

Guia de operações do Cisco IQ Virtual Appliance v1.2.0

Introdução

O Cisco IQTM 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 Cisco IQ AI Assistant, otimizam os resultados operacionais e a experiência do usuário do Cisco IQ, fornecendo entendimento contextual que capacita você a tomar decisões proativas e informadas e simplificar processos para o envolvimento e o sucesso do cliente.

O Cisco IQ On-Prem Air-Gapped é um dos modos de implantação do Cisco IQ, projetado para clientes em setores altamente regulamentados com requisitos rigorosos de conformidade, domínio sobre dados e segurança. Nesse modo, o Cisco IQ é fornecido como uma máquina virtual (VM) independente, conhecida como Cisco IQ Virtual Appliance (VA). O VA é executado inteiramente nas instalações do cliente e opera em total isolamento de redes externas. Para manter esse isolamento, as atualizações de software e os pacotes de manutenção são obtidos do Cisco IQ SaaS e transferidos para o VA por meio de um processo aprovado e manual.

O Cisco IQ On-Prem Air-Gapped estende os principais recursos do Cisco IQ SaaS para ambientes com isolamento térmico, permitindo que equipes de missão crítica operem com velocidade e inteligência de diagnóstico comparáveis às empresas conectadas em nuvem.

Para acessar o Cisco IQ VA, abra um navegador compatível e navegue até <https://<fqdn-of-the-appliance>>. Faça login usando o nome de usuário e a senha do administrador definidos durante o processo de instalação.

 **Note:** O Cisco IQ VA está atualmente limitado a clientes inscritos no programa de disponibilidade controlada. O acesso de download para o software do sistema VA e pacotes operacionais adicionais (módulos, regras e direitos) do portal Cisco IQ está disponível exclusivamente para clientes selecionados. Entre em contato com seu representante de conta para obter mais informações.

Gerenciamento de Conexões (Coleta de Dados)

O Cisco IQ VA é uma solução local para coleta de dados de rede 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 consiste em:

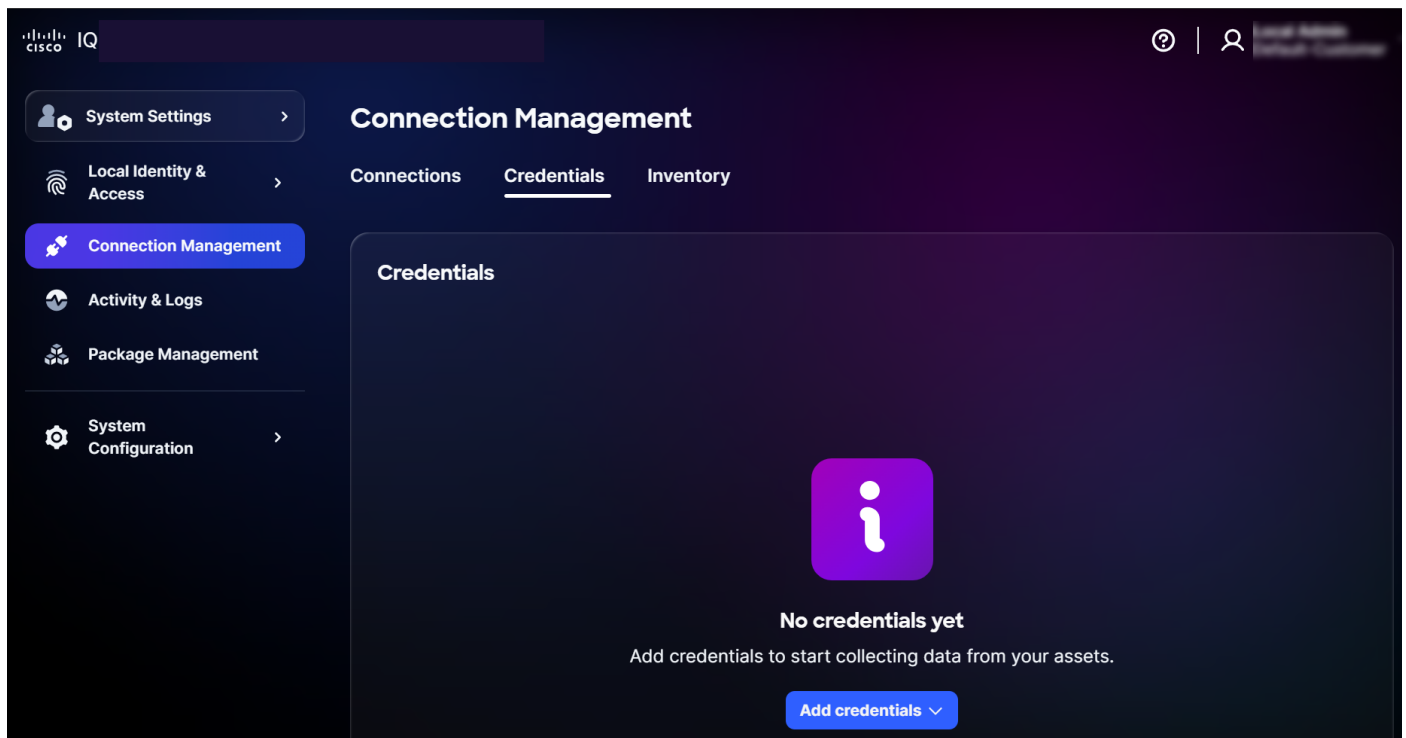
- Criando conjuntos de credenciais: Estabeleça os protocolos de autenticação (por exemplo, SNMP (Simple Network Management Protocol) v1/v2c/v3) para se comunicar com seus dispositivos de rede. A centralização de credenciais por zona de segurança ou local (por exemplo, "SanJose-SNMPv3") permite que você 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

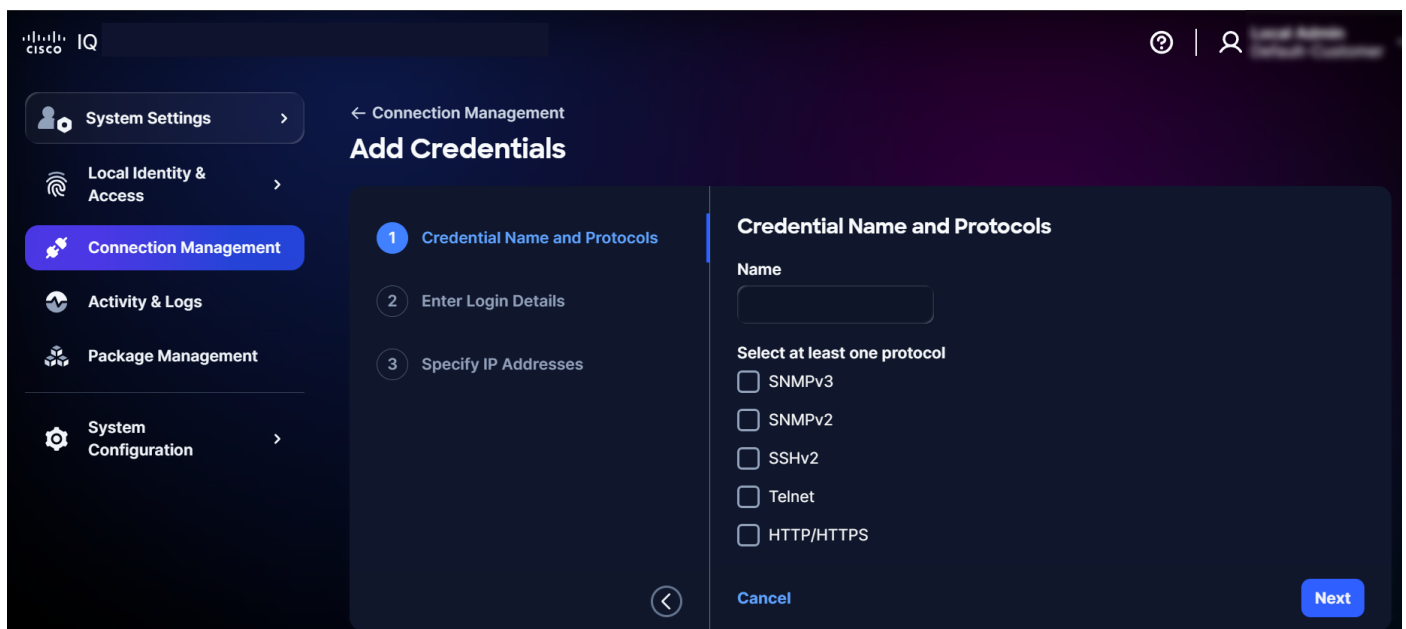
Primeiro você deve adicionar credenciais para executar a coleta de dados. Para adicionar credenciais:

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



Guia Credenciais

3. Clique em Adicionar credenciais.



Adicionar Credenciais

4. Insira um Nome.

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

6. Clique em Next.

Add Credentials

1. Credential Name and Protocols

2. Enter Login Details

3. Specify IP Addresses

SNMPv3

Username

Engine ID (optional)

Authorization algorithm

Authorization password [Show](#)

Privacy algorithm (optional)

Privacy password (optional) [Show](#)

[Cancel](#) [Back](#) [Next](#)

Adicionar detalhes de credenciais



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

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

8. Clique em Next.

Add Credentials

1. Credential Name and Protocols

2. Enter Login Details

3. Specify IP Addresses

Specify IP Addresses

Included IPs

e.g. *-*-*, 192.168.1.0/24, 172.16.*.*

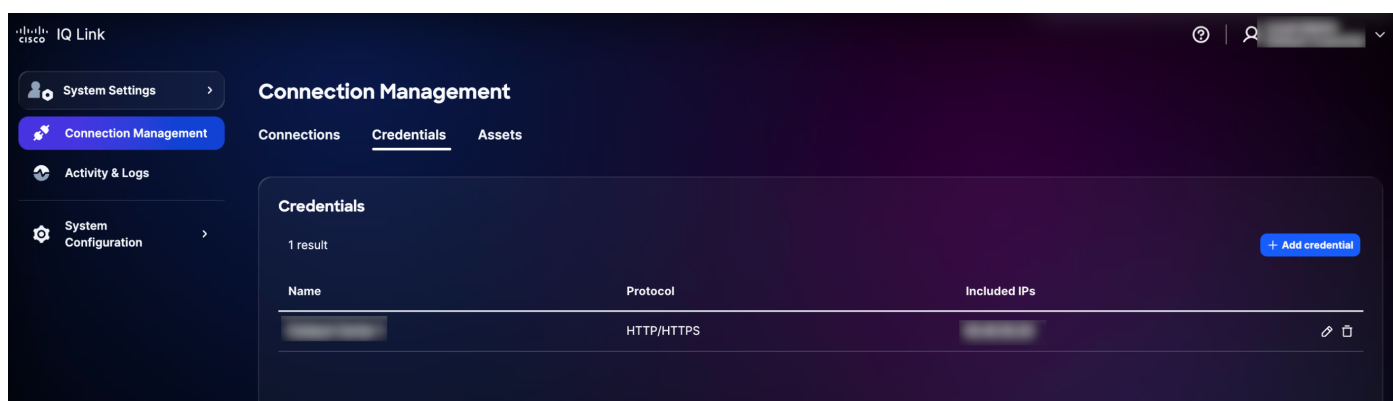
[Cancel](#) [Back](#) [Save and add another credential](#) [Save](#)

Especificar Endereços IP

9. Insira os IPs incluídos.

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

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



Credenciais Adicionadas

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

Seleção de Credencial e Lógica de Correspondência

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

- Classificação de prioridade: Quando vários conjuntos de credenciais se aplicam a um dispositivo, o Cisco IQ os avalia com base em como eles correspondem especificamente ao dispositivo; o sistema aplica a seguinte prioridade, com correspondências mais específicas tendo precedência:
 - Correspondência de IP exata: Prioridade mais alta
 - Correspondência Curinga à Direita: A prioridade depende do número de estrelas à direita; menos estrelas indicam uma correspondência mais específica e, portanto, maior prioridade

- Regras de Formatação Curinga: Caracteres curinga (*) são suportados apenas como caracteres à direita em um endereço IP; elas devem ser aplicadas da direita para a esquerda.
 - Formatos suportados:
 - 1.2.3.* (prioridade máxima)
 - 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 1: 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)

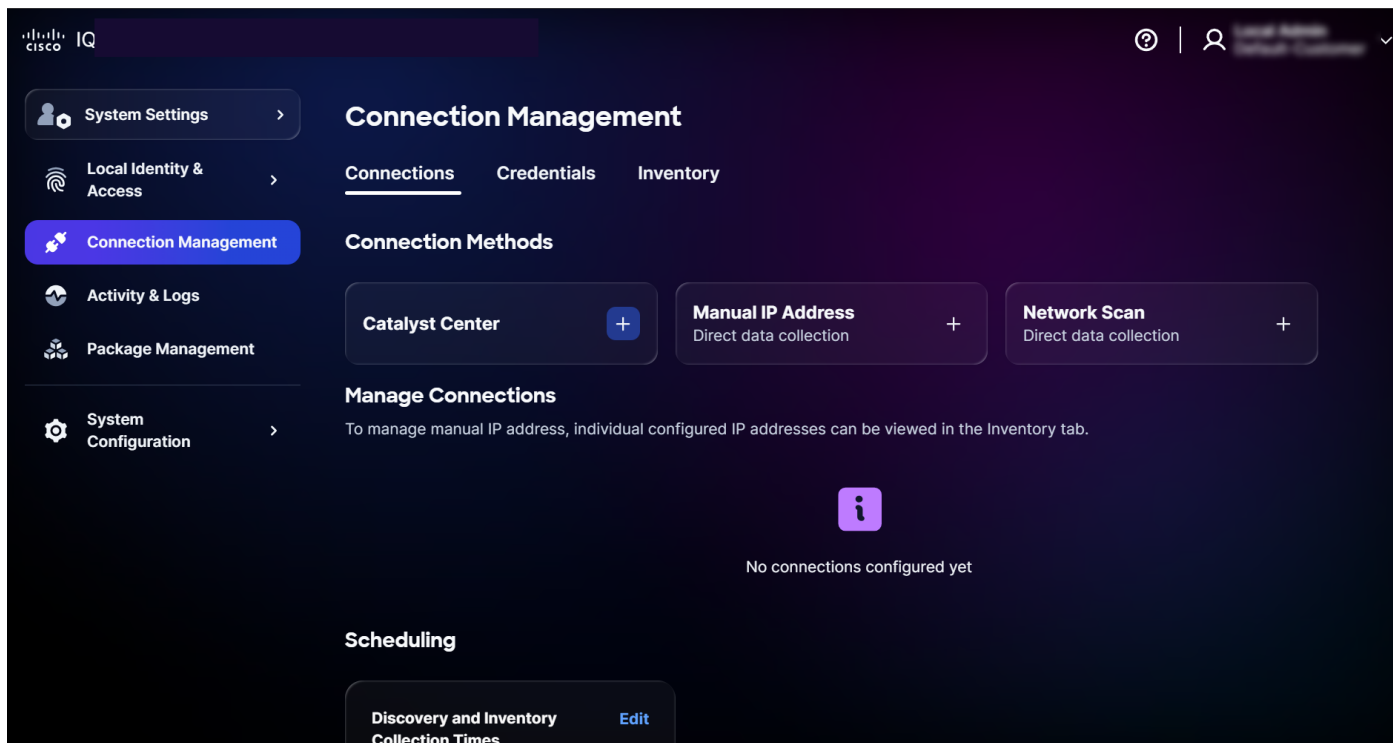
 Note: Se um dispositivo se enquadra em várias categorias sobrepostas, o sistema sempre seleciona o conjunto de credenciais com a especificidade mais alta (em outras palavras, o menor número de curingas à direita).

Coleta de dados usando o Catalyst Center

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

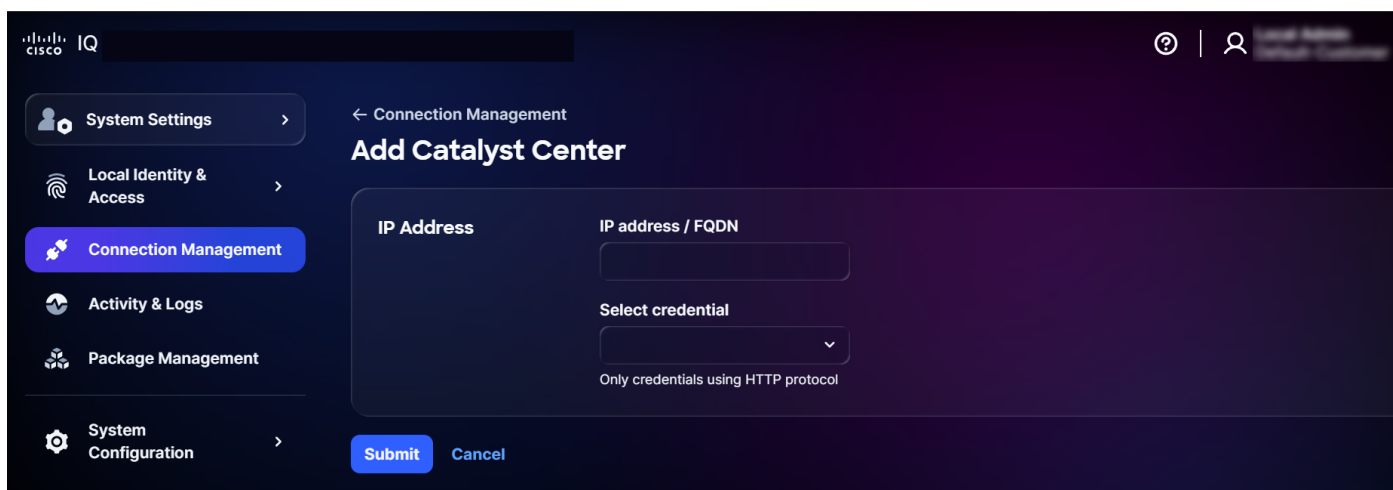
Para coleta de dados usando o Catalyst Center:

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 Selecionar credencial.
5. Clique em Submit. Uma confirmação é exibida (pode levar até 75 minutos). Você pode exibir o Catalyst Center recém-adicionado em Conexões Configuradas.

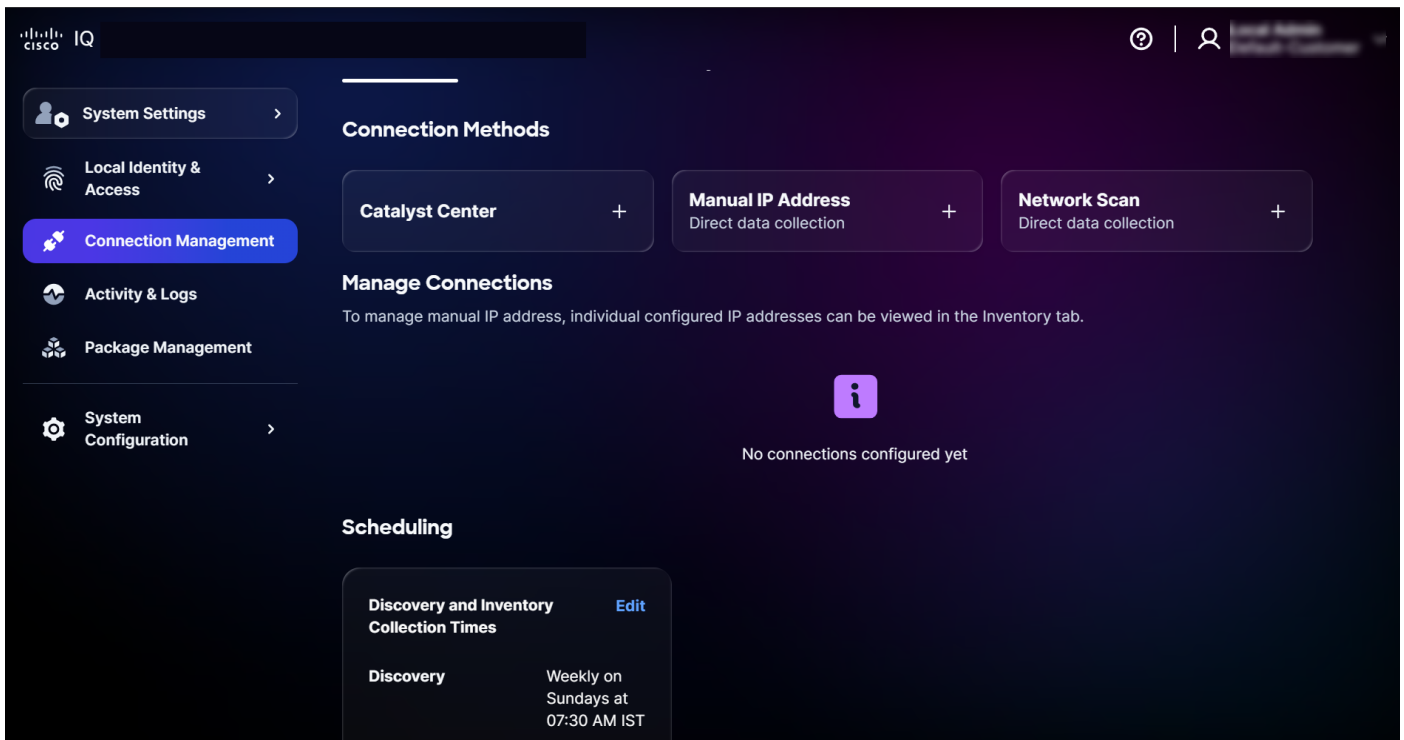
6. Programar uma coleta. Consulte [Agendamento](#) para obter mais detalhes.

 Note: O Cisco IQ VA 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 a programação para alinhar-se com os requisitos e janelas de manutenção da sua organização.

Coleta manual de dados

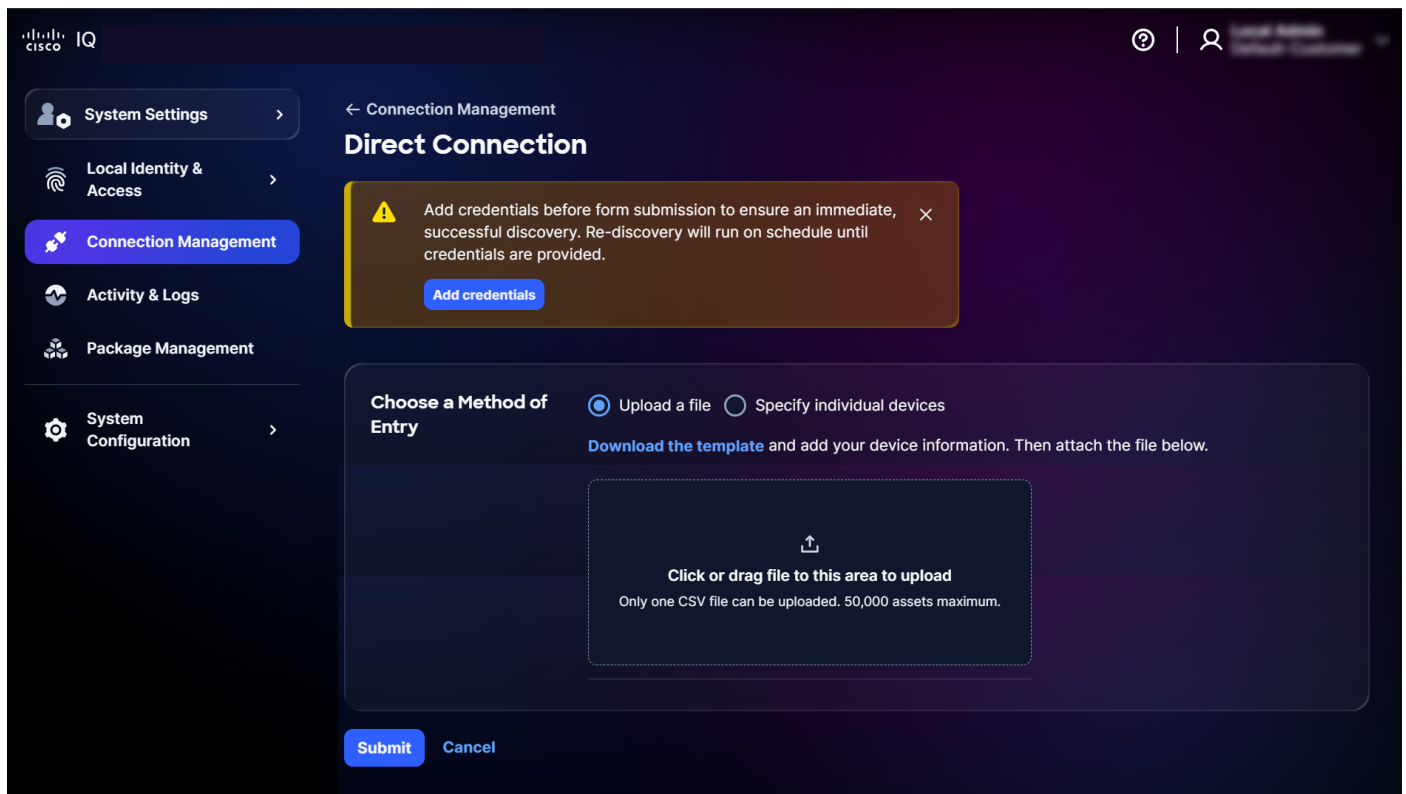
Para adicionar dispositivos para conexão direta de dados:

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



Gerenciamento de conexões

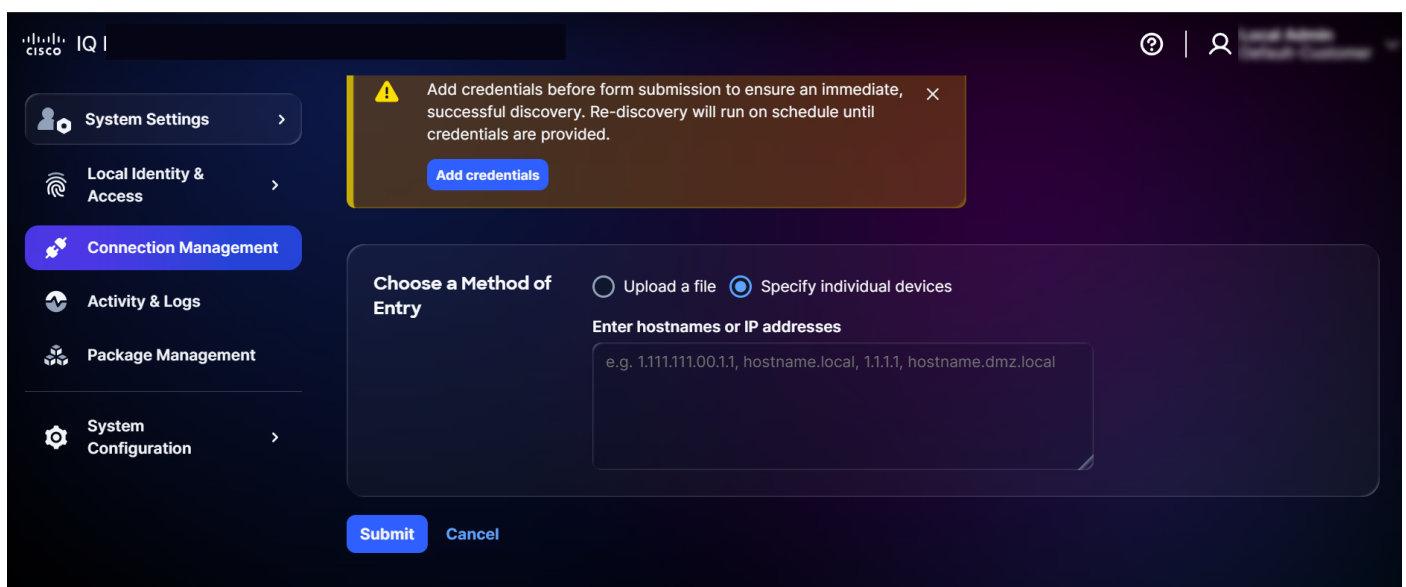
2. Clique em Manual IP Address. A página Conexão direta é exibida com duas (2) opções para coletar dados.



Carregar arquivo

3. Clique na opção preferida em Escolher um método de entrada e forneça as informações do dispositivo usando um dos seguintes métodos:

- Carregar um arquivo: Clique ou arraste e solte o arquivo



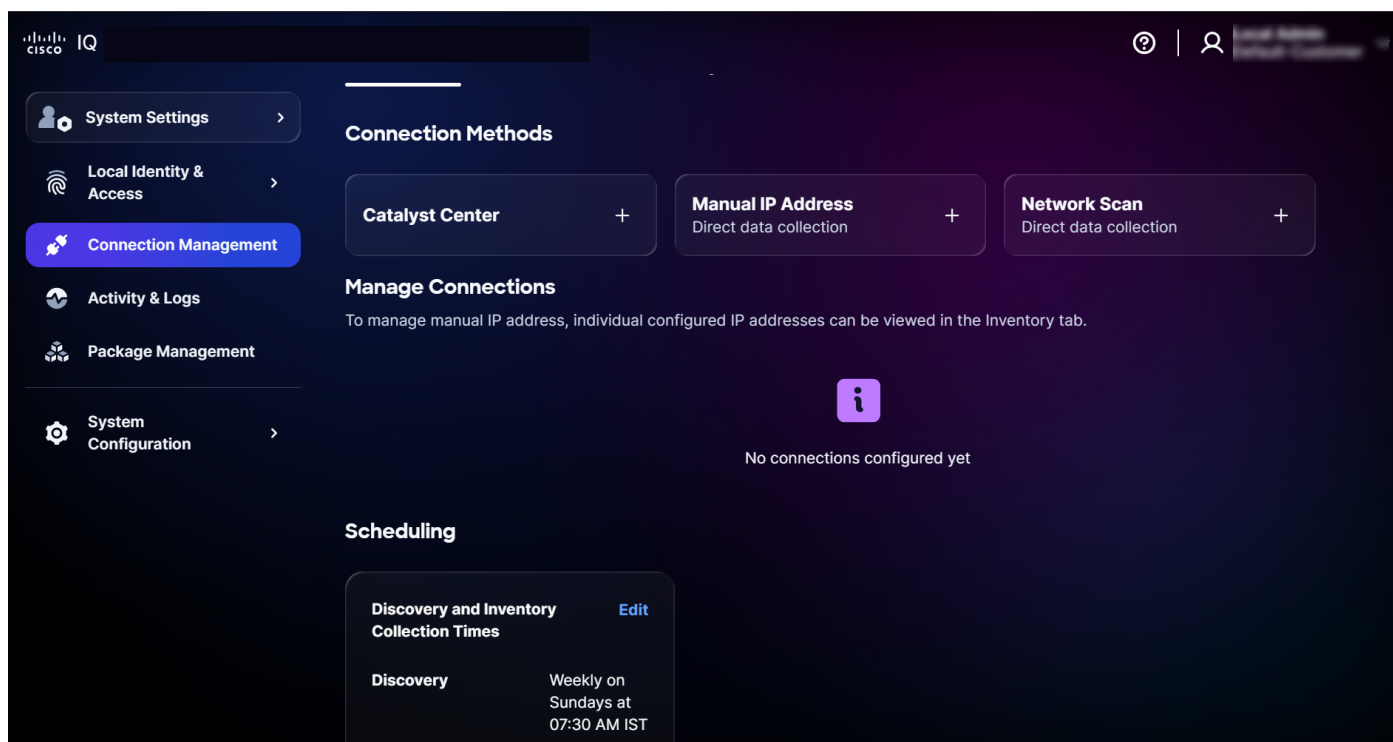
Especificar dispositivos individuais

- 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
4. Clique em Submit. Você será redirecionado para a guia Ativos após o envio bem-sucedido.
 5. Programar uma coleta. Consulte [Agendamento](#) para obter mais detalhes.

 Note: O Cisco IQ VA 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.

Verificação de rede

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



Verificação de rede

2. Clique em Network Scan (Verificação em rede). A página Connect Assets by Network Scan é exibida com três (3) opções.

- Especificar intervalo de IPs: Definir um intervalo de endereços IP para dispositivos de destino dentro desse intervalo para tarefas de descoberta ou gerenciamento de rede
- Especificar o protocolo de descoberta (CDP/LLDP): Escolher o protocolo de descoberta de rede a ser usado
- Upload de arquivo: Carregar um arquivo, como arquivos de configuração ou dados

3. Insira Name.

4. Insira IP Start e IP End.

5. Em Schedule Scan, escolha Frequency and Time.

6. Clique em Connect assets.

Programação

O agendamento permite definir quando o Cisco IQ VA 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.

The screenshot shows the Cisco IQ 'Edit Schedule' page. On the left is a sidebar with navigation links: System Settings, Local Identity & Access, Connection Management (selected), Activity & Logs, Package Management, and System Configuration. The main content area is titled 'Edit Schedule' and has a back arrow labeled 'Connection Management'. It contains two configuration sections. The first section, 'Schedule Discovery', has three fields: 'Frequency' set to 'Weekly', 'Time' set to '07:30', and 'Day' set to 'Sunday'. The second section, 'Schedule Inventory Collection', has three fields: 'Frequency' set to 'Daily', 'Time' set to '05:30', and a clock icon with 'IST'. At the bottom of the main area are 'Submit' and 'Cancel' buttons.

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 qualquer alteração feita nos agendamentos de descoberta ou coleta seja sincronizada e refletida com precisão no Virtual Appliance.

Instalando pacotes (módulos, regras e direitos)

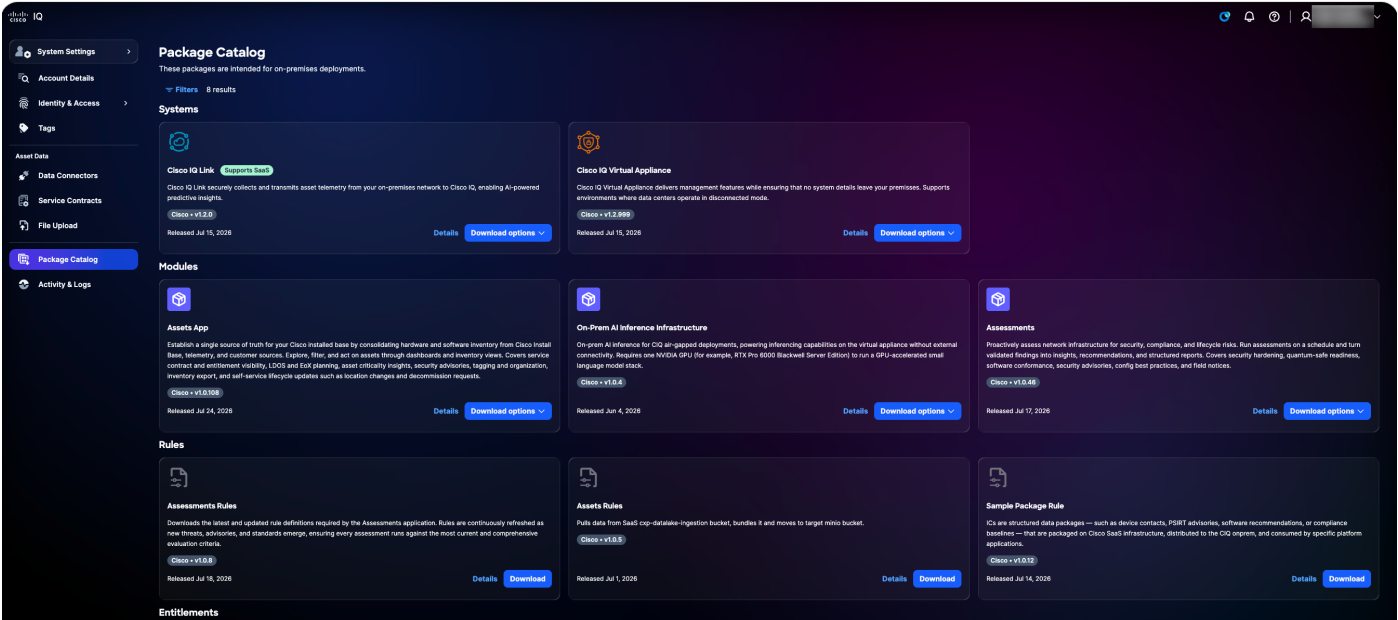
Você pode gerenciar o ciclo de vida do software (isto é, instalação e configuração) de módulos operacionais, regras, direitos e recursos especializados com IA dentro do VA. Você pode instalá-los fazendo o download das versões mais recentes do Cisco IQ (SaaS) navegando até o Catálogo de pacotes. O Catálogo de Pacotes exibe as instâncias de software disponíveis para você. Ele permite que você monitore e gerencie atualizações sem interrupções, garantindo o controle e o gerenciamento eficientes das instâncias do sistema.

Adicionando módulos

Um módulo é um pacote de software autônomo que fornece funcionalidade central dentro do VA. É um serviço independente com seu próprio ciclo de vida, permitindo instalação, manutenção e redimensionamento. O consumo de recursos, incluindo CPU, Unidade de processamento gráfico (GPU) e RAM, é atribuído dinamicamente com base no tamanho da implantação (Pequeno,

Médio ou Grande) selecionado durante a instalação inicial.

- 1. Faça login no [Cisco IQ](#).
- 2. Navegue até Configurações do sistema > Catálogo de pacotes.



Catálogo de Pacotes

- 3. Na placa de módulo desejada, clique em Download options > Installation packages. A janela Download é aberta.



Note: O módulo Avaliação é usado para as imagens de exemplo.

Download Assessments

System version

System v1.2.0

Build type

Application version

-

Cancel

Download

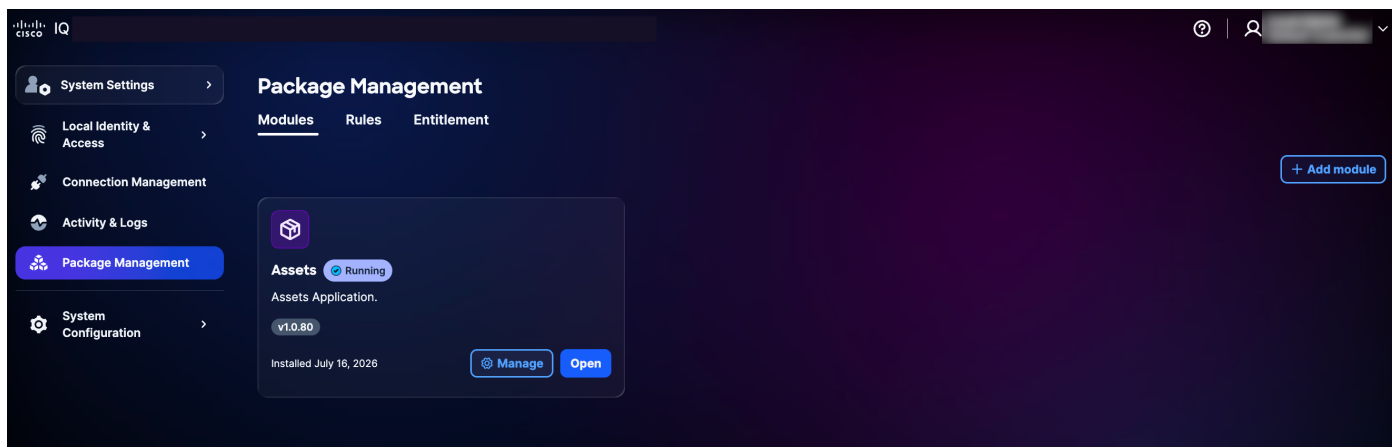
Download

4. Escolha uma Versão do sistema na lista suspensa.
5. Escolha um Tipo de construção na lista suspensa.
6. Clique em Download para salvar o arquivo localmente.



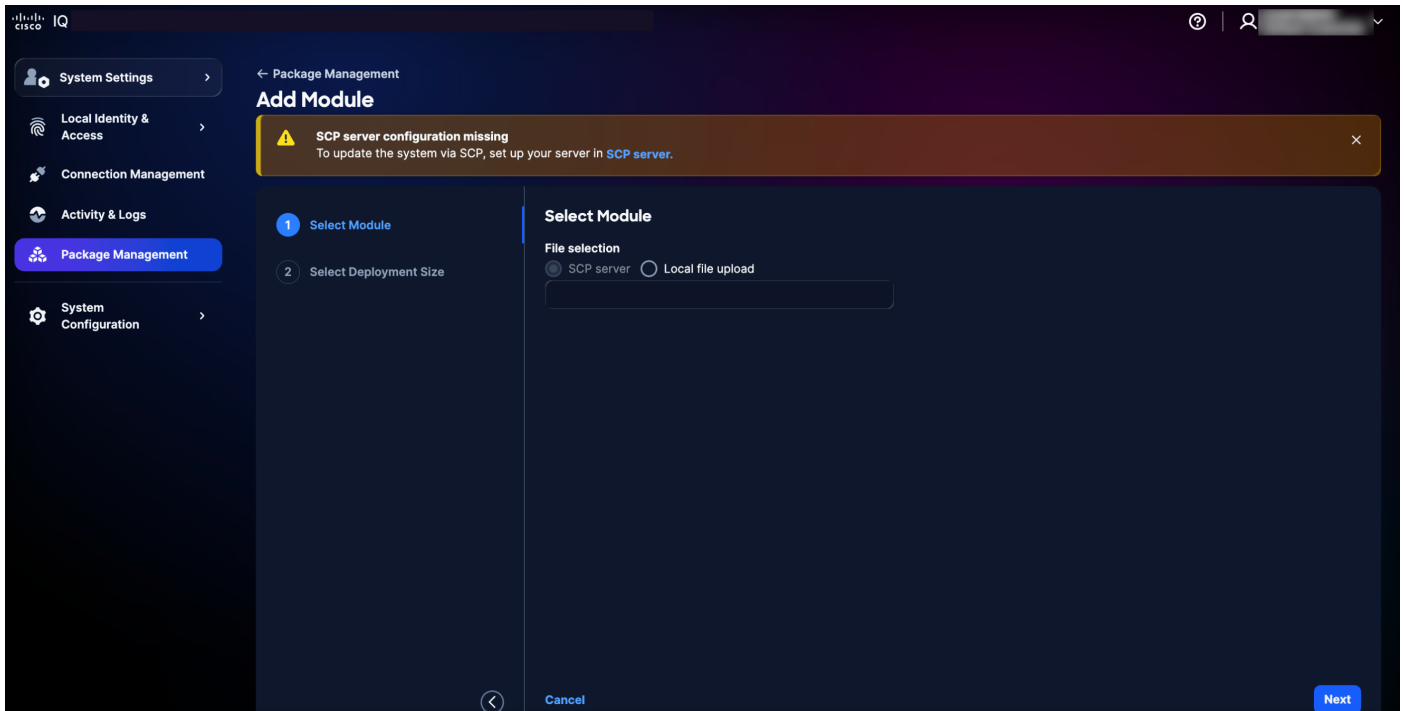
Note: Os arquivos de instalação são grandes (10-25 GB); verifique se você tem espaço em disco suficiente antes de fazer o download.

