

Guia de primeiros passos do Cisco IQ

Introdução

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

Este documento fornece informações sobre como começar a usar o Cisco IQ e seus aplicativos. Para obter mais informações, consulte os documentos [Notas de Versão do Cisco IQ](#) ou [Perguntas Frequentes do Cisco IQ](#).

Integração


Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos antes de usar o Cisco IQ.

Navegadores compatíveis

O Cisco IQ é compatível com as versões estáveis mais recentes dos seguintes navegadores:

- Google Chrome
- Microsoft Edge
- Safari Apple
- Mozilla Firefox

 Note: O suporte é limitado às versões atuais do navegador e as versões mais antigas podem não fornecer funcionalidade completa ou podem não ser suportadas quando novas atualizações forem lançadas.

Conta da Cisco

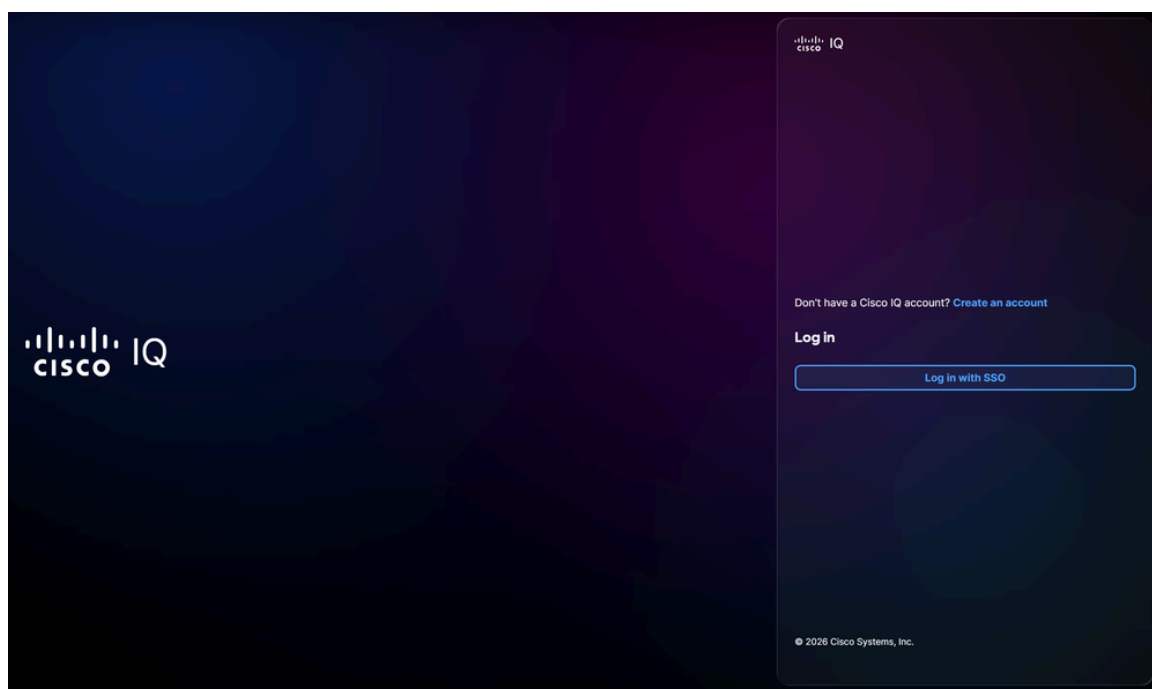
Para acessar o Cisco IQ, você deve ter uma conta Cisco.com. Consulte [Ajuda de login e conta](#) para obter mais informações sobre contas da Cisco.

Criação de conta

Criação de uma nova conta Cisco IQ

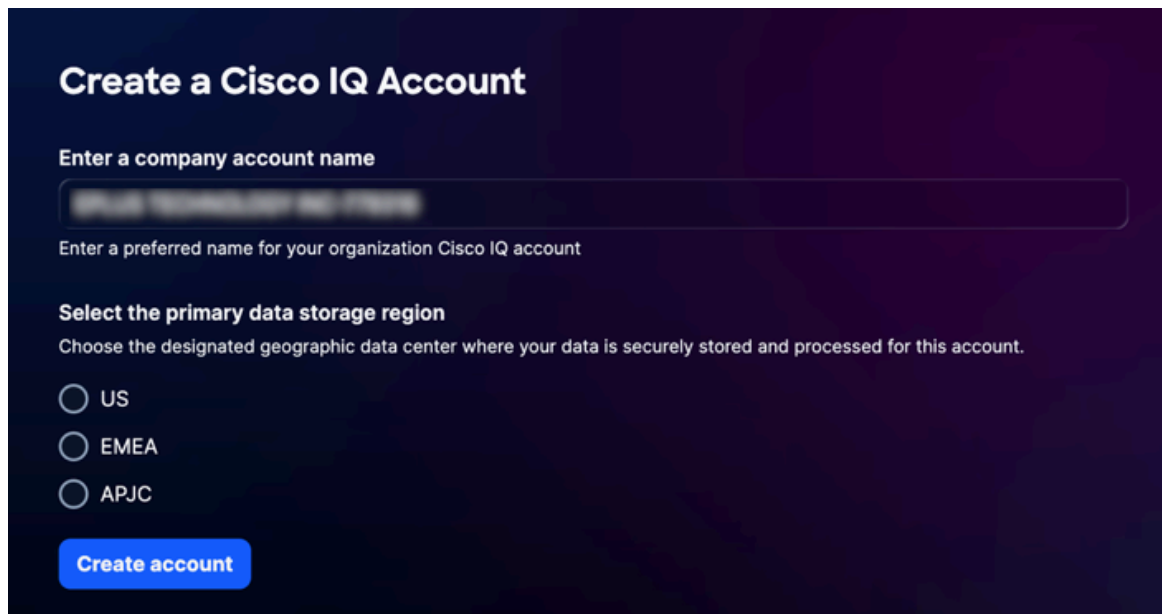
Para criar uma nova conta do Cisco IQ:

