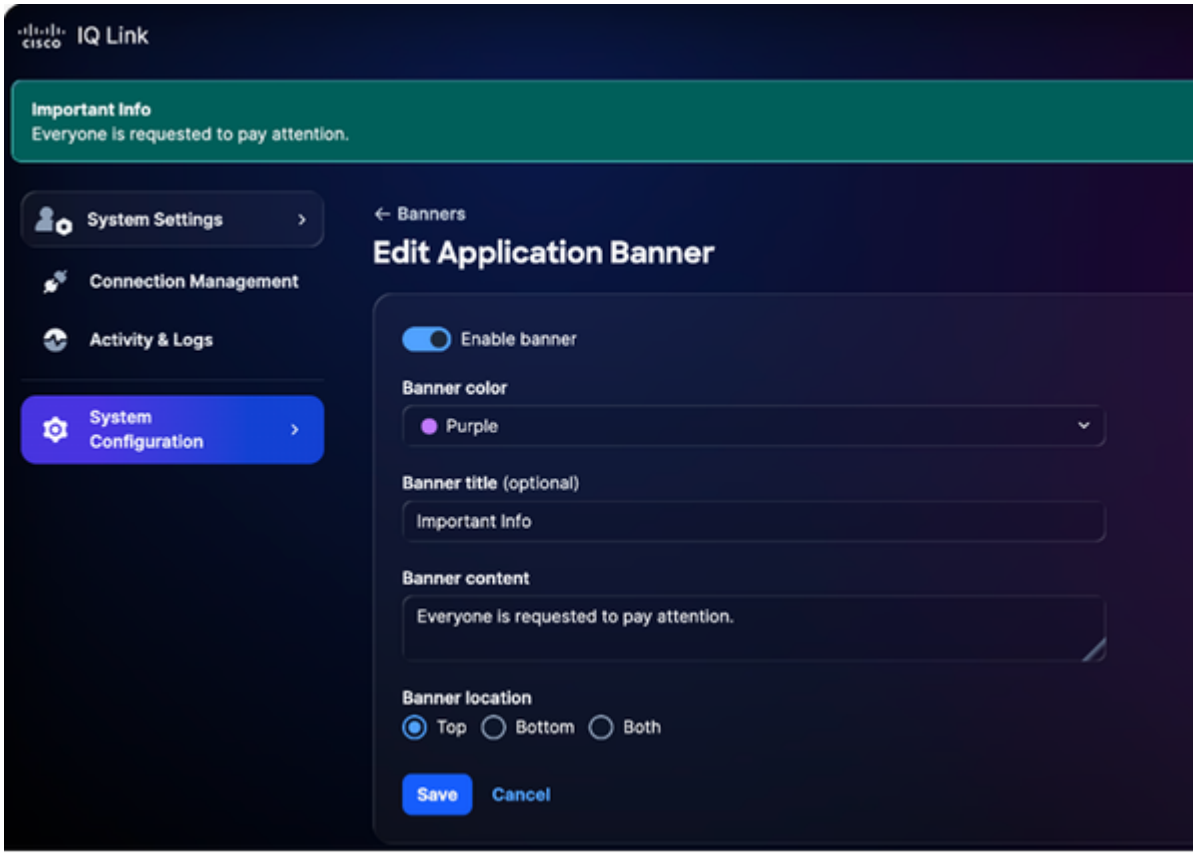
7. Selecione um local de banner.
8. Click Save. O banner é exibido no aplicativo.

## Editando banners

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


Editar banner do aplicativo

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

Você pode coletar arquivos de diagnóstico e de log 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:

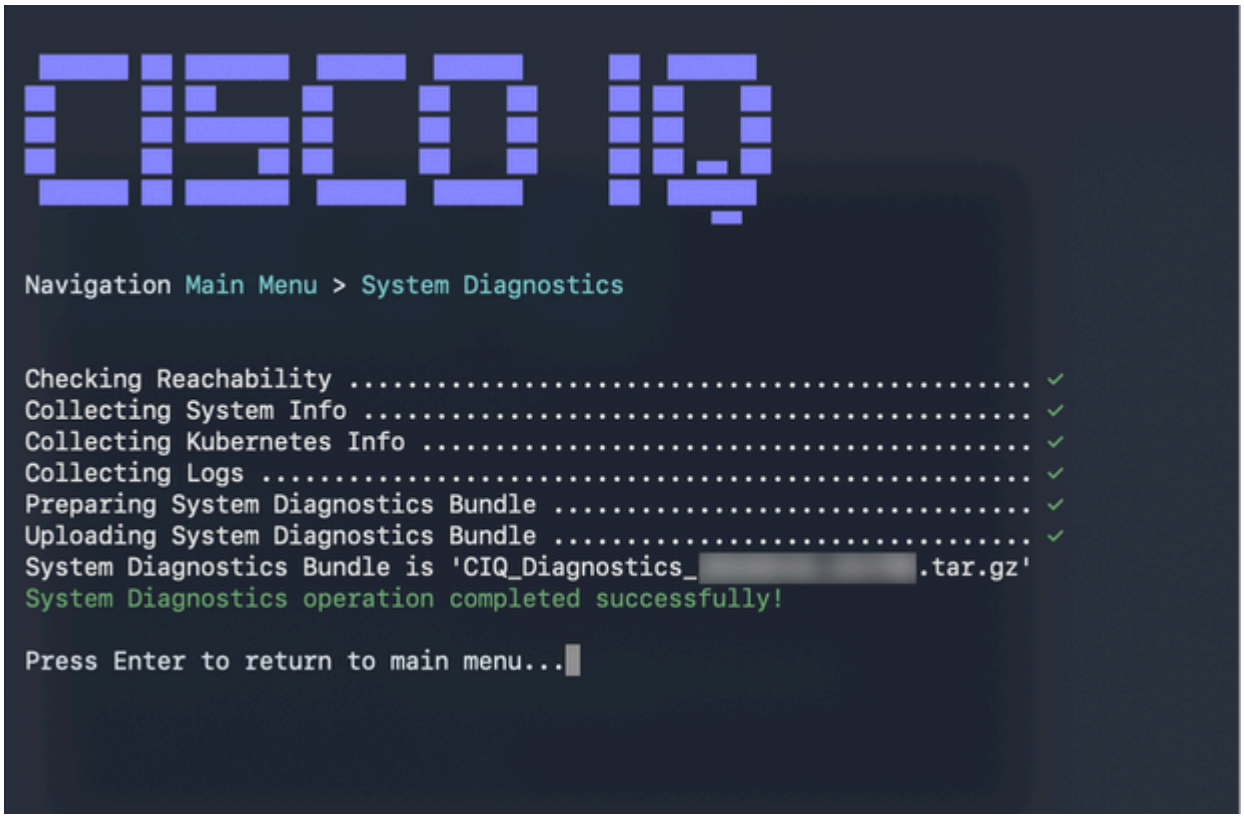
1. Faça login no Cisco IQ.


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 Concluída

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.