7. Navegue para VA.
8. Navegue até Home > System Settings > Package Management. A página Gerenciamento de Package é exibida com as seguintes tabs:
 - Módulos
 - Regras
 - Direitos



Módulos

9. Clique em Add module.

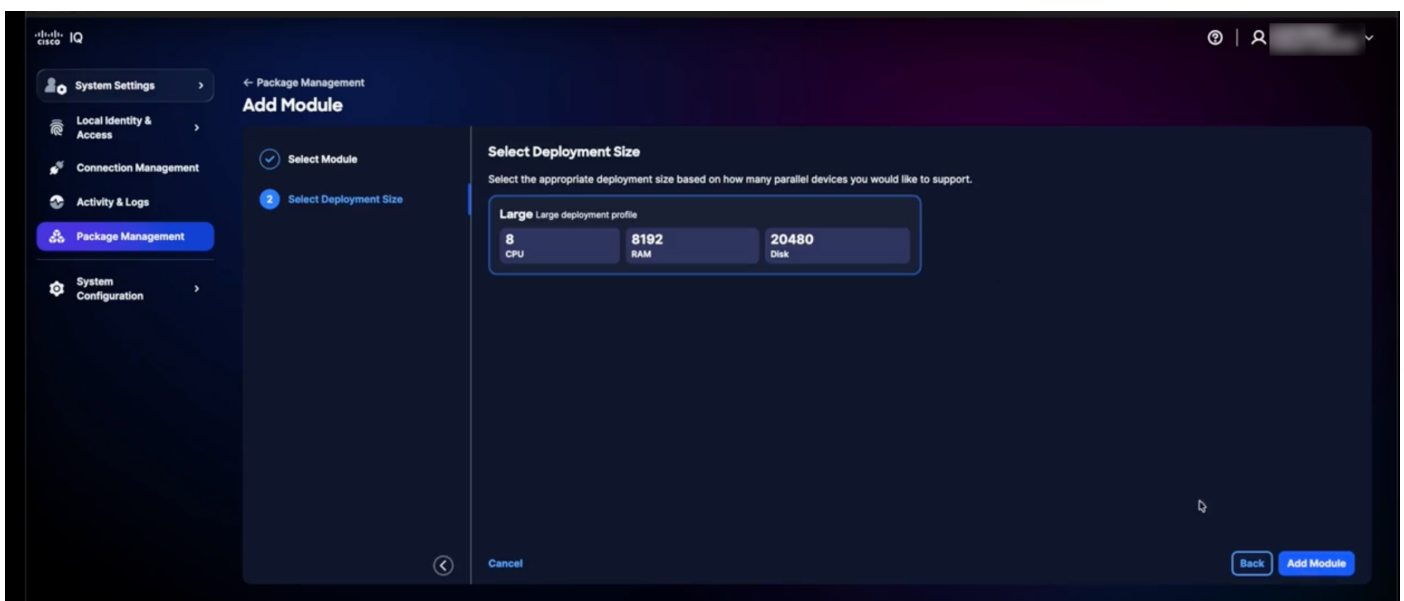


Adicionar módulo

10. Escolha sua opção preferida de seleção de arquivo:

- Servidor SCP: Insira o nome exato do arquivo do pacote de instalação (recomendado para arquivos grandes)
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado (não recomendado para arquivos de 30 GB ou mais devido ao tempo de carregamento)

11. Clique em Next.

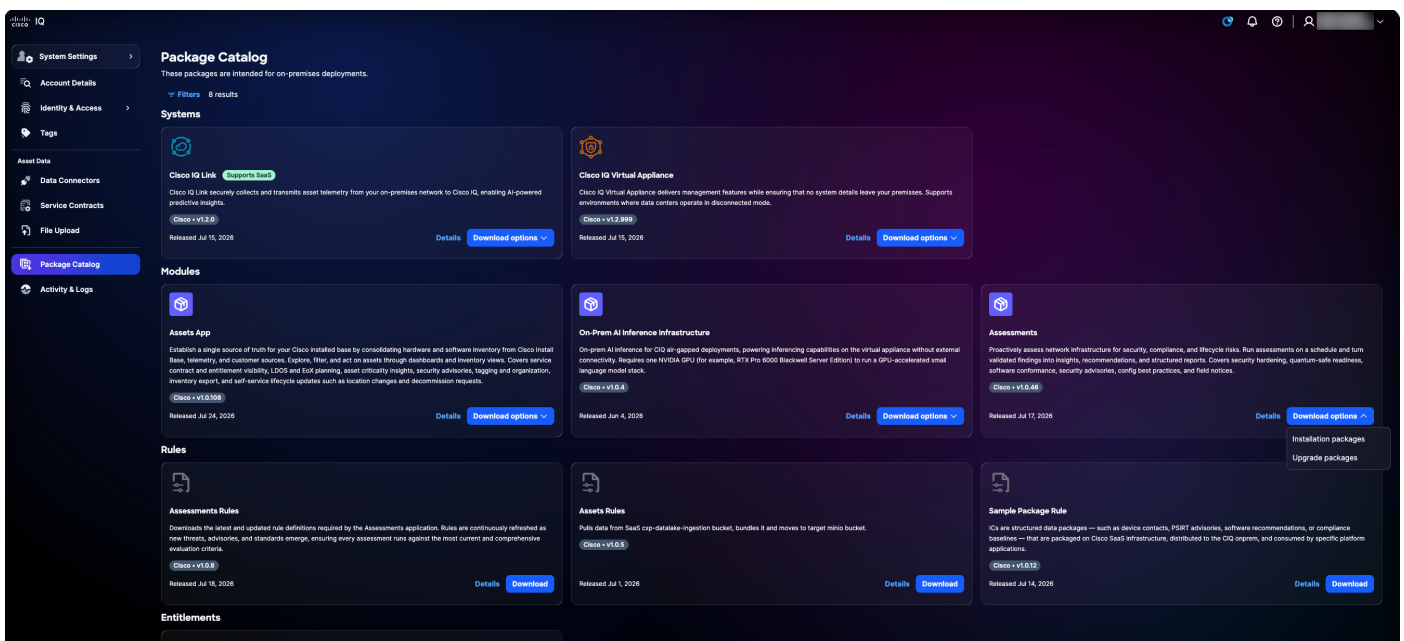


Tamanho da Implantação

- Escolha o Tamanho da Implantação (por exemplo, Pequeno, Médio ou Grande). Esses tamanhos são predefinidos e determinam os requisitos de recursos.
- Clique em Add Module. O módulo recém-instalado é exibido na guia Modules no Package Management. Depois de concluído, o status do módulo muda para "Em execução" e o botão Abrir se torna disponível.

Atualizando um módulo

Os módulos mais recentes estão sendo continuamente atualizados no Catálogo de Pacotes (no Cisco IQ). Para atualizar para a versão mais recente:



Conectar recursos por digitalização em rede

- Na placa de módulo desejada, clique em Download options > Upgrade packages. A janela Download é aberta.



Note: O módulo Avaliação é usado como exemplo para as imagens.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

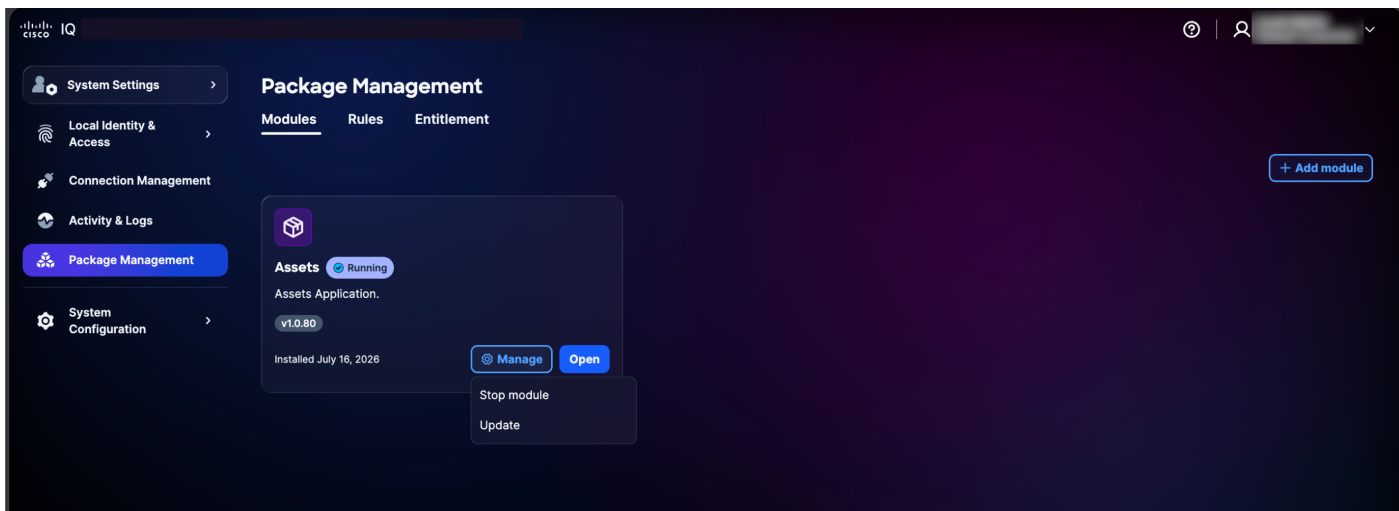
Download

Download

2. Escolha uma versão do sistema na lista suspensa.
3. Escolha uma versão do aplicativo atual na lista suspensa.
4. Escolha um Tipo de construção na lista suspensa.
5. Clique em Download para salvar o arquivo localmente.
6. Navegue para VA e conclua a instalação do arquivo baixado.

Gerenciamento de módulos

Após adicionar um módulo, você pode modificá-lo na página Gerenciamento de Package clicando em Gerenciar. As opções de modificação disponíveis incluem o redimensionamento e a atualização para uma versão superior. Para gerenciar um módulo:



Tipo de atualização

1. Na página Gerenciamento de Package, clique em Gerenciar > Atualizar para o módulo desejado.
2. Escolha o Tipo de atualização:
 - Alterar somente o tamanho da implantação
 - Atualizar versão
3. Se Alterar tamanho da implantação estiver selecionado, clique em Próximo e escolha o novo tamanho da implantação na página seguinte.

OU

Se Atualizar versão estiver selecionado, a opção Seleção de arquivo será exibida. Escolha SCP Server e insira o nome exato do arquivo do pacote de instalação ou escolha Carregamento de arquivo local e arraste e solte o arquivo de instalação baixado.

4. Clique em Next. A página Selecionar Programação de Atualização é exibida.
5. Escolha entre as seguintes opções do botão de opção para atualizar a programação:
 - Atualizar agora
 - Atualizar Depois



Note: Alguns módulos suportam atualizações sem nenhum tempo de inatividade. Se for necessário tempo de inatividade, um banner exibirá os detalhes.

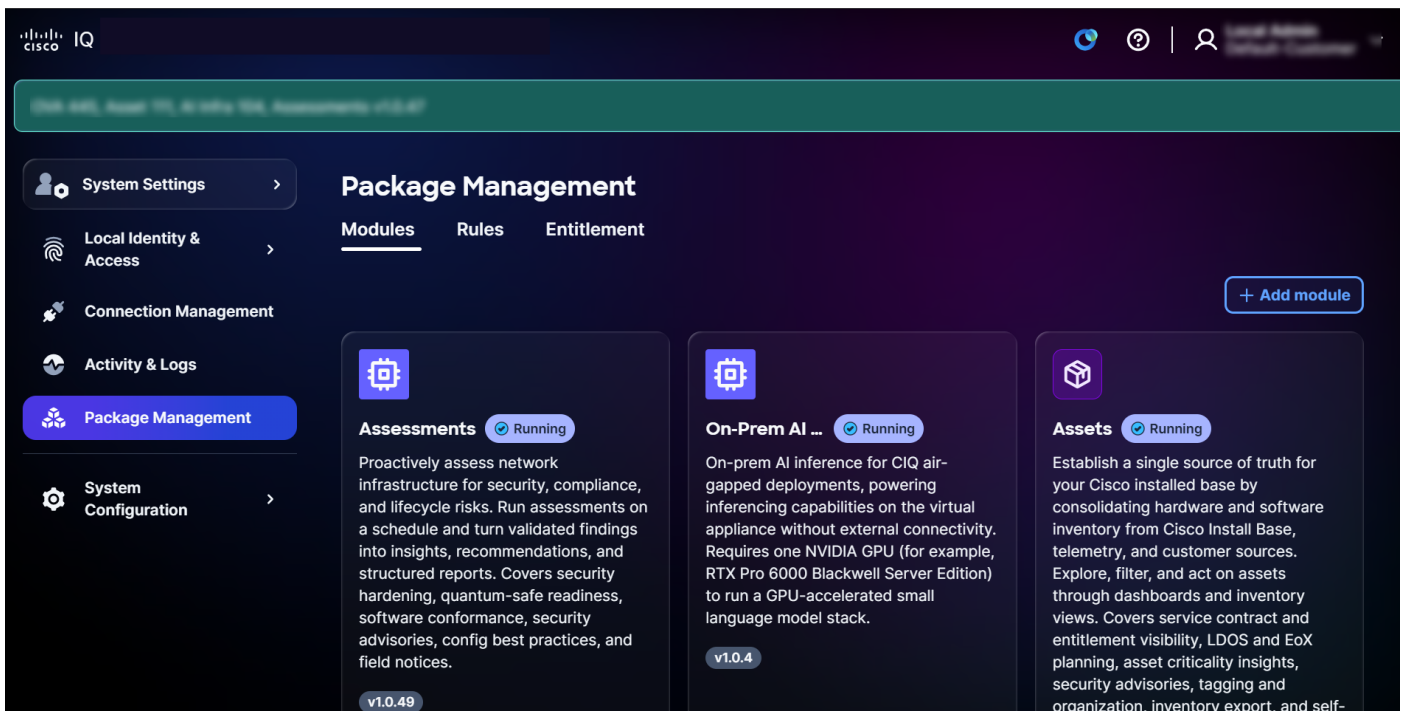
6. Se Atualizar mais tarde estiver selecionado, insira a Data e a Hora.
7. Clique em Next. O Resumo da atualização é exibido.

 Note: Você pode acessar as Notas de versão no Resumo da atualização.

8. Clique em Atualizar módulo e navegue até a guia Módulo. O módulo exibe um status de "atualização agendada".

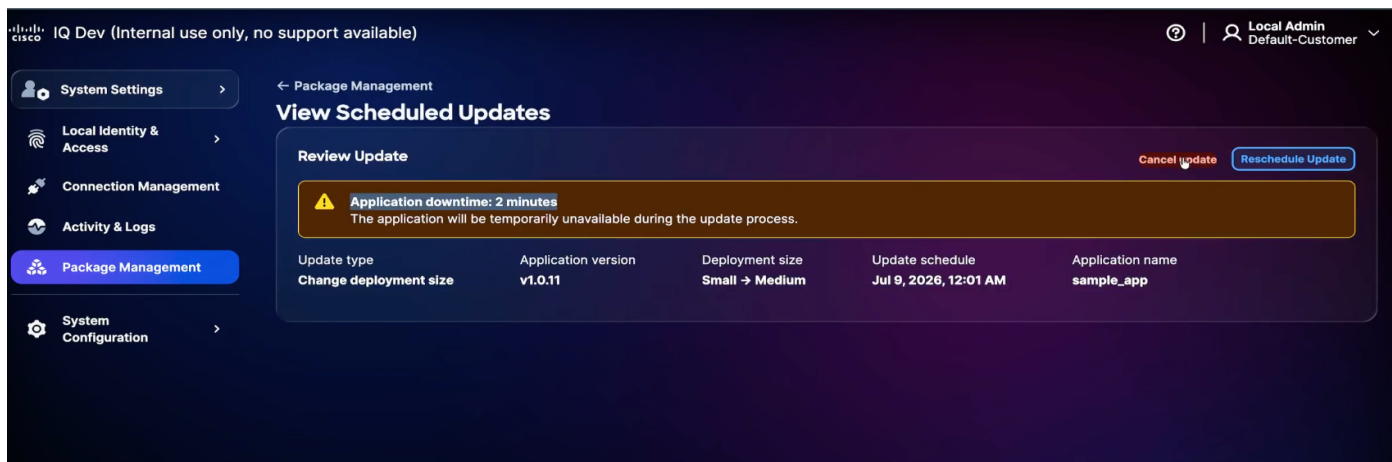
Edição de Agendamentos

Você também pode exibir, editar ou cancelar atualizações agendadas. Para editar ou cancelar uma atualização agendada:



Editando Agenda

1. Na página Gerenciamento de Package, clique em Gerenciar > Exibir atualização programada do módulo desejado. A janela View Scheduled Updates é exibida.



Agendar Atualizações

2. Clique em Cancelar atualização ou Reprogramar atualização conforme necessário.
3. Siga as instruções na tela para concluir as operações.



Note: Se uma operação de módulo (por exemplo, instalação, upgrade ou redimensionamento) falhar, escolha uma das seguintes opções:

Repetir: A interface do usuário exibe um botão Repetir, permitindo que você tente a operação novamente. Logs: Se um erro persistir, clique em Logs para exibir informações de diagnóstico detalhadas. Esse é o principal método para identificar a causa de falhas na instalação ou no tempo de execução.

Instalando regras

Uma regra é um componente especializado ou "complemento" que estende ou modifica a funcionalidade de um módulo existente. As regras não são projetadas para serem executadas como programas autônomos; eles são "conectados" a um módulo para fornecer regras, lógica ou recursos específicos. As regras estão vinculadas a módulos específicos. Quando uma regra é instalada, ela é vinculada ao módulo que ela suporta. As regras permitem que o sistema seja atualizado ou personalizado sem exigir uma atualização completa do módulo principal. Se um novo conjunto de regras ou recursos for necessário, basta adicionar uma nova regra ao módulo existente.

Para fazer download de uma regra:

1. Faça login no [Cisco IQ](#).

2. Navegue até Configurações do sistema > Catálogo de pacotes.
3. No cartão de regras desejado, clique em Download.



Note: A imagem de exemplo a seguir é para uma regra de Ativos.

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

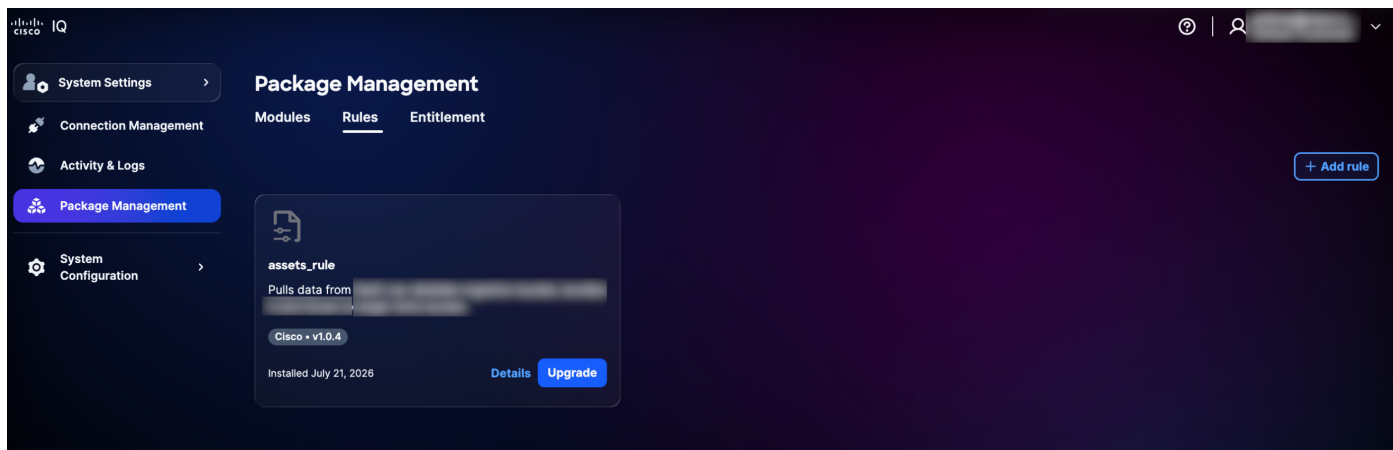
Download

4. Escolha uma versão do aplicativo de destino na lista suspensa.
5. Clique em Download para salvar o arquivo localmente.



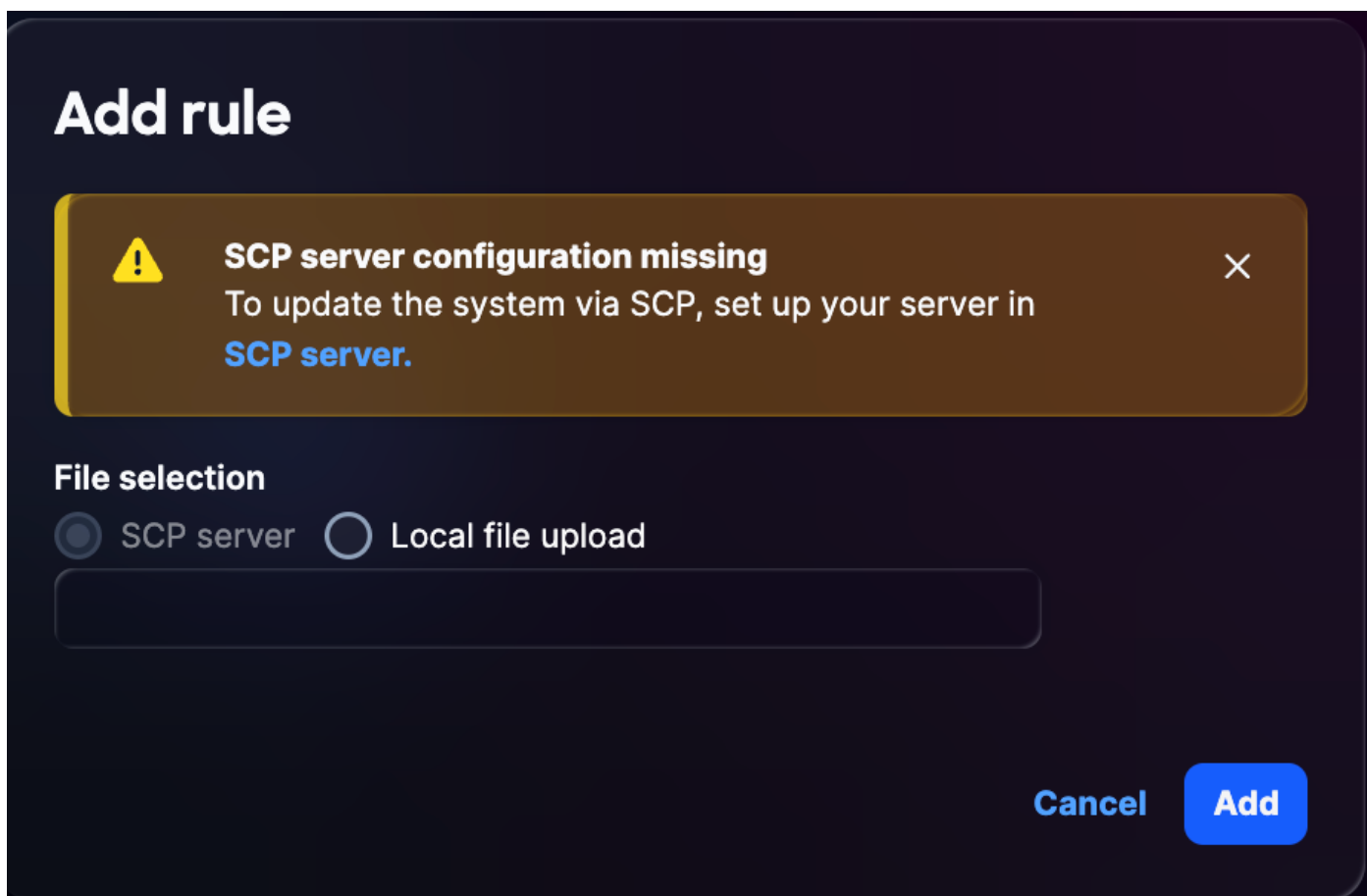
Note: Os arquivos de instalação são grandes (10 a 25 GB); verifique se você tem espaço em disco suficiente antes de fazer o download.

6. Navegue para VA.
7. Navegue até Home > System Settings > Package Management. A página Gerenciamento de Package é exibida com as seguintes tabs.
 - Módulos
 - Regras
 - Direitos
8. Clique na guia Rules.



Gerenciamento de pacotes

9. Clique em Adicionar regra.



Adicionar regra

10. Escolha sua opção preferida de seleção de arquivo:

- Servidor SCP (Secure Copy Protocol, protocolo de cópia segura): Insira o nome exato do

arquivo do pacote de instalação. Este método é recomendado para arquivos grandes.

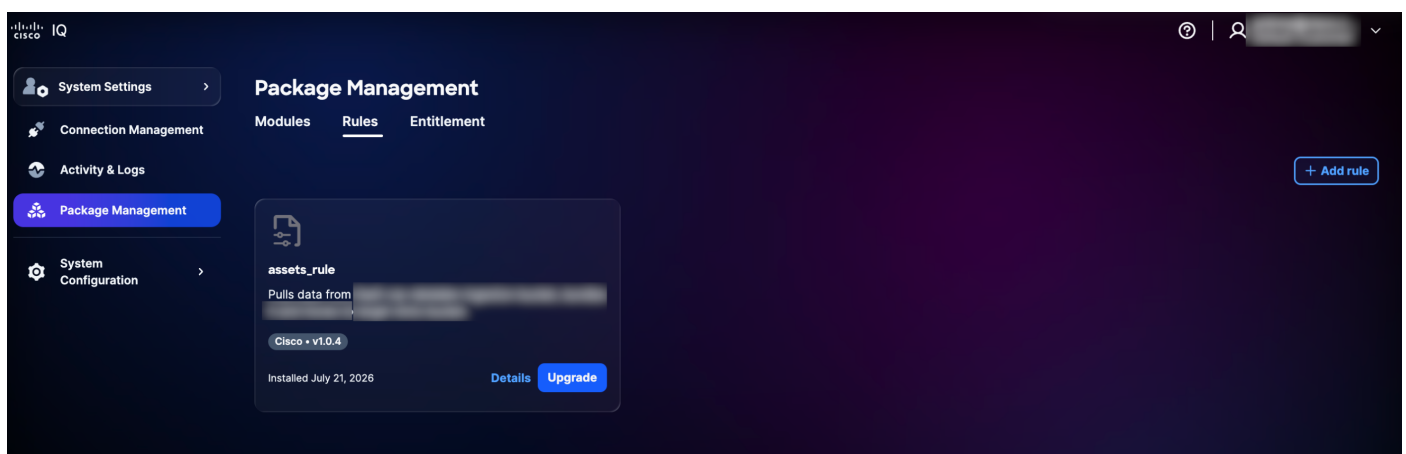
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado.

11. Clique em Add. A regra adicionada é exibida em Gerenciamento de Pacotes.

Atualizando regras

Para atualizar regras:

1. Navegue para Configurações do sistema > Gerenciamento de pacote em VA.



Atualização

2. Na regra desejada, clique em Atualizar. A janela Atualizar regra é aberta.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Regra de atualização

3. Escolha sua opção preferida de seleção de arquivo:

- Servidor SCP (Secure Copy Protocol, protocolo de cópia segura): Insira o nome exato do arquivo do pacote de instalação. Este método é recomendado para arquivos grandes.
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado.

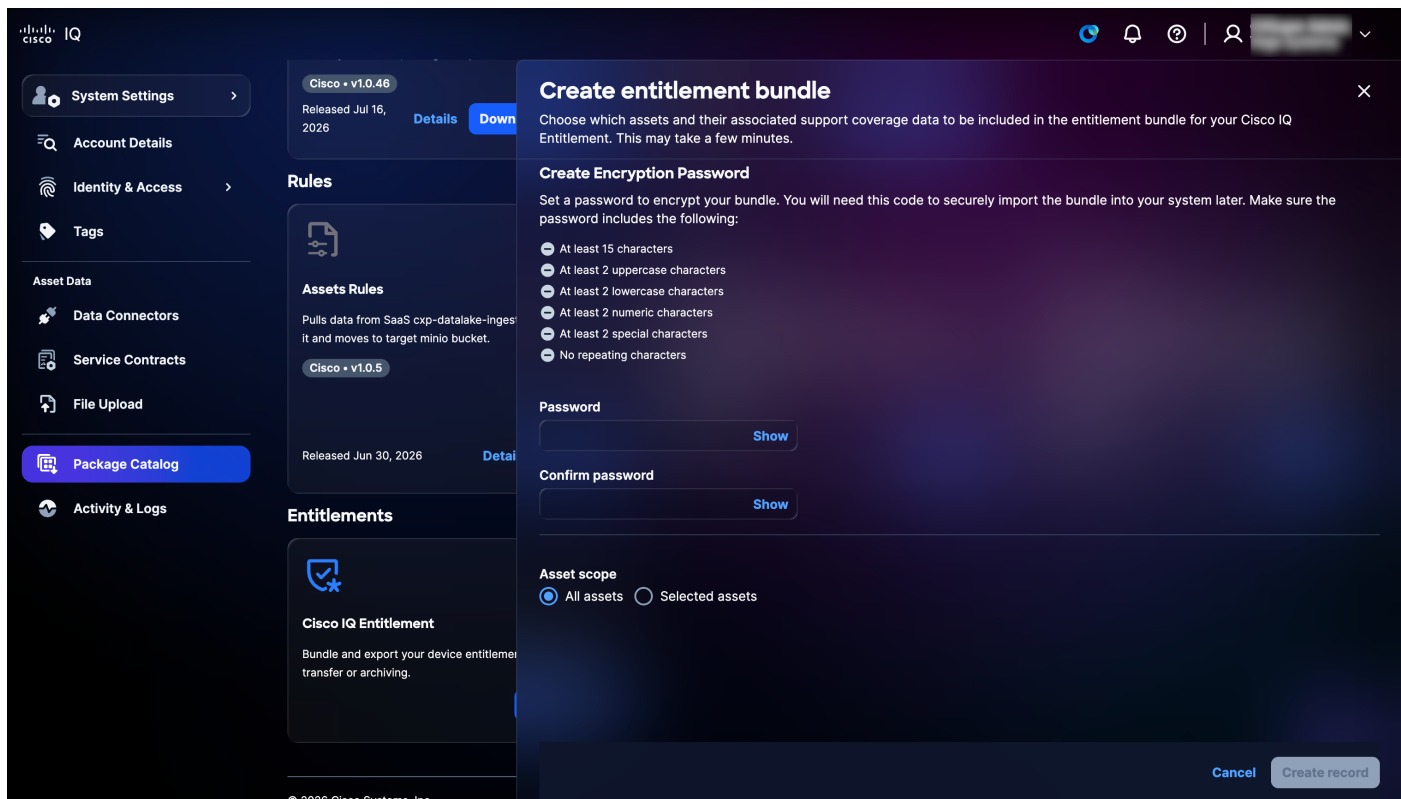
4. Clique em Add.

 Note: Essas regras são aplicadas na coleta de telemetria de dispositivo agendada recorrente. Para aplicação imediata, você pode iniciar manualmente a coleta de telemetria do dispositivo.

Instalando direitos

Uma habilitação valida o direito da sua organização de usar recursos, módulos ou serviços de software específicos. Para instalar um direito:

1. Faça login no [Cisco IQ](#).
2. Navegue até Configurações do sistema > Catálogo de pacotes.
3. No cartão de direito, clique em Criar registro. A janela Criar pacote de direitos é aberta.



Criar pacote de direitos

4. Digite uma senha. Consulte as regras de criação de senha exibidas na tela.
5. Insira a mesma senha novamente em Confirmar senha.
6. Escolha o botão de opção Escopo do ativo preferido.
 - Todos os ativos: Inclui todos os ativos vinculados a você
 - Ativos selecionados: Permite selecionar dispositivos específicos alinhados ao seu ambiente; se essa opção estiver selecionada, marque as caixas de seleção de todos os ativos aplicáveis
7. Clique em Criar registro para salvar o arquivo localmente.

 **Note:** Depois de criar o pacote de direitos, não saia da tela atual. Se você navegar para outra página, o pacote será invalidado e você deverá gerá-lo novamente para habilitar a opção de download.

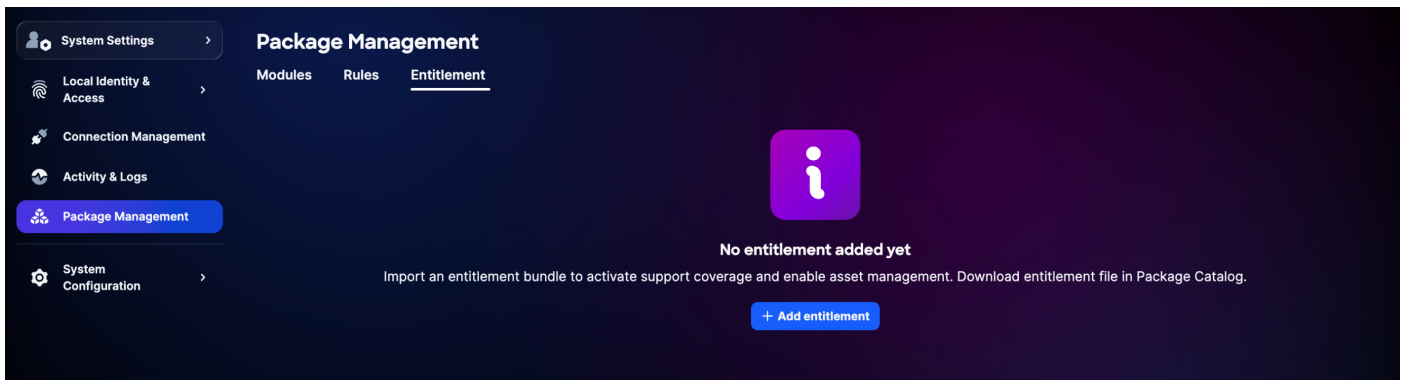
 **Note:** Os arquivos de instalação são grandes (10 a 25 GB); verifique se você tem espaço em disco suficiente antes de fazer o download.

8. Faça login no VA.
9. Navegue até Home > System Settings > Package Management. A página Gerenciamento

de Package contém as seguintes tabs:

- Módulos
- Regras
- Direitos

10. Clique na guia Entitlements.



Guia Qualificação

11. Clique em Add Entitlement.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

Adicionar Direito

12. Escolha sua opção preferida Seleção de arquivo.

- Servidor SCP (Secure Copy Protocol, protocolo de cópia segura): Insira o nome exato do arquivo do pacote de instalação; este método é recomendado para arquivos grandes
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado

13. Digite uma senha.

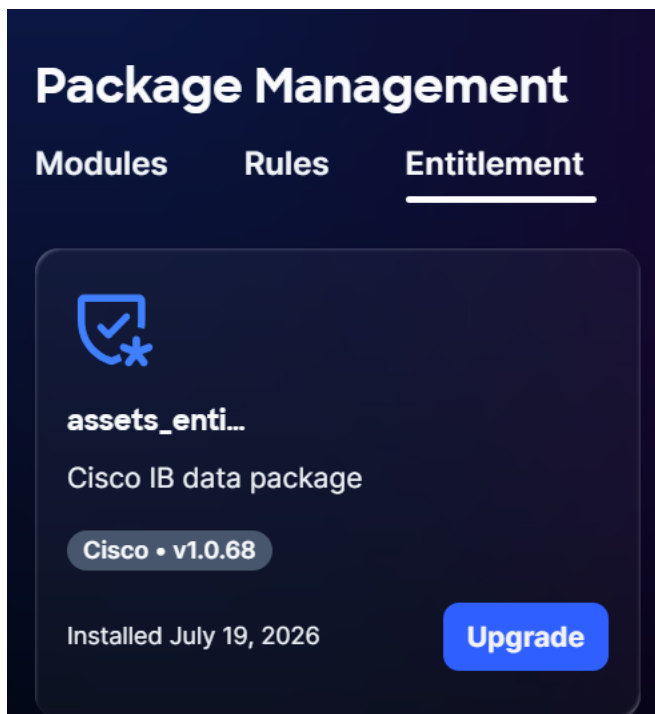
14. Clique em Add. O direito recém-instalado é exibido na guia Entitlement no Package Management.

15. Para habilitar direitos, aguarde de 5 a 10 minutos após adicioná-los e inicie a coleta de telemetria do dispositivo.

 Note: Adicionar um contrato de serviço no processo de qualificação adiciona todos os dispositivos vinculados a esse contrato ao inventário de ativos de dispositivos no local. Você tem opções para filtrar dispositivos por número de série, usar várias IDs de conta ou selecionar dispositivos específicos para gerenciar direitos.

Atualizando direitos

Para atualizar um direito:



Atualização de qualificação

1. Na Qualificação desejada, clique em Atualizar.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

Show

Cancel

Add

Qualificação para atualização

2. Escolha sua opção preferida de seleção de arquivo:

- Servidor SCP (Secure Copy Protocol, protocolo de cópia segura): Insira o nome exato do arquivo do pacote de instalação; este método é recomendado para arquivos grandes
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado

3. Digite uma senha.

4. Clique em Add.

Recursos acionados por IA

O módulo de infraestrutura de interferência de IA no local permite recursos de IA no local em VA. Ele executa um Small Language Model (SLM) localmente, permitindo que o sistema responda aos prompts acionados por IA. Uma vez instalado, você pode interagir com ele diretamente na interface VA.

Há suporte para os seguintes tipos de consulta:

- Ativos: Identificar ativos em risco devido ao status de fim da vida útil, moeda ou não conformidade do software, vulnerabilidades de segurança e falhas na cobertura do contrato
- Inventário: Solicite análise orientada por IA sobre os ativos em seu inventário

O pacote de instalação da infraestrutura de interferência de IA no local está disponível no Catálogo de pacotes do Cisco IQ e é distribuído da mesma forma que outros módulos, como Ativos.

 Note: Somente uma (1) infraestrutura de interferência de IA local pode ser executada por GPU de cada vez. A instalação leva aproximadamente de 40 a 45 minutos para ser concluída. Os arquivos de instalação são grandes (aproximadamente 30 GB); verifique se você tem espaço em disco suficiente antes de fazer o download.

Pré-requisitos para infraestrutura de interferência de IA no local

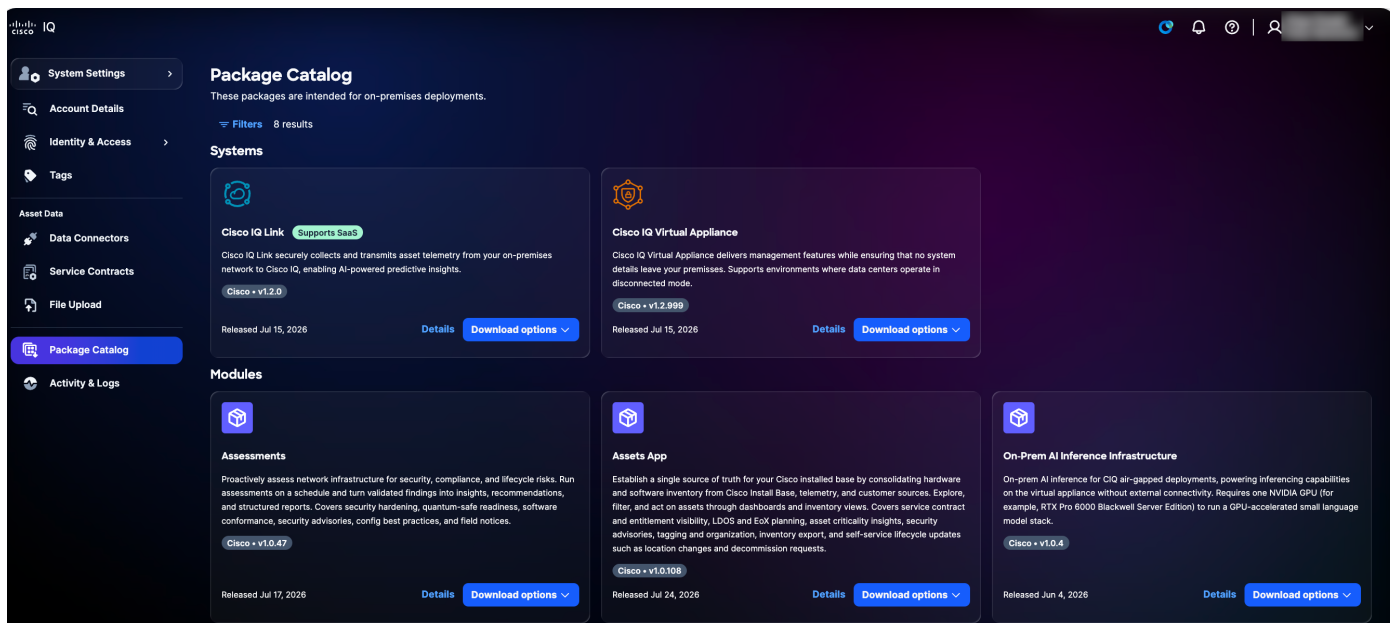
Antes de instalar a infraestrutura de interferência de IA no local, as seguintes condições devem ser atendidas:

- O VA deve incluir uma VM com acesso à GPU; o SLM requer uma GPU e não pode ser executado sem uma
- A VM da GPU deve ter 80 GB ou mais de VRAM da GPU disponível

Instalação da infraestrutura local de interferência de IA

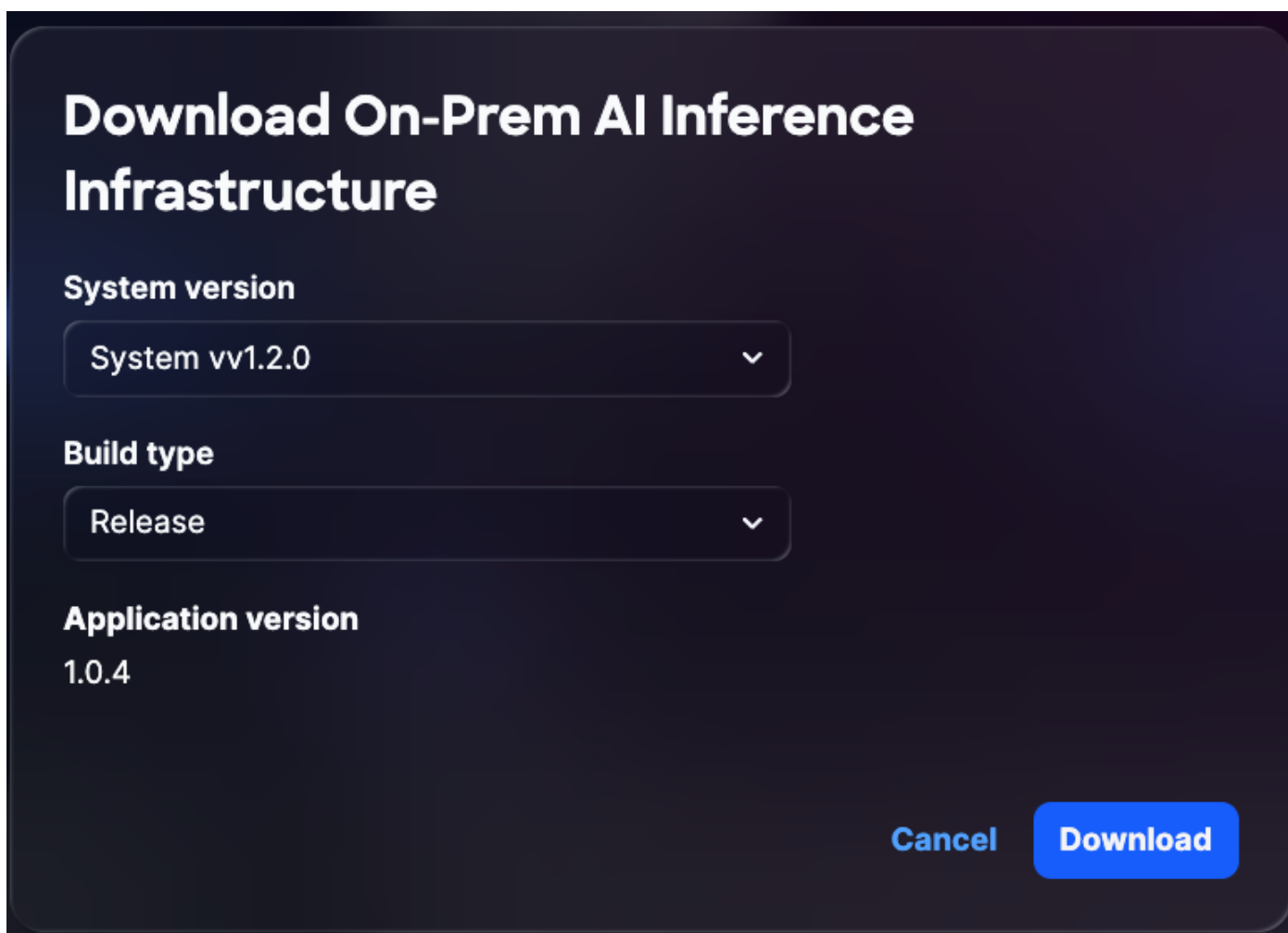
Para instalar a infraestrutura de interferência de IA local no VA, faça o download do módulo Infraestrutura de interferência de IA local do Cisco IQ SaaS:

1. Faça login no [Cisco IQ](#).
2. Navegue até Configurações do sistema > Catálogo de pacotes.



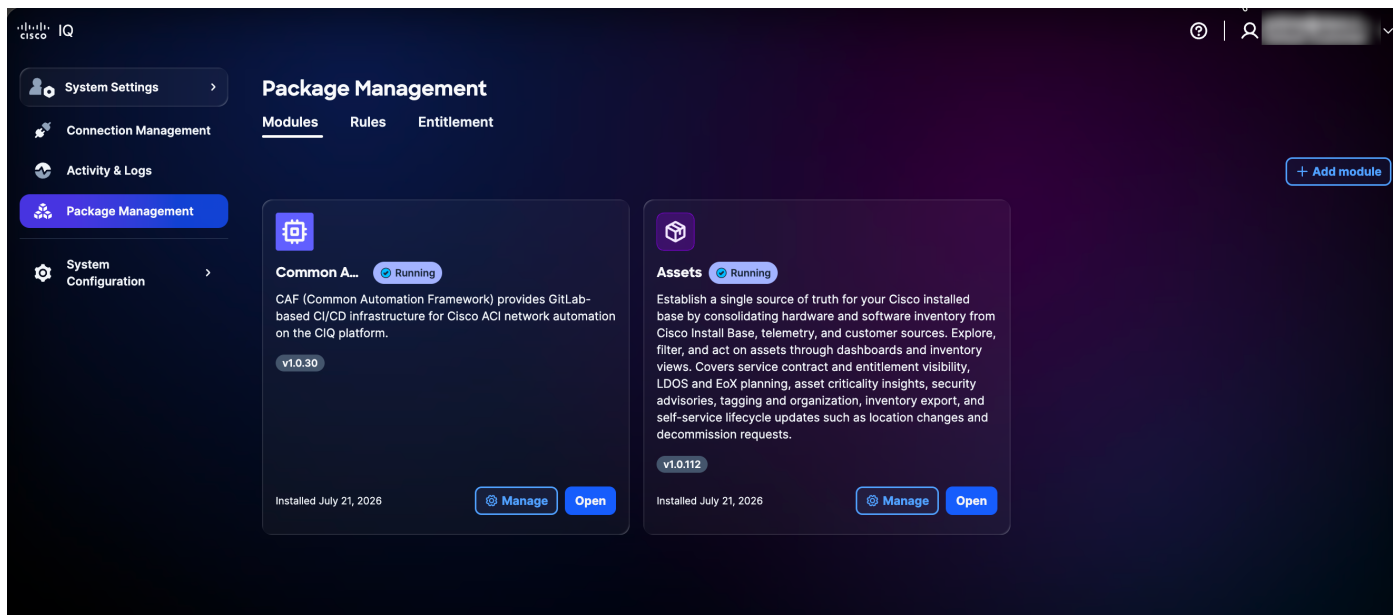
Pacote de instalação

3. Na placa On-Prem AI Inference Infrastructure, clique em Download options > Installation packages. A janela Download Application é aberta.