1. Navegue até [Cisco IQ](#). A página Cisco Log in é exibida.



Login no Cisco IQ

2. Clique em Criar uma conta.
3. Insira suas credenciais de ID do Cisco Connection Online (CCO) no campo Email.
4. Clique em Next.
5. Insira sua Senha.
6. Clique em Verify. A página Create a Cisco IQ Account é exibida.



Create a Cisco IQ Account

Enter a company account name

Enter a preferred name for your organization Cisco IQ account

Select the primary data storage region

Choose the designated geographic data center where your data is securely stored and processed for this account.

US

EMEA

APJC

Create account

Crie uma conta Cisco IQ


7. Insira o nome exclusivo que deseja usar para a conta Cisco IQ da sua organização no campo Insira um nome de conta da empresa.
8. Selecione a região de armazenamento de dados principal.
9. Clique em Criar conta. Você é redirecionado para a Barra Inicial do Cisco IQ.


Migração de contas de nuvem CX para o Cisco IQ


 **Note:** Somente administradores de conta podem migrar contas de nuvem CX existentes para o Cisco IQ.

Se você tiver uma conta da CX Cloud, poderá migrar os dados da CX Cloud para o Cisco IQ. Os seguintes dados são migrados automaticamente da conta existente do CX Cloud:

- Usuários e grupos de usuários (exclui usuários e grupos de parceiros)
- Contratos
- Adição de fonte de dados em nuvem para Intersight, Webex, Rede de Longa Distância Definida por Software (SD-WAN) e Meraki

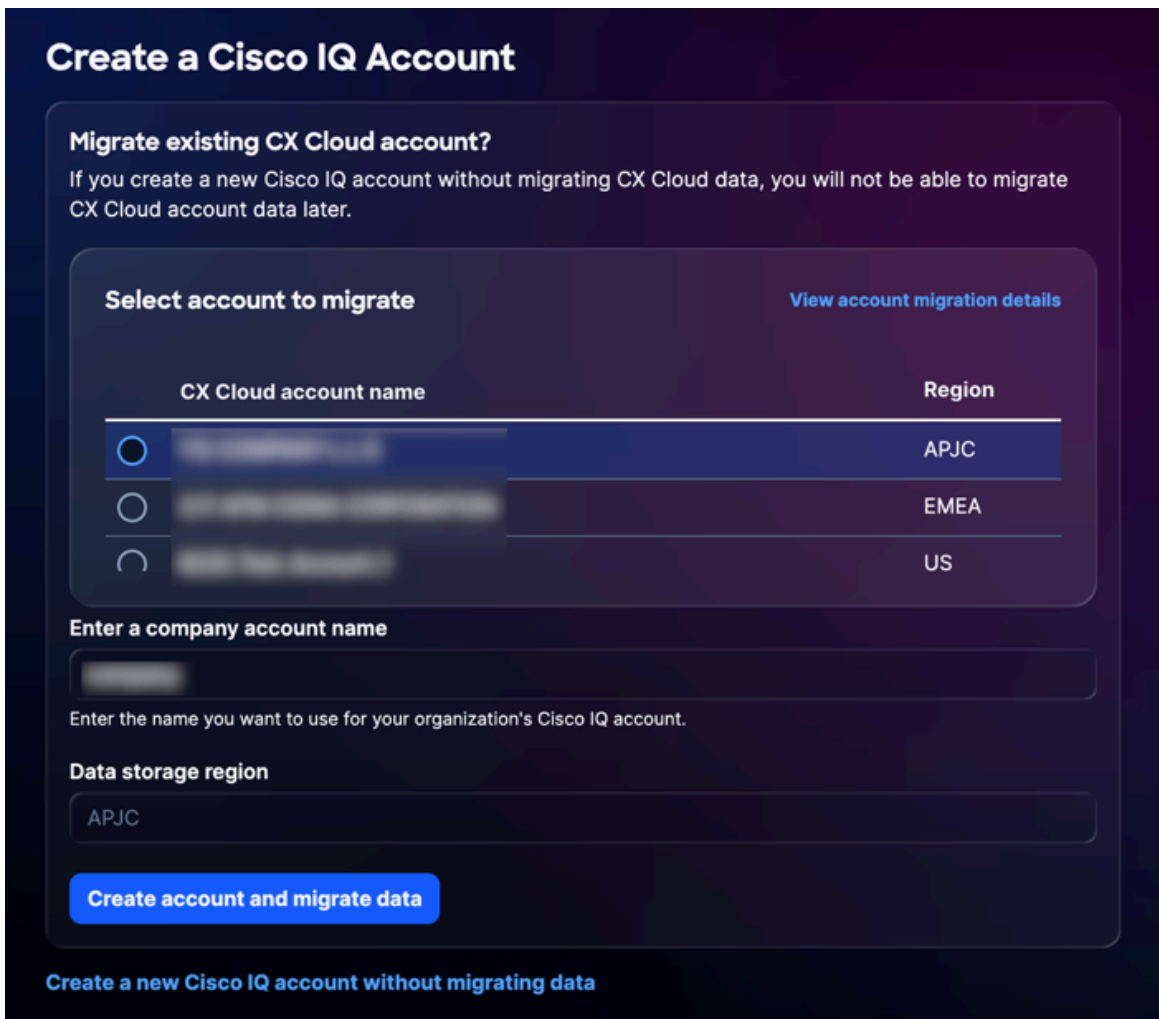
 **Note:** Para garantir uma transição tranquila e obter insights mais precisos da inteligência personalizada, preditiva e proativa baseada em IA do Cisco IQ, considere validar e organizar seus dados de conta da nuvem CX antes da migração.

 aviso: Se você criar uma nova conta do Cisco IQ sem migrar os dados da CX Cloud, não poderá migrar os dados da conta da CX Cloud mais tarde.

 Note: Somente uma conta de nuvem CX pode ser migrada por vez. Se precisar migrar contas adicionais, repita as etapas descritas nesta seção.

Para migrar uma conta existente do CX Cloud:

1. Navegue até [Cisco IQ](#). A página Cisco Log in é exibida.
2. Clique em Criar uma conta.
3. Insira suas credenciais de ID do Cisco Connection Online (CCO) no campo Email.
4. Clique em Next.
5. Insira sua Senha.
6. Clique em Verify. A página Create a Cisco IQ Account é exibida.



Create a Cisco IQ Account

Migrate existing CX Cloud account?
If you create a new Cisco IQ account without migrating CX Cloud data, you will not be able to migrate CX Cloud account data later.

Select account to migrate [View account migration details](#)

CX Cloud account name	Region
<input checked="" type="radio"/> [Redacted]	APJC
<input type="radio"/> [Redacted]	EMEA
<input type="radio"/> [Redacted]	US

Enter a company account name
[Redacted]

Enter the name you want to use for your organization's Cisco IQ account.

Data storage region
APJC


Create account and migrate data

[Create a new Cisco IQ account without migrating data](#)

Selecionar Conta de Nuvem CX

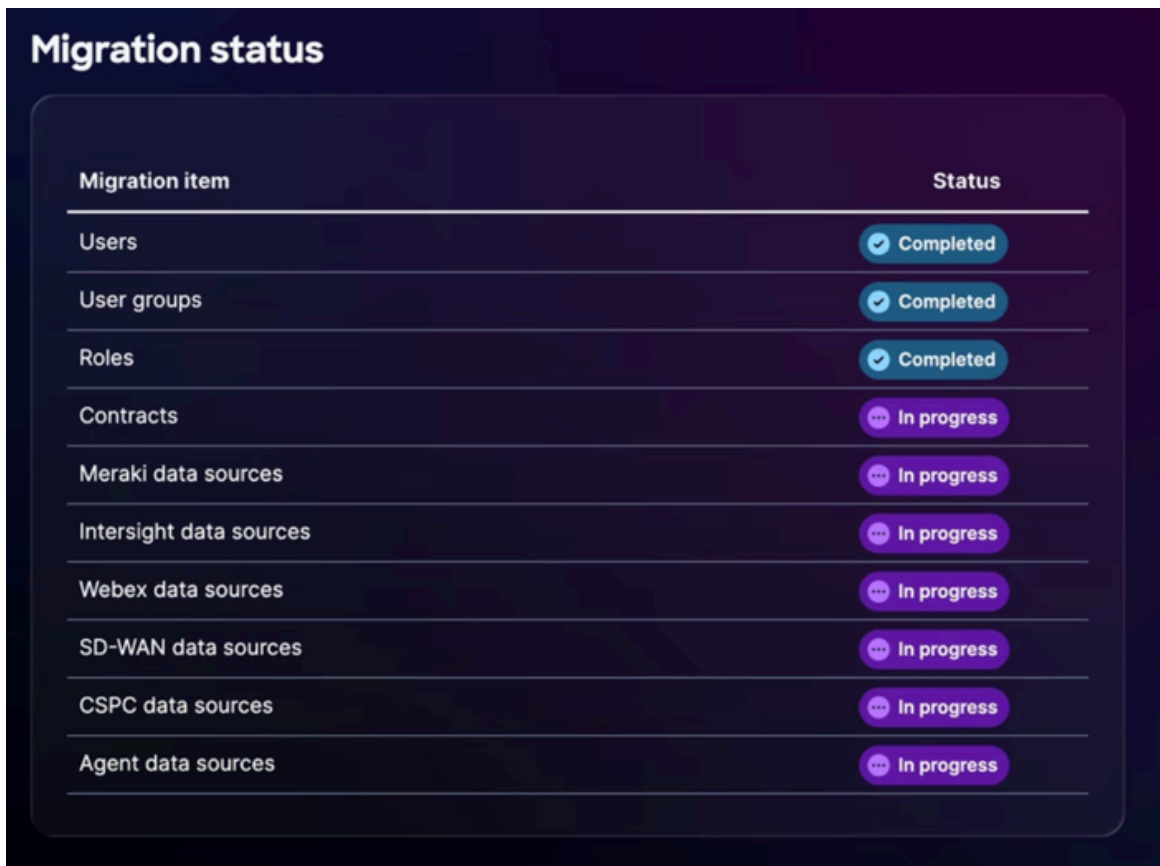
7. Selecione a conta CX Cloud da qual deseja migrar dados.