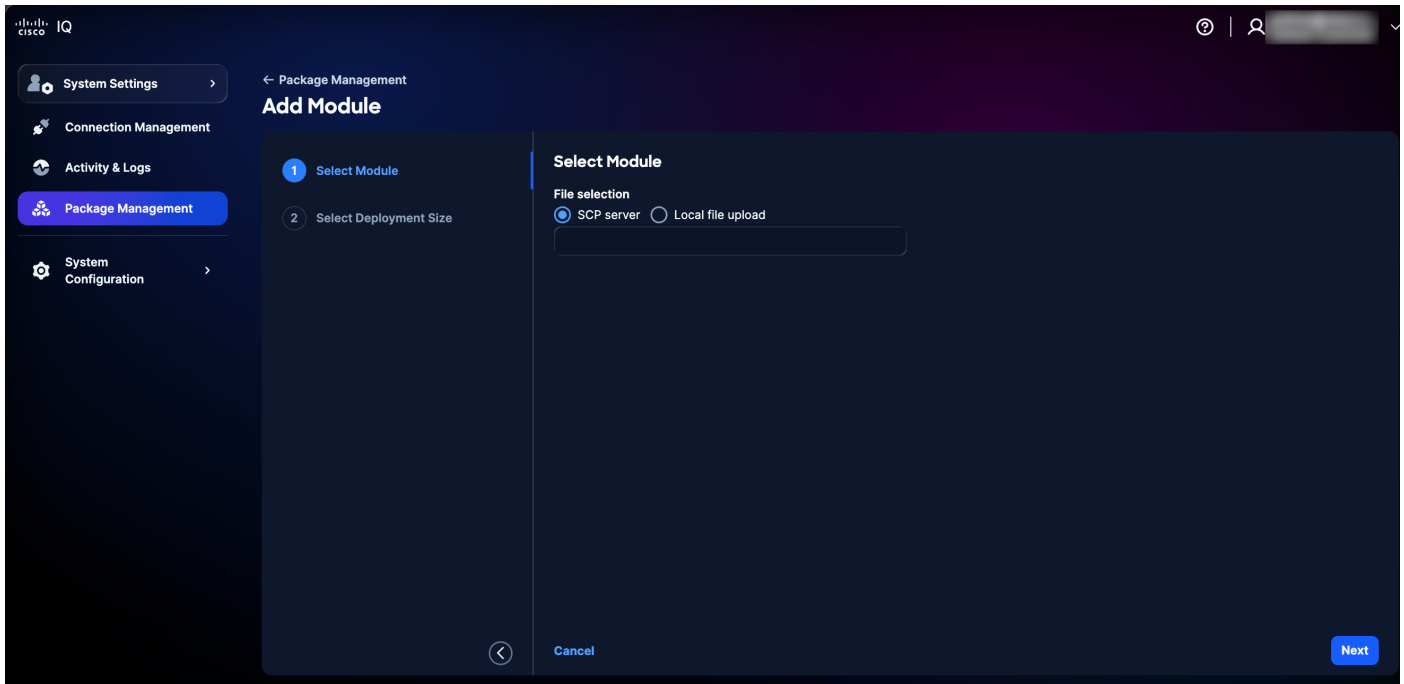
Faça o download da infraestrutura de inferência de IA

4. Escolha uma versão do sistema na lista suspensa.
5. Escolha um Tipo de construção na lista suspensa.
6. Clique em Download.
7. Navegue para VA.



Gerenciamento de pacotes

8. Navegue até Home > System Settings > Package Management. A página Gerenciamento de Package é exibida com as seguintes tabs:
 - Módulos
 - Regras
 - Direitos
9. Na guia Modules, clique em Add modules.



Selecionar módulo

10. Escolha sua opção preferida de seleção de arquivo:

- Servidor SCP: Insira o nome exato do arquivo do pacote de instalação (recomendado para arquivos grandes).
- Carregamento de arquivo local: Arraste e solte o arquivo de instalação baixado (não recomendado para arquivos de 30 GB ou mais devido ao tempo de carregamento). Note: O método de carregamento de arquivo local tem um limite de 20 minutos. Se o processo de carregamento exceder essa duração, a instalação falhará. Usar um servidor SCP é o método preferido para garantir uma instalação bem-sucedida e estável.

11. Clique em Next. O sistema começa a carregar o arquivo.

12. Escolha um Tamanho da Implantação (por exemplo, Pequeno, Médio ou Grande).

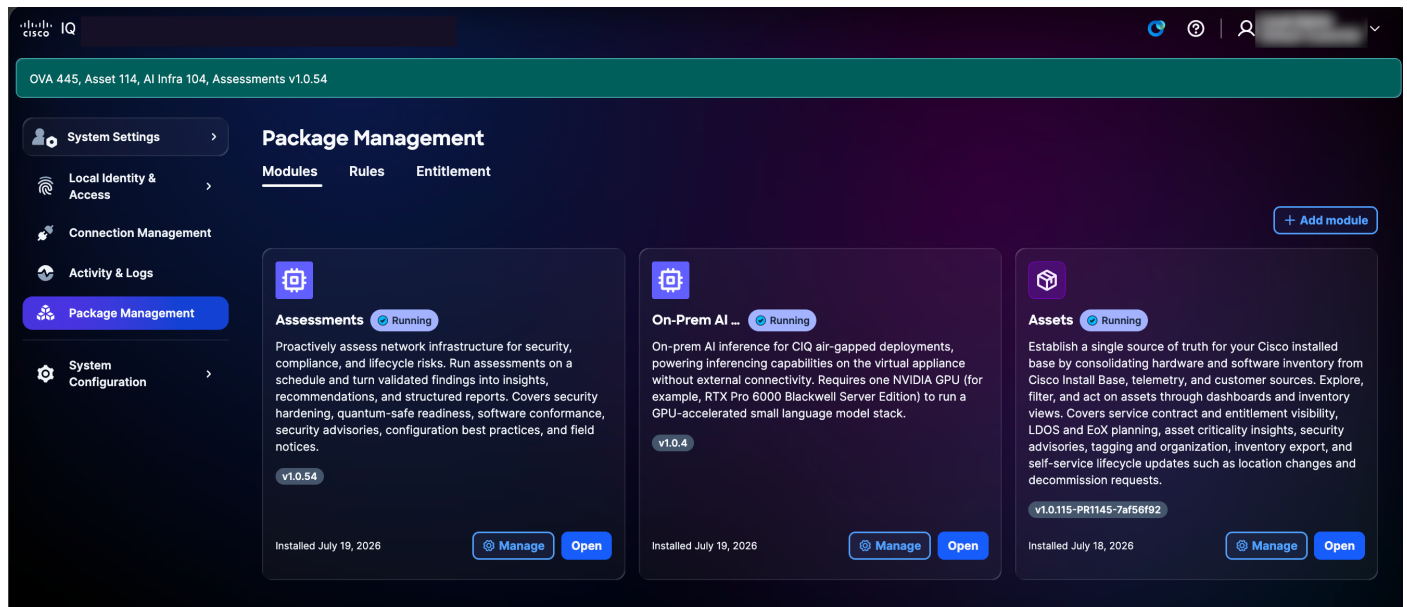
13. Clique em Add Module. A instalação é iniciada e leva aproximadamente de 40 a 45 minutos para ser concluída.

Quando a instalação estiver concluída, a infraestrutura de interferência de IA local será exibida na guia Module no Package Management.

 Note: Somente um módulo de infraestrutura de interferência de IA local pode ser executado por GPU. O módulo usa aproximadamente 90% da VRAM da GPU. Não há suporte para a tentativa de instalar uma instância adicional na mesma GPU.

Gerenciamento do módulo de infraestrutura de interferência de IA local

Uma vez instalado, o módulo de infraestrutura de interferência de IA no local pode ser gerenciado na guia Aplicativos em Gerenciamento de pacotes.



Edição da infraestrutura de interferência de IA

Para gerenciar o módulo, clique em Gerenciar ao lado do módulo Infraestrutura de interferência de IA local. Consulte [Gerenciamento de módulos](#) para obter mais detalhes.

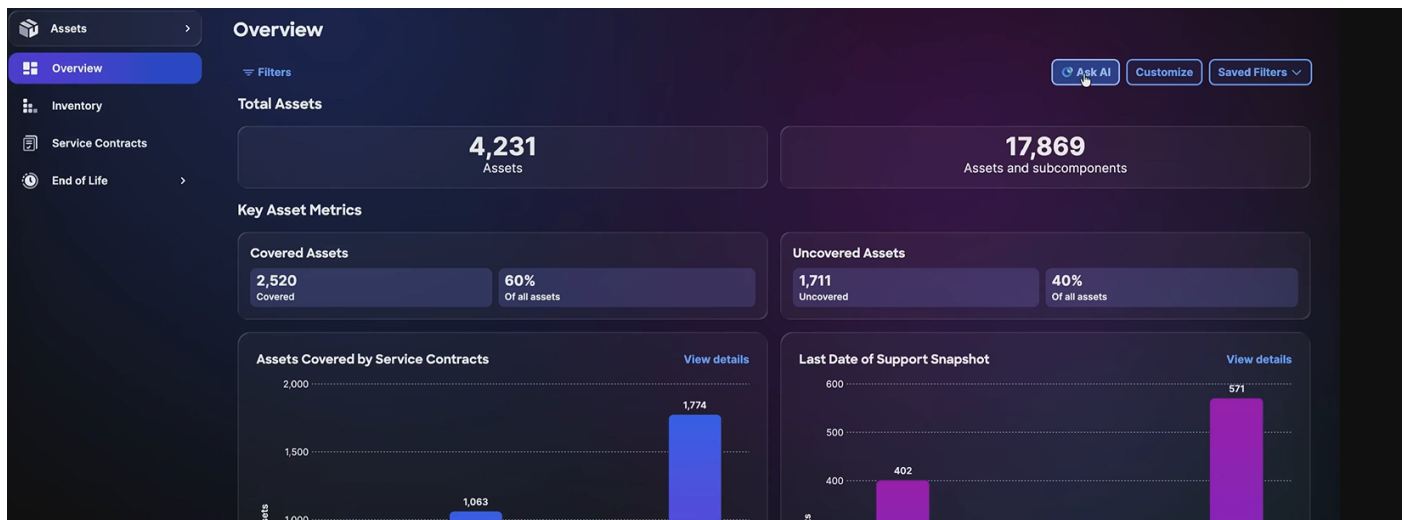
Usando recursos acionados por IA

Após a instalação bem-sucedida do módulo de infraestrutura de interferência de IA local, o botão Ask AI fica disponível na interface VA.

Pergunte à IA em Ativos

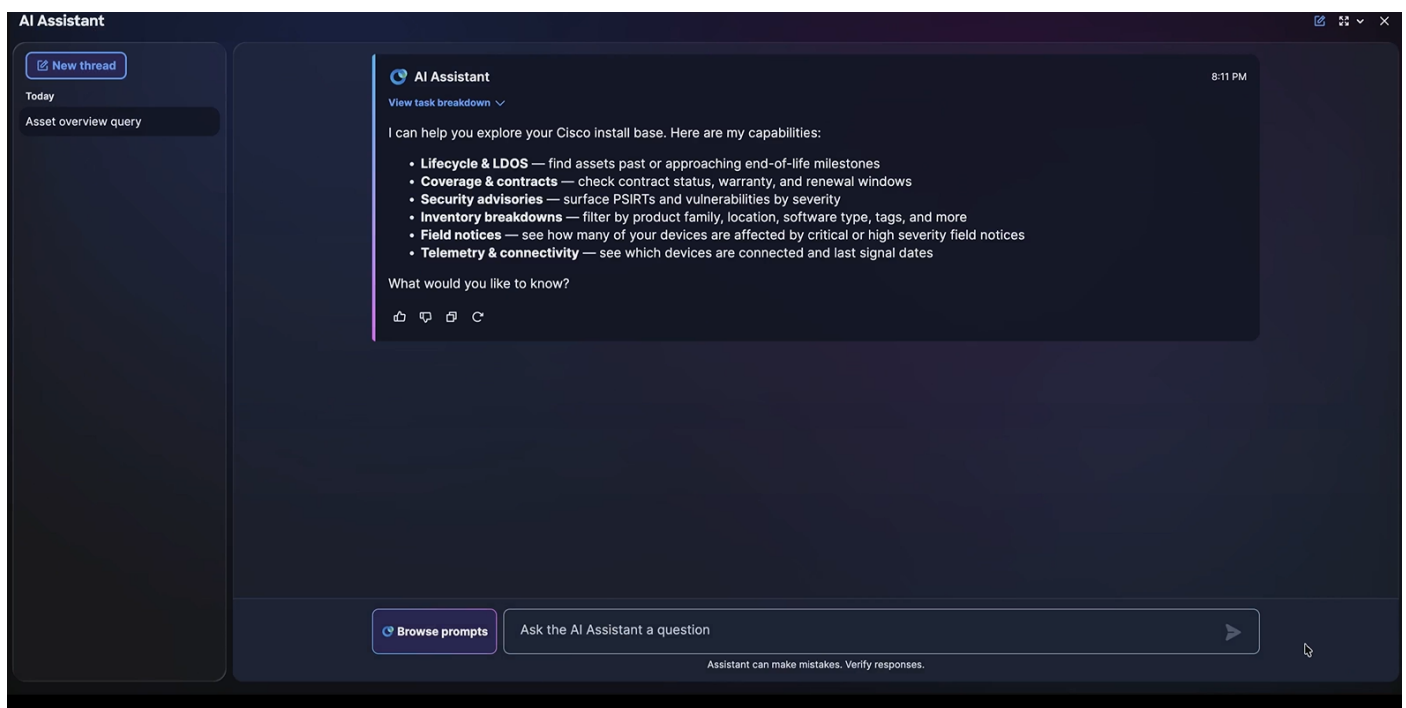
Para usar Perguntar IA em Ativos:

1. Escolha o menu Início > Ativos. A página Ativos é exibida.



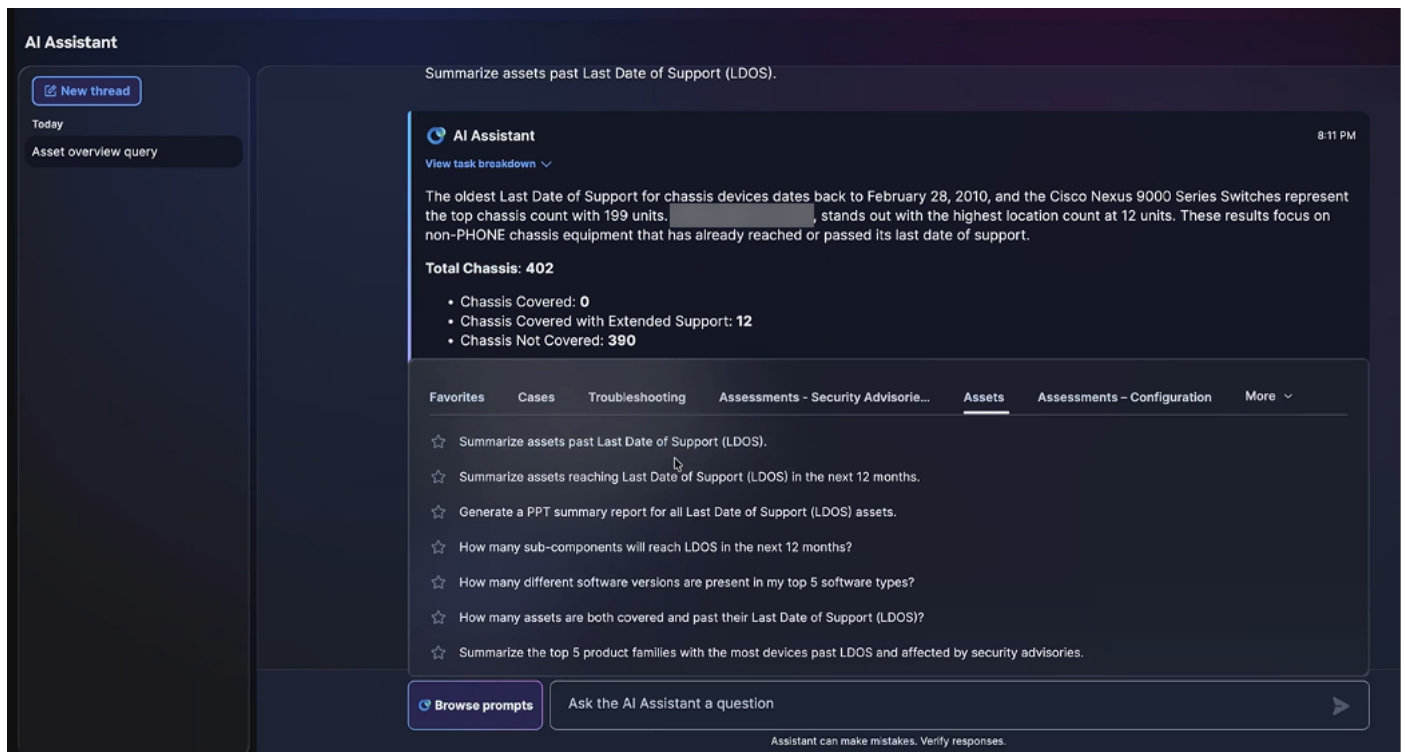
Página Ativos

2. Clique em Ask AI. A infraestrutura de interferência de IA local é lançada.



Procurar Prompts

3. Clique em Browse prompts para exibir os prompts disponíveis ou insira uma pergunta personalizada no campo Ask the AI Assistant a question.



Conjunto de Prompts

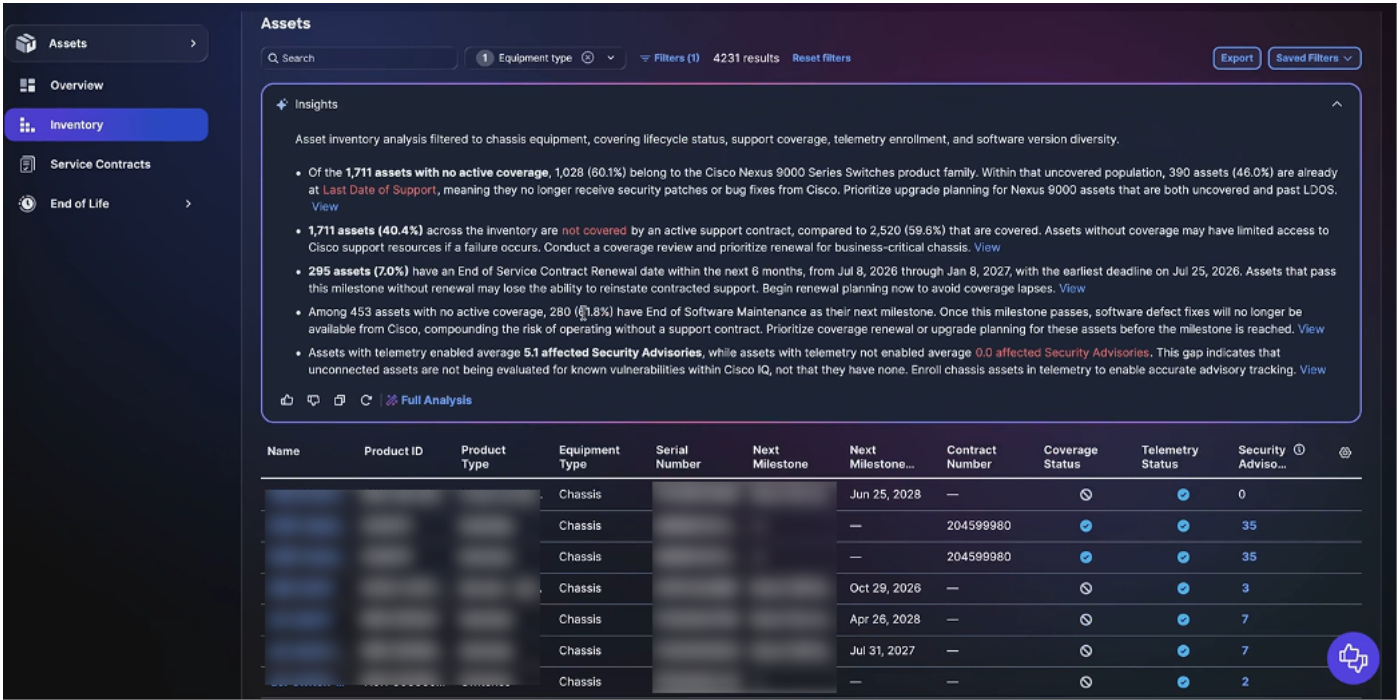
4. Clique no prompt desejado ou pressione Enter. O SLM local gera uma resposta.

Análise de IA no inventário

O módulo Infraestrutura de interferência de IA no local fornece análise automatizada orientada por IA na seção Inventário. Os resultados da análise são exibidos automaticamente assim que os dados de inventário são preenchidos.

Para exibir a análise do AI no Inventário:

1. Selecione o menu Home > Inventory. A página Inventário é exibida.



Inventário

2. Exibir a análise gerada por AI. Os resultados são exibidos na exibição de inventário quando os dados estão disponíveis.
-  Note: Clique em Análise Completa para obter visualizações como gráficos, painéis e gráficos que fornecem informações adicionais.

Recursos comuns para módulos

Esta seção detalha as principais funcionalidades compartilhadas em todos os módulos. Esses recursos oferecem uma experiência de usuário consistente, otimizam o desempenho do sistema e simplificam os fluxos de trabalho administrativos

Analizando Dados

O painel Insights oferece uma análise dos dados nessa página orientada por IA, fornecendo insights práticos para melhorar a segurança e a integridade do seu ambiente de rede.

-  Note: O recurso Análise só está disponível em páginas selecionadas.

Assets

Q Search Product family Product ID Location Tags Filters (1) 1716 results Reset filters Export

Insights

- 69 assets that are **not covered** by any support contract have already reached **Last Date of Support**, leaving them without security patches or bug fixes. Prioritize upgrades or replacements for these assets to mitigate operational risks. [View](#)
- 175 Cisco Catalyst 9300 Series Switches (49.7% of **not covered** assets) lack active support contracts, which may limit access to Cisco support resources. Align renewal planning with the channel partner for these business-critical switches. [View](#)
- 73 assets with **telemetry not enabled** are at **End of Software Maintenance**, reducing visibility within Cisco IQ for proactive alerts and lifecycle planning. Enable telemetry for these assets to restore full monitoring capabilities. [View](#)
- 75 assets (4.4%) have **coverage expiring** between **Apr 24, 2026** and **Oct 24, 2026**, with the earliest deadline on **Apr 30, 2026**. Review these contracts to avoid lapses in vendor support and potential cost increases. [View](#)
- 75 assets (4.4%) have **End of Service Contract Renewal** dates between **May 1, 2026** and **Oct 24, 2026**, starting with a deadline on **May 1, 2026**. Coordinate with the selling partner to renew these contracts before expiry. [View](#)

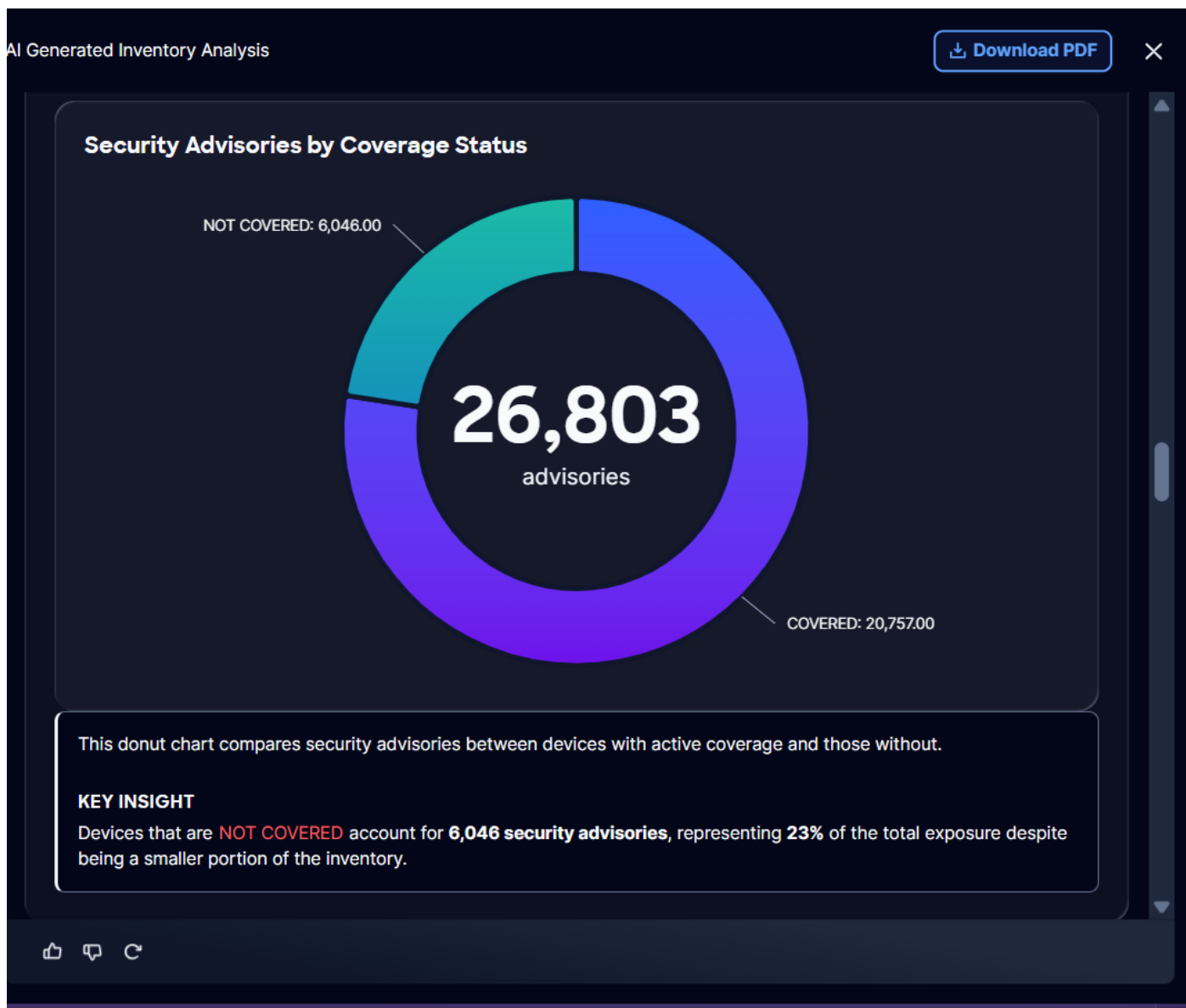
Full Analysis

Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milesto...	Contract Number	Coverage Status	Telemetry Status	Security
		Cloud and ...		End of Ser...	Jun 25, 2028	—	🔒	🔵	0
		Switches		End of Ser...	Jan 29, 2027	—	🔒	🔵	4
		Switches		—	—		🔒	🔵	23
		Switches		—	—		🔒	🔵	23
		Switches		—	—		🔒	🔵	23

Painel de Insights

As seguintes opções estão disponíveis no painel Insights:

- Clique no ícone Expandir para expandir o painel e exibir informações adicionais
- Clique no ícone Thumbs Up ou Thumbs Down para fornecer feedback sobre as informações geradas pelo AI
- Clique em Análise Completa para exibir informações adicionais, análise mais profunda e visualizações como gráficos, painéis e gráficos



Análise completa

As seguintes opções estão disponíveis em uma análise completa:

- Clique em Download do PDF para salvar uma cópia offline da análise para seu registro ou para colaboração

Exportando informações

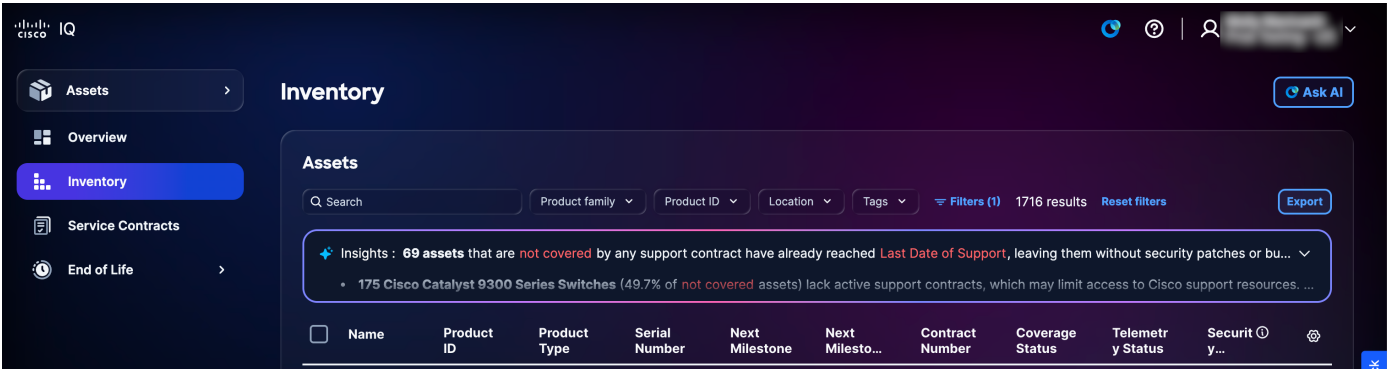
O recurso de exportação permite exportar modos de exibição personalizados de informações de ativos e segurança no formato .xls ou .csv.



Note: O recurso de exportação está disponível apenas para páginas selecionadas.

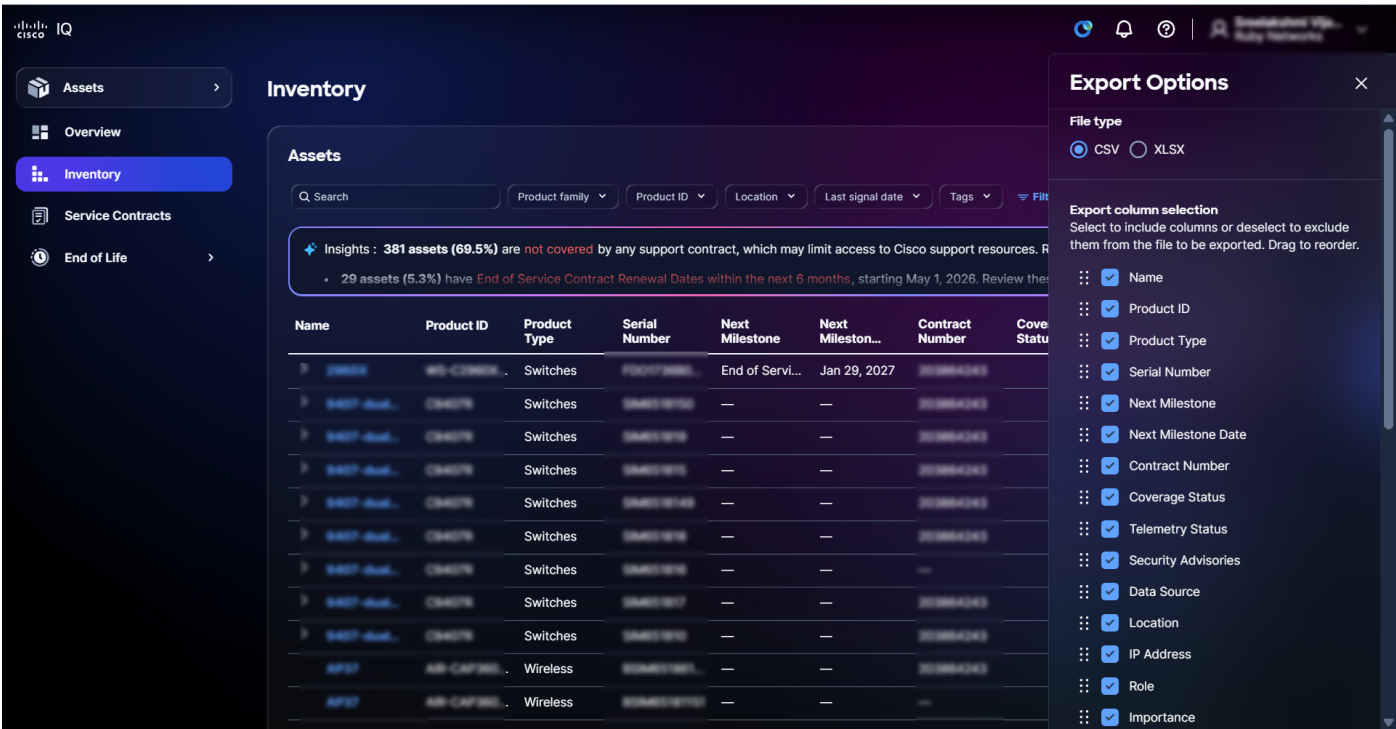
Para exportar informações de uma página:

1. Navegue até a página.



Exportação de Inventário no Módulo Ativos

2. Clique em Exportar. As Opções de exportação são exibidas.



Opções de exportação

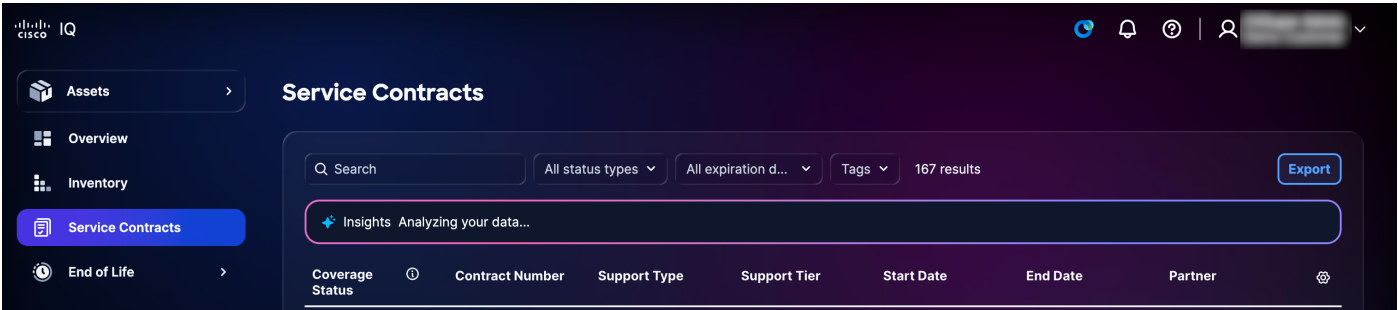
3. Selecione um tipo de arquivo.

4. Marque as caixas de seleção nas colunas desejadas.

5. Clique em Exportar. O arquivo é baixado para a pasta de download local do navegador.

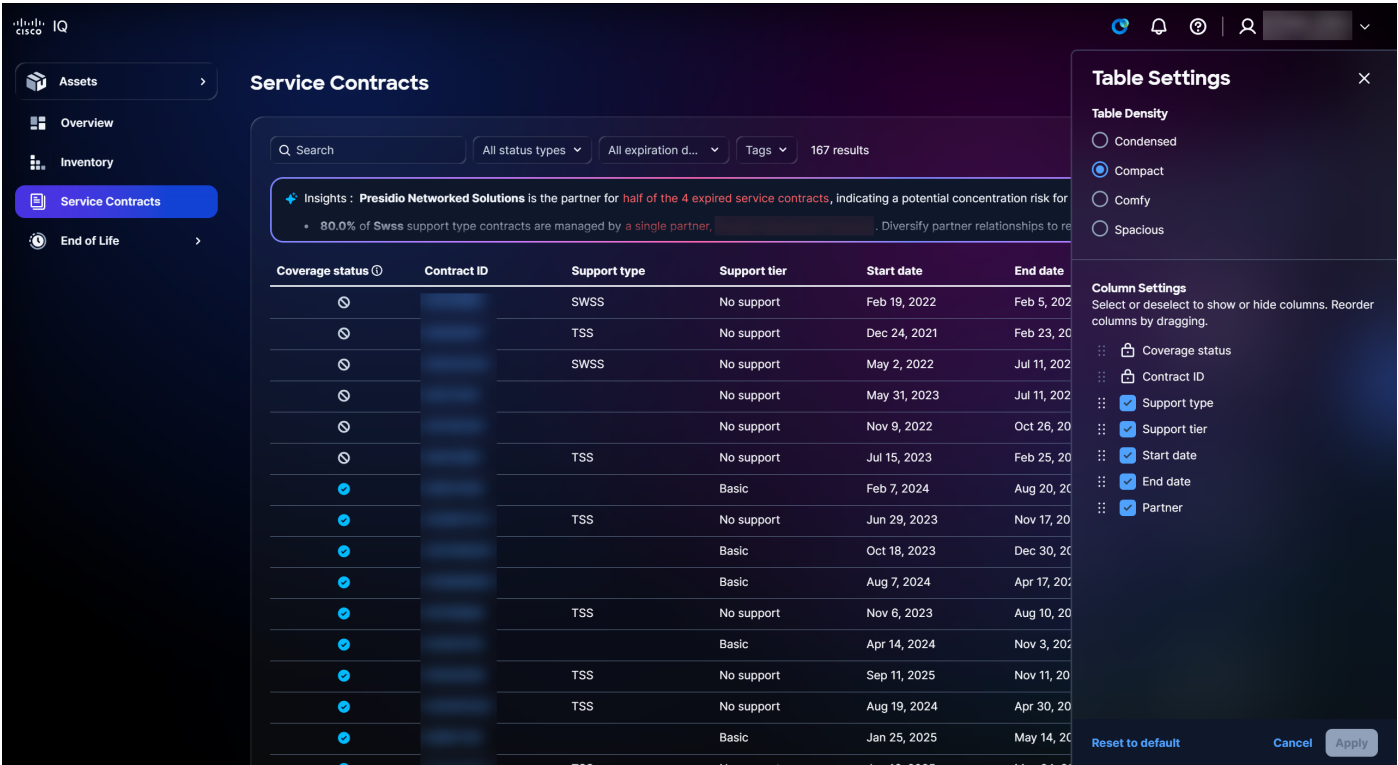
Configurações da tabela

Você pode definir as configurações da tabela para criar exibições personalizadas e refinadas para diferentes recursos do módulo.



Configurações da tabela

Para alterar as colunas exibidas nas páginas selecionadas, clique no ícone Configurações da tabela. As configurações da tabela são exibidas.