8. Insira o nome exclusivo que deseja usar para a conta Cisco IQ da sua organização.

 Note: A região de armazenamento de dados da conta original é preenchida automaticamente e migrada para a conta da empresa Cisco IQ. Para alterar a região de armazenamento de dados, você deve criar uma nova conta da empresa Cisco IQ.

9. Clique em Criar conta e migrar dados. A página Status da migração é exibida.

A página Status da migração exibe o status de conclusão dos dados que estão sendo migrados para o Cisco IQ. Os seguintes status estão disponíveis:



Migration item	Status
Users	Completed
User groups	Completed
Roles	Completed
Contracts	In progress
Meraki data sources	In progress
Intersight data sources	In progress
Webex data sources	In progress
SD-WAN data sources	In progress
CSPC data sources	In progress
Agent data sources	In progress

Status da migração


- Em andamento: Os dados estão em processo de migração
- Concluído: Migração concluída
- Não é possível migrar: A migração de dados está incompleta e o Cisco IQ não consegue migrar os dados

Se não for possível migrar os dados, você deverá migrá-los manualmente para a nova conta da empresa Cisco IQ. Consulte [Configurações do sistema](#) para obter mais informações sobre como adicionar dados adicionais ao Cisco IQ.

10. Quando o processo de migração estiver concluído, clique em Continuar. Você é

redirecionado para a Launchpad do Cisco IQ.

Como iniciar sessão em contas existentes

 Note: Os clientes com uma conta Cisco IQ existente que não foram adicionados a uma conta da empresa devem entrar em contato com o administrador de conta da empresa para solicitar acesso à conta.

Para efetuar login em uma conta existente:

1. Navegue até [Cisco IQ](#). A página Cisco Log in é exibida.
2. Clique em Efetuar login com SSO.
3. Insira suas credenciais de ID do CCO no campo Email.
4. Clique em Next.
5. Insira sua Senha.
6. Clique em Verify.

Se você tiver uma conta, será redirecionado para o Launchpad do Cisco IQ.

Se você tiver mais de uma conta, será redirecionado para a página Bem-vindo ao Cisco IQ.


Welcome to Cisco IQ!

Select an account below

Account name	Region
[blurred]	US
[blurred]	US
[blurred]	US
[blurred]	US


Selecionar nome da conta

Getting Started

 Note: Antes de começar, certifique-se de que você já tenha feito a integração completa com o Cisco IQ. Consulte [Onboarding](#) para obter mais informações.

Níveis de suporte

Os níveis de suporte do Cisco IQ definem o acesso e os recursos disponíveis para você no Cisco IQ e são projetados para melhorar sua experiência de suporte e serviços profissionais. Esses níveis estão vinculados ao seu contrato de suporte válido da Cisco e determinam quais recursos e ferramentas você pode utilizar, desde insights e soluções de problemas orientados por IA até gerenciamento de ativos e contratos. Compreender seu nível garante que você possa aproveitar totalmente os recursos do Cisco IQ, mantendo a conformidade com seus direitos contratuais. A tabela a seguir destaca os recursos do Cisco IQ disponíveis para cada nível.

 Note: Os recursos são cumulativos em todos os níveis de suporte; os níveis mais altos incluem todos os recursos dos níveis mais baixos.

	Nível Básico	Nível Padrão	Nível de Assinatura
	Saiba o que você tem	Priorizar para resiliência da operação	Acelere a excelência operacional
Clareza total do cenário	<p>Rastreie todos os ativos e subcomponentes da Cisco com alta confiança usando os seguintes recursos.</p> <ul style="list-style-type: none"> • Inventário de ativos • Relatórios EOL (End-of-Life, fim da vida útil) • Relatórios de cobertura de serviço • Painel Última data de suporte (LDOS) 	<p>Use os seguintes recursos para analisar o desempenho da sua rede e determinar onde alocar recursos, ajudando-o a tomar decisões conscientes sobre investimentos em infraestrutura.</p> <ul style="list-style-type: none"> • Informações sobre EOL¹ • Informações sobre a cobertura do serviço¹ • Informações sobre LDOS¹ • Informações sobre a importância dos ativos¹ • Marcação de ativos 	
Resiliência proativa	<p>Obtenha visibilidade de notificações importantes que ajudam a identificar e lidar com possíveis riscos no seu ambiente usando os seguintes recursos.</p> <ul style="list-style-type: none"> • Relatórios de avisos de segurança • Relatórios de Avisos de Campo 	<p>O Cisco IQ transforma dados em percepções correlacionando riscos de ativos, permitindo que você identifique e priorize os riscos de segurança mais críticos.</p> <ul style="list-style-type: none"> • Percepções da Consultoria de Segurança¹ • Segurança fortalecendo insights¹ 	<p>Os recursos a seguir fornecem recomendações práticas para ajudar a melhorar a postura de segurança e otimizar as configurações no seu ambiente.</p> <ul style="list-style-type: none"> • Recomendações de configuração¹ • Recomendações para fortalecer a

		<ul style="list-style-type: none"> • Informações de notificação de campo¹ • Informações de configuração¹ 	segurança ¹
Resolução rápida	<p>Gerencie seus casos de suporte e acompanhe o status da resolução em um local para resolver problemas mais rapidamente usando os seguintes recursos.</p> <ul style="list-style-type: none"> • Gerenciamento de casos • Solução de problemas de autoatendimento¹ 	<p>Use o seguinte recurso para rastrear tendências de caso e métricas de eficiência para mostrar melhoria operacional contínua. O Cisco IQ oferece um assistente de resolução contextual para ajudá-lo a resolver problemas ativos e investigar causas básicas.</p> <ul style="list-style-type: none"> • Informações do caso¹ 	

¹ Suporta conexão de telemetria e dispositivo através do Cisco IQ Link, Catalyst Center, Intersight, Meraki, SD-WAN Manager e WebEx Control Hub.

Recursos básicos

O nível de suporte Básico fornece controle básico por meio de suporte confiável e reativo, incluindo acesso a especialistas técnicos de suporte ao produto, solução de problemas por autoatendimento e gerenciamento centralizado de casos. Para garantir visibilidade total, o Cisco IQ unifica a telemetria de ativos, as informações de contrato e o histórico de suporte, oferecendo uma visão abrangente dos ciclos de vida de ativos, avisos de segurança e avisos de campo. Além disso, você pode fortalecer sua experiência técnica acessando os recursos básicos de aprendizado disponíveis na [Cisco U](#).

A tabela a seguir descreve os recursos disponíveis para o tier de suporte Básico.

Capacidade	Descrição
Inventário de ativos	O Inventário de ativos fornece uma lista atualizada e visualizações avançadas para produtos de hardware, modelos e números de série, versão do SO, local de instalação e detalhes da cobertura do serviço. Ele

	também fornece uma maneira de filtrar por "Último Sinal", que é quando a Cisco sabia que o ativo estava ativo com base em casos do Centro de Assistência Técnica (TAC), renovação de contrato, telemetria, etc.
Relatório EOL	Os relatórios de EOL fornecem uma lista atualizada e visualizações avançadas para hardware e software que se aproximam, atingem ou ultrapassaram as etapas de EOL de fim de vendas para LDOS, permitindo o planejamento de atualização de tecnologia e ciclo de vida.
Relatório de cobertura do serviço	Os relatórios de cobertura de serviço fornecem uma lista atualizada e visualizações avançadas para ativos cobertos e não cobertos.
Painel LDOS	O painel do LDOS oferece uma visão centralizada dos marcos do LDOS, permitindo melhor planejamento de ativos e previsão de orçamento antes que o hardware ou o software atinja o fim da vida útil, permitindo a redução do risco operacional.
Orientações de Segurança	As recomendações de segurança fornecem uma solução automatizada que detecta exposições, prioriza vulnerabilidades com base na gravidade e criticidade do risco e fornece percepções de nível executivo para acelerar a mitigação de ameaças críticas, aprimorando assim a resiliência da empresa contra ameaças em evolução.
Field Notices	Os avisos de campo fornecem uma solução automatizada que detecta problemas de produtos não relacionados à segurança, prioriza problemas com base na gravidade do impacto e na criticidade e fornece percepções de nível executivo para acelerar a resolução de problemas operacionais críticos, aprimorando assim a resiliência da empresa e mantendo o desempenho ideal.
Gerenciamento de casos	O Gerenciamento de casos fornece uma lista atualizada de casos do Cisco TAC, incluindo contagens de casos, status, gravidade e RMAs (Return Material Authorizations, Autorizações de devolução de materiais) associados aos casos. Ele também permite abrir casos do TAC (por meio de início cruzado com o Support Case Manager (SCM)) e atualizar rapidamente as informações do caso para facilitar a resolução.
Solução de problemas de autoatendimento ¹	A solução de problemas self-service fornece uma maneira de resolver problemas instantaneamente com o Cisco IQ AI Assistant. Essa ferramenta interativa fornece solução de problemas contextuais e recomendações de especialistas em tempo real diretamente da base de

	conhecimento verificada da Cisco, permitindo que você resolva problemas sem a necessidade de abrir um caso de suporte.
--	--

¹ Suporta conexão de telemetria e dispositivo através do Cisco IQ Link, Catalyst Center, Intersight, Meraki, SD-WAN Manager e WebEx Control Hub.

Recursos padrão

O nível de suporte padrão aumenta a eficiência operacional, fornecendo triagem centralizada para problemas em nível de solução e um proprietário de caso dedicado que se coordena com os especialistas técnicos necessários. Você pode reduzir os riscos de forma proativa usando insights baseados em IA que correlacionam dados de ativos com a importância dos negócios, oferecendo visibilidade clara de suas avaliações de inventário, segurança e configuração. Além disso, você pode alinhar a experiência da sua equipe com as necessidades específicas da sua empresa por meio de planos de aprendizado personalizados disponíveis na [Cisco U](#).

A tabela a seguir descreve os recursos disponíveis para a camada de suporte Padrão.