Opções de Configuração de Tabela

Alterando a exibição da tabela

Para alterar a exibição da tabela:

1. Selecione uma das seguintes opções de Densidade da tabela:

- Condensado: Minimiza elementos visuais e espaçamento para exibir mais informações
- Compacto: Reduz o espaço em branco e reduz o espaçamento entre os elementos da UI
- Comfy: Utiliza mais espaço em branco e maior espaçamento entre os elementos
- Espaçoso: Enfatiza espaços em branco abundantes e elementos de interface do usuário maiores

2. Clique em Apply.

Adição e remoção de colunas

Para adicionar ou remover colunas:

1. Marque ou desmarque as caixas de seleção Configurações da coluna.
2. Clique em Apply.



Note: A coluna Name não pode ser removida da exibição de tabela.

Alteração da Ordem das Colunas

Para alterar a ordem das colunas:

1. Arraste e solte o nome da coluna para organizar os itens na ordem desejada.
2. Clique em Apply.

Personalização de painéis

O recurso Painel personalizado permite personalizar painéis padrão por meio de uma variedade de opções de personalização intuitivas:

- Reorganizar os widgets ou painéis do painel usando a funcionalidade arrastar e soltar

- Remova todos os componentes que não sejam relevantes para o fluxo de trabalho
- O layout personalizado do painel é armazenado com segurança no seu perfil de usuário e aplicado automaticamente em todas as sessões e dispositivos
- Restaure o layout original do painel com uma simples opção de redefinição

Para personalizar um painel de controle:

1. Navegue até o painel.



Personalizar

2. Clique em Personalizar.



Editar painel

3. Altere o painel conforme desejado:

- Reorganizar: Arraste e solte os widgets no layout desejado
- Remover: Clique no ícone Excluir para remover um widget
- Reinicialização: Clique em Redefinir para padrão para redefinir o painel para seu layout original

4. Click Save. Uma mensagem Painel salvo é exibida.

O layout do painel é aplicado automaticamente em todas as sessões e dispositivos.

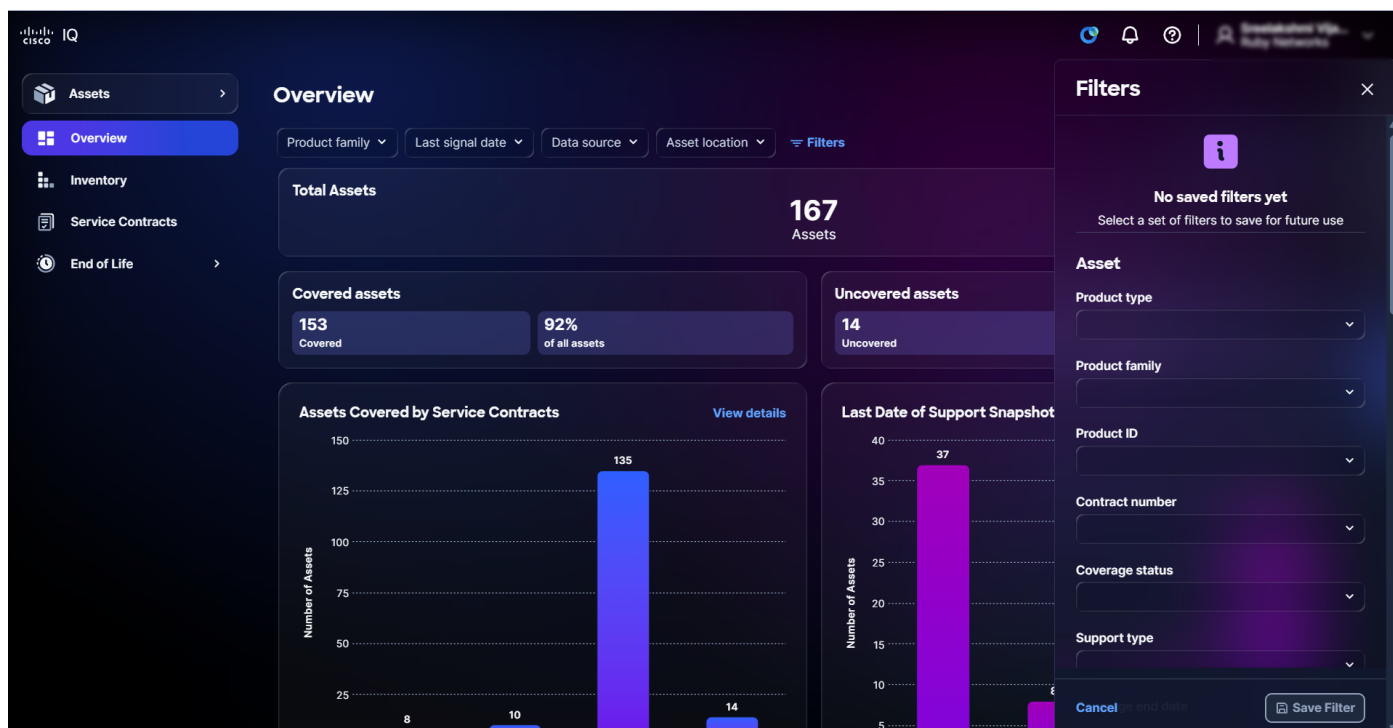
Personalização de filtros

Você pode salvar configurações de filtro personalizadas para qualquer exibição de painel, permitindo que você retorne facilmente às suas configurações preferenciais conforme necessário. Todas as preferências de filtro são armazenadas com segurança por usuário e por conta, garantindo uma experiência personalizada e consistente sempre que você acessa o Cisco IQ.

Criação de um filtro

Para criar um filtro personalizado:

1. Navegue até o painel.
2. Clique em Filtros.



Filtros

3. Escolha os filtros desejados nas listas suspensas.
4. Clique em Save Filter. A janela Filtro salvo por nome é aberta.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

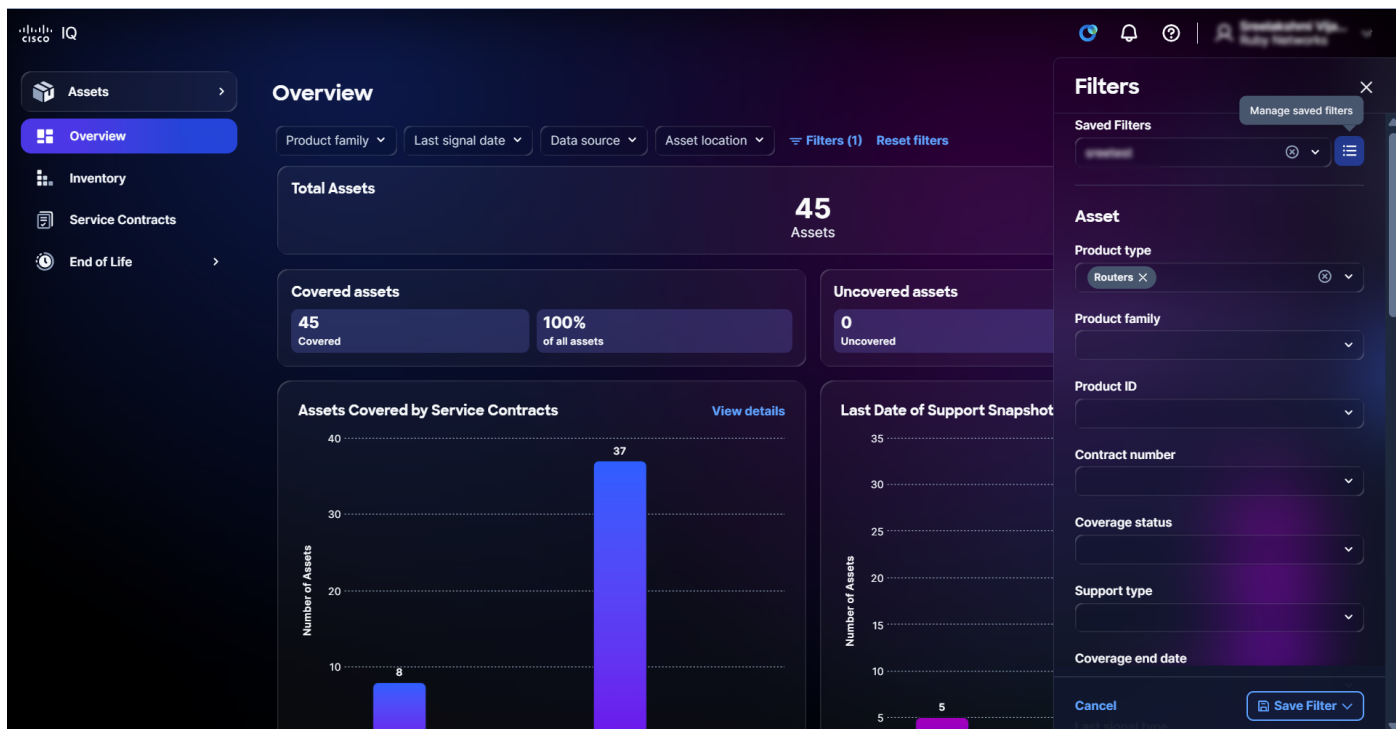
Nome do filtro

5. Insira um nome de Filtro.
6. Clique em Save Filter para confirmar.

Edição de um nome de filtro

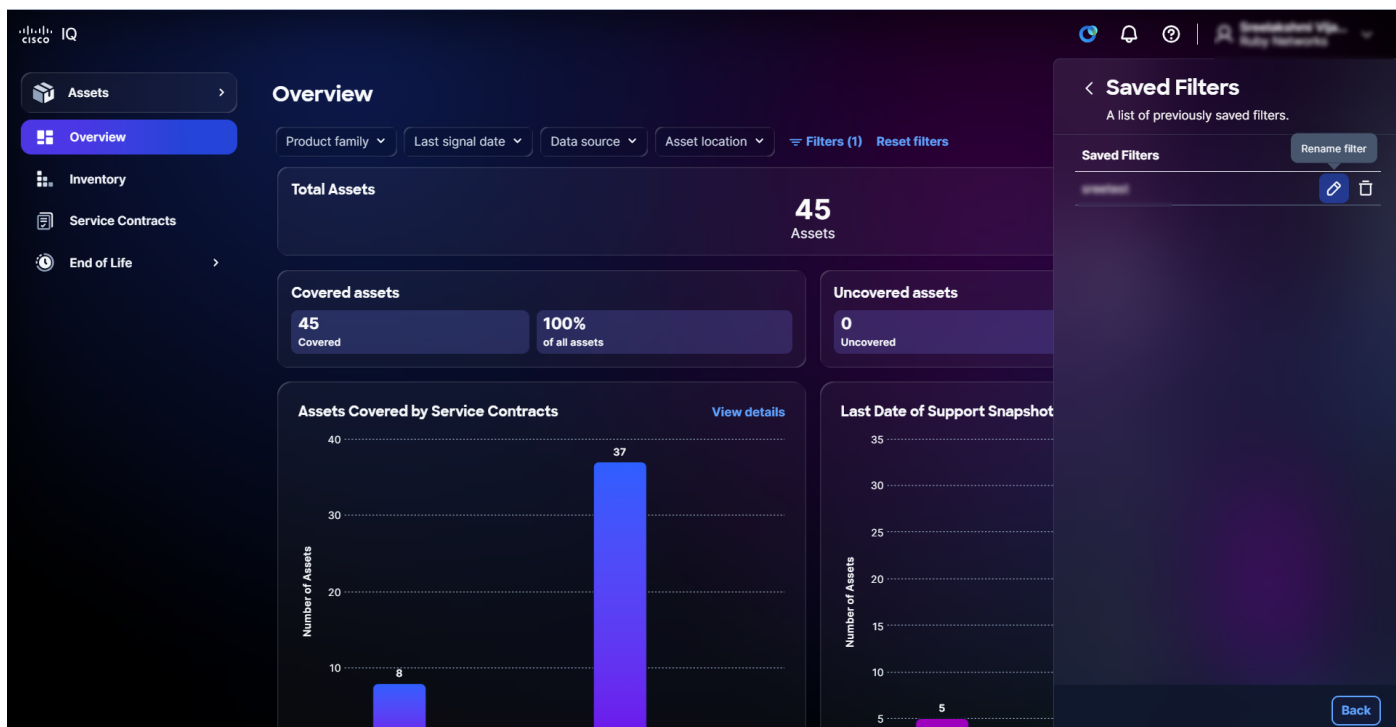
Para editar um filtro personalizado:

1. Clique em Filtros.



Gerenciar filtros salvos

2. Clique no ícone Gerenciar filtros salvos.
3. Navegue até o filtro.



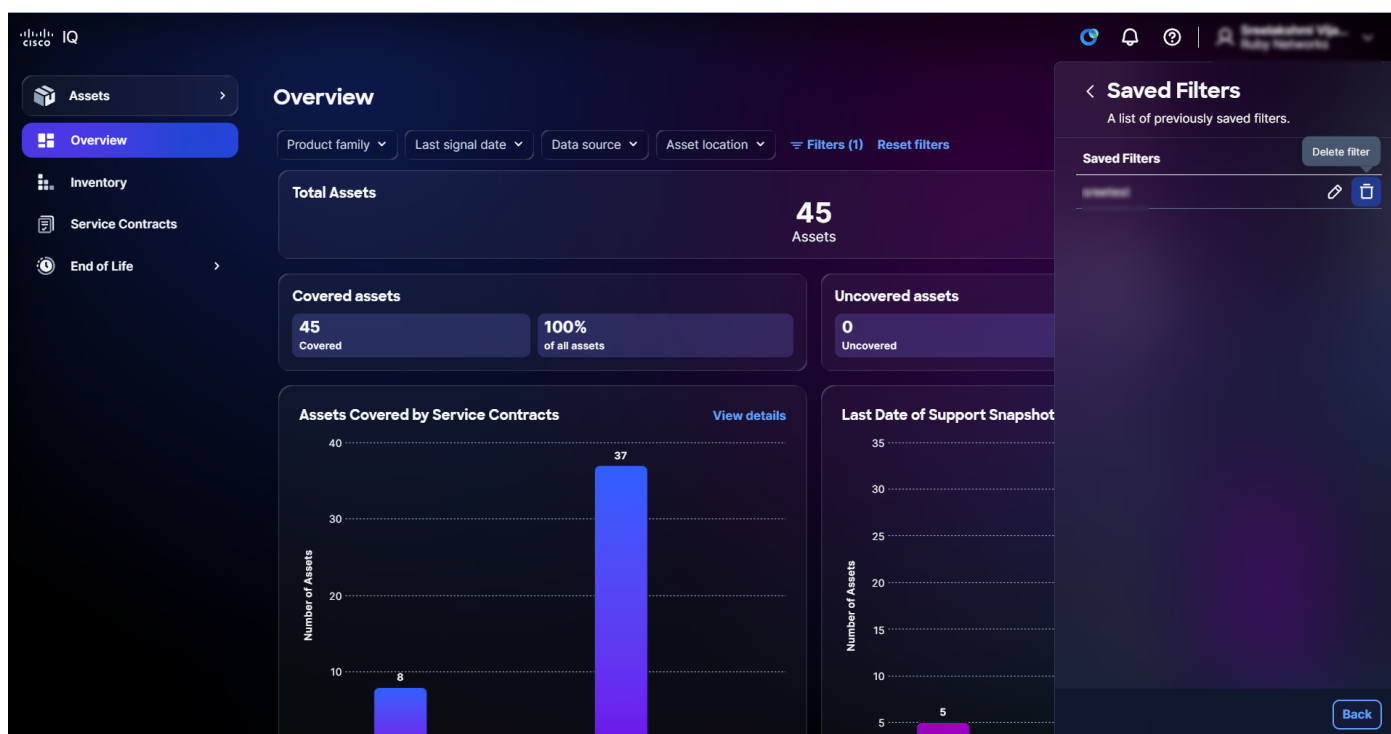
Editar filtro

4. Clique no ícone Edit. A janela Filtro de nome salvo é aberta.
5. Edite o nome do filtro.
6. Clique em Save Filter para confirmar.

Exclusão de um filtro

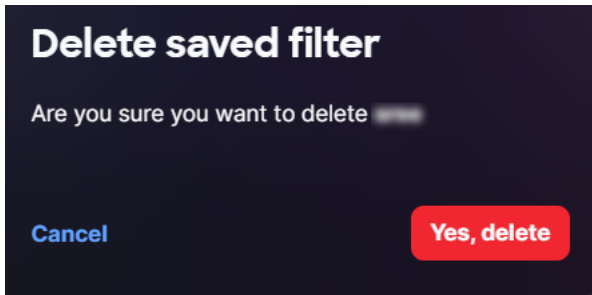
Para excluir um filtro personalizado:

1. Clique em Filtros.
2. Clique no ícone Filtros salvos gerenciados
3. Navegue até o filtro.



Excluir filtro salvo

4. Clique no ícone Delete (Excluir). A janela Excluir filtro salvo é aberta.



Excluir confirmação de filtro salvo

5. Clique em Sim, excluir para confirmar.

Módulo Ativos

O módulo Ativos oferece visibilidade abrangente e recursos de gerenciamento para ativos da Cisco e serve como base do Cisco IQ, fornecendo uma lista centralizada de todos os dispositivos em uma organização. Coletando informações de várias fontes, ele atua como uma única fonte verdadeira para o inventário de dispositivos. Manter uma lista de ativos completa e precisa é essencial, já que outros módulos do Cisco IQ, como o módulo Avaliações, dependem desses dados para avaliar a integridade e a segurança de seus dispositivos.

Conceitos principais

O módulo Ativos baseia-se nos seguintes conceitos principais:

- **Ativo:** Qualquer dispositivo físico, hardware ou software inventariado e gerenciado como parte da prestação de serviços da Cisco com rastreamento detalhado de sua identidade, função, cobertura de serviço e ciclo de vida
- **Ativos de Origem em Contrato:** Os ativos são incluídos no inventário diretamente dos dados do contrato de serviço vinculado, e não por telemetria. O Cisco IQ absorve os seguintes tipos de equipamentos dos dados do contrato: Chassi, módulos, fontes de alimentação e ventiladores. Esses ativos estarão visíveis no Inventário mesmo se nenhuma conexão de telemetria estiver presente
- **Última data de suporte (LDOS):** Rastreamento de marcos de fim da vida útil e fim do suporte para produtos da Cisco
- **Cobertura do serviço:** Contratos de suporte ativos, garantias e níveis de qualificação associados a uma parte específica de hardware ou software
- **Marca do ativo:** Um rótulo definido pelo usuário atribuído a um ativo para organização,

filtragem e fluxos de trabalho operacionais

- Sinal do dispositivo: Refere-se à última vez que a Cisco observou um dispositivo (por seu número de série) com base na telemetria do dispositivo, casos de suporte e renovações de contrato; Os dados de telemetria de ativos são incluídos e aprimorados por meio de um pipeline de dados multicamada

Módulo Acessando ativos

Para acessar os recursos de gerenciamento de ativos no Cisco IQ, escolha o menu Início > Ativos ou clique em Ativos na seção Aplicativo da guia Página inicial > Launchpad. A página Visão geral é exibida.

Visão geral dos ativos

A página Visão geral exibe um painel que permite avaliar rapidamente a integridade e o status dos dispositivos.

100% Assets, Asset ID, Asset ID, Asset ID, Asset ID



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

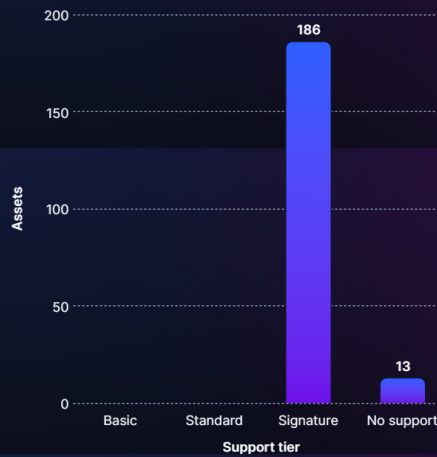
13

Uncovered

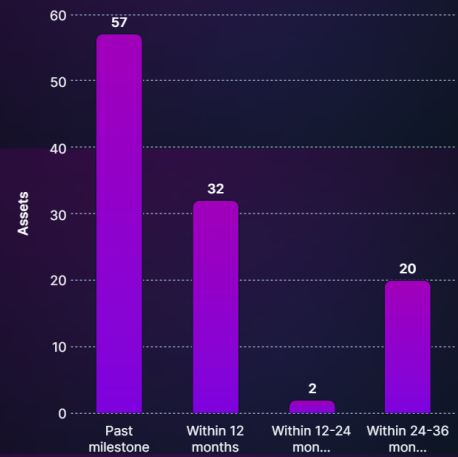
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

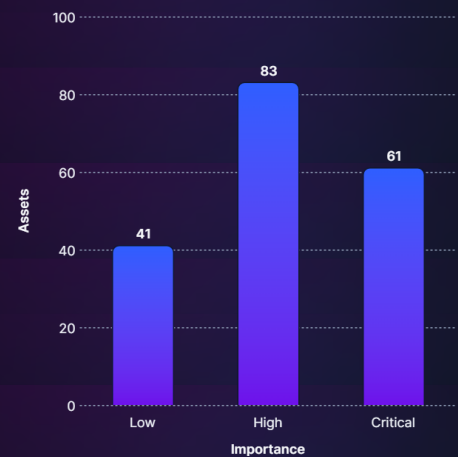
Assets With Critical or High Security Advisories [View details](#)



Of the 186 assets with telemetry enabled, 170 have critical or high Security Advisories

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

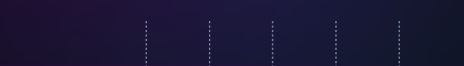


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



Visão geral dos ativos

O painel exibe as seguintes informações:

- Total de ativos: O número total de ativos na conta do Cisco IQ
- Principais métricas de ativos: Principais métricas adicionais, como status de telemetria, avisos de segurança críticos e informações de LDOS
- Ativos cobertos: Número total e percentagem de ativos abrangidos por contratos de serviços
- Ativos não cobertos: Número total e percentagem de ativos não cobertos por contratos de serviços
- Ativos cobertos por contratos de serviço: Uma divisão do número de ativos (hardware ou software) cobertos pelos contratos de serviço, categorizada por nível de direito
- Último Instantâneo de Data de Suporte: Repartição do número de ativos que passaram pelo LDOS ou que atingiram o LDOS
- Ativos com telemetria ativada: Número total e percentual de ativos com telemetria habilitada
- Ativos sem Telemetria Habilitada: Número total e percentual de ativos sem telemetria habilitada
- Ativos com avisos de segurança críticos ou altos: Percentual do total de ativos com telemetria habilitada e que têm recomendações de segurança críticas ou altas
- Ativos por importância: Uma divisão da prioridade atribuída a um dispositivo em relação a outros dispositivos na rede.
- Desagregação dos ativos: Uma exibição detalhada de informações de ativos, como famílias de produtos, locais de instalação, versões de software e funções de ativos

Filtrando exibições de ativos

Você pode filtrar a exibição de painel escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis.

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibindo Detalhes de Ativos

Ao clicar em Exibir detalhes, a página é redirecionada para a página Inventário. Consulte [Inventário](#) para obter mais informações.

Insights sobre a importância dos ativos

O Cisco IQ inclui o Asset Criticality Insights, um novo recurso no módulo Ativos que prevê a função funcional e a importância comercial dos dispositivos de rede. Analisando as configurações de dispositivos e os recursos ativados, os Asset Criticality Insights ajudam a identificar quais ativos têm o maior impacto na rede, para que você possa priorizá-los para correção de segurança, atualizações de software, planejamento de EOL (End-of-Life, fim da vida útil) e decisões de cobertura.

 Note: Os Insights de Criticidade de Ativos estão disponíveis exclusivamente para ativos com níveis Padrão ou Assinatura que tenham conexões de telemetria ativas. Certifique-se de que seus ativos atendam aos requisitos de configuração para preencher esses insights no painel.

Os Insights de Criticidade de Ativos estão disponíveis no aplicativo Ativos nas seguintes áreas:

- Visão geral dos ativos: Filtrar e exibir detalhamentos de resumo por atributos do Asset Criticality Insights
- Inventário de ativos: Exibir, pesquisar, filtrar e classificar dispositivos por Função e Importância
- Detalhes do ativo: Exibir função e importância de dispositivos individuais, com dicas informativas explicando cada valor

Substituição de Funções e Classificações de Importância

O Cisco IQ prevê automaticamente a função e a importância de cada ativo com base nos dados de telemetria. Os administradores de conta podem corrigir manualmente essas classificações quando a previsão automatizada não reflete com precisão a função ou a importância do ativo na rede.

 Note: Os controles de substituição estão disponíveis somente para Administradores de Conta. Os valores de Função e Importância são somente leitura para todas as outras funções de usuário.

Sobrepondo Classificações da Tabela de Inventário

Para sobrepor Função ou Importância para um ou mais ativos:

1. Navegue até Ativos > Inventário.
2. Clique na caixa de seleção da linha de ativos desejada. Para atualizar vários ativos simultaneamente, marque várias caixas de seleção.

The screenshot displays the Cisco IQ Inventory management interface. On the left is a sidebar with navigation options: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main header shows 'Inventory' and an 'Ask AI' button. Below the header, there's a search bar and filter controls indicating 20 results. An 'Insights' box provides a summary: 'Of the 1 assets where Coverage Status is not covered, 1 (100.0%) have Product Description NCS 560 Route...'. Below this, a table lists 4 selected items. The table columns are: Name, Product ID, Product Name, Equipment Name, Serial Number, Next Mile, Next Mile, Contract, Coverage, Telemetry, and a selection checkbox. The table shows 4 items selected. The interface includes a sidebar with 'Assets', 'Overview', 'Inventory', 'Service Contracts', and 'End of Life' sections. The main content area has a search bar, filters (2), 20 results, and buttons for Export and Saved Filters. An insights section shows that 1 asset (100.0%) has a Coverage Status of 'not covered'.

	Name	Product ID	Product Name	Equipment Name	Serial Number	Next Mile	Next Mile	Contract	Coverage	Telemetry	
☐			Modules	Module		—	—		✓	✓	0
☐			Modules	Module		—	—		✗	✓	0
☒			Unified ...	Chassis		—	—		✓	✓	1
☐			Storage...	Chassis		—	—		✓	✓	0

Função e importância

3. Na coluna Função ou Importância, escolha o valor correto na lista suspensa da linha do ativo.
4. Clique em Aplicar para confirmar a substituição.

Ativos com valores substituídos manualmente exibem um indicador visual na coluna Função ou Importância.

 Note: Para remover uma substituição configurada anteriormente e retornar à previsão automatizada, selecione a opção de traço (—) na lista suspensa Função ou Importância.

Sobrepondo Classificações dos Detalhes do Ativo

Para sobrepor Função ou Importância da view detalhada do ativo:

1. Navegue até Ativos > Inventário e clique em um ativo.
2. No painel de detalhes de ativos, localize os campos Função e Importância.
3. Clique na lista suspensa do campo que deseja atualizar e selecione o valor correto.
4. Clique em Apply para confirmar.

Uma exibição detalhada do ativo também exibe uma explicação dos atributos de telemetria que informaram a previsão automatizada original, para ajudar a determinar se uma substituição é apropriada.

Exibindo a Trilha de Auditoria de Sobreposição

Todas as substituições de Função e Importância são registradas em uma trilha de auditoria no nível da conta. Para acessar a trilha de auditoria:

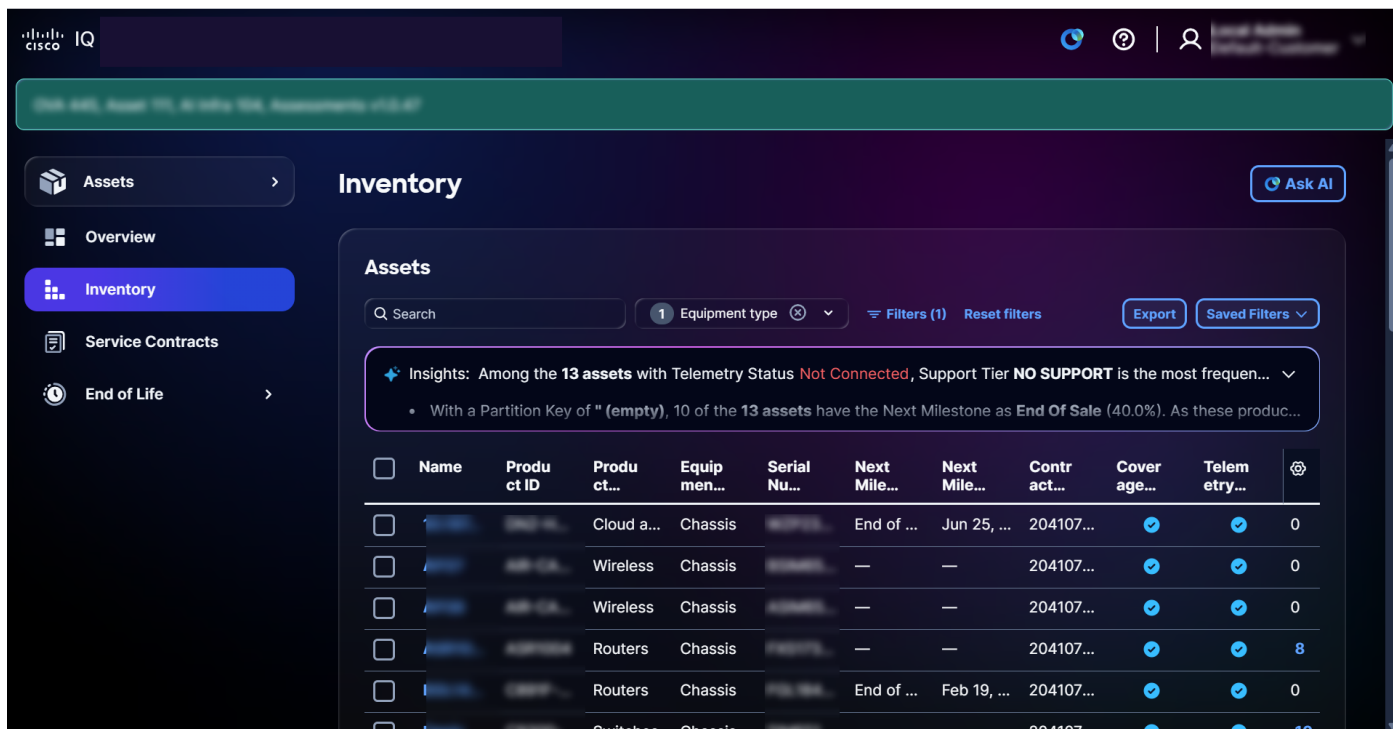
1. Escolha Início > Configurações do sistema > Atividade e registros.
2. Escolha Filtros > Tipo de ação > substituir para exibir somente eventos de substituição.

A trilha de auditoria exibe o nome do ativo, os valores novos e anteriores, o usuário que fez a alteração e a data e a hora da alteração. A trilha de auditoria pode ser exportada usando a opção Export.

 Note: A trilha de auditoria pode ser filtrada por intervalo de datas, usuário e nome do ativo.

Inventário

A página Inventário fornece uma lista de todos os ativos da Cisco na conta do Cisco IQ.



Inventário

Pesquisando e filtrando exibições do Inventário de ativos

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar ativos inserindo o nome do ativo no campo Pesquisar.

 Note:

- Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.
- Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Análise de inventário

O painel Insights na página Inventory exibe uma análise orientada por IA que fornece um resumo de ativos com foco na cobertura de suporte, conectividade e marcos. Clique em Análise Completa para obter visualizações como gráficos, painéis e gráficos que fornecem informações adicionais. Consulte [Analisando Dados](#) em Recursos Comuns do Módulo para obter mais detalhes.

Exportando inventário

Clique em Exportar para salvar uma lista de inventário filtrada no formato .xls ou .csv. Consulte [Exportando informações](#) em Recursos comuns de módulo para obter mais detalhes.

Exibindo Detalhes do Ativo

Clique em um ativo para exibir os detalhes do ativo. Uma exibição de detalhes do ativo é exibida com as seguintes guias:

- Detalhes: Exibe detalhes do ativo, como informações sobre o produto, dados de sinal, identidade, local, garantia e cobertura

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Details

Product Alerts

Hardware

Software

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Ask AI

Detalhes do ativo

- Alertas do produto: Exibe alertas de produtos relacionados, como avisos de segurança e

aviso de campo

- Hardware: Fornece uma visão detalhada do cronograma para as datas de EOL do hardware (por exemplo, Fim das vendas, Última remessa e Última data de suporte)
- Software: Fornece uma visão detalhada do cronograma para o EOL do software

Tags de ativos

As etiquetas de inventário são etiquetas personalizadas que você atribui aos ativos de inventário no Cisco IQ. Uma marca é um par chave:valor, por exemplo, Ambiente:Produto ou Rótulo:Campus, que você define. Você pode atribuir etiquetas a ativos individuais ou a vários ativos de uma só vez e pode filtrar seu inventário por etiqueta para localizar rapidamente os ativos importantes para você.

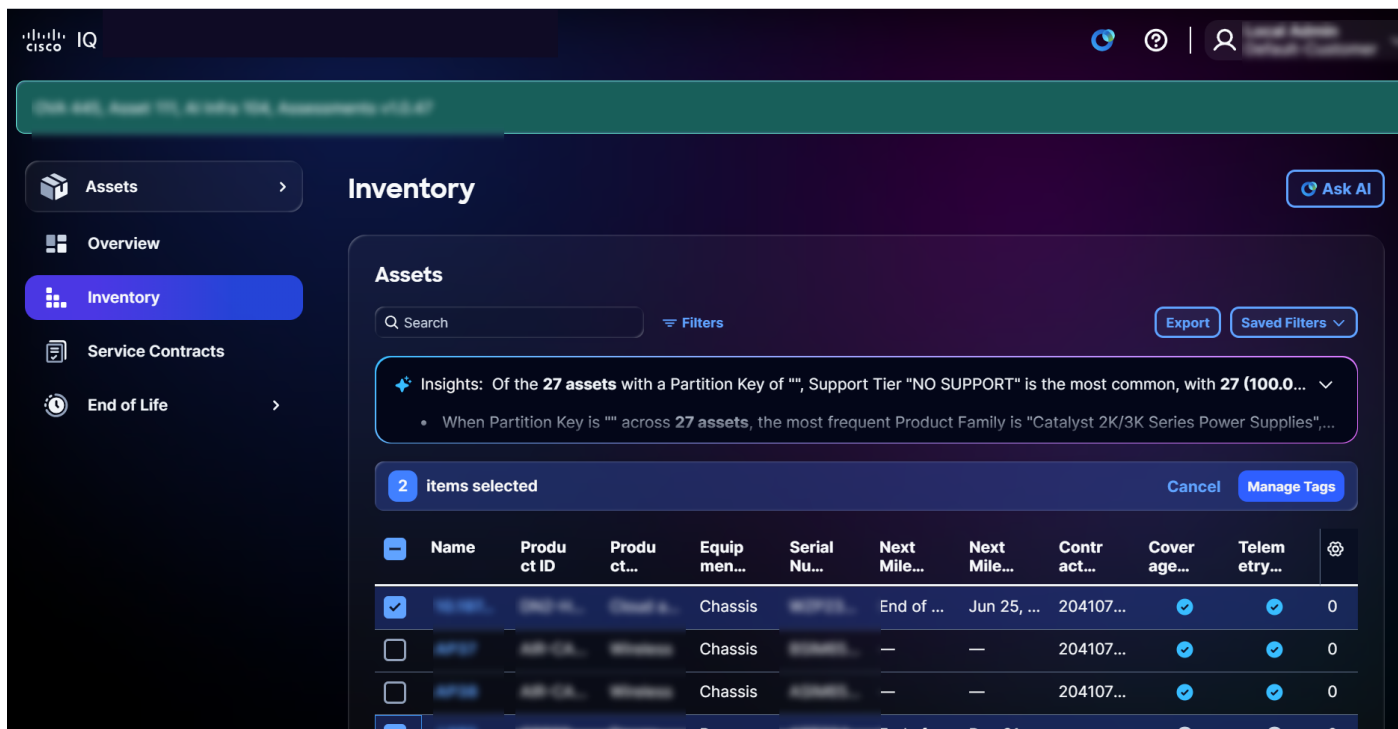
 **Note:** Depois que uma etiqueta é criada por um administrador de conta, os usuários podem atribuir uma etiqueta a um ativo.

Atribuição de marcas

A atribuição de etiquetas aos ativos selecionados na exibição Inventário permite a organização e a categorização de ativos para filtragem, geração de relatórios e gerenciamento avançados.

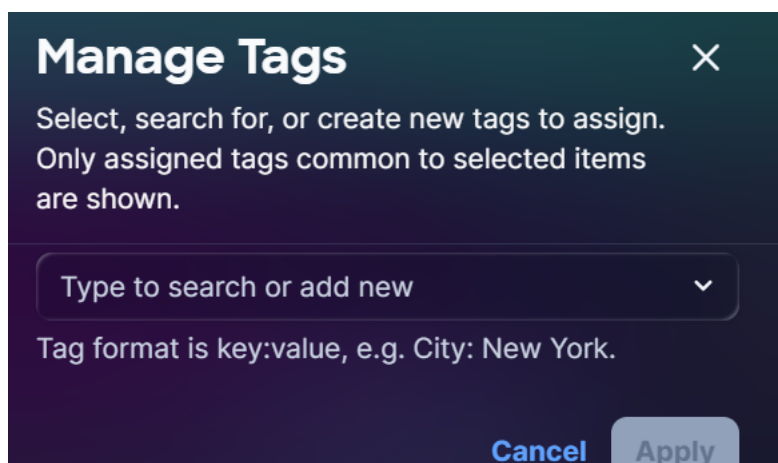
Para atribuir uma etiqueta a um ativo:

1. Navegue até Ativos > Inventário.



Marcação de ativos

2. Marque as caixas de seleção dos ativos desejados.
3. Clique em Gerenciar marcas. A janela Gerenciar marcas é aberta.



Atribuição de marcas

4. No campo de texto, insira ou selecione o nome da tag nas opções existentes e pressione Enter.



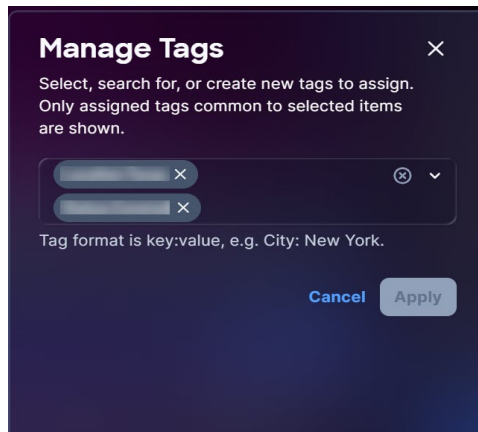
Note: As marcas estão no formato key:value (por exemplo, Cidade:NYC).

5. Clique em Apply.

Remoção de tags de ativos

Para remover uma tag de um ou mais ativos:

1. Navegue até Ativos > Inventário.
2. Marque a caixa de seleção ao lado de um ou mais ativos.
3. Clique em Gerenciar tags. A janela Gerenciar marcas é aberta.



Remoção de marcas

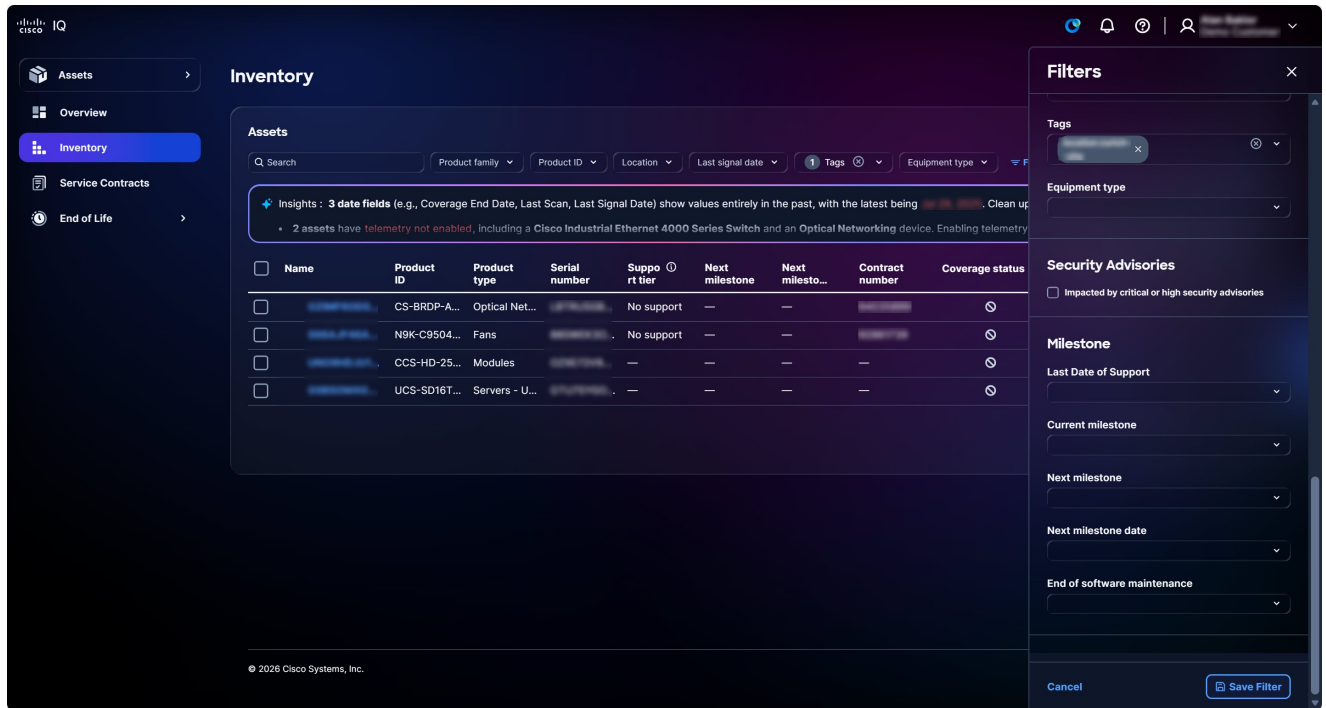
4. Clique no X em qualquer tag para removê-la da seleção.
5. Clique em Apply.

Uso de tags de ativos como filtros

Depois de criar uma marca, você pode usá-la como um filtro.