Capacidade	Descrição
Informações sobre EOL ¹	Os insights de EOL fornecem consulta, resumo, visualização e relatórios inteligentes de marcos de EOL para permitir a priorização personalizada do ciclo de vida e o planejamento de atualização de tecnologia.
Informações sobre a cobertura do serviço ¹	Os insights de cobertura de serviços fornecem uma visualização e análise dos detalhes da cobertura de serviços e marcos de renovação, permitindo a priorização personalizada das atualizações de cobertura e do planejamento de renovação.
Marcação de ativos	A marcação de ativos oferece uma maneira de organizar o inventário de acordo com as necessidades da empresa usando etiquetas de ativos, permitindo a organização flexível de ativos de hardware e software por departamento, local ou projeto como pares de valor-chave.
Informações sobre LDOS ¹	Os insights LDOS fornecem uma visualização e análise de ativos além ou próximos de suas metas de LDOS, permitindo priorização personalizada do ciclo de vida e planejamento de atualização de tecnologia.
Informações sobre a	Os Asset Criticality Insights permitem a avaliação e identificação das

importância dos ativos ¹	funções dos ativos e sua importância relativa na rede para priorizar os esforços de mitigação de riscos e aumentar a resiliência operacional.
Percepções da Consultoria de Segurança ¹	Os Security Advisory Insights fornecem consultas, resumos, visualizações e relatórios inteligentes de ativos afetados pelos Security Advisories, permitindo a priorização personalizada de resposta a riscos e incidentes de segurança.
Segurança fortalecendo insights ¹	O Security Hardening Insights fornece uma solução automatizada que avalia as configurações do dispositivo, identifica falhas de fortalecimento de segurança com base na gravidade do impacto e na criticidade e fornece informações de nível executivo para acelerar a implementação de medidas de fortalecimento críticas. Ele aumenta a resiliência da empresa e reduz a superfície de ataque contra ameaças em evolução, ao mesmo tempo em que permite a priorização personalizada de uma postura de segurança aprimorada por meio de consultas, resumos, visualizações e relatórios inteligentes de ativos em risco.
Informações de notificação de campo ¹	Os insights de campo fornecem consulta inteligente, resumo, visualização e relatórios de ativos afetados pelos avisos de campo, permitindo priorização personalizada de risco e resposta a problemas conhecidos.
Informações de configuração ¹	O Configuration Insights fornece uma solução automatizada que avalia as configurações de dispositivos em relação às práticas recomendadas da Cisco com base em experiência comprovada em campo. Consultas, resumos, visualizações e relatórios inteligentes dos ativos afetados permitem a priorização personalizada e aceleram a correção de falhas críticas de configuração, melhorando a resiliência da infraestrutura e reduzindo o risco operacional na rede.
Informações do caso ¹	Os insights de casos fornecem consultas, resumos, visualizações e relatórios inteligentes sobre casos do Cisco TAC, permitindo o monitoramento personalizado da eficiência operacional.

¹ Suporta conexão de telemetria e dispositivo através do Cisco IQ Link, Catalyst Center, Intersight, Meraki, SD-WAN Manager e WebEx Control Hub.

Recursos de assinatura

O nível de suporte de assinatura baseia-se no nível de suporte padrão para elevar seu desempenho operacional por meio de Contratos de nível de serviço de restauração definidos e

acesso a uma equipe dedicada de especialistas familiarizados com seu ambiente exclusivo. Esse nível se concentra em evitar interrupções antes que elas afetem suas operações, fornecendo proteção proativa de segurança, eliminação sistemática de causas básicas e análise contínua orientada por especialistas de seus ativos. Além disso, você pode utilizar o [treinamento de certificação Cisco U](#) avançado e laboratórios de prática virtual para desenvolver proficiência técnica profunda.


A tabela a seguir descreve os recursos disponíveis para a camada de suporte de Assinatura.

Capacidade	Descrição
Recomendação de configuração ¹	A Recomendação de configuração fornece recomendações acionáveis para lidar com possíveis erros de configuração e inconsistências.
Recomendações para fortalecer a segurança ¹	As Recomendações de Fortalecimento de Segurança fornecem uma solução automatizada que fornece recomendações genéricas específicas para cada verificação de fortalecimento com falha, tratando os problemas de segurança subjacentes de forma clara e concisa.

¹ Suporta conexão de telemetria e dispositivo através do Cisco IQ Link, Catalyst Center, Intersight, Meraki, SD-WAN Manager e WebEx Control Hub.

Comece a jornada dos administradores


Ao fazer login em sua conta recém-criada ou migrada do Cisco IQ pela primeira vez, a página Welcome exibe uma jornada Get Started. A jornada do Guia de introdução difere dependendo se a conta foi criada com ou sem dados migrados.

 Note: A experiência de jornada do Guia de introdução varia de acordo com as permissões de RBAC (Role-Based Access Control, controle de acesso baseado em função).

Nova conta via criação

A jornada do Get Started para contas recém-criadas orienta você pelas etapas iniciais de integração necessárias para configurar seu ambiente Cisco IQ e explorar o Cisco IQ.


Conexão de produtos de nuvem da Cisco

 Note: Você deve conectar pelo menos um (1) produto de nuvem para que esta etapa seja concluída.

Conectar os dados de seus produtos em nuvem da Cisco ao Cisco IQ é a maneira mais rápida de começar a usar seus recursos avançados e personalizados. Você pode receber insights personalizados em minutos após configurar suas conexões de dados.

Para conectar seus produtos de nuvem da Cisco, consulte [Conectores de Dados](#).


Vinculando contratos de serviço

 Note: Você deve vincular pelo menos um (1) contrato de serviço para que esta etapa seja concluída.