Para usar uma tag como filtro:

1. Navegue até a página Inventário.
2. Clique em Filtros. A janela Filtros é aberta.

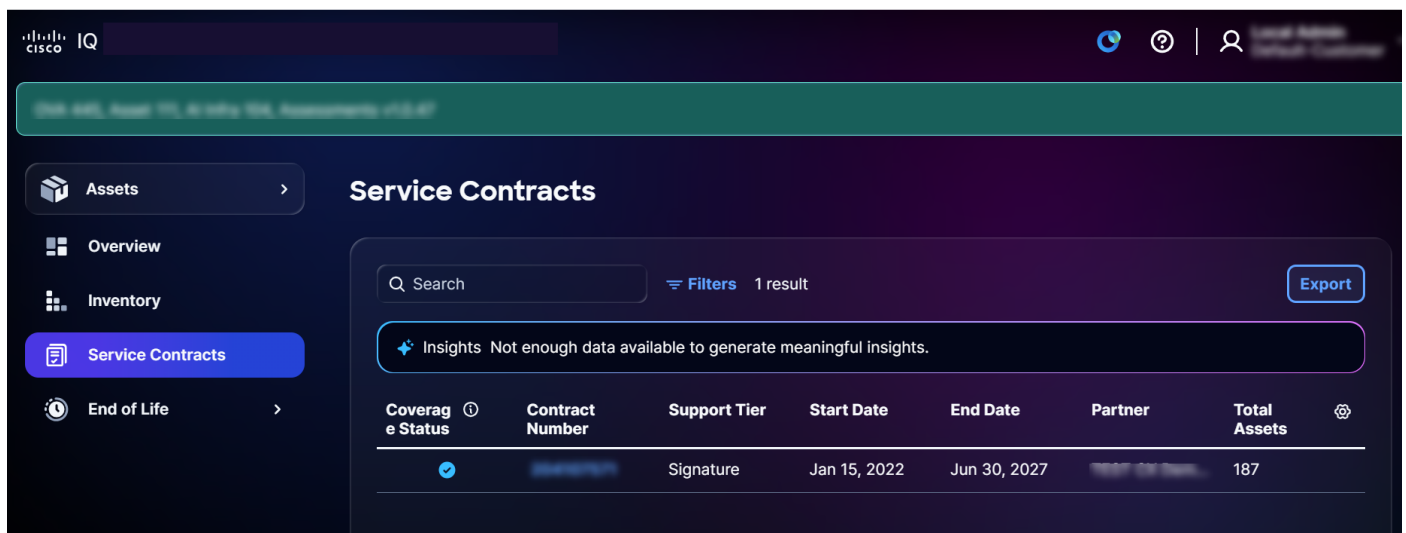


Uso da marca como filtro

- Na lista suspensa Marcas, marque as caixas de seleção das marcas desejadas. Depois de selecionar a etiqueta, a visualização na página Inventário é atualizada para a visualização filtrada.

Contratos de serviço

A página Contratos de serviço agiliza a supervisão do contrato de suporte fornecendo resumos e informações detalhadas do contrato, oferecendo suporte a estratégias eficazes de planejamento e cobertura de renovação.



Contratos de serviço

Pesquisando e filtrando exibições para contratos de serviço

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas. Você também pode procurar contratos de serviço inserindo o número do contrato no campo Pesquisar.

Exportação de contratos de serviço

Clique em Exportar para salvar uma lista filtrada de contratos no formato .xls ou .csv. Consulte [Exportando informações](#) em Recursos comuns de módulo para obter mais detalhes.

Resumo do EA de serviços

A página Resumo do Services Enterprise Agreement (EA) oferece uma visão consolidada do crescimento da base instalada em todo o portfólio de ativos. Os dados são originados diretamente dos registros da base instalada da Cisco, proporcionando a você e às equipes de contas uma visão consistente das alterações do portfólio ao longo do tempo.

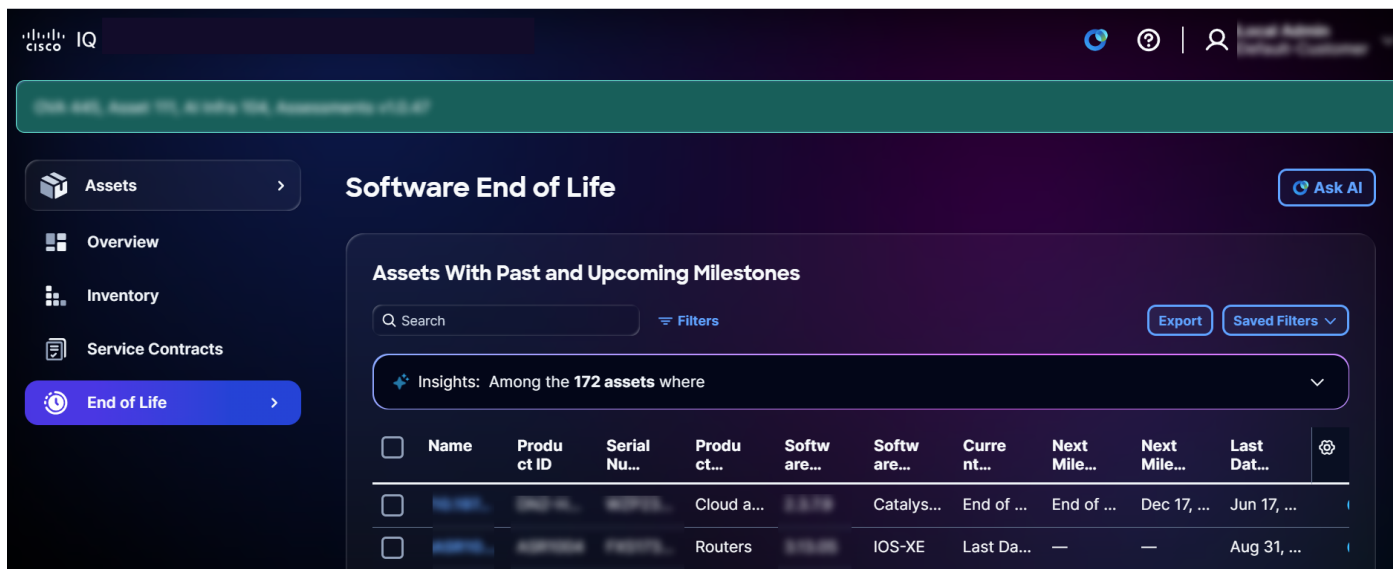
A página Resumo do EA de Serviços exibe as seguintes informações:

- Ativos adicionados: Novos ativos adicionados à base instalada durante o período de geração de relatórios
- Alteração líquida: A alteração geral no tamanho da Base Instalada para o período de geração de relatórios

 Note: O acesso à página Resumo do EA de Serviços pode estar sujeito aos requisitos de função e permissão. Entre em contato com o administrador da conta se essa página não estiver visível na sua navegação.

Fim da vida útil

As páginas Fim da vida útil do hardware e Fim da vida útil do software fornecem informações detalhadas de EOL, proporcionando aos usuários o suporte necessário para gerenciar de forma proativa os ciclos de atualização do produto e a cobertura de suporte. Clicar em um ativo nas páginas Fim da vida útil o redireciona para o ativo relevante na página Inventário.



Fim da vida útil do software

Análise do fim da vida útil

O painel Insights na página End of Life exibe uma visão geral dos ativos acionada pela IA com um Último dia de suporte definido. Clique em Análise Completa para obter visualizações como gráficos, painéis e gráficos que fornecem informações adicionais. Consulte [Analisando Dados](#) em Recursos Comuns do Módulo para obter mais detalhes.

Exportando fim da vida útil

Clique em Exportar para salvar uma lista filtrada de ativos EOL no formato .xls ou .csv. Consulte [Exportando informações](#) em Recursos comuns de módulo para obter mais detalhes.

Módulo de avaliações

O módulo de Avaliações fornece uma estrutura de avaliação que permite que você investigue e reduza proativamente os riscos relacionados à segurança, estabilidade, capacidade, conformidade e envelhecimento, mantendo as redes seguras, estáveis e confiáveis.

Conceitos principais

O módulo de avaliações se baseia nos seguintes conceitos principais:

- **Avaliação:** Uma avaliação sistemática das entidades de infraestrutura em função de critérios predefinidos para medir o desempenho, a conformidade, a segurança ou a capacidade operacional; As avaliações são acionadas sob demanda, em uma programação ou por um evento
- **Execução da avaliação:** Uma instância ou uma única execução de uma avaliação; Cada execução cria um novo registro de execução que rastreia o escopo, o mecanismo de acionamento, o timestamp e os dados resultantes produzidos pela avaliação
- **Localizando:** Uma observação validada e acionável que identifica uma lacuna, um risco, um problema ou um estado digno de nota. Os resultados representam os dados de nível básico durante uma avaliação
- **Informações:** Uma conclusão analítica de nível superior derivada de padrões ou tendências em vários achados. Os insights interpretam o que as descobertas significam em um contexto operacional ou de negócios mais amplo
- **Recomendação:** Uma receita específica e acionável vinculada a descobertas ou insights; As recomendações fornecem orientações claras sobre as etapas necessárias para resolver problemas identificados ou capitalizar oportunidades
- **Relatório:** Um documento estruturado que agrega descobertas, percepções e recomendações para um público-alvo; Os relatórios são o principal produto final para a comunicação dos resultados da avaliação a clientes, executivos e equipes técnicas

Acessando o módulo Avaliações

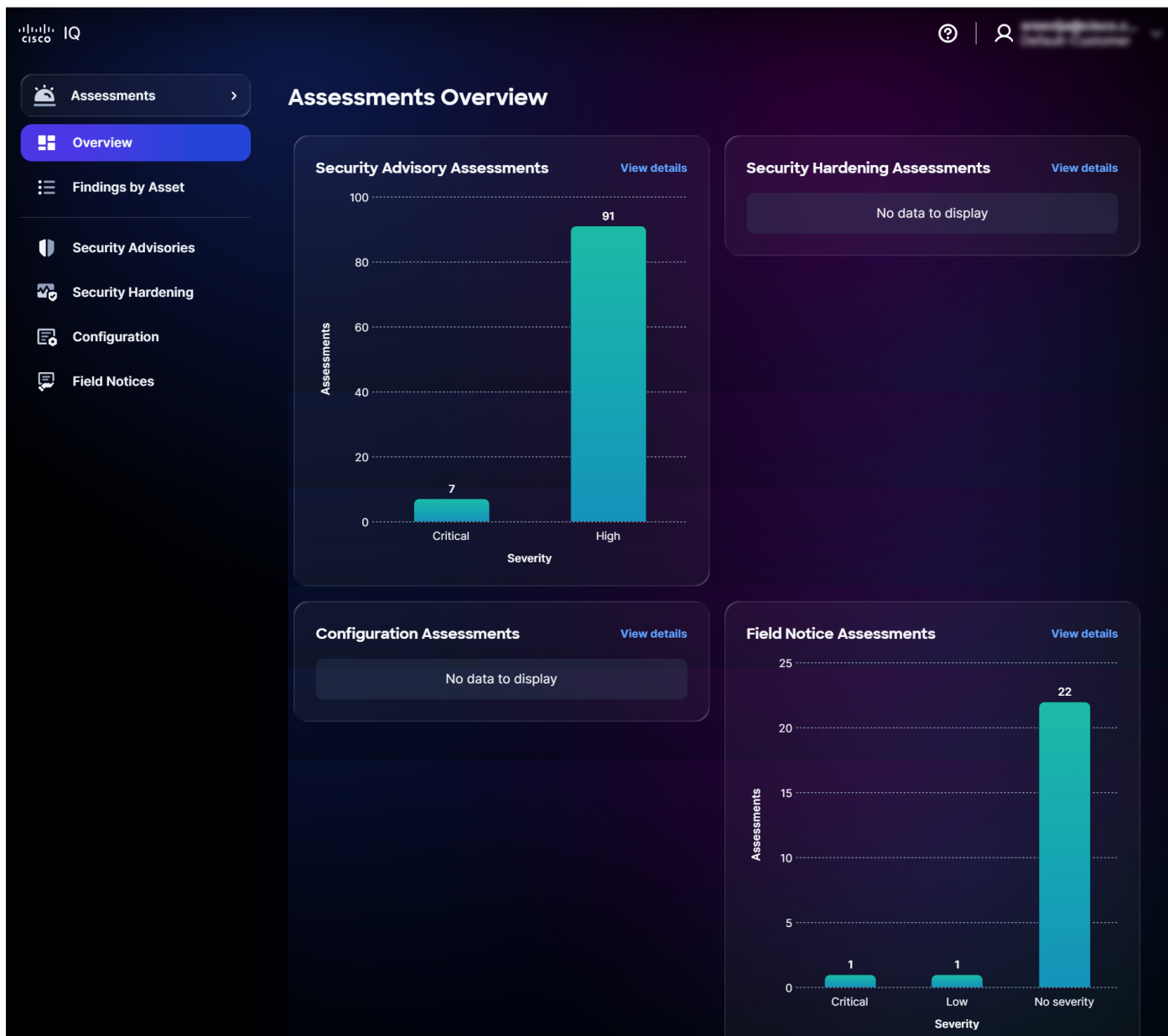
Para acessar os recursos de segurança e avaliação no Virtual Appliance, escolha o menu Início > Avaliações ou clique em Avaliações na seção Aplicativo da guia Página inicial > Launchpad. A página Visão geral das avaliações é exibida.



Note: O módulo de avaliação também pode ser iniciado em System Configuration > Package Management.

Visão geral das avaliações

A página Assessment Overview exibe o seguinte painel:



Visão geral das avaliações

O painel exibe as seguintes informações:

- Avaliações de consultoria de segurança: Exibe avaliações de avisos de segurança, categorizadas por Gravidade crítica e alta
- Avaliações de fortalecimento da segurança: Exibe ativos que falham nas regras de proteção de segurança, categorizados por severidade Alta, Média, Baixa e Informativa
- Avaliações de configuração: Exibe ativos que falham nas regras de conformidade de configuração, categorizados por gravidade crítica, alta, média, baixa e informativa
- Avaliações de notificação de campo: Exibe avaliações de avisos de campo, categorizados por Gravidade Crítica, Alta e Não aplicável



Note: Você só pode exibir os ativos aos quais tem direito de acesso.

Descobertas por ativo

A página Descobertas por ativo fornece uma lista de ativos que foram avaliados usando pelo menos uma das seguintes avaliações: Avisos de segurança, Fortalecimento da segurança, Configuração e Avisos de campo.

The screenshot shows the 'Findings by Asset' page in the Cisco IQ interface. The page has a dark theme. On the left, there is a sidebar with navigation links: 'Assessments', 'Overview', 'Findings by Asset' (highlighted in blue), 'Security Advisories', 'Security Hardening', 'Configuration', and 'Field Notices'. The main content area is titled 'Findings by Asset' and contains a search bar, a 'Filters' button, and a '208 results' indicator. Below this is a table with the following columns: 'Name', 'Importance', 'IP Address', 'Serial Number', 'Security Advisory', 'Security Hardening', 'Configuration', 'Field Notice', and 'Signature'. The table displays 5 rows of data, all with 'Low' importance and a 'Signature' link. The top right of the page shows user information and a search bar.

Name	Importance	IP Address	Serial Number	Security Advisory	Security Hardening	Configuration	Field Notice	Signature
Findings by Asset	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Findings by Asset	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Findings by Asset	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Findings by Asset	Low	10.10.10.10	1000000000	5	11	32	1	Signature
Findings by Asset	Low	10.10.10.10	1000000000	5	11	32	1	Signature

Constatações por ativos

Pesquisando e filtrando exibições de descobertas por ativo

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode pesquisar descobertas por ativo no campo Pesquisar.



Note:

- Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.
- Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

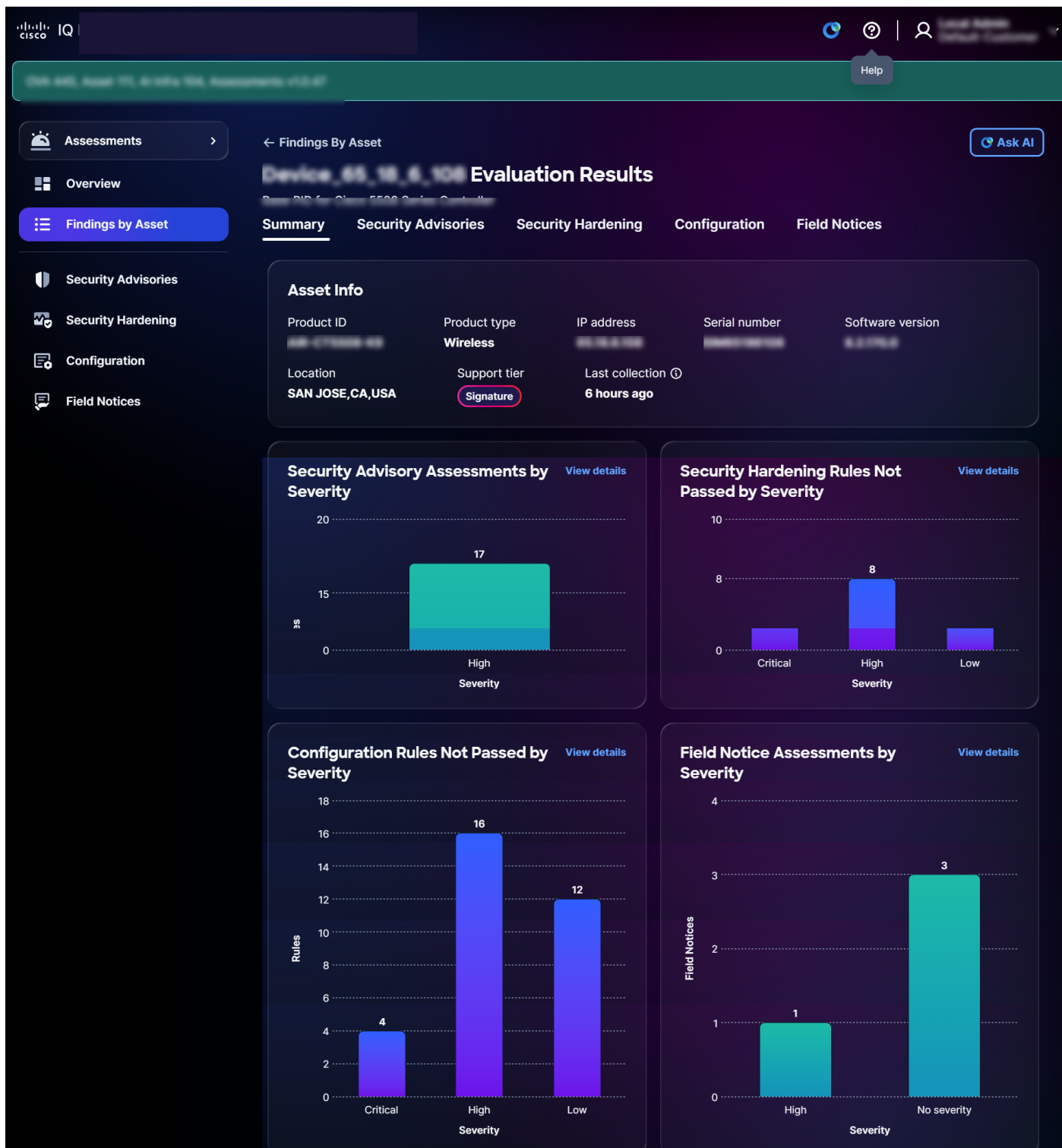
Exportando Descobertas por Ativo

Para exportar a exibição de lista Descobertas por ativo, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Exibição de Descobertas por Detalhes do Ativo

Para exibir os detalhes de Descobertas por ativo, clique em um Ativo. As guias a seguir exibem detalhes do ativo selecionado:

- **Resumo:** Fornece informações detalhadas de ativos, incluindo o número de Avisos de Segurança, Fortalecimento da Segurança, Configuração e Avisos de Campo
- **Avisos de segurança:** Fornece uma lista de avaliações relacionadas do Security Advisory
- **Fortalecimento da segurança:** Fornece uma lista de ativos que falham nas regras de Proteção de Segurança
- **Configuração:** Fornece uma lista de ativos que falham nas regras de Práticas Recomendadas de Configuração
- **Notas de campo:** Fornece uma lista de avaliações de Field Notice relacionadas



Descobertas por detalhes do ativo

Ao clicar em Exibir Detalhes em um bloco, a página redireciona para a página relevante dentro do módulo.

Ao clicar em Exibir detalhes completos do ativo, a página de exibição de detalhes do ativo é exibida.

Orientações de Segurança

As avaliações do Security Advisory identificam vulnerabilidades e as priorizam com base em seu risco, gravidade e criticidade, aprimorando, assim, os recursos de gerenciamento de riscos da empresa. As Consultorias de segurança fornecem insights granulares sobre vulnerabilidades, ajudam a acelerar a mitigação de ameaças críticas e garantem o alinhamento com a conformidade e os objetivos de negócios. Isso fortalece a postura de segurança, otimiza a alocação de recursos e promove a resiliência contra ameaças em evolução em toda a empresa. Os avisos de segurança são atualizados automaticamente no Cisco IQ assim que são lançados.

A página Recomendações de Segurança fornece uma lista de todas as Recomendações de Segurança com vulnerabilidades detectadas na organização. Clicar em uma recomendação na lista de avaliações da Recomendação de Segurança navega para a view detalhada correspondente.

Security Advisories

About the Assessments

These assessments compare your assets against Cisco Security Advisories. Security Advisories flag product security vulnerabilities that may need action to prevent incidents.

Security Advisory Assessments

Search Filters 98 results Export Saved Filters

Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12		Oct 4, 2019
Cisco IOS and I...	High	0	1		Sep 25, 2019
Cisco IOS and I...	High	1	0		Mar 23, 2016
Multiple Vulner...	High	0	1		Jan 11, 2016
Cisco IOS and I...	High	0	1		Jul 26, 2017
Cisco IOS and I...	High	1	0		Sep 28, 2016

Orientações de Segurança

Pesquisando e Filtrando Views para Recomendações de Segurança

Você pode filtrar a exibição de lista escolhendo um filtro na lista suspensa. Você também pode procurar avaliações de Consultoria de segurança inserindo o nome da avaliação no campo Pesquisar.

 Nota: Alguns filtros podem estar ocultos, dependendo das configurações de zoom da tela. Alguns filtros podem estar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões. Os valores de gravidade ausentes são exibidos como "-" com uma dica de ferramenta descritiva.

Exportando Avisos de Segurança

Para exportar as avaliações do Security Advisory, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Exibindo Detalhes da Avaliação da Consultoria de Segurança

Clique em uma avaliação para visualizar detalhes adicionais sobre ela. A página de detalhes fornece informações como a Pontuação do Common Vulnerability Scoring System (CVSS), Vulnerabilidades e Exposições Comuns (CVE), Severidade e um link para o Cisco Security Advisory mencionado.

Você pode exibir os seguintes tipos de resultados na tabela Resultado da avaliação:

- Afetado: Indica que o ativo ou componente tem uma vulnerabilidade confirmada que pode ser explorada por um invasor, exigindo correção
- Potencialmente afetado: Indica que o ativo ou componente apresenta sinais que podem conduzir a vulnerabilidade, mas não está definitivamente confirmado; pode ser necessária uma investigação adicional

The screenshot shows the Cisco IQ interface for Security Advisories. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area is titled 'Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability'. It includes an 'About the Assessment' section with a description of the vulnerability, severity (High), CVE, CVSS score, version (1.1), first published date (Sep 25, 2019), and last updated date (Oct 4, 2019). Below this is the 'Asset Results' section, which displays a table of affected assets. The table has columns for Asset, Result, Product ID, IP Address, Serial Number, and Support Tier. The results show several assets marked as 'Potentially Affected' with a yellow warning icon. A search bar and filter options are visible above the table.

About the Assessment

A vulnerability in the common Session Initiation Protocol (SIP) library of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on an internal data structure.... [Show more](#)

Severity	CVE	CVSS score
High		

Version	First published	Last updated
1.1	Sep 25, 2019	Oct 4, 2019

References

[Security Advisory](#)

Asset Results

Q Search Filters 12 results Export Saved Filters

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

Detalhes das recomendações de segurança

Pesquisando e filtrando exibições para resultados da avaliação de ativos

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar ativos inserindo o nome do ativo no campo Pesquisar.



Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibindo Resultados da Avaliação de Ativo

Para exibir detalhes de um resultado de avaliação, clique em um ativo na tabela Assessment Outcome. A página de detalhes Assessment Result (Avaliação de resultado) do ativo é exibida.

Result

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

- ✓ Matched on software type
- ✓ Matched on chassis product ID
- ✓ Matched on module product ID

Additional Verification Needed

1) Software Releases are not checked for the automation of this Security Advisory. You must manually check your software release against the information in the advisory. 2) Module/Chassis PID level Automation is not done for the following product families. Please refer to the Security Advisory for the impacted PIDs and determine the Vulnerability of the device Cisco 4000 Series Integrated Services Routers Cisco Catalyst 6800 Series Switches Cisco Network Convergence System 5500 Series Routers

About the Assessment

A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware...

[Show more](#)

Severity	CVE	CVSS score
High	65_10_4_108	6.7
First published	Last updated	
May 13, 2019	Nov 20, 2019	
References		
Security Advisory		

About the Asset View evaluated asset

Product ID	Product type	IP Address
65_10_4_108	Switches	10.10.10.10
Serial Number	Software version	Location
1010101010	10.10.10	SAN JOSE, CA, USA
Support tier		
Signature		

Detalhes do resultado

Exportando Resultados de Ativo para Avisos de Segurança

Para exportar resultados de ativos, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Fortalecimento da segurança

O Security Hardening fornece visibilidade automatizada e quase em tempo real da postura de segurança da sua infraestrutura de rede, avaliando continuamente roteadores, switches e firewalls em relação aos padrões do setor. Ele identifica falhas de configuração e fornece orientação prática de remediação, permitindo que os administradores de contas reduzam efetivamente a superfície de ataque e mantenham um alinhamento consistente com as rigorosas práticas recomendadas de segurança da Cisco. Ao centralizar o monitoramento

de conformidade e simplificar o processo de fortalecimento, o módulo transforma o gerenciamento de segurança de uma tarefa reativa em uma estratégia proativa orientada por dados, garantindo uma rede corporativa resiliente e segura.

 **Note:** As Avaliações de proteção de segurança estão disponíveis exclusivamente para ativos com níveis de suporte Padrão.

Exibindo Avaliações de Proteção de Segurança

A página Avaliação de Fortalecimento da Segurança exibe as seguintes informações:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you...
[Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations

179

Assets included

146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

179 results

Export

Saved Filters

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Soft war...
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

Fortalecimento da segurança

- Sobre a avaliação: Fornece detalhes adicionais resumindo a finalidade da avaliação
- Resultado da Execução: Fornece um resumo dos resultados da avaliação de ativos, incluindo o número total de avaliações de regras e ativos incluídos
- Avaliações de regra: Fornece informações detalhadas sobre a regra, incluindo Severidade, Ativos Avaliados, Não Aprovados, Aprovados, Inconclusivos, Não Aplicáveis e Tipo de software
- Severity: Fornece o nível de importância ou impacto da avaliação da regra

- Ativos avaliados: Fornece o número total de ativos que foram avaliados de acordo com os critérios da regra
- Não aprovado: Fornece os ativos que não atenderam aos critérios da regra durante a avaliação
- Aprovado: Fornece os ativos que atenderam aos critérios da regra durante a avaliação
- Inconclusivo: Fornece os ativos para os quais a avaliação não pôde determinar a falha
- Não aplicável: Indica os ativos ou cenários em que a regra não se aplica ou não é relevante
- Tipo de software: Fornece o tipo de software dos ativos

Pesquisando e Filtrando Views para Regras

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar uma regra inserindo o nome da regra no campo Pesquisar.



Nota: Alguns filtros podem estar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibição de Detalhes de Avaliação de Regra

Para exibir detalhes adicionais sobre uma avaliação de regra, clique em uma regra. A página de detalhes da avaliação da regra é exibida com as seguintes informações:

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The main title is 'Minimum Password Length Policy', evaluated on Jul 20, 2026, at 5:39 AM. The interface includes a sidebar with navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (selected), Configuration, and Field Notices. The main content area is divided into sections: 'About the Rule' (explaining the policy to check 'Min. Password length' in show switch config), 'Results Summary' (showing 31 assets evaluated, 0 Passed, 31 Didn't pass, 0 Inconclusive, and 0 Not applicable), and 'Asset Results' (a table of 31 results). The table has columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. All results shown are 'Didn't pass' with a 'Signature' link.

Exibição de Regra

- Sobre a regra: Fornece detalhes sobre a regra, como Severidade, Tipo de software, Versão e Ativos avaliados e inclui links rotulados descritivos para documentação de origem relevante
- Resumo dos resultados: Fornece um resumo dos resultados de ativos relacionados à regra, como Aprovado, Não aprovado, Inconclusivo e Não aplicável
- Resultados dos ativos: Fornece uma lista de ativos com detalhes como Ativo, Resultado, ID do produto, Número de série, Endereço IP e Camada de suporte

 **Note:** O Cisco IQ fornece orientação clara quando uma descoberta de avaliação é "Inconclusiva", explicando a causa (por exemplo, falta de telemetria ou SO não suportado) e recomendando etapas como verificação da coleta de dados, atualização de credenciais ou atualização de dados. Também são fornecidos links rotulados para a documentação relevante para ajudar a resolver problemas.

Pesquisando e filtrando exibições de regras de ativo

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando

em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar resultados da avaliação de ativos inserindo o nome do ativo no campo Pesquisar.



Nota: Alguns filtros podem estar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exportação de Resultados de Ativo

Para exportar os resultados de avaliação das regras, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Pesquisando e filtrando exibições para resultados de ativos

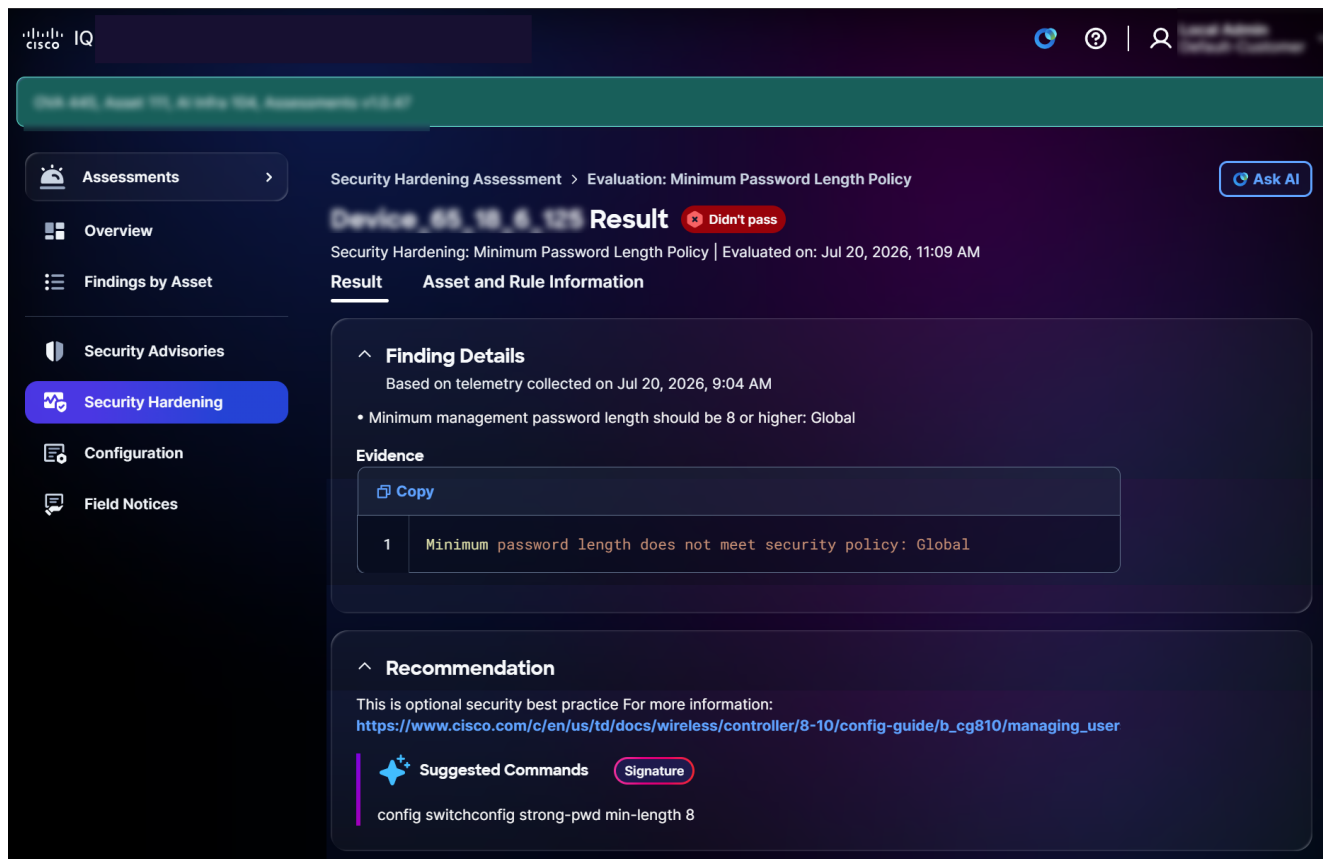
Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar resultados de ativos inserindo o nome do ativo no campo Pesquisar.



Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibindo Resultados de Ativo para Proteção de Segurança

Clique em um ativo em Resultados de ativos para exibir seus detalhes. A página de detalhes do resultado do ativo exibe informações de acordo com seu nível ou nível de direito.



Nível Padrão de Fortalecimento da Segurança

- Camada Padrão
- Localizando detalhes: Fornece informações sobre os desvios de configuração identificados durante a avaliação, juntamente com registros de evidências
- Recomendações: Fornece orientação para abordar as descobertas e garantir a consistência da configuração

Exibindo Informações de Ativo e Regra para Proteção de Segurança

Para exibir os detalhes de um ativo e suas regras, clique na guia Informações do ativo e da regra. A página Informações sobre ativos e regras é exibida.

Sobre o ativo: Fornece os detalhes do ativo, como ID do produto, tipo de produto, endereço IP, número de série, versão do software, Localização e Camada de suporte

- Sobre a regra: Fornece detalhes da regra (incluindo severidade e tipo de software) e a importância dessa verificação de proteção específica

Configuração

As avaliações de configuração avaliam seus ativos em relação às práticas recomendadas com base na experiência comprovada da Cisco para detectar desvios de configuração que possam afetar a disponibilidade, a segurança ou o desempenho em sua infraestrutura. Cada

regra de prática recomendada é avaliada em todos os ativos cobertos, e as descobertas são priorizadas por gravidade para garantir a consistência da configuração, a resiliência aprimorada e o risco operacional reduzido.

 **Note:** As avaliações de configuração estão disponíveis exclusivamente para ativos com níveis de suporte Padrão.

Exibindo avaliações de configuração

A página Avaliação da configuração exibe as seguintes informações:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b...
[Show more](#)

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations

729

Assets included

146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

729 results

Export

Saved Filters

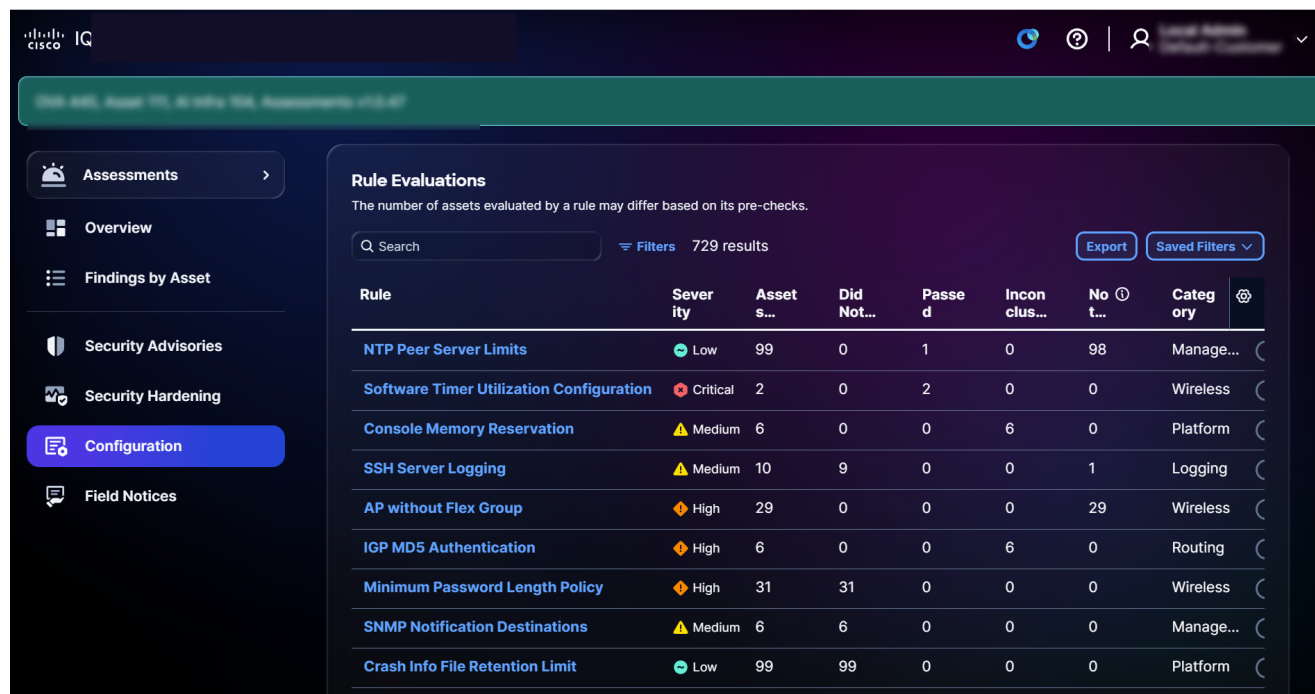
Rule	Severity	Asset S...	Did Not...	Passes	Inconclus...	No t...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

Avaliação da configuração

- Sobre a avaliação: Fornece detalhes adicionais resumindo a finalidade da avaliação
- Resumo: Fornece um resumo da execução da configuração como Regras avaliadas e Ativos avaliados
- Informações: Fornece insights sobre as falhas de configuração identificadas geradas através da análise de padrões e uma correlação de descobertas; eles são exibidos como cartões-chave agrupados de forma inteligente para destacar as áreas mais críticas que exigem atenção

- **Avaliações de regra:** Fornece informações detalhadas sobre a regra, incluindo Severidade, Ativos Avaliados, Não Aprovados, Aprovados, Inconclusivos, Não Aplicáveis, Categoria e tipo de Software
- **Severity:** Fornece o nível de importância ou impacto da avaliação da regra
- **Ativos avaliados:** Fornece o número total de ativos que foram avaliados de acordo com os critérios da regra
- **Não aprovado:** Fornece o número total de ativos que não atenderam aos critérios da regra durante a avaliação
- **Inconclusivo:** Fornece o número total de ativos para os quais a avaliação não pôde ser executada
- **Aprovado:** Fornece os ativos que atenderam aos critérios da regra durante a avaliação
- **Não aplicável:** Indica os ativos ou cenários em que a regra não se aplica ou não é relevante
- **Categoria:** Fornece a área de domínio à qual a regra pertence
- **Tipo de software:** Indica o tipo de ativos de software aos quais a regra se aplica

Pesquisando e Filtrando Views para Regras



Rule Evaluations
The number of assets evaluated by a rule may differ based on its pre-checks.

Search: Filters 729 results Export Saved Filters

Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging
AP without Flex Group	High	29	0	0	0	29	Wireless
IGP MD5 Authentication	High	6	0	0	6	0	Routing
Minimum Password Length Policy	High	31	31	0	0	0	Wireless
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform

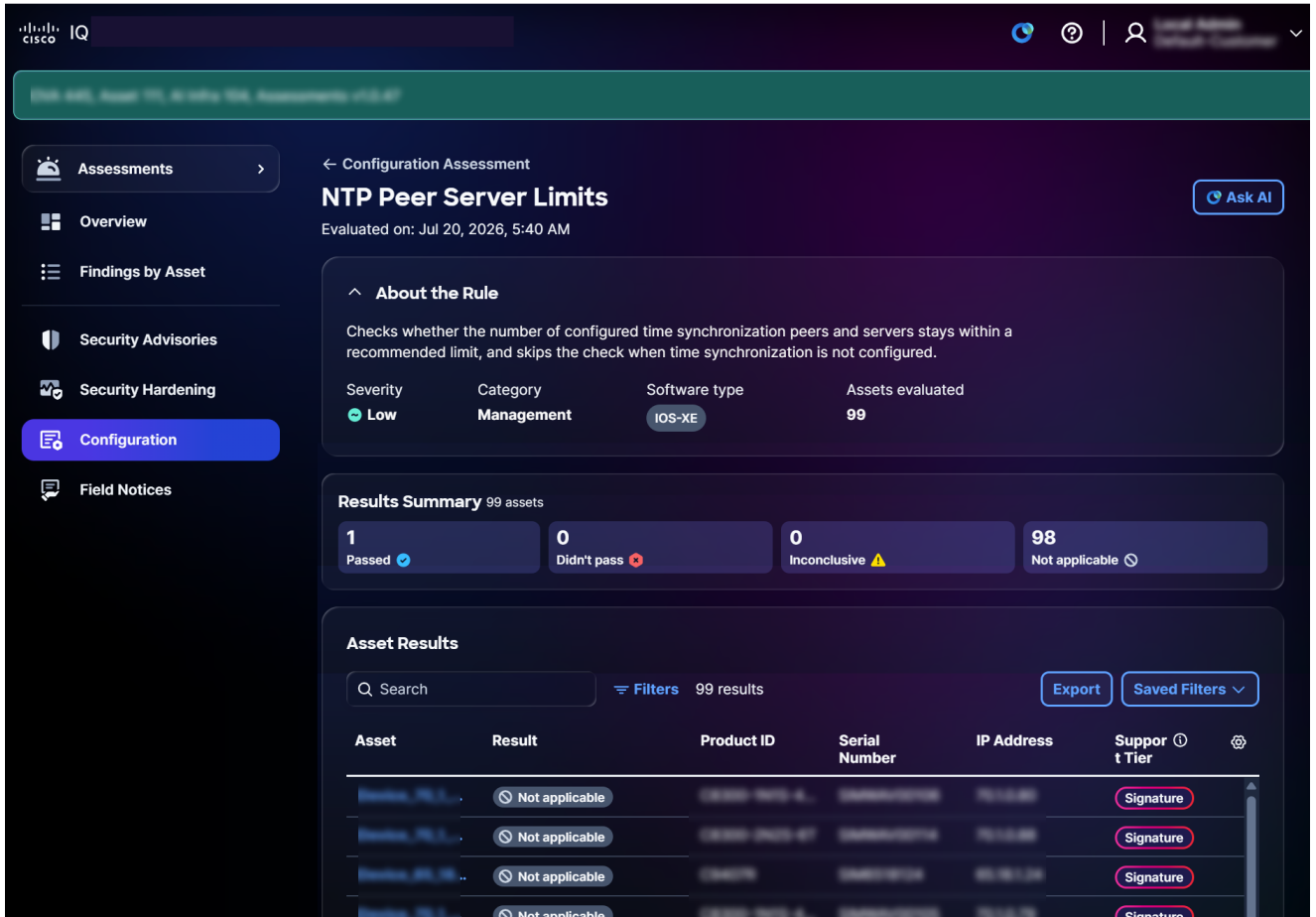
Avaliações de regra

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar uma regra inserindo o nome da regra no campo Pesquisar.

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibição de Detalhes de Avaliação de Regra

Para exibir detalhes adicionais sobre uma avaliação de regra, clique em qualquer regra. A página de detalhes da avaliação da regra é exibida com as seguintes informações:



The screenshot shows the Cisco IQ interface for a Configuration Assessment. The main heading is 'NTP Peer Server Limits', evaluated on Jul 20, 2026, at 5:40 AM. The assessment is categorized as 'Low' severity, 'Management' category, and 'IOS-XE' software type, with 99 assets evaluated. The 'Results Summary' shows 1 Passed, 0 Didn't pass, 0 Inconclusive, and 98 Not applicable. The 'Asset Results' table lists individual assets with their results, product IDs, serial numbers, IP addresses, and support tiers.