A vinculação de contratos une dados de contratos associados a diferentes membros da equipe e incorpora ativos não conectados ao seu inventário por telemetria, permitindo visibilidade centralizada da cobertura de suporte e evitando surpresas na renovação.

Para vincular seus contratos de serviço, consulte [Contratos de serviço](#).


Conexão de dispositivos no local

 Note: Você deve registrar pelo menos um (1) Cisco IQ Link para que esta etapa seja concluída.

Para estabelecer comunicação com seus dispositivos locais, você deve configurar o Cisco IQ Link. O Cisco IQ Link traz todo o poder do Cisco IQ para seus dispositivos locais que ainda não são gerenciados por uma plataforma de nuvem da Cisco. O Cisco IQ Link pode ser instalado como uma máquina virtual (VM) em seu data center e vinculado à sua conta Cisco IQ.

Para conectar seus dispositivos locais, consulte [Conectores de Dados](#).

Gerenciando o acesso do usuário

 Note: Você deve adicionar pelo menos dois (2) usuários para que esta etapa seja concluída.

Os recursos de controle de acesso simples do Cisco IQ são projetados para equipes pequenas e grandes empresas. Você pode adicionar usuários e atribuir funções de administrador ou somente

exibição a grupos e indivíduos.

Para adicionar usuários e atribuir permissões, consulte [Usuários](#).

Explorando o Cisco IQ

Explore os recursos e aplicativos do Cisco IQ disponíveis para você, incluindo:

- Barra Inicial: Acesse aplicativos, descubra novos recursos e crie painéis
- Aplicativo de ativos: Consulte [Aplicativo de ativos](#) para obter mais detalhes
- Aplicativo de avaliações: Consulte [Assessment Application](#) para obter mais detalhes
- Aplicativo de suporte: Consulte [Aplicativo de Suporte](#) para obter mais detalhes
- Assistente Cisco IQ AI: Consulte [AI Assistant](#) para obter mais detalhes
- Configurações do sistema: Gerencie as configurações da sua conta, conceda acesso aos usuários, configure conexões de dados e exiba atividades e logs da sua conta; consulte [Configurações do sistema](#) para obter mais detalhes

Nova conta via migração

Se sua nova conta do Cisco IQ foi criada por meio de migração, as informações de sua conta anterior já estarão disponíveis. Como resultado, a jornada de Introdução às contas recém-migradas limita-se à análise da migração, detalhada abaixo.

Revisão da migração

Para revisar a migração:

- Verifique se seus contratos migraram com êxito em Home > Configurações do sistema > Contratos de serviço
- Valide se todas as conexões de dados necessárias estão configuradas corretamente em Home > Configurações do Sistema > Conectores de Dados
- Verifique os dados do usuário migrados com êxito e conceda acesso aos usuários migrados ativando suas contas em Início > Configurações do sistema > Identidade e acesso > Usuários
- Verifique se seus ativos migraram com êxito em Home > Ativos > Inventário

Comece a jornada dos usuários em geral

Ao fazer login em sua conta do Cisco IQ pela primeira vez, a página Welcome exibe uma jornada Get Started. Essa jornada o guia pelos recursos do Cisco IQ e fluxos de trabalho comuns.

 Note: A experiência de jornada do Início varia com base nas permissões de RBAC.

Explorando o Cisco IQ

Explore os recursos e aplicativos do Cisco IQ disponíveis para você, incluindo:

- Barra Inicial: Acesse aplicativos, descubra novos recursos e crie painéis
- Aplicativo de ativos: Consulte [Aplicativo de ativos](#) para obter mais detalhes
- Aplicativo de avaliações: Consulte [Assessment Application](#) para obter mais detalhes
- Aplicativo de suporte: Consulte [Aplicativo de Suporte](#) para obter mais detalhes
- Assistente Cisco IQ AI: Consulte [AI Assistant](#) para obter mais detalhes

Gerando seu primeiro relatório de IA

O recurso de análise habilitado por IA do Cisco IQ gera relatórios direcionados e personalizáveis com base em ativos selecionados que podem ser adaptados às suas necessidades de negócios específicas.

Consulte [Aplicação de ativos](#) para obter mais informações sobre como gerar seu primeiro relatório do AI.

Como fazer uma pergunta ao Cisco IQ AI Assistant

A etapa final da sua jornada de Introdução é iniciar o Cisco IQ AI Assistant de qualquer lugar e fazer uma pergunta sobre seus ativos, casos ou avaliações.