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Router, 78.1...	Not applicable	CISCO 7810-A...	0000000000000000	78.10.0.0	Signature
Router, 78.1...	Not applicable	CISCO 7810-A...	0000000000000000	78.10.0.0	Signature
Router, 78.1...	Not applicable	CISCO 7810-A...	0000000000000000	78.10.0.0	Signature
Router, 78.1...	Not applicable	CISCO 7810-A...	0000000000000000	78.10.0.0	Signature

Avaliação

- Sobre a regra: Fornece detalhes sobre uma regra como Severidade, Categoria, Tipo de software e Ativos avaliados e inclui links rotulados descritivos para documentação de origem relevante
- Resumo dos resultados: Fornece resultados gerais de ativos exibindo o número de ativos nos status Aprovado, Não aprovado, Inconclusivo e Não aplicável
- Resultados do ativo: Fornece uma lista de ativos afetados pela regra selecionada com status do resultado

 Note: O Cisco IQ fornece orientação clara quando uma descoberta de avaliação é "Inconclusiva", explicando a causa (por exemplo, falta de telemetria ou SO não suportado) e recomendando etapas como verificação da coleta de dados, atualização

 de credenciais ou atualização de dados. Também são fornecidos links rotulados para a documentação relevante para ajudar a resolver problemas. O módulo Avaliação suporta a seleção de várias categorias para regras, permitindo o processamento simultâneo e a avaliação em várias categorias de regras.

Exportação de Resultados de Ativo

Para exportar resultados de ativos para regras, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Pesquisando e filtrando exibições para resultados de ativos

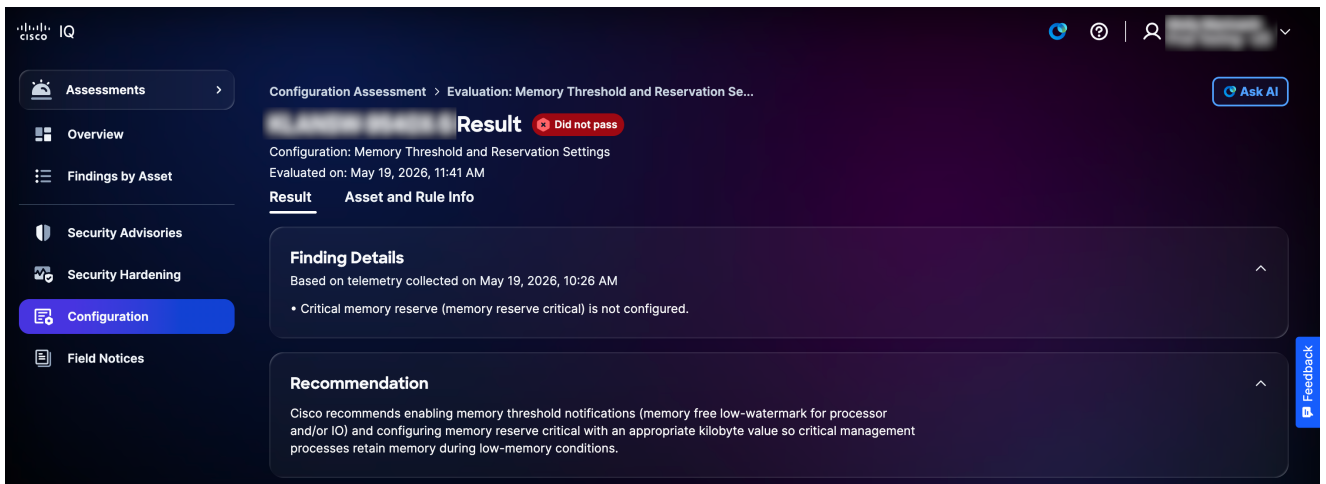
Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar resultados de ativos inserindo o nome do ativo no campo Pesquisar.

 **Note:** Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibindo resultados de ativos para avaliações de configuração

Para exibir detalhes dos resultados de ativos, clique em um ativo nos resultados de ativos.

A página de detalhes do resultado do ativo exibe informações de acordo com seu nível ou nível de direito.



The screenshot displays the Cisco IQ interface for a Configuration Assessment. The left sidebar shows navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area shows the assessment details for 'Configuration: Memory Threshold and Reservation Settings', evaluated on May 19, 2026, at 11:41 AM. The result is 'Did not pass'. The 'Finding Details' section states: 'Based on telemetry collected on May 19, 2026, 10:26 AM' and 'Critical memory reserve (memory reserve critical) is not configured.' The 'Recommendation' section suggests enabling memory threshold notifications and configuring memory reserve critical with an appropriate kilobyte value. An 'Ask AI' button is visible in the top right corner.

Camada Padrão de Configuração

- Camada Padrão
- Localizando detalhes: Fornece informações sobre os desvios de configuração identificados durante a avaliação, juntamente com registros de evidências

- **Recomendações:** Fornece orientação para abordar as descobertas e garantir a consistência da configuração

Exibindo Informações de Ativo e Regra para Avaliações de Configuração

Para exibir detalhes de informações de ativos e regras, clique na guia Informações de ativos e regras.

The screenshot displays the Cisco IQ Configuration Assessment interface. On the left is a navigation sidebar with options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area shows a configuration assessment for 'Device_70_1_0_00'. The assessment title is 'Configuration Assessment > Evaluation: NTP Peer Server Limits'. The result is 'Not applicable'. Below this, the 'Asset and Rule Info' section is expanded, showing details about the asset and the rule.

About the Asset				
Product ID	Product type	IP address	Serial number	Software version
Device_70_1_0_00	Routers	10.1.1.1	1000000000000000	15.2.2
Location	Support tier			
SAN JOSE, CA, USA	Signature			

About the Rule		
Checks whether the number of configured time synchronization peers and servers stays within a recommended limit, and skips the check when time synchronization is not configured.		
Severity	Category	Software type
Low	Management	IOS-XE

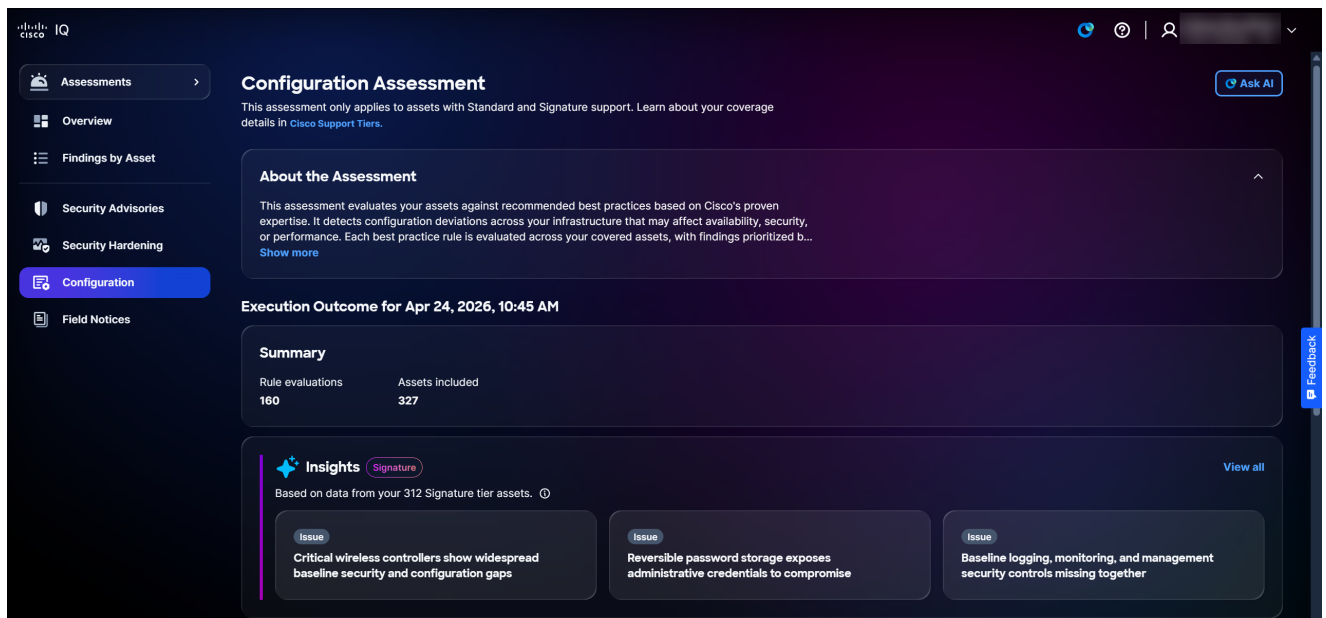
Informações sobre ativos e regras

A página Informações sobre ativos e regras é exibida com as seguintes informações:

- **Sobre o ativo:** Fornece os detalhes de um ativo, como ID do produto, tipo de produto, endereço IP, número de série, versão do software, Local e camada de suporte
- **Sobre a regra:** Fornece detalhes de uma regra, como Severidade, Categoria e Tipo de software

Exibindo Insights

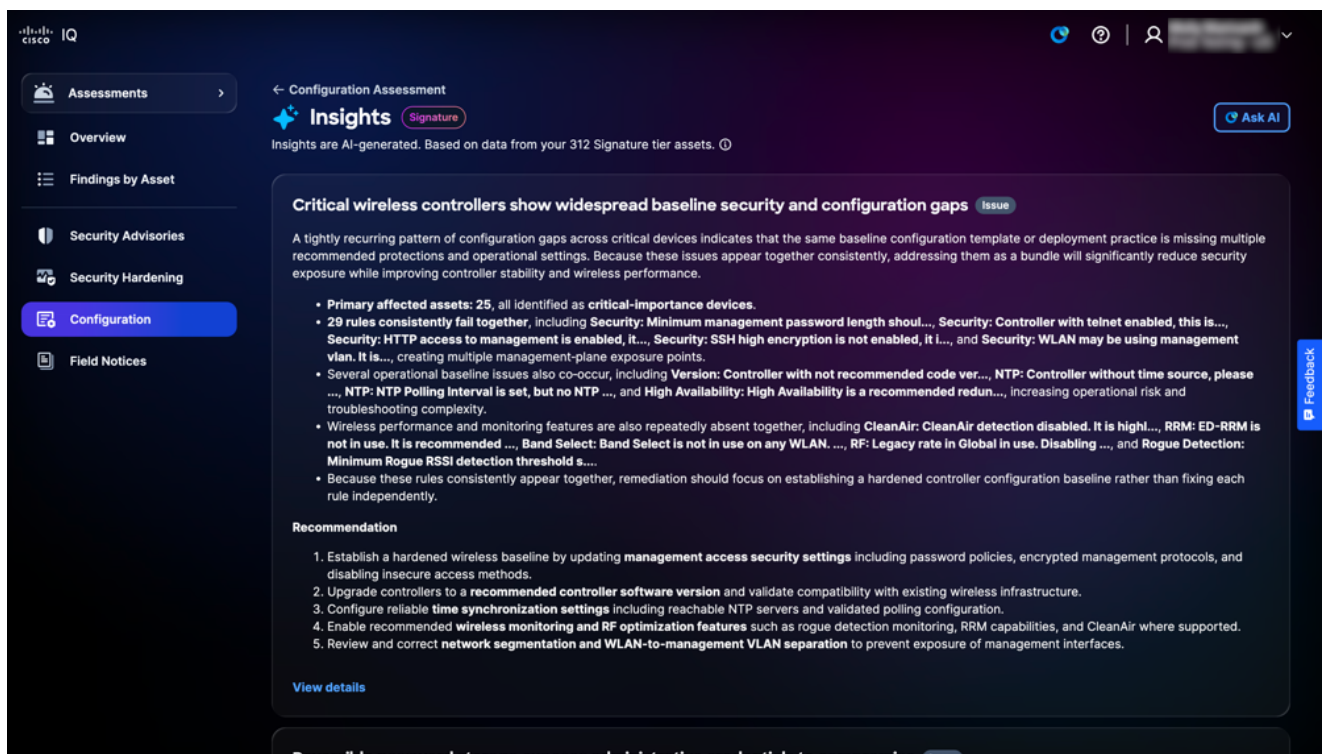
Os insights são gerados por IA e servem como um painel inteligente que sintetiza dados de avaliação em cartões-chave priorizados, destacando as disparidades de configuração críticas em várias descobertas. Ele permite que você enfrente com eficiência os riscos de infraestrutura mais impactantes, concentrando-se nessas áreas urgentes. Ele também destaca os pontos fortes ao identificar áreas onde sua infraestrutura está tendo um bom desempenho, de acordo com as práticas recomendadas.



Percepções

Para exibir detalhes do Insights:

1. No painel Insights, clique em View all. A página Insights exibe todos os insights.



Página Insights

2. Clique em Exibir detalhes ou clique em qualquer cartão. A página de detalhes Insights é exibida com as seguintes informações:

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support. ⓘ

Details **Source Findings**

Insight

A tightly recurring pattern of configuration gaps across critical devices indicates that the same baseline configuration template or deployment practice is missing multiple recommended protections and operational settings. Because these issues appear together consistently, addressing them as a bundle will significantly reduce security exposure while improving controller stability and wireless performance.

- **Primary affected assets:** 25, all identified as **critical-importance devices**.
- **29 rules consistently fail together**, including **Security: Minimum management password length should be 12 characters**, **Security: Controller with telnet enabled, this is insecure**, **Security: HTTP access to management is enabled, it is insecure**, **Security: SSH high encryption is not enabled, it is insecure**, and **Security: WLAN may be using management vlan. It is insecure**, creating multiple management-plane exposure points.
- Several operational baseline issues also co-occur, including **Version: Controller with not recommended code version**, **NTP: Controller without time source, please use NTP**, **NTP: NTP Polling Interval is set, but no NTP server is configured**, and **High Availability: High Availability is a recommended redundancy feature**, increasing operational risk and troubleshooting complexity.
- Wireless performance and monitoring features are also repeatedly absent together, including **CleanAir: CleanAir detection disabled. It is highly recommended**, **RRM: ED-RRM is not in use. It is recommended**, **Band Select: Band Select is not in use on any WLAN**, **RF: Legacy rate in Global is in use**, **Disabling Rogue Detection: Minimum Rogue RSSI detection threshold should be -90 dBm**, and **Rogue Detection: Minimum Rogue RSSI detection threshold should be -90 dBm**.
- Because these rules consistently appear together, remediation should focus on establishing a hardened controller configuration baseline rather than fixing each rule independently.

Recommendation

1. Establish a hardened wireless baseline by updating **management access security settings** including password policies, encrypted management protocols, and disabling insecure access methods.
2. Upgrade controllers to a **recommended controller software version** and validate compatibility with existing wireless infrastructure.
3. Configure reliable **time synchronization settings** including reachable NTP servers and validated polling configuration.
4. Enable recommended **wireless monitoring and RF optimization features** such as rogue detection monitoring, RRM capabilities, and CleanAir where supported.
5. Review and correct **network segmentation and WLAN-to-management VLAN separation** to prevent exposure of management interfaces.

Affected Assets

Q Search Product type Product family Product ID Filters 25 results Export

Name	Product ID	Serial Number	IP Address
Cisco WLC 8540	WLC8540-001	12345678901234567890	10.10.10.10
Cisco WLC 8540	WLC8540-002	12345678901234567890	10.10.10.11
Cisco WLC 8540	WLC8540-003	12345678901234567890	10.10.10.12

Detalhes dos Insights

- **Informações:** Fornece um resumo que destaca os padrões recorrentes de desvios de configuração identificados através de uma análise abrangente em várias descobertas, bem como áreas de excelência em sua infraestrutura onde as configurações se alinham com as práticas recomendadas
 - **Recomendação:** Fornece etapas acionáveis para remediar as falhas de configuração identificadas
 - **Ativos afetados:** Fornece uma lista de dispositivos específicos onde o desvio de configuração foi identificado conforme definido na seção Insight
3. Clique em Source Findings. A página Descobertas da Origem exibe as descobertas individuais detalhadas que suportam suas percepções.

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support.

Details

Source Findings

Q SearchSeverityResult725 resultsExport

Asset	Rule	Severity	Serial Number	Result
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass
	High Availability: High Availa...	Low		Did not pass

Descobertas da fonte

Você pode filtrar a exibição de tabela escolhendo um filtro nas listas suspensas Severidade e Resultado.



Note: Recomendações e ativos afetados são opcionais, dependendo do resultado de cada insight.

Field Notices

Os avisos de campo identificam problemas significativos de produtos não relacionados à segurança e os organizam com base na gravidade do impacto e na criticidade, melhorando a capacidade da organização de gerenciar riscos de produtos. Os avisos de campo oferecem percepções acionáveis sobre defeitos do produto, aceleram a mitigação por meio de atualizações ou soluções recomendadas e garantem o alinhamento com objetivos operacionais e comerciais. Isso reforça a confiabilidade do produto, otimiza a alocação de recursos e promove a resiliência contra os desafios cada vez maiores dos produtos em toda a empresa.

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Field Notices

Ask AI

^

About the Assessments

These assessments compare your assets against Cisco Field Notices. Field Notices flag non-security product issues that may need action to prevent incidents.

Field Notice Assessments

Q Search

Filters 47 results

Export

Saved Filters

Assessment	Severity	Affected Assets	Potentially Affected Assets
FN74350 - Cisco Unified Border ...	Critical	0	24
FN74223 - Some Cisco NCS 540 ...	Critical	0	3
FN74267 - Cisco NCS-55A2 and ...	Critical	0	1
FN74353 - Cisco Network Conve...	High	0	1

Field Notices

Pesquisando e Filtrando Views para Avisos de Campo

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas. Você também pode procurar avaliações de avisos de campo inserindo o nome da avaliação no campo Pesquisar.

Exibindo Avaliações para Avisos de Campo

Para exibir detalhes adicionais sobre um aviso de campo, clique em uma Avaliação. Os seguintes detalhes da avaliação são exibidos:

- Sobre as avaliações: Fornece detalhes adicionais resumindo a finalidade da avaliação
- Avaliações de notificação de campo: Exibe uma lista de ativos afetados pelo aviso de campo selecionado, incluindo ativos com vulnerabilidades detectadas

The screenshot displays the Cisco IQ interface for Field Notices. The top navigation bar includes the Cisco logo, a search bar, and a 'Help' button. The left sidebar contains a list of navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices (highlighted). The main content area shows a specific Field Notice titled 'FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided'. The notice is categorized as 'Critical' and was last updated on 'Dec 11, 2024'. Below the notice details, there is a section for 'Asset Results' which includes a search bar, a filter button, and a table of affected assets. The table has columns for Asset, Result, Product ID, Serial Number, Product Type, Product Family, and Sup po... (Support point). The table shows three rows of assets, all with a 'Potentially affected' result.

Asset	Result	Product ID	Serial Number	Product Type	Product Family	Sup po...
Device_70_1...	Potentially affected			Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected			Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected			Routers	Cisco Network...	Signature

Exibindo Avaliações para Avisos de Campo

Pesquisando e filtrando exibições para resultados de ativos para avisos de campo

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou clicando em Filtros e escolhendo uma opção na lista de filtros disponíveis. Você também pode procurar resultados de ativos inserindo o nome do ativo no campo Pesquisar.



Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela. Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exportação de Resultados de Ativo para Avisos de Campo

Para exportar resultados de ativos de avaliação para avisos de campo, clique em Exportar. Consulte [Exportando informações](#) para obter mais informações.

Exibindo Resultados da Avaliação de Ativo para Avisos de Campo

Para exibir os detalhes do resultado da avaliação de um ativo, clique em um ativo em Resultados da avaliação de ativos. A página de detalhes do resultado da avaliação do ativo é exibida.

Você pode exibir os seguintes tipos de resultados:

- Afetado: Indica ativos que atendem a todos os critérios automaticamente verificados

quanto a um Field Notice e não exigem verificação manual adicional para confirmar que eles foram afetados

- Potencialmente afetado: Indica ativos que atendem a todos os critérios verificados automaticamente para um Field Notice, mas exigem verificação manual adicional para confirmar se eles foram realmente afetados

Os prompts a seguir estão disponíveis na guia Assessments - Security Hardening:

- Quais são as práticas recomendadas de fortalecimento da segurança da Cisco para dispositivos de rede?
- Como fortalecer meus dispositivos Cisco IOS XE?
- Liste as principais etapas de proteção de segurança para roteadores e switches.
- Quais são as configurações de proteção de linha de base recomendadas para dispositivos Cisco?
- Quantos ativos violam as práticas recomendadas de fortalecimento da segurança?

Autenticação Local

Os administradores de conta devem usar as seguintes credenciais para fazer login no VA com êxito:

- Nome de usuário padrão: admin
- Senha Default: A senha que é definida durante o processo de instalação do VA; consulte o Guia de introdução 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.

Definindo 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).



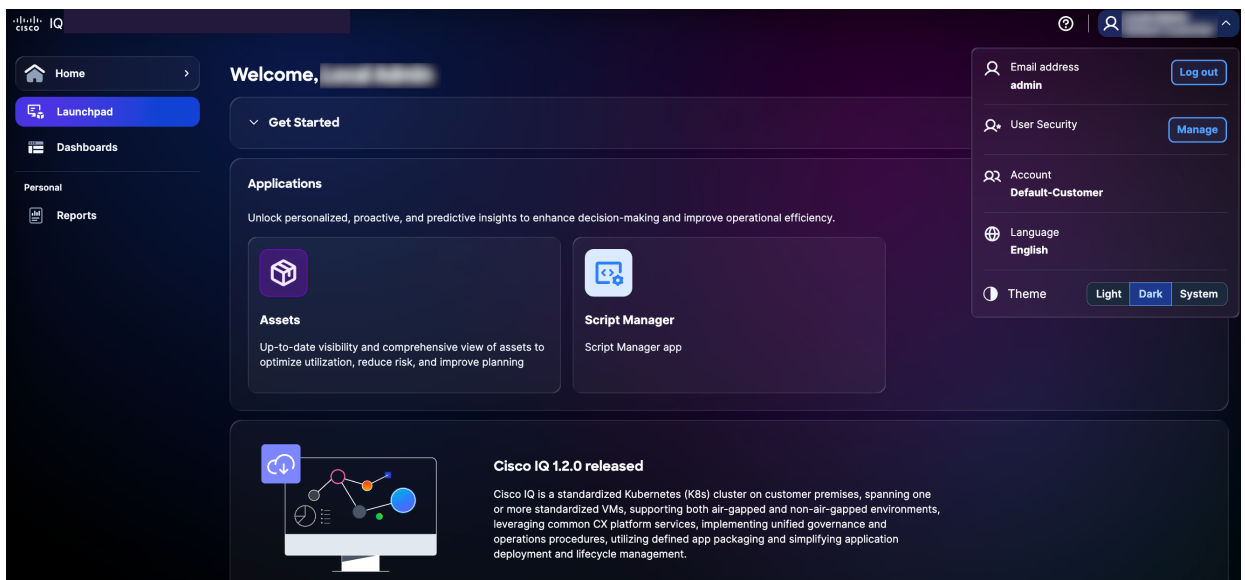
Note: Você tem três (3) tentativas para inserir a senha correta em um período de 15 minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 30 minutos para proteger sua segurança. Não é possível tentar fazer login durante o período de bloqueio. O sistema 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 login 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 Home page, clique no ícone User Profile. O menu suspenso é aberto.



Usar segurança

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



The screenshot shows the 'User Security' section of the Cisco IQ interface. The 'Change Password' tab is active. It lists password requirements: at least 15 characters, at least 2 uppercase characters, at least 2 lowercase characters, at least 2 numeric characters, at least 2 special characters, and no repeating characters. There are input fields for 'Password', 'New password', and 'Confirm password', each with a 'Show' button. A 'Save' button is at the bottom.

User Security

Change Password Security Questions

Change Password
Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

Password [Show](#)

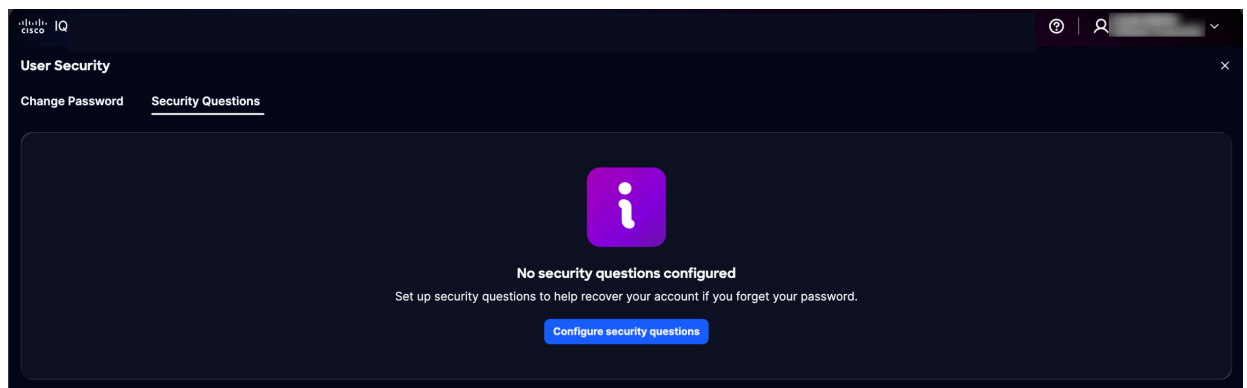
New password [Show](#)

Confirm password [Show](#)

[Save](#)

Perguntas de segurança

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



The screenshot shows the 'User Security' section of the Cisco IQ interface. The 'Security Questions' tab is active. It displays a message: 'No security questions configured. Set up security questions to help recover your account if you forget your password.' There is a 'Configure security questions' button.

User Security

Change Password **Security Questions**

No security questions configured
Set up security questions to help recover your account if you forget your password.

[Configure security questions](#)

Guia Perguntas de segurança

4. Clique em Configure security questions.



User Security

[Change Password](#)[Security Questions](#)

Security Questions

Set up security questions to help recover your account if you forget your password. You must answer all questions.

Question 1 *

Select a security question

Answer *

Question 2 *

Select a security question

Answer *

Question 3 *

Select a security question

Answer *

Question 4 *

Select a security question

Answer *

Question 5 *

Select a security question

Answer *

Configurar perguntas de segurança

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



Note: As respostas não diferenciam maiúsculas de minúsculas, por exemplo, "SMITH" e "smith" são considerados iguais. Espaços extras são ignorados, significando que "Smith" e "Smith" são tratados de forma idêntica. Lembre-se de como você digitou sua resposta (por exemplo,



nomes completos versus apelidos). Use respostas diretas das quais você se lembrará anos mais tarde. Escolha perguntas com respostas que não serão alteradas com o tempo.



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 a senha do 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 será desativada).

Pré-requisitos

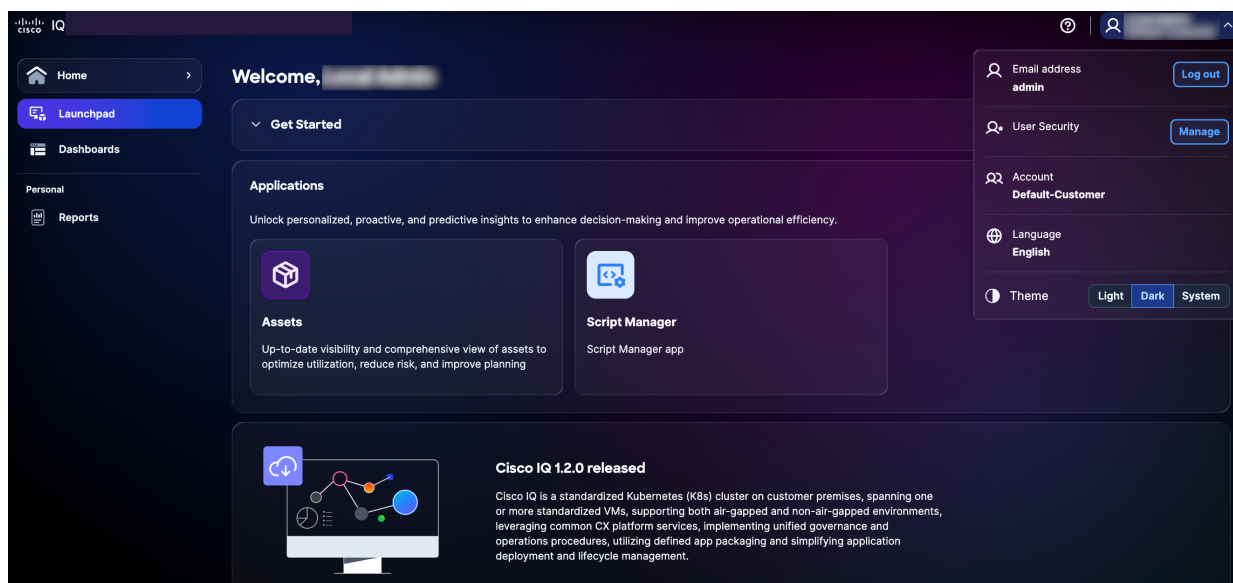
Para gerenciar senhas, as seguintes condições devem ser atendidas:

- 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
- Você conhece a senha atual

Alteração de Senhas

Para alterar a senha:

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



Gerenciar Segurança 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.

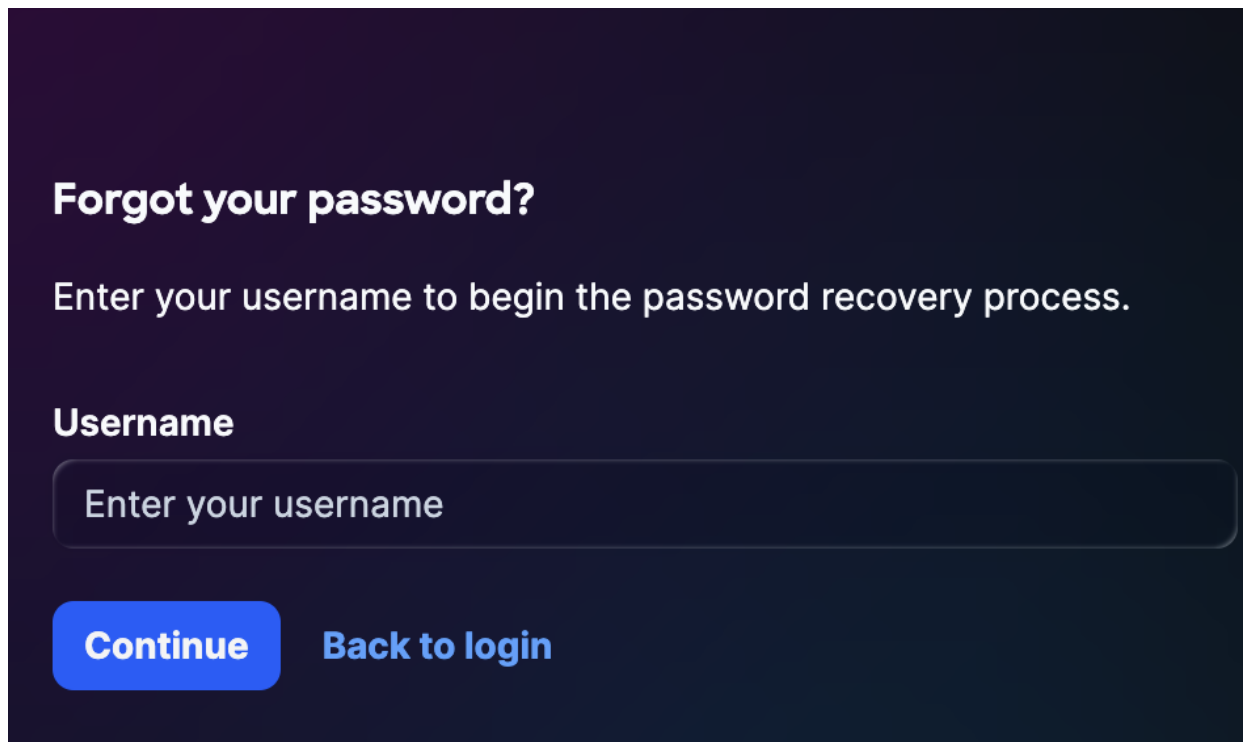
A senha é atualizada no sistema Cisco IQ, incluindo o Cisco IQ VM.

Redefinição de uma senha esquecida

Você pode redefinir uma senha usando o processo de verificação de pergunta de segurança.

Para redefinir uma senha esquecida:

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



The screenshot shows a dark-themed login page with the heading "Forgot your password?". Below the heading is the instruction "Enter your username to begin the password recovery process." There is a text input field labeled "Username" with the placeholder text "Enter your username". At the bottom of the form are two buttons: a blue "Continue" button and a "Back to login" link.

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.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

Verificar identidade

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

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password

Back to login

Redefinir senha

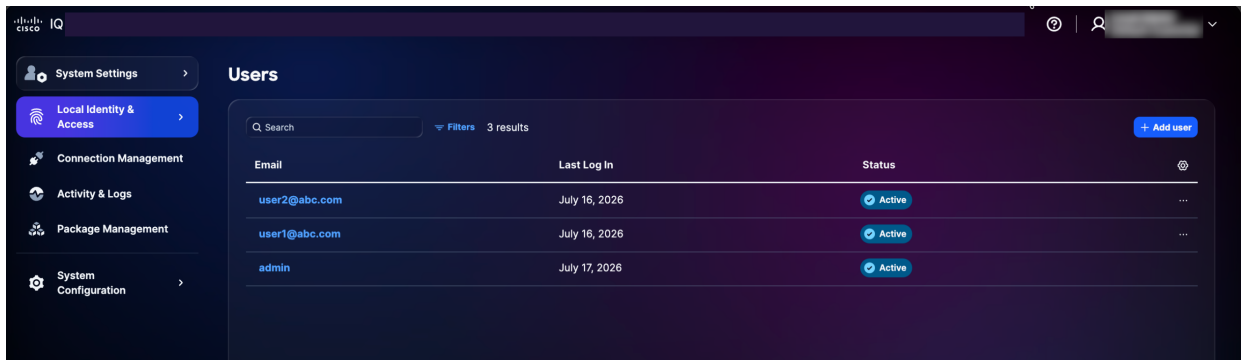
 Note: Você tem três (3) tentativas para inserir a senha correta em um período de 15 minutos. Se todas as três (3) tentativas forem malsucedidas, sua conta será temporariamente bloqueada por 30 minutos para proteger sua segurança. Não é possível tentar fazer login durante o período de bloqueio. O sistema 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 login ou redefinir sua senha.

- Digite a nova senha.
- Digite a senha novamente para confirmá-la.
- Clique em Submit.

Adicionando usuários locais

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

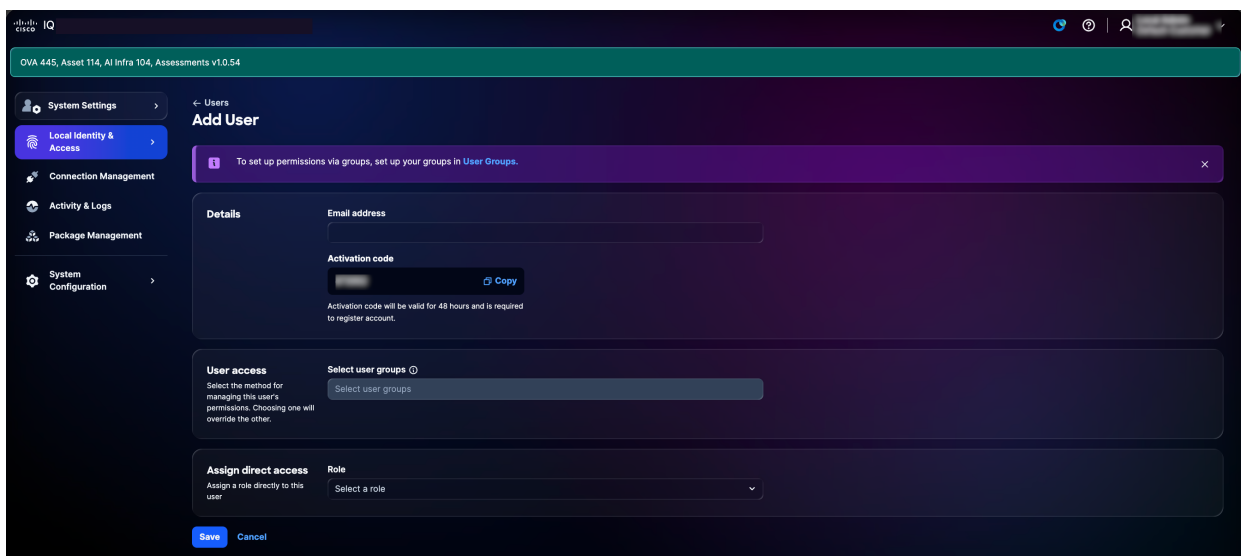
1. Navegue até Configurações do sistema > Identidade local e acesso > Usuários. A página Usuários é exibida. Ela lista todos os usuários locais existentes, juntamente com seus status.



Página Usuários

 Note: 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. 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.

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



Adicionar usuário

3. Insira o endereço de e-mail.
4. Insira o código de ativação.

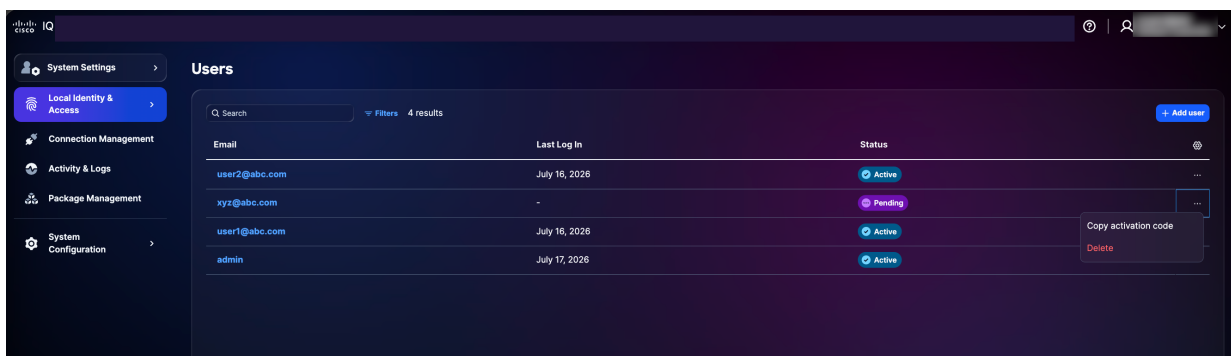
 Note: O código de ativação é exibido por padrão. Compartilhe o código de ativação exibido com o usuário, conforme necessário para o registro.

5. Em 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 suspensa Função. Há duas (2) funções disponíveis:
 - Visualizador: Exibir e acessar aplicativos
 - Administrador da conta: Acesse módulos e gerencie configurações do sistema, exceto Gerenciamento do sistema e Provedor de identidade (IDP)
7. Click Save. O novo usuário é criado e exibido na lista de usuários no estado Pendente. Pendente indica que o usuário ainda não concluiu a autoativação.
8. Localize o usuário recém-criado na lista e confirme se a coluna Status exibe Pending.
9. Clique no ícone More Options ao lado do usuário recém-criado.



Copiar Código de Ativação

10. Selecione o Copy activation code na lista suspensa. O código de ativação é copiado para a área de transferência.
11. 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.



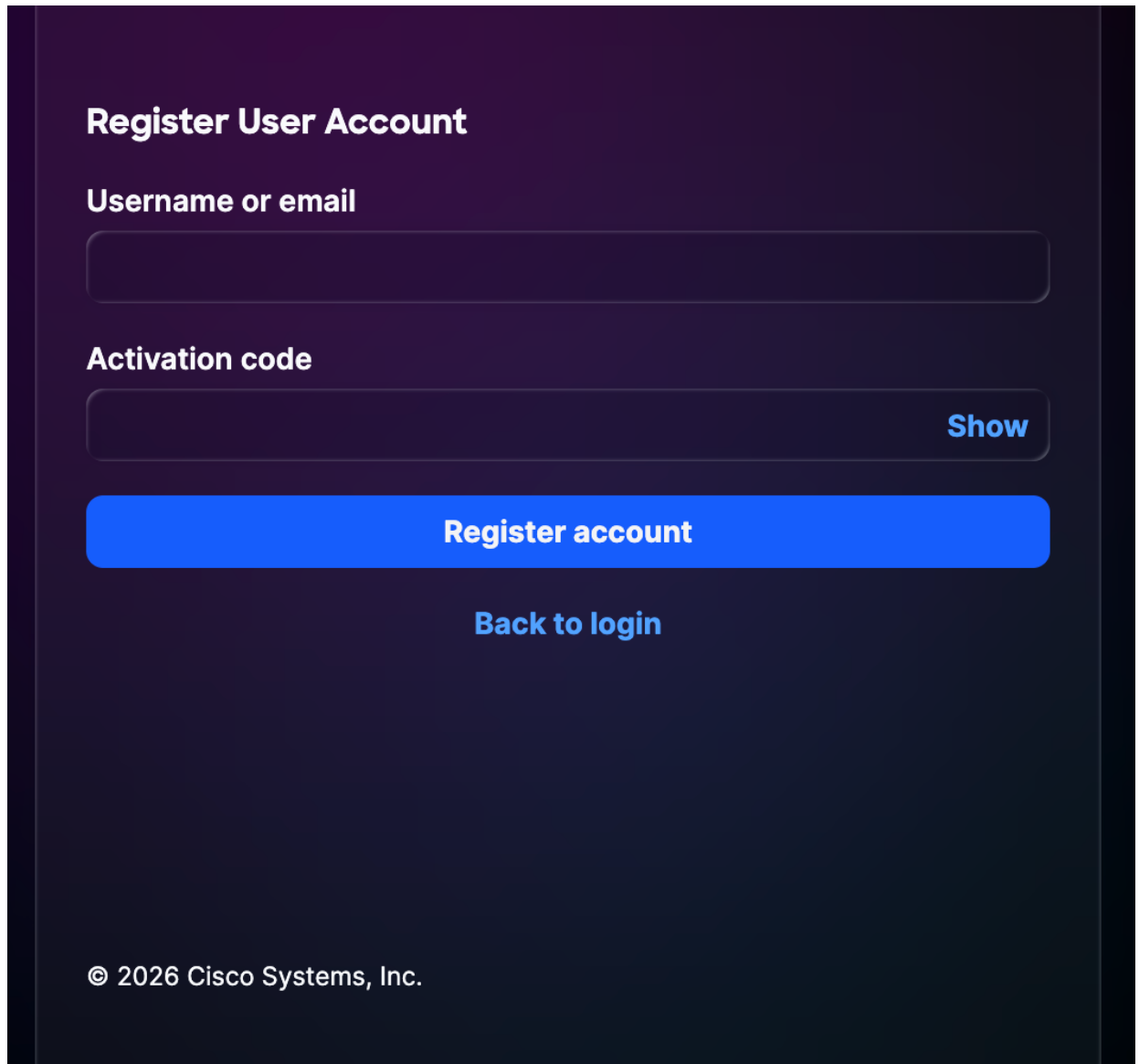
Note: Não compartilhe o código de ativação em canais não seguros. Se o código for perdido ou comprometido, use o ícone Menu para gerar novamente um novo código de ativação, que invalida o anterior. Os códigos de ativação são válidos por 48 horas. Se o código expirar, entre em contato com o administrador da conta para solicitar um novo código.