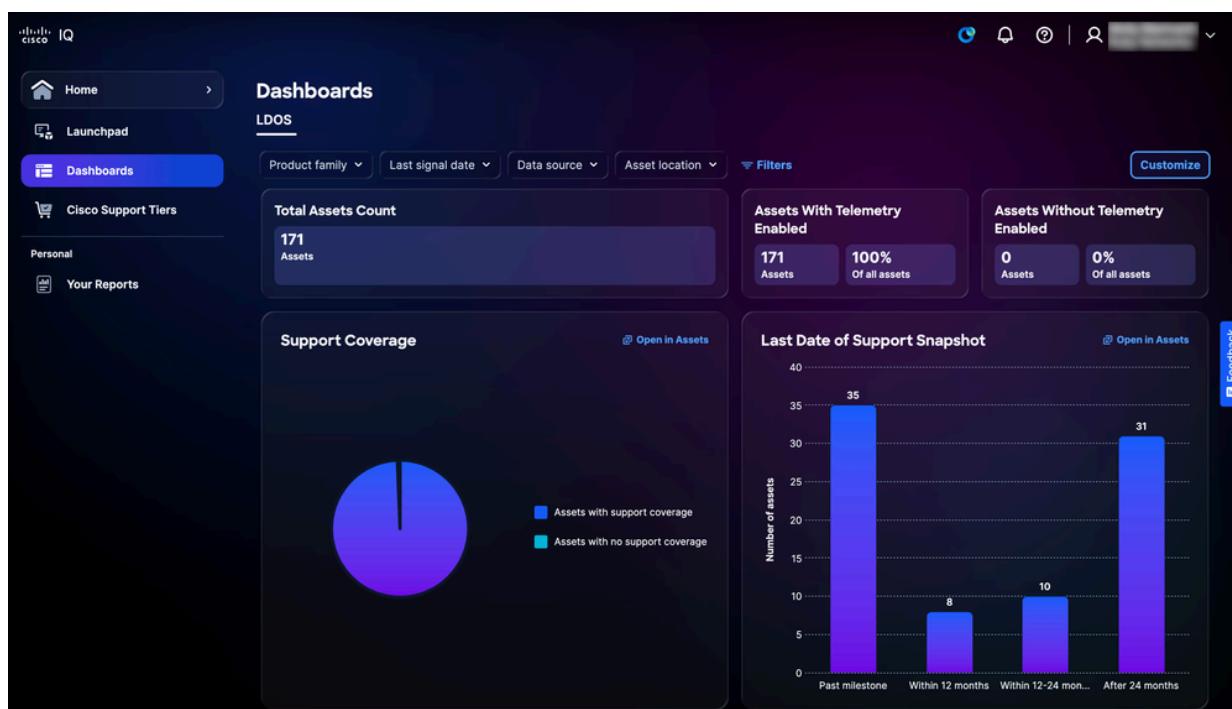
Consulte [AI Assistant](#) para obter mais informações sobre como usar o Cisco IQ AI Assistant.

Painéis

A guia Painéis fornece uma visualização dos seguintes painéis disponíveis no Cisco IQ.

Painel LDOS

O painel do LDOS fornece informações abrangentes e detalhadas sobre as métricas do LDOS, permitindo a visibilidade do cliente, capacitando os usuários para gerenciar riscos de forma proativa e oferecendo suporte à tomada de decisões mais eficiente e informada.



Painel LDOS

Filtrando exibições para o painel do LDOS

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

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

 Note: Há filtros diferentes disponíveis, dependendo das funções e permissões do usuário.

Exibição de Detalhes do Painel do LDOS

Ao clicar em Abrir em ativos, a página redireciona para a página [Inventário](#). Consulte [Inventário](#)

para obter mais detalhes.

Níveis de suporte da Cisco

A página Camadas de suporte da Cisco fornece uma visão geral de quais recursos estão disponíveis para a camada de suporte adquirida e o número de ativos relacionados a contratos de suporte vinculados, permitindo que você compreenda facilmente os recursos de suporte incluídos e tome medidas para gerenciá-los e analisá-los. Consulte [Camadas de suporte](#) para obter informações mais detalhadas sobre os recursos da camada de suporte.

Cisco Support tier	Basic 0 assets	Standard 0 assets	Signature 0 assets
Assets			AI-powered feature
Asset inventory	✓	✓	✓
End of Life	✓	✓	✓
Service coverage	✓	✓	✓
Last Date Of Support dashboard	✓	✓	✓
End-of-Life insights		✓	✓
Service coverage insights		✓	✓
Last Date Of Support insights		✓	✓
Asset criticality insights		✓	✓
Asset tagging		✓	✓

Níveis de suporte da Cisco

Seus relatórios

O recurso Relatórios permite que você centralize e gerencie insights gerados por IA no Cisco IQ, salvando-os em uma lista personalizada de Seus Relatórios, garantindo que você tenha acesso rápido e seguro aos seus próprios dados.

Report Name	Description	Created	Created from	
> Past-LDOS Assets Ove...	Summary of 52 assets past Last Date of Support,...	Apr 20, 2026, 4:...	Assets (AI Assistant)	...
> Security Advisory Expo...	Overview of security advisories sorted by affecte...	Apr 20, 2026, 3:...	Assessments	...
> Security Advisory Expo...	Overview of security advisories sorted by affecte...	Apr 20, 2026, 3:...	Assessments	...
> Asset Inventory Risk O...	Critical coverage gaps, lifecycle deadlines, and te...	Apr 20, 2026, 3:...	Assets	...

Seus relatórios

Configurações do sistema

Para navegar até o menu Configurações do sistema, escolha Início > Configurações do sistema. A página Detalhes da conta é exibida.

 Note: As configurações do sistema estão disponíveis apenas para administradores de conta.

Detalhes da conta


O recurso Configurações do sistema facilita o gerenciamento, o controle de acesso e a alocação de dados, garantindo visibilidade e acesso abrangentes para administradores de conta. Ao exibir a página Detalhes da Conta, a seção Detalhes exibe as seguintes informações:

- Nome da conta
- Tipo de conta
- Região de armazenamento de dados
- Usuários
- Data de criação