12. Para fazer logoff, clique no ícone User Profile no canto superior direito e selecione Logout. Você retornará à página de login do Cisco IQ.

Registrando novas contas de usuário

Para registrar a nova conta de usuário:

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

A screenshot of a web form titled "Register User Account" on a dark purple background. The form contains two input fields: "Username or email" and "Activation code". The "Activation code" field has a "Show" button to its right. Below the input fields is a large blue button labeled "Register account". Below the button is a link labeled "Back to login". At the bottom left of the form, there is a copyright notice: "© 2026 Cisco Systems, Inc."

Register User Account

Username or email

Activation code

 [Show](#)

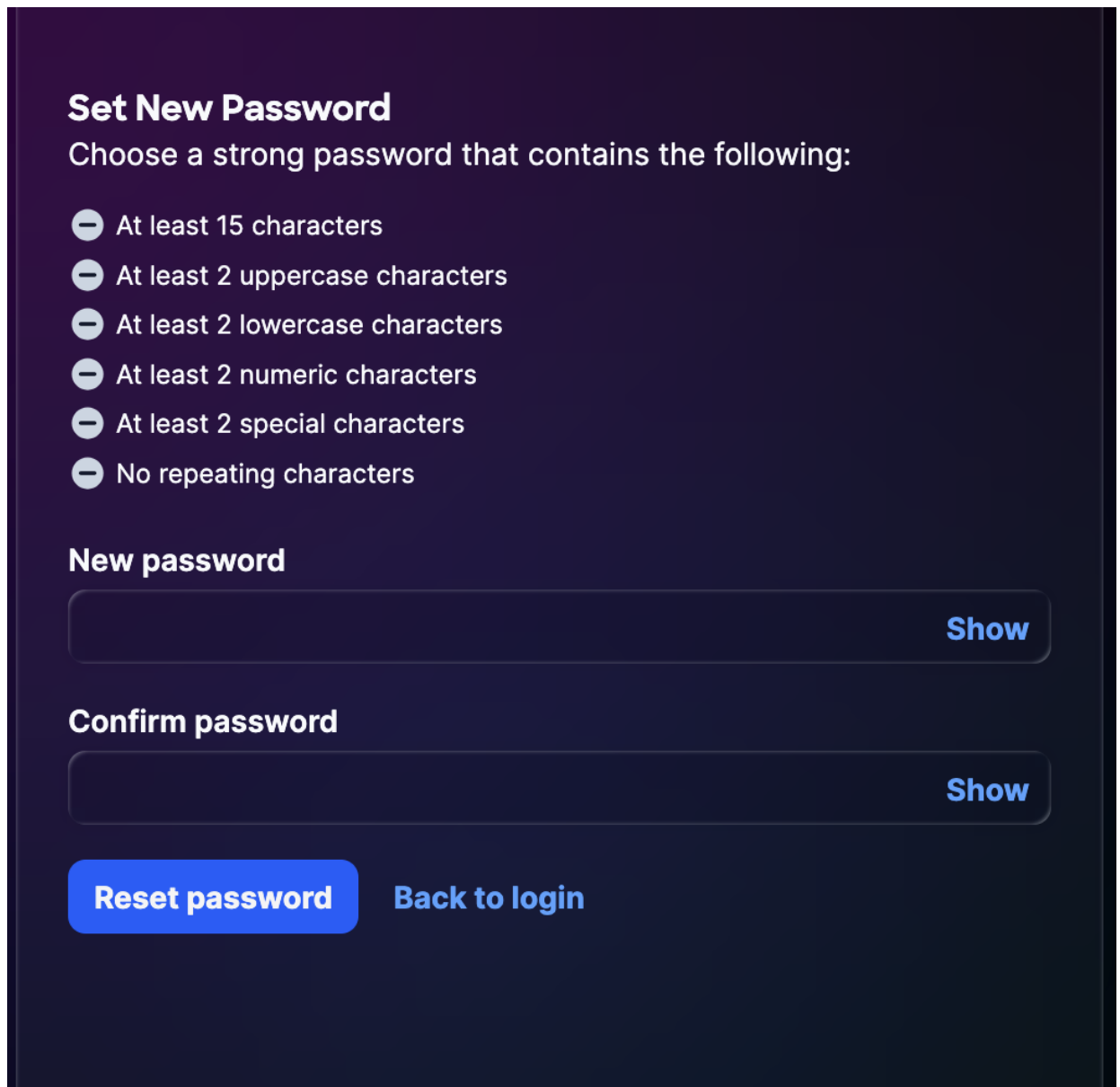
Register account

[Back to login](#)

© 2026 Cisco Systems, Inc.

Nova conta de usuário

2. Insira o nome de usuário ou o endereço de email 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.



Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password **Back to login**

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 [Como Configurar Perguntas de Segurança](#)).

Gerenciamento de grupos de usuários locais

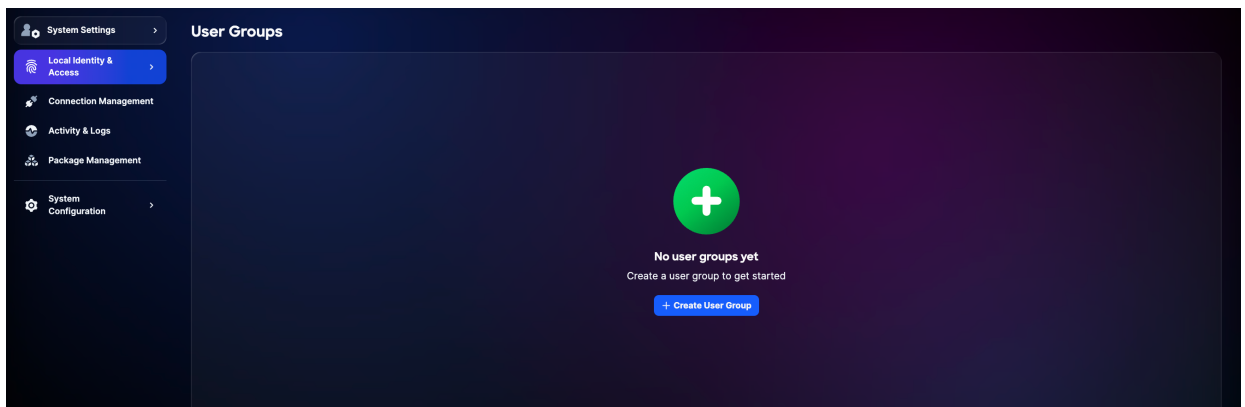
Os grupos de usuários permitem que o administrador de contas gerencie funções para vários usuários locais de uma só vez. Em vez de atribuir uma função a cada usuário individualmente, você pode criar um grupo, anexar uma função e um conjunto de usuários a ele e atualizar a função ou a associação em um 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. Consulte [Adição de Usuários Locais](#) para obter mais informações.

Criando um grupo de usuários

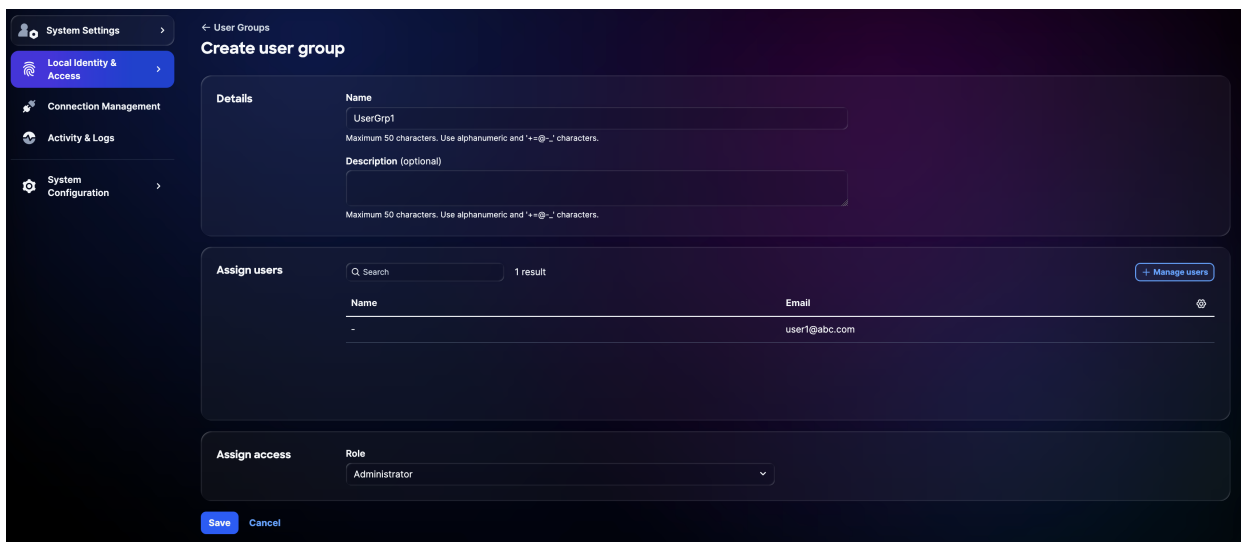
Para criar um grupo de usuários:

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; alfanuméricos 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 módulos (somente leitura)
- Administrador: Acessar módulos e gerenciar configurações do sistema

4. Click Save.

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. Escolha o ícone Mais Opções > Editar do grupo desejado. A página Editar grupo de usuários é exibida.

The screenshot shows the 'Edit user group' page within a system settings application. The left sidebar contains navigation links: System Settings, Local Identity & Access (highlighted), Connection Management, Activity & Logs, and System Configuration. The main content area is titled 'Edit user group' and includes the following sections:

- Details:** Contains input fields for 'Name' (pre-filled with 'UserGp1') and 'Description (optional)'. Both fields have a maximum character limit of 50 and allow alphanumeric characters, '+', '=', '@', '-', '\', and '_'.
- Assign users:** Features a search bar with the text '1 result' and a '+ Manage users' button. Below is a table with columns 'Name' and 'Email'. One user is listed with the email 'user1@abc.com'.
- Assign access:** Includes a 'Role' dropdown menu currently set to 'Administrator'.

At the bottom of the form are 'Save' and 'Cancel' buttons.

Editar grupo de usuários

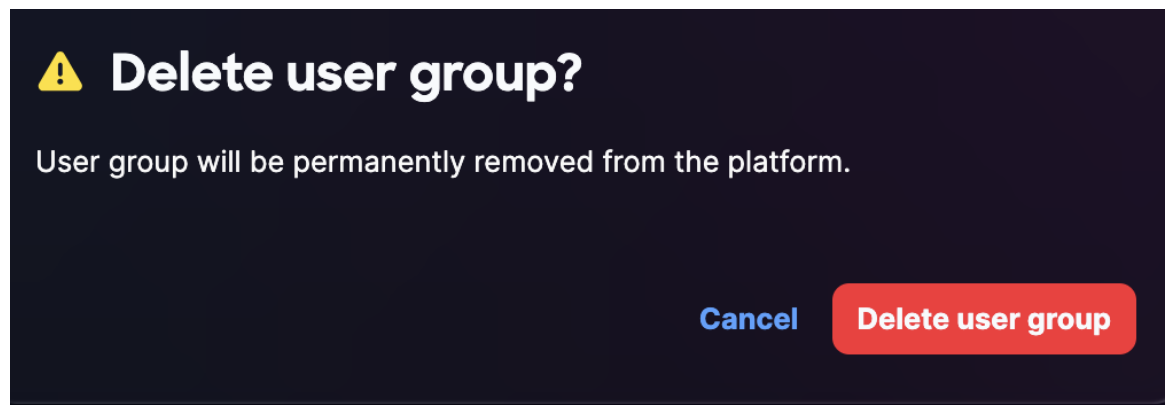
3. Faça as alterações desejadas.
4. Click Save.

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 fazer logon no VA, os administradores de conta podem definir várias configurações. Os administradores de conta podem fazer login usando a administração local ou a configuração do IDP.

Configuração SAML do Okta IDP para SSO

Pré-requisitos para Configurar SAML IDP

- Acesso de administrador local ao Cisco IQ
- 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.

Tabela 2: Atributos 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 3: Parâmetros de configuração SAML

Parâmetro	Configuração	Exemplo
Audiência (ID da Entidade)	Nome de domínio totalmente qualificado (FQDN)	mymanagementhost.mydomain.com
	Ponto de extremidade de Serviço de Cliente de Asserção (ACS - Assertion Customer Service) SAML	https://mymanagementhost.mydomain.com/saml/acs
URL de Logon Único	Endereço de e-mail	NA
Formato de ID do Nome	Nome de usuário	NA

5. Configure as instruções de atributo.



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: .*

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

Tabela 4: 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 do SP (Provedor de serviços) são necessários somente para o IDP do AD FS (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

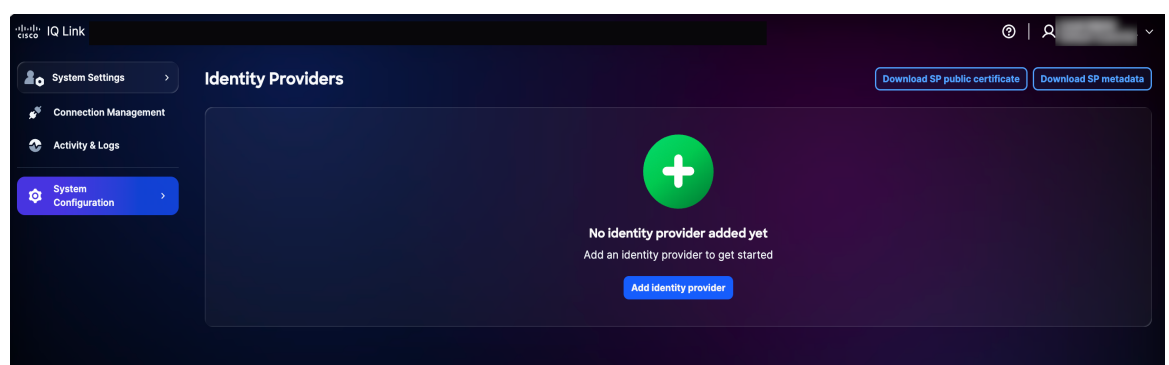
8. Clique no ícone Download para fazer o download do arquivo "IDP Metadata XML".

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

Adicionando o Okta IDP

Para adicionar um IDP no Cisco IQ:

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



Página inicial do IDP



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

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

The screenshot shows the 'Add Identity Provider' page in the Cisco IQ Link interface. On the left is a sidebar with navigation options: 'System Settings', 'Connection Management', 'Activity & Logs', and 'System Configuration' (highlighted in blue). The main content area has a header 'Identity Providers' and a title 'Add Identity Provider'. It contains three main sections: 1. 'Identity provider name *' with a text input field labeled 'Enter identity provider name'. 2. 'Domains' with a text input field labeled 'Enter domain names' and an 'Add' button. 3. 'Organization IDP metadata *' with a dashed box containing an upload icon and the text 'Select or drag file to this area to upload' and 'Only one file can be uploaded at 5 MB or less'. At the bottom, there is a toggle switch for 'Enable single log out (SLO)' and 'Save' and 'Cancel' buttons.

Adicionar provedor de identidade

3. Insira o nome do provedor de identidade.
4. Clique em Add para adicionar um nome de domínio configurado do Cisco IQ ao campo Domain(s).
5. Arraste e solte ou carregue o arquivo de metadados SAML obtido do aplicativo IDP no campo Metadados IDP da organização. Esse arquivo

contém detalhes do certificado e da entidade SP.

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

7. Click Save.

Configuração do mapeamento de função

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

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user	General Account... × ▼
	▼
	▼
	▼
	▼

+ Add identity provider role

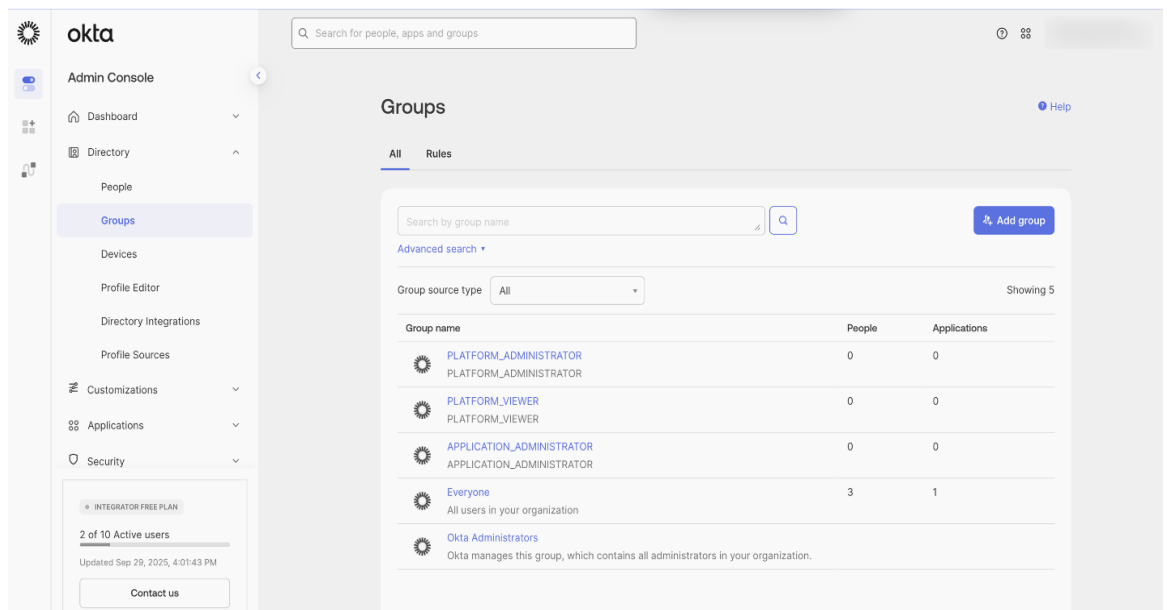
Save

Mapear Funções de Usuário

- 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.



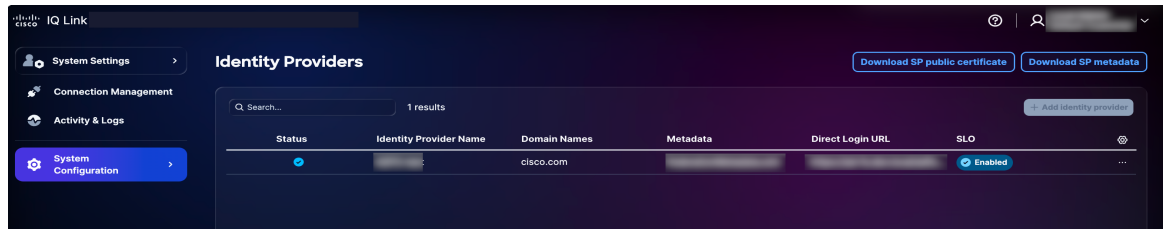
Referência de Mapeamento de Função

3. Mapeie funções adicionais conforme necessário clicando em Adicionar função do provedor de identidade.
4. Click Save. Uma vez configurada, a página de login exibe uma opção para efetuar login com o SSO (via IDP).

Configuração de logoff único

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

1. Na página inicial dos Provedores de identidade, clique em Download SP public certificate.



Certificado público SP

2. Salve o arquivo baixado 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. Insira o URL do SLO (por exemplo, https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout).
6. Insira o emissor da controladora (por exemplo, ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com).
7. Clique em Submit.
8. Baixe o arquivo de metadados IDP novamente.
9. Na página Provedores de identidade, escolha o ícone Mais opções do IDP adicionado > Editar.
10. Ative o botão de alternância Ativar logoff único (SLO).
11. Carregue o arquivo de metadados recém-baixado.
12. Use a seguinte lista de verificação para verificar a funcionalidade SSO e SLO:

Lista de verificação:

- O login do administrador local foi bem-sucedido
- O portal do IDP está configurado e provisionado
- O IDP é adicionado ao Cisco IQ com status de "Êxito"
- Os mapeamentos de função são configurados e testados
- Os metadados da controladora são baixados e o certificado é extraído
- Se o SLO estiver habilitado, a configuração do SLO será concluída com o certificado de assinatura real
- O fluxo de SSO e SLO de ponta a ponta foi testado com êxito

Solução de problemas de IDP

As tabelas a seguir listam problemas comuns e possíveis soluções para ajudar a identificar e resolver rapidamente problemas relacionados a status de IDP, erros de certificado, falhas de login de SSO e configuração de SLO:

Tabela 5: 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 Active Directory (AD) Federation Services (FS) como o SAML IDP para o Cisco IQ, suportando autenticação baseada em senha e Public Key Infrastructure (PKI) ou baseada em certificado.

Pré-requisitos para Configurar ADFS IDP SAML para SSO

- O ADFS 6.0+ é recomendado
- Windows Server 2016 + (recomendado 2019)
- Integração do AD configurada com contas de usuário
- Certificados SSL/TLS no servidor ADFS
- Acesso de administrador ao Cisco IQ
- Acesso administrativo ao servidor ADFS (Windows Server)
- Acesso do PowerShell no servidor ADFS
- Conectividade de rede entre ADFS e Cisco IQ
- Autoridade de Certificação Corporativa (CA) (instalada ou acessível)
- Privilégios de Administrador de Domínio ou Administrador Corporativo (necessário apenas para PKI)

- Detalhes de configuração do servidor ADFS (conforme listado na tabela abaixo)

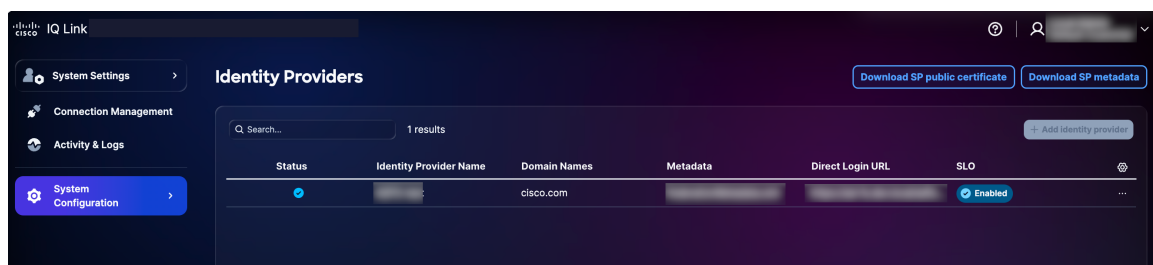
Tabela 6: Visão geral do fluxo de autenticação

Item	Descrição	Exemplo
FQDN do Cisco IQ	Nome de host de implantação de usuário	<Your-CIQ-FQDN> Por exemplo, dev35-23.cx-xxx-xxx.cisco.com
URL do Servidor ADFS	Endereço do servidor ADFS do usuário	https://<Your-ADFS-HOSTNAME> Por exemplo, https://adfs.dev.local
Domínio da empresa	Domínio de e-mail	<Seu-Domínio>
Grupos do AD	Nomes de Domínio (DN) do grupo do Ative Directory	CN=Função - Desenvolvedores do CXIQ OU=Groups, DC=dev, DC=local
Nome da autoridade de certificação (PKI)	Nome da autoridade de certificação corporativa	<Seu-Nome-da-CA>
Porta de autenticação de certificado (PKI)	Porta TLS alternativa do ADFS	49443
Impressão Digital de Certificado SSL	Certificado SSL do servidor ADFS	<Sua IMPRESSÃO DIGITAL COM CERTIFICAÇÃO SSL>

Configurando SAML de ADFS Base

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 Download SP metadata para fazer download desses arquivos.
3. Copie e salve os arquivos service-provider-metadata.xml e service-

provider-certificate.crt no servidor ADFS (por exemplo, C:\.

4. Faça login 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 salvo como parte da etapa 3.
10. Clique em Procurar para selecionar o arquivo de metadados do provedor de serviços e concluir o upload do arquivo.
11. Clique em Next.
12. Insira um nome de exibição (por exemplo, "Cisco IQ"), adicione as 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, MFA do Azure, Senha ocasional (TOTP) com base no tempo configurada).

Se esta política estiver 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
```

To set “Permit everyone” (no MFA requirement), run the following command:
Set-AdfsRelyingPartyTrust -TargetName “

```
”
```

```
-AccessControlPolicyName “Permit everyone”
```

You can also create the trust through 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/permit”, Value =  
“true”);
```

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 7: 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	Autenticação de PKI/certificado	O ADFS mapeia o certificado de cliente para um usuário do AD via 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 - Produção").

```
$relyingPartyName = "Your-RP-Name"
```

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"
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@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.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = 'email'
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

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

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

Write-Host "Regras de reivindicação configuradas com êxito!" -Cor de primeiro plano verde

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 executando o seguinte comando:

```
$username = "username"
```

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 usando o seguinte comando:

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

Saída de exemplo:

CN=Função - Desenvolvedores CXIQ,OU=Grupos de funções,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 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
```

- 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:-ca.cer" -CertStoreLocation  
"Cert:"
```

3. Aplicar 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:

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

4. Verifique a 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 ECU (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 ECU 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 Active Directory Information e inclua um email nos campos Subject e SAN

aviso: Os campos Assunto e SAN devem conter um Nome 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,
```

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 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 na autoridade de certificação 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:

```
EEnable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate/transport  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate/transport
```

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

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

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”) `\  
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”)
```


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 erros de 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 associação com negociação de certificado de cliente habilitada 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 habilitada usando o seguinte comando:

```
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)" -Fore
```

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

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

3. Verifique se nenhum certificado não autoassinado permanece no repositório Raiz Confiável 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 8: Configurações do Registro 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 SystemCertificates 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 repositório LocalMachine:

```
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 de 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 Meta  
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://<seu-servidor-adfs>/FederationMetadata/2007-06/FederationMetadata.xml>, substituindo "<seu-servidor-adfs>" pelo nome de host do seu servidor ADFS.
2. 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:

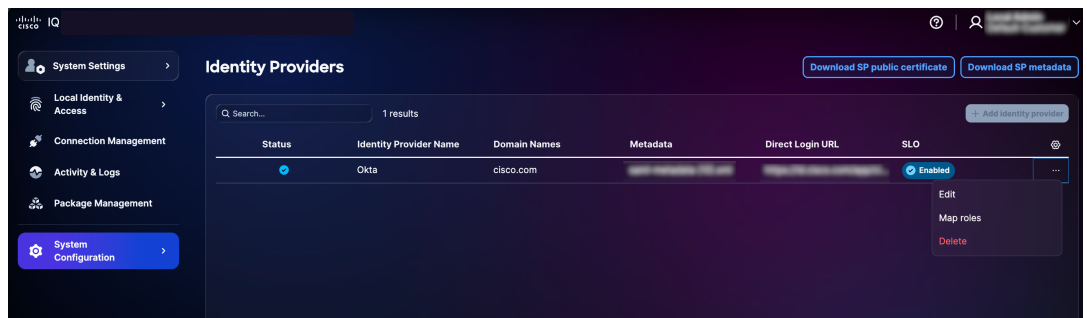
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

O sistema consulta o AD diretamente via LDAP (Lightweight Directory 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=exemplo,
DC=com CN=Função - Visualizadores CXIQ, OU=Grupos, DC=dev,
DC=exemplo, DC=com

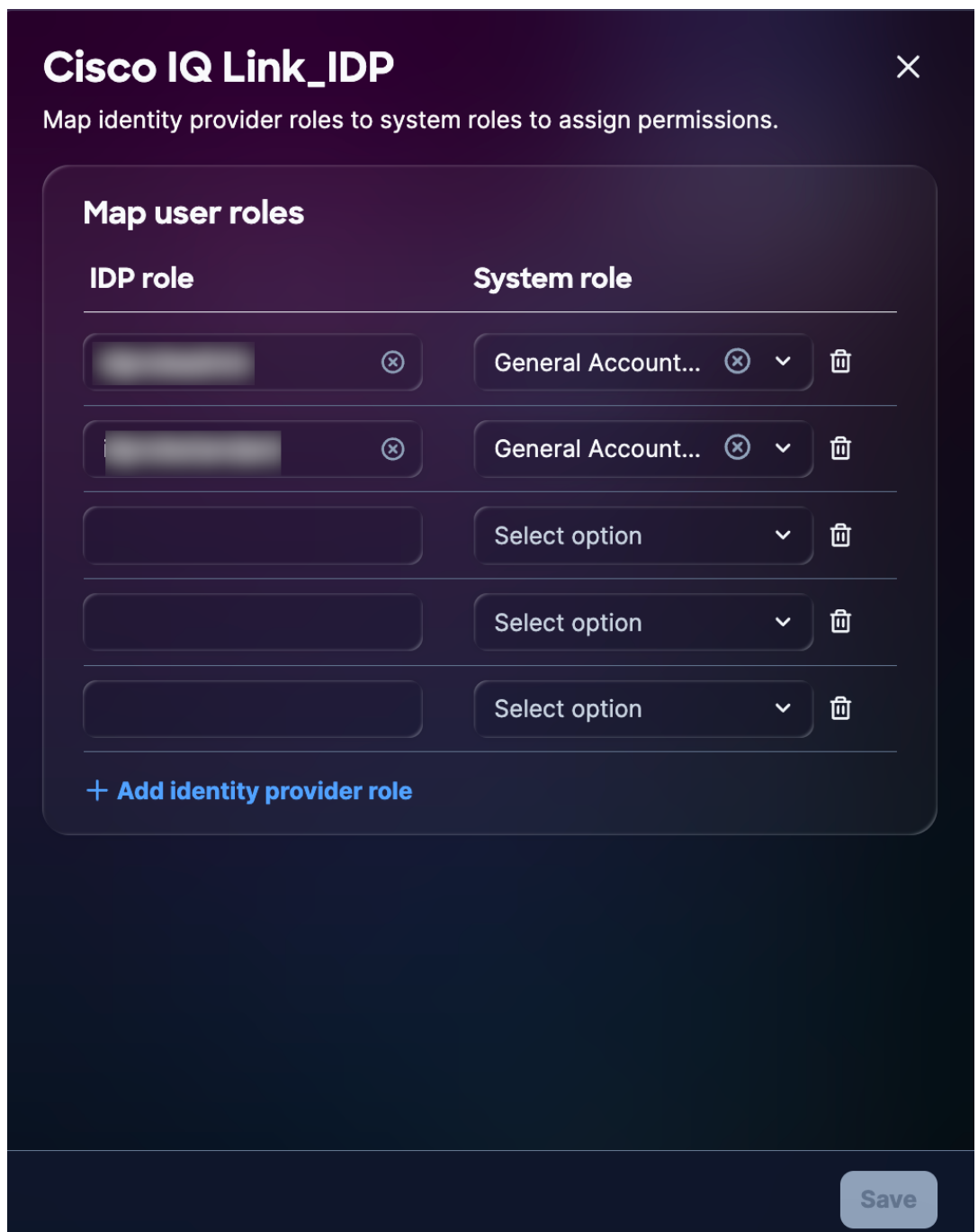
Se os grupos necessários não estiverem listados, eles deverão ser criados no AD por um Administrador de Conta para que você possa concluir o mapeamento de função do ADFS.

Para configurar o mapeamento de função:



Mapeamento de função

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



Mapeamento de função

2. Insira uma função IDP para a função do 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. 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 DNs completos.

3. Click Save. 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 começar a testar completamente o fluxo de PKI no navegador, verifique se o certificado do usuário está instalado no MacOS Keychain (consulte [Importação do certificado do usuário na máquina cliente \(MacOS\)](#)). Para testar:

1. Navegue até o URL de login do SAML do aplicativo. O ADFS apresenta opções de certificado e senha.
2. Escolha Autenticação de certificado. 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 o login 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 9: 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
Falha na descritografia	"Falha ao descriptografar a asserção" nos logs	Verificar configuração na configuração de certificado ADFS

Problema	Sintomas/Descrição	Causas / Verificações / Soluções e Correções
Loop de login	Preso na autenticação ou loop de login	- URL do ACS inválida: Verifique: https://your-fqdn/saml/acs - Incompatibilidade de cookies: Verificar cookies do navegador para o domínio correto

Comandos de Diagnóstico para Solução de Problemas

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

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

```
curl -k https://
```

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

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

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
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 - Production" |  
Select-Object SamlEndpoints
```

Configuração de SAML do Microsoft Entra ID para SSO

Esta seção fornece orientação para configurar a ID do Microsoft Entra (ID do Entra) como o SAML IDP para o Cisco IQ, suportando tanto o PKI baseado em senha e como a Autenticação Baseada em Certificado (CBA).

Pré-requisitos para Configurar o Entra ID SAML para SSO

- Locatário da ID da Entra (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 10: 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

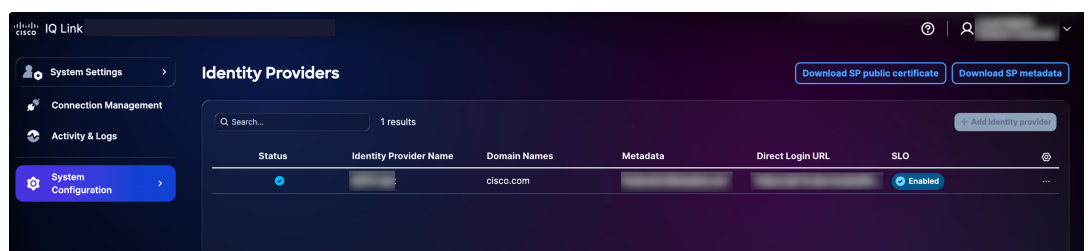
Criando uma aplicação empresarial

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 (sem 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 de 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:

4. No aplicativo empresarial, navegue para Logon único e escolha SAML.
5. Na seção Configuração SAML Básica, clique em Editar e insira o seguinte:

- Identificador (ID da entidade): <SEU-CIQ-FQDN>
- URL de resposta (URL ACS): https://<YOUR-CIQ-FQDN>/saml/acs
- URL de Logon: https://<YOUR-CIQ-FQDN>/saml/login
- URL de logoff: https://<YOUR-CIQ-FQDN>/saml/logout

6. 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.

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

8. Configure as seguintes declarações:

Tabela 11: 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/uniqueidentifier
nome dado	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/uniquestring
sobrenome	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/uniquestring
nome	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/uniquestring
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

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 do 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 Apply.



Note: Crie funções que correspondam aos seus requisitos de mapeamento de funções do Cisco IQ (por exemplo, Administradores CXIQ, Desenvolvedores CXIQ ou 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 funciona somente para grupos sincronizados do AD local
- A origem da ID de grupo envia Universally Unique Identifier (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, escolha Single Sign-On > SAML Signing Certificate.
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 da 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 12: Funções do sistema

Função do sistema	Função IDP (Valor da Função do Aplicativo)	Descrição
general_account_administrator	Administradores do CXIQ	Permissões totais para todas as ações
general_account_viewer	Desenvolvedores do CXIQ	Acesso somente leitura
general_account_viewer	Visualizadores CXIQ	Acesso somente leitura



Note: Use as cadeias de caracteres do Valor da Função de Aplicativo exatamente como configuradas na ID do Entra (consulte [Configuração de Funções de Aplicativo](#) para obter mais detalhes)

4. Click Save. 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 success"
```

Saída esperada

Autenticação compatível com SAML 2.0 bem-sucedida para o usuário:
user@domain.com com o nome completo: Grupos N/A e 1

Grupo extraído: Administradores CXIQ (original: Administradores do CXIQ)

Total de grupos extraídos: 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 AD CS com CA empresarial configurada (por exemplo, "DEV-ADCS-CA")
- Acesso de administrador do PowerShell no servidor de autoridade de certificação
- O UPN do certificado deve corresponder à ID de usuário principal do Entra
- 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> pela sua Entra ID UPN (por exemplo, user@ciqtestdev.onmicrosoft.com).

3. Para gerar o certificado, execute os seguintes comandos:

```
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
    "
```

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 Get Info.
3. Em Trust, defina como "Always Trust".



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 certificação.
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 Lista de Certificados Revogados (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 de destino.
4. Em Configure, defina o nível de proteção como Single-factor 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 SAN (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 13: 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 do Logon Único SAML para obter mais detalhes). Verifique se o usuário tem o atributo de e-mail preenchido.
Total de grupos extraídos: 0	Declaração de grupos não configurada ou origem incorreta	Use user.assignedroles como origem. Verifique se o usuário está atribuído a uma Função de Aplicativo (consulte Atribuição de Usuários a Funções de Aplicativo para obter mais detalhes).
Declarações de grupos duplicadas	user.groups e user.assignedroles	Remova a declaração user.groups. Mantenha apenas

Problema	Causa	Reparar
	ativos	user.assignedroles. Use a abordagem Funções de aplicativo (consulte Configuração de funções de aplicativo para obter mais detalhes).
Grupos exibidos como UUIDs	O atributo de origem é "ID do grupo"	
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. Publique a CRL em uma URL publicamente acessível ou use a abordagem de CA autoassinada (consulte Solução alternativa da CRL para problemas de acessibilidade para obter mais detalhes).
AADSTS500191	CRL não alcançável pela Internet	Verifique se o certificado do usuário é importado no MacOS Keychain Access (consulte Importação do certificado do usuário na máquina do cliente (MacOS) para obter mais detalhes), o CBA é habilitado no Entra ID com as configurações necessárias (consulte Habilitação do CBA nos métodos de autenticação do Entra ID para obter mais detalhes) e o Chrome é reiniciado para aplicar as alterações.
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	
Asserção SAML expirada	Desvio de relógio entre sistemas	Aumentar clock_skew_seconds na configuração do plugin (o padrão é 300; use 30000 para o laboratório).
Status "Incompleto" no dispositivo virtual	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 o Cisco Discovery Protocol (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 um Aplicativo Empresarial (sem galeria) na ID do Entra
- Configurar uma 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 o XML de Metadados de Federação

Configuração do Cisco IQ

- Adicione um IDP 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 ECU de Autenticação de Cliente
- Emitir um certificado de usuário com um UPN correspondente ao usuário da ID Entra
- Exportar um certificado do usuário como um arquivo PFX e instalá-lo 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 em métodos de autenticação
- Configurar associação de nome de usuário (PrincipalName e

userPrincipalName)

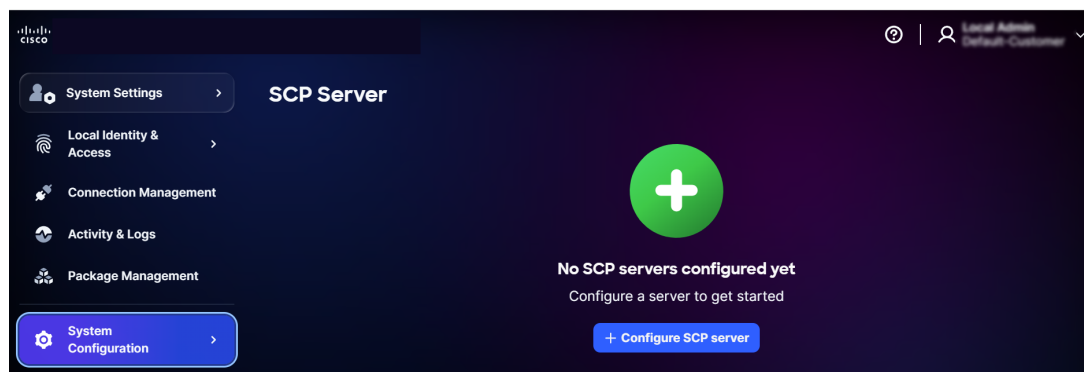
- Verificar se o login do CBA funciona de ponta a ponta

Adicionando Servidor SCP

Um servidor SCP é um pré-requisito para importar arquivos de atualização que são essenciais para adicionar, atualizar ou corrigir a instalação do Cisco IQ.

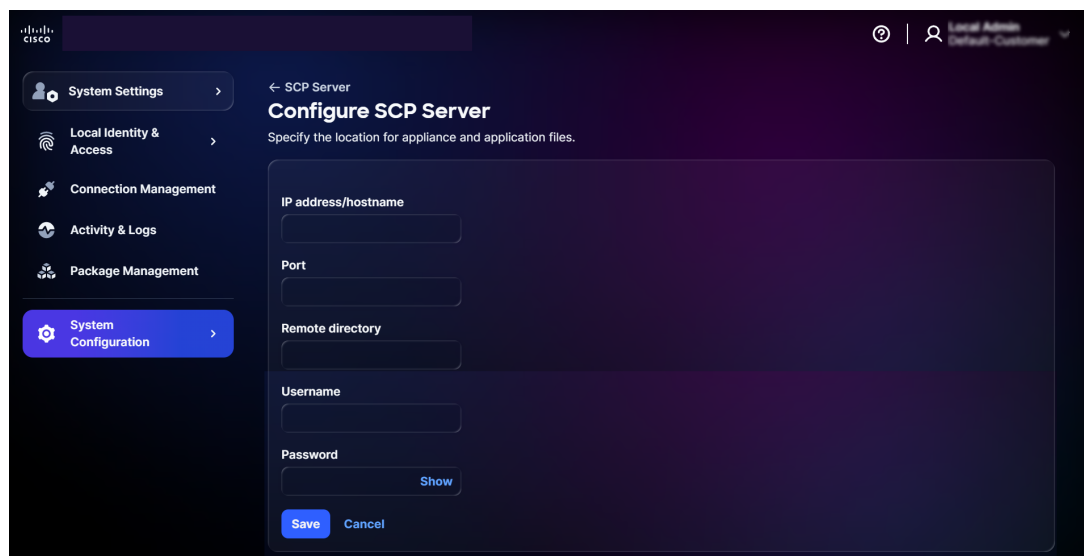
Para adicionar um Servidor SCP:

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. A página Configurar Servidor SCP é exibida.



Configurar Servidor SCP

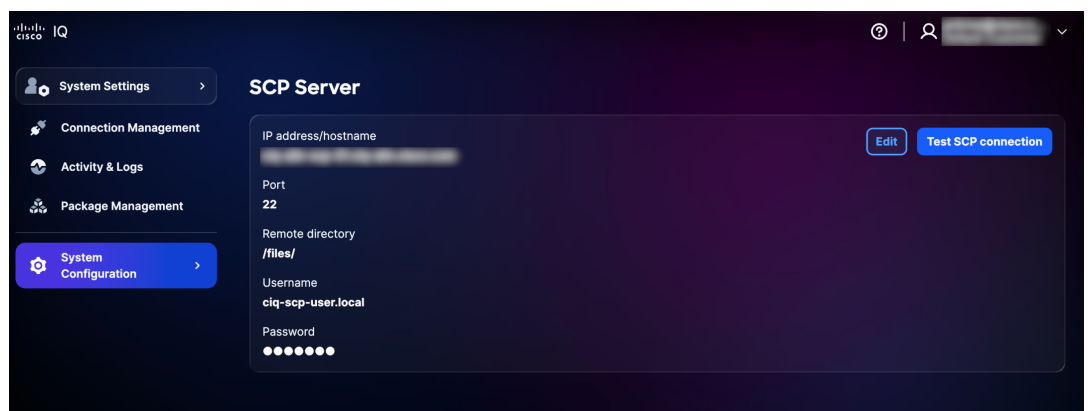
3. Insira um endereço IP/nome de host.

4. Insira uma Porta.
5. Insira um Diretório remoto.
6. Digite um nome de usuário.
7. Digite uma senha.
8. Click Save. Uma confirmação é exibida.

Edição de um servidor SCP existente

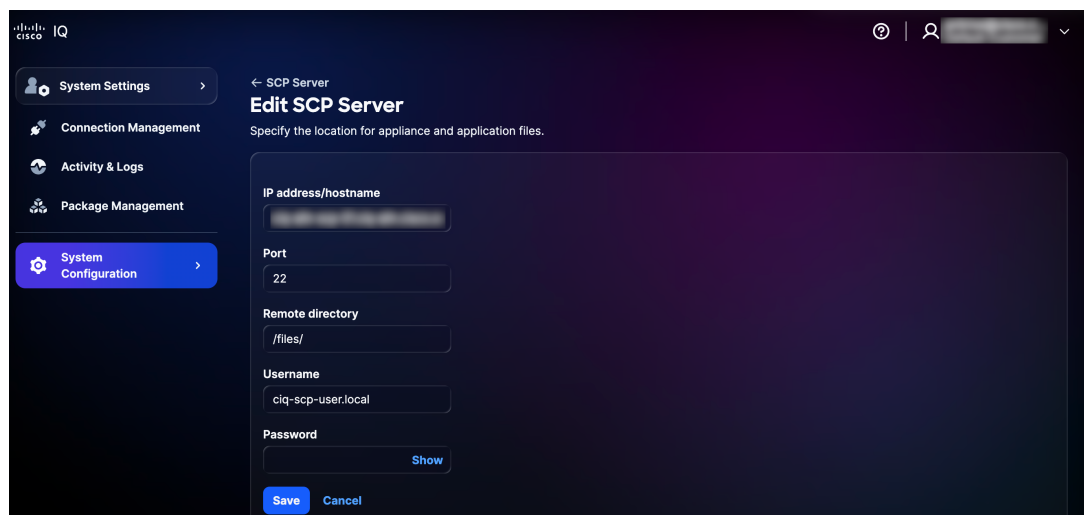
Para editar um servidor SCP existente:

1. Navegue até a página Servidor SCP.



Servidor SCP adicionado

2. Clique em Editar do servidor SCP existente desejado.



Editando o Servidor SCP

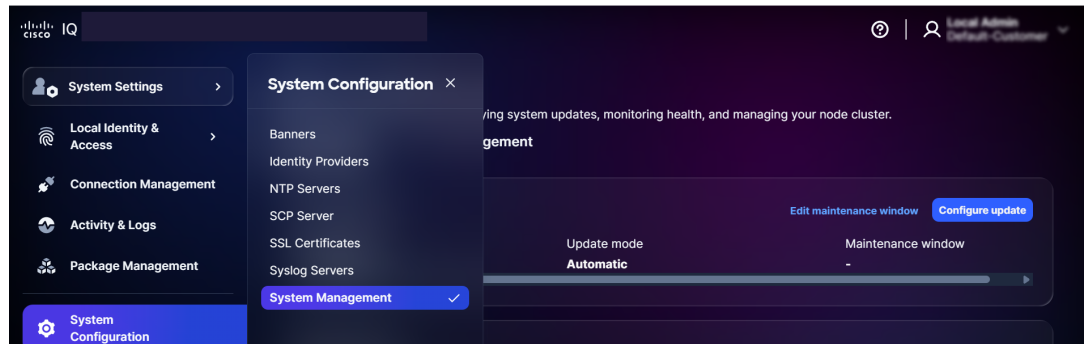
3. Modifique os detalhes conforme necessário.
4. Click Save.

Gerenciamento do sistema

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

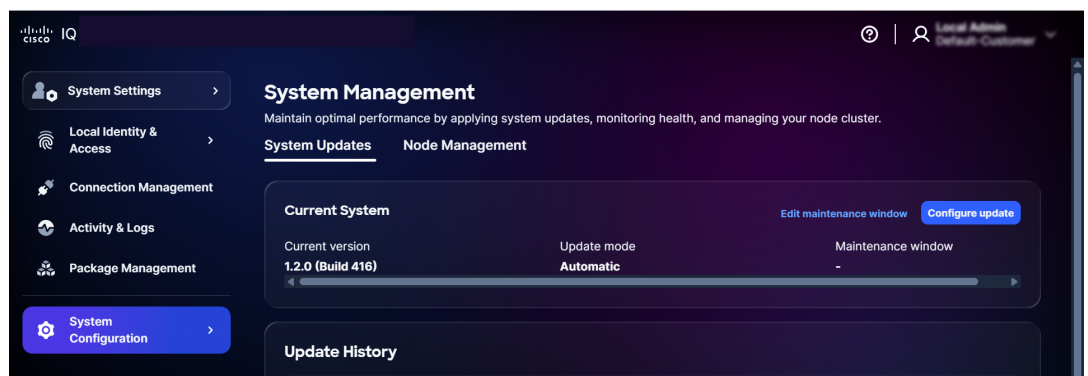
Reagendando a atualização do sistema

Para reprogramar a atualização do sistema:



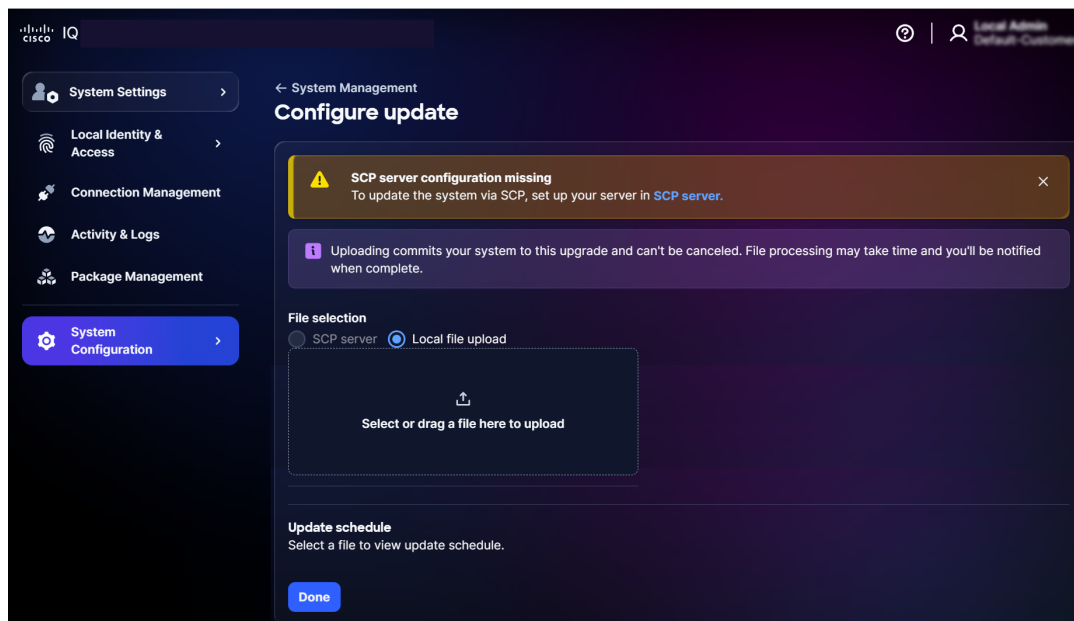
Gerenciamento do sistema

1. Em Configurações do sistema, 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 Configure update. A página Configurar atualização é exibida.



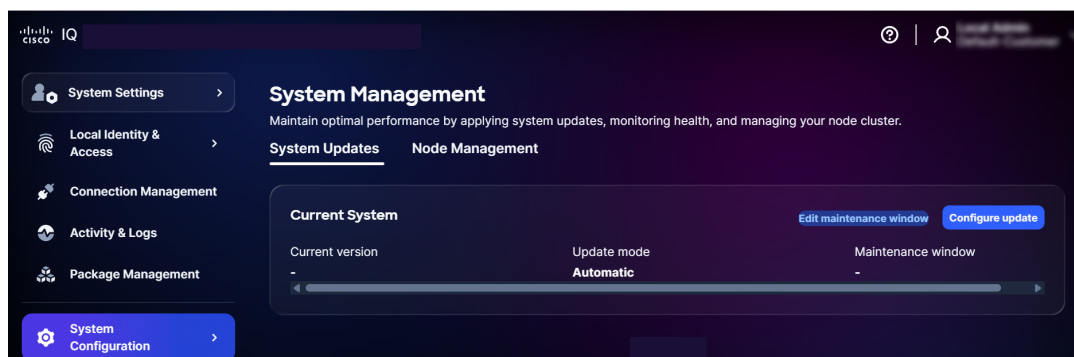
Configurar atualização

3. Escolha o Agendamento de atualização para agendar outro horário.
4. Aguarde até que o upload do arquivo seja concluído; a duração depende do tamanho do pacote e da velocidade da rede.

Confirme a atualização bem-sucedida verificando o ícone de marca de seleção exibido na coluna Atualizar status.

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:



Editar Manutenção

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

Edit maintenance window

Select the day and time to reserve for future updates. If an update can't be completed during the maintenance window, it will occur on the last day of the grace period.

Day Time IST

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. No caso de uma falha de atualização, o sistema executa até duas (2) tentativas automáticas. Uma terceira tentativa está agendada, mas requer iniciação manual.

Gerenciamento de nó

1. Navegue até System Configuration > System Management > Node Management para exibir e gerenciar os nós no seu cluster.

Status	Node	Node Type	IP	Netmask	Gateway	Last System Update	CPU	Memory	Storage	
Online	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 20...	1%	30%	2%	

Gerenciamento de nó

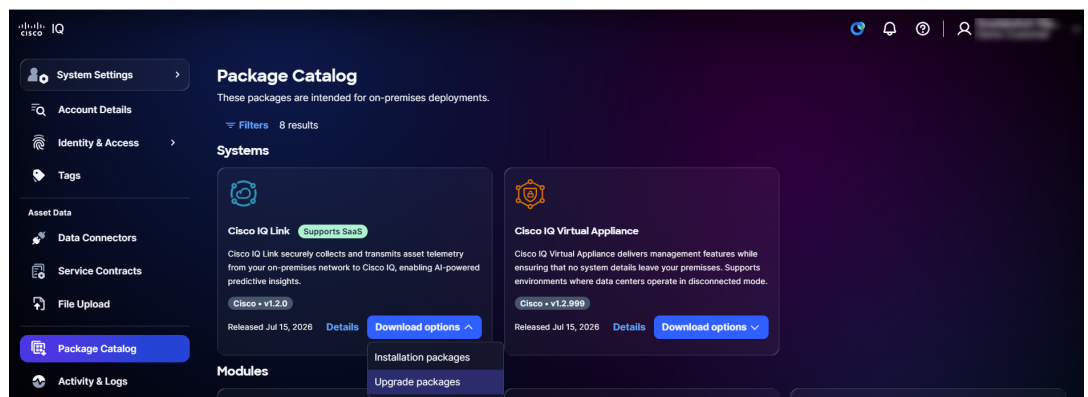
2. A lista de nós exibe o status, o nome do host, o tipo de nó, o endereço IP, a máscara de rede, o gateway e o horário da última sincronização de cada nó.

 Note: Uma marca de seleção azul na coluna Status indica que o nó está ativo.

Atualizando manualmente o sistema

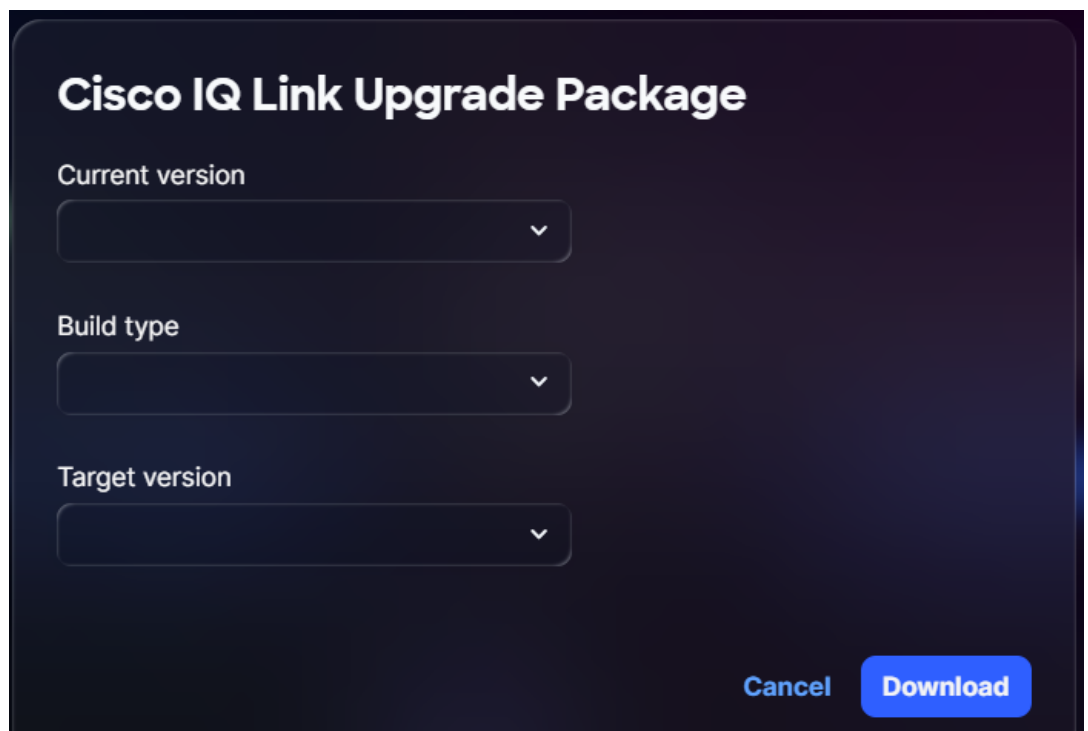
Em cenários onde a distribuição automática do Cisco IQ SaaS está indisponível ou atrasada, você pode executar manualmente uma atualização do sistema fazendo o download do pacote de atualização diretamente do Cisco IQ SaaS. Para atualizar manualmente o sistema:

1. Faça login no [Cisco IQ SaaS](#).
2. Navegue até Home > System Settings > Package Catalog.



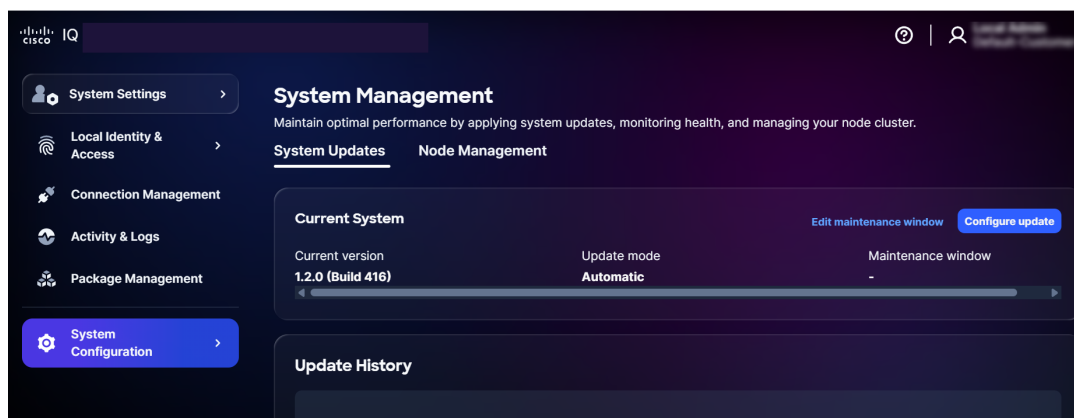
Catálogo de software

3. Na placa Cisco IQ Virtual Appliance, clique em Download options > Upgrade packages.



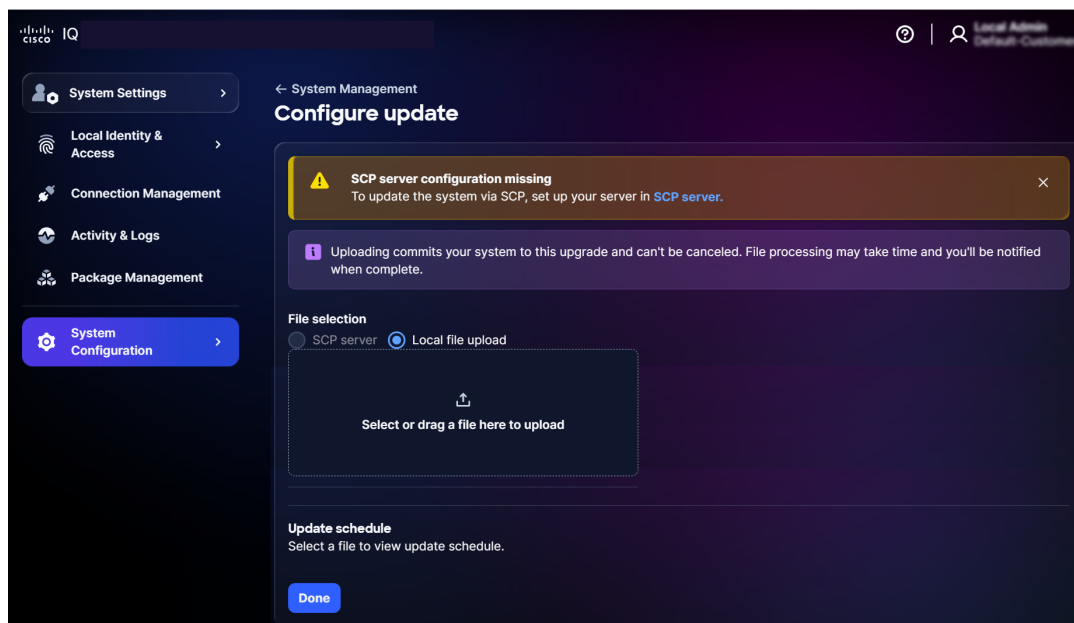
Pacote de atualização

- Escolha a Versão atual na lista suspensa.
- Escolha o Tipo de construção na lista suspensa.
- Escolha a versão de Destino na lista suspensa.
- Clique em Download. O pacote de atualização é baixado.
- Navegue até Cisco IQ VA.
- Em Configurações do sistema, escolha Configuração do sistema > Gerenciamento do sistema.



Configurar atualização

- Clique em Configure update.



Carregamento de arquivo local

- Clique no botão de opção Local file upload.

12. Selecione ou arraste o arquivo do pacote de atualização baixado para o campo de carregamento.
13. Aguarde até que o upload do arquivo seja concluído; a duração depende do tamanho do pacote e da velocidade da rede.

Configuração de Certificados SSL

Um certificado autoassinado padrão é pré-instalado e habilitado no Cisco IQ, mas você pode, opcionalmente, 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.

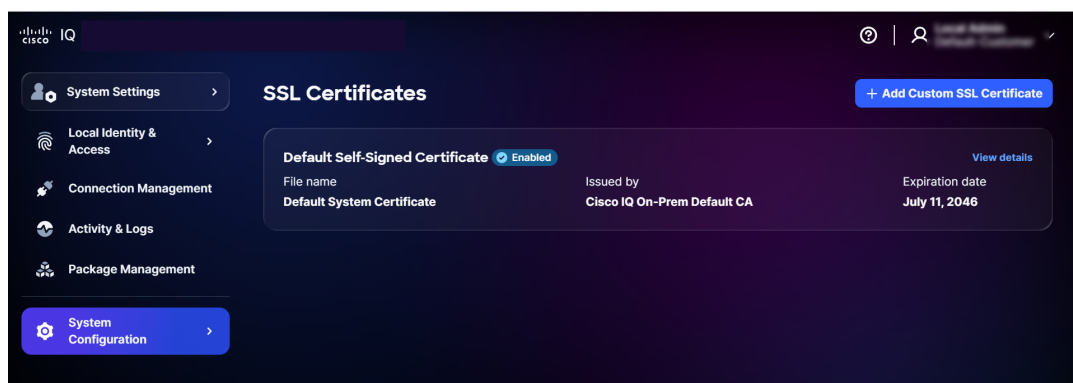


Note: O certificado deve ter pelo menos 90 dias de validade. Um certificado é considerado "prestes a expirar" quando tem menos de 90 dias até a expiração. Após adicionar, editar ou excluir um certificado SSL, você deve carregar o novo certificado SSL conforme descrito em [Concluindo a configuração do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

Adicionando certificado SSL personalizado

Para adicionar um certificado SSL personalizado:

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



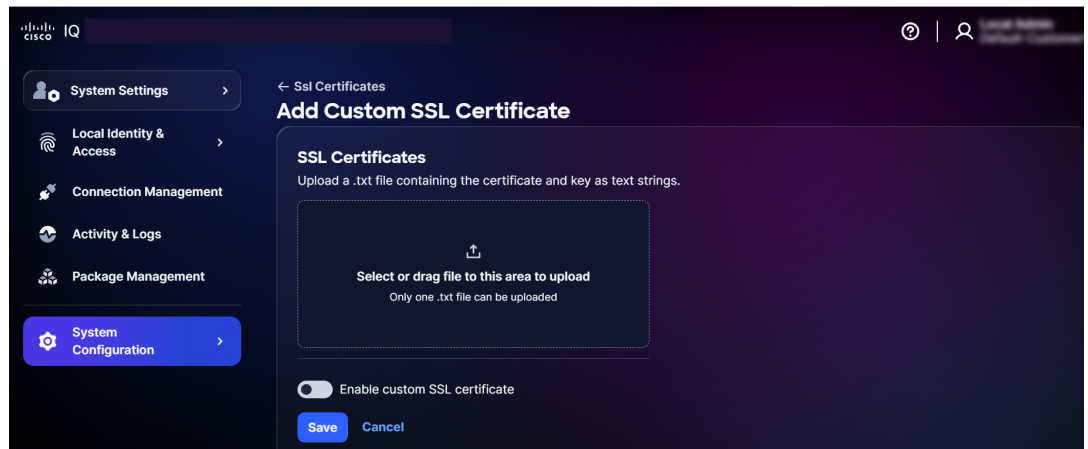
Adicionando Certificado SSL

2. Clique em Adicionar certificado SSL personalizado.



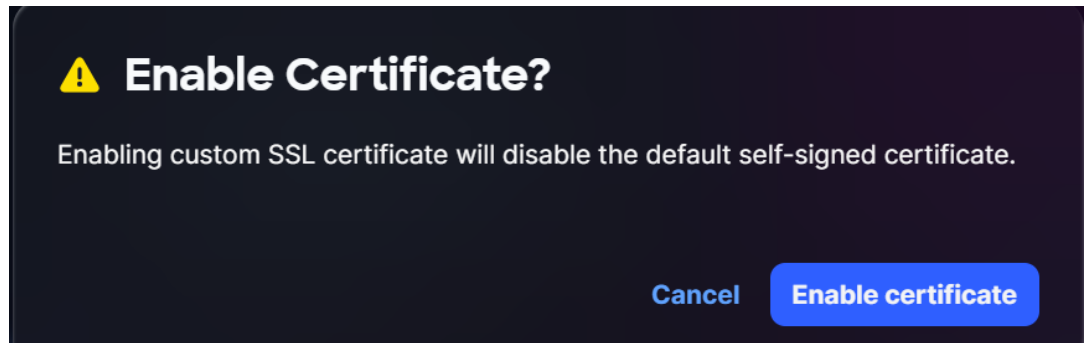
Note: Carregue um arquivo .txt que inclua o certificado e a

-
- ✎ chave codificados para 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 na seção Certificado SSL.
4. Ative o botão de alternância Ativar certificado SSL personalizado.



Habilitar certificado

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

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

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

Editando Certificado SSL Personalizado

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.
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 Certificado SSL Personalizado

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

Para excluir:

1. Navegue até o certificado SSL pessoal desejado.
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.

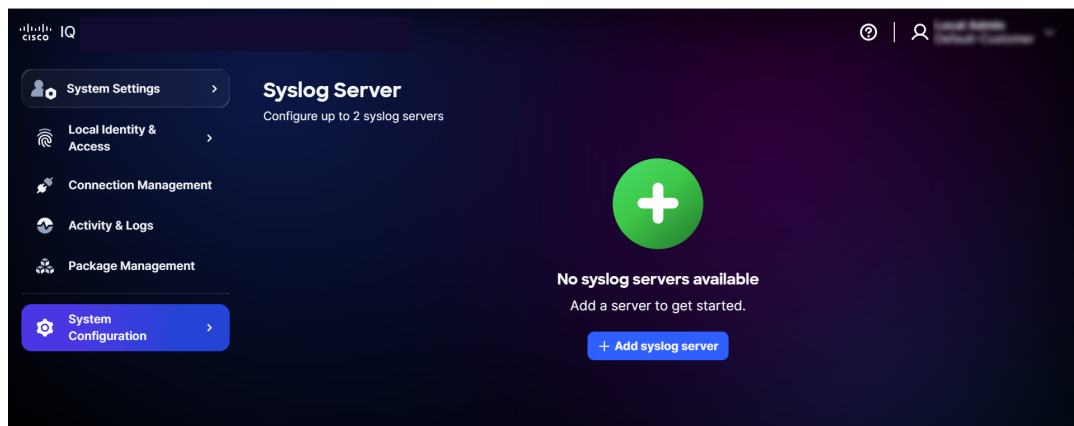


Note: O servidor Syslog deve ser especificado como um endereço IP e não como um FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado).

Adicionando Servidor Syslog

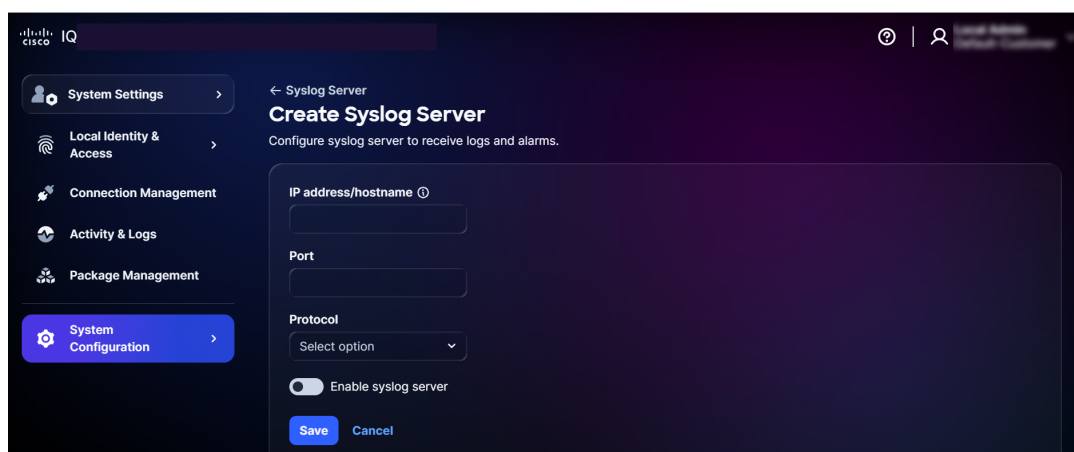
Para adicionar um Servidor syslog:

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. Digite Port.
5. Selecione o protocolo aplicável na lista suspensa Protocolo (por exemplo, UDP, 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 Servidor Syslog Configurado

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.

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

Excluindo Servidor Syslog Configurado

Para excluir um servidor syslog configurado:

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

Event	Action	Email	User	Date and time	Activity type	Reporting group	Log level	Affected resource	Error code	Account
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Syslog ...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
POST /...	Create	admin	Local A...	2026-0...	data_cr...	932dfd...	error	API Res...	403	unknown
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	error	Banner	404	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	Applica...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	User Pr...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...

Atividade e registros

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

Atividade e logs:

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

As seguintes opções de filtro estão disponíveis:

- Última data registrada: 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: Filtros para um código de erro específico

Banners

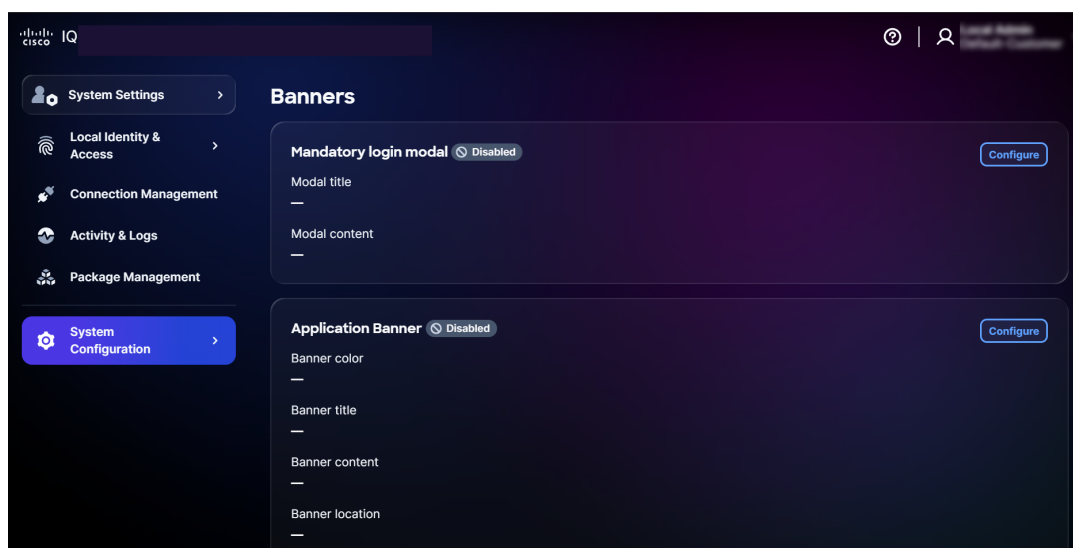
Os administradores de conta podem configurar banners de todo o sistema para atender aos padrões de segurança e conformidade.

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

Configurando banners modais de login obrigatórios

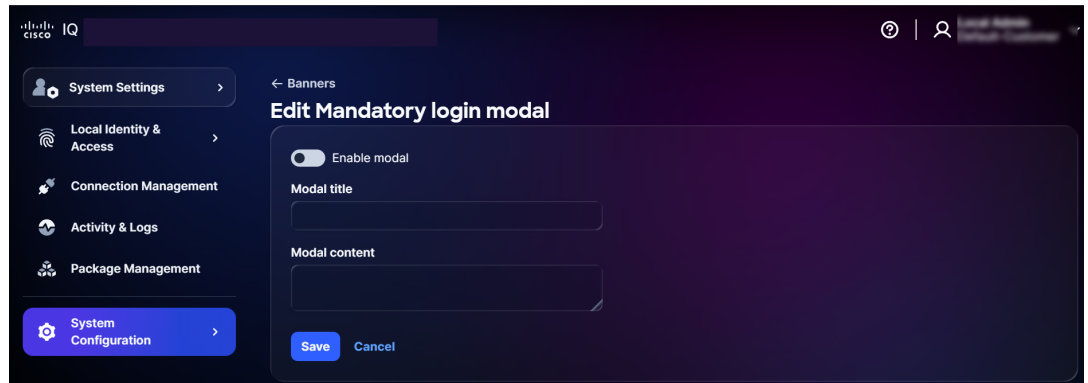
Para configurar um banner obrigatório:

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.



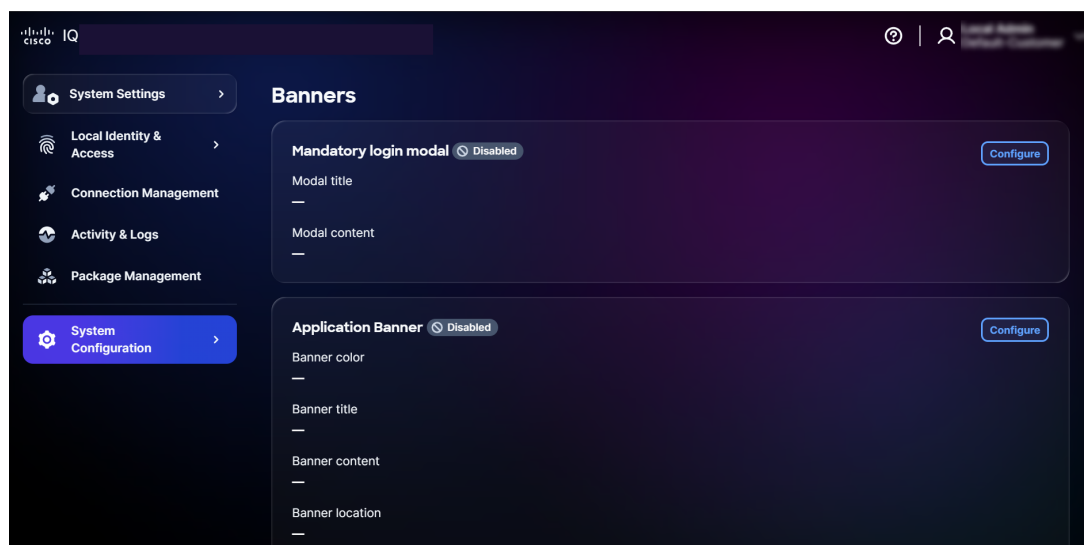
Editar banner modal de login obrigatório

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

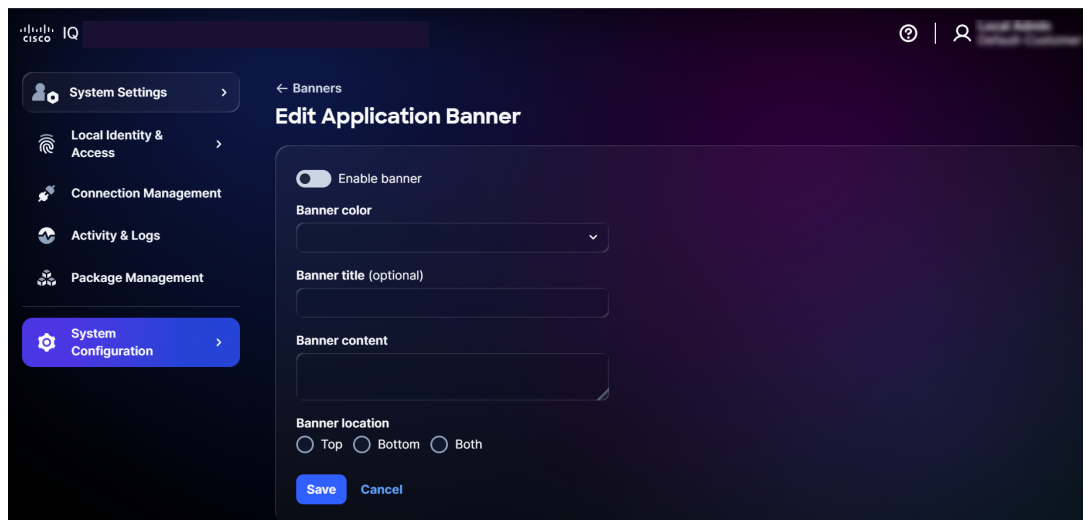
Para configurar um banner de aplicativo:

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.



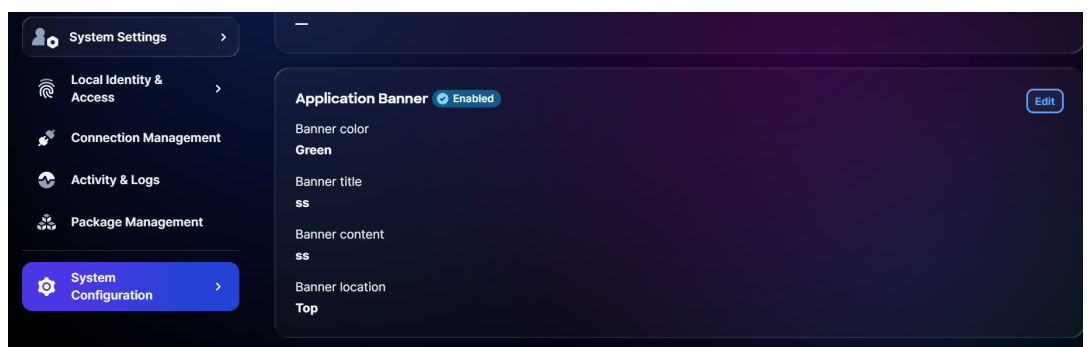
Editar banner do aplicativo

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

Editando banners

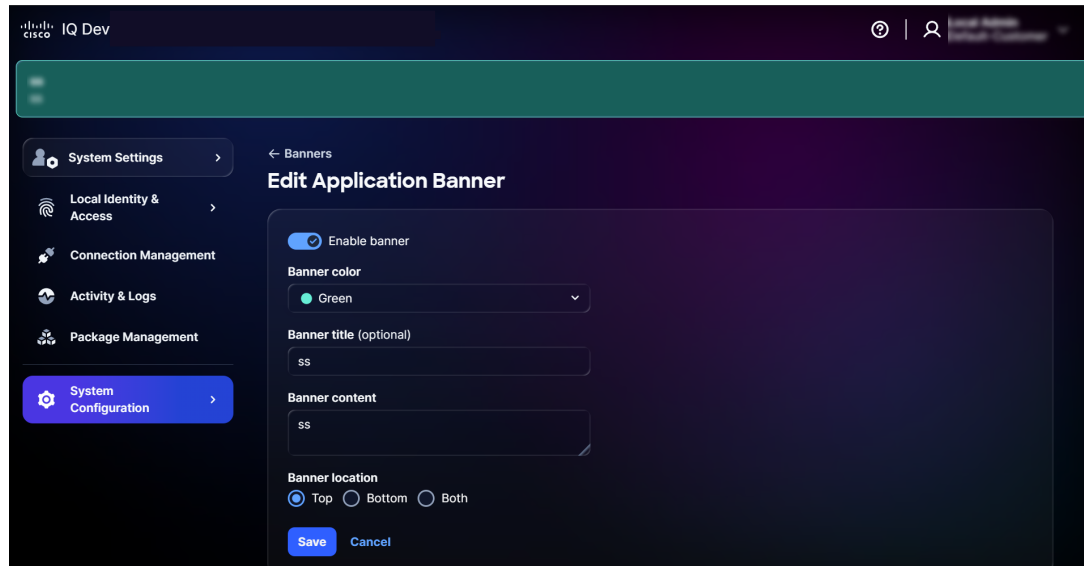
Para editar um banner:

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



Editar banners

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



Editar banner do aplicativo

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

Troubleshooting

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.

```

Cisco IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem      Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit

```

Menu principal

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

```

Cisco IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

[Enter SCP/SFTP Server Address: ]
Valid IP address ✓
[Enter SCP/SFTP Server Port (e.g. 22): ]
Valid port ✓
[Enter SCP/SFTP Server Path (e.g. /var/log/support/): ]
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

[Select protocol [1]/[2] (default: SCP): 1]
scp
✓ Selected protocol: SCP
[Enter Username: ]
Valid username ✓
[Enter Password: ]

Continue with System Diagnostics? ([c]ontinue/[B]ack):

```

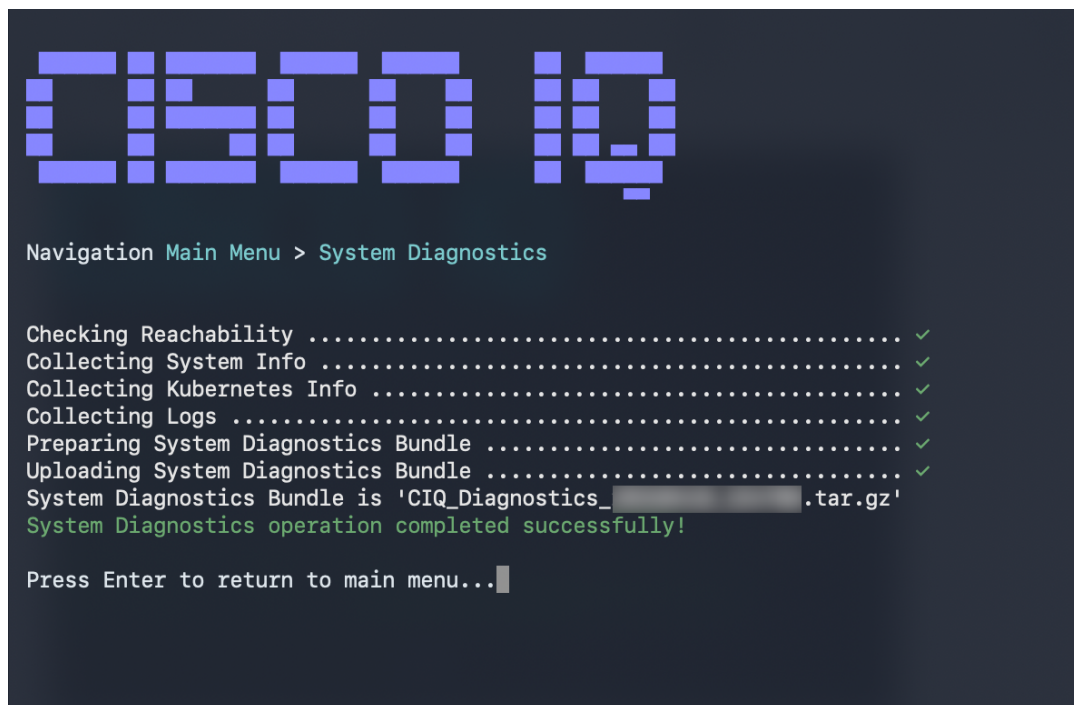
Diagnóstico do sistema

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.

A screenshot of a terminal window with a dark background. At the top, the Cisco logo is displayed in a stylized, blocky font. Below the logo, the text "Navigation Main Menu > System Diagnostics" is shown in a light blue color. The main part of the terminal displays a list of diagnostic steps, each followed by a green checkmark: "Checking Reachability", "Collecting System Info", "Collecting Kubernetes Info", "Collecting Logs", "Preparing System Diagnostics Bundle", and "Uploading System Diagnostics Bundle". Below this list, a message states "System Diagnostics Bundle is 'CIQ_Diagnostics_XXXXXXXXXX.tar.gz'" where XXXXXXXXXX is a placeholder for a hexadecimal string. The final line of the diagnostic process is "System Diagnostics operation completed successfully!" in green. At the bottom, a prompt says "Press Enter to return to main menu..." with a cursor.

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.

Módulo de suporte

Você pode criar casos de suporte específicos de módulo e VA a partir do Cisco IQ SaaS. O módulo de suporte está disponível no Cisco IQ SaaS e oferece uma visão consolidada de seus casos de suporte. Ele permite

filtrar, classificar e personalizar a exibição da lista de casos, oferecendo visibilidade de casos abertos e fechados que você tem direito de acessar. Para obter informações mais detalhadas sobre o módulo de suporte no Cisco IQ SaaS, consulte o [Guia de introdução do Cisco IQ SaaS](#).



Note: Os clientes do Cisco IQ VA podem acessar a maioria dos recursos do módulo Cisco IQ SaaS Support, incluindo casos de abertura do Technical Assistance Center (TAC) relacionados ao Cisco IQ VA e seus módulos, bem como a criação e o gerenciamento de casos de produtos.

Criando um caso de suporte

Você pode criar casos de VA e específicos de módulo no Cisco IQ SaaS. Para criar um caso:

1. Faça login no [Cisco IQ \(SaaS\)](#).
2. Clique no ícone Help > Report an Issue. A janela Relatar um problema é aberta.

Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Relatar um problema

3. Forneça os detalhes necessários.
4. Clique em Submit.

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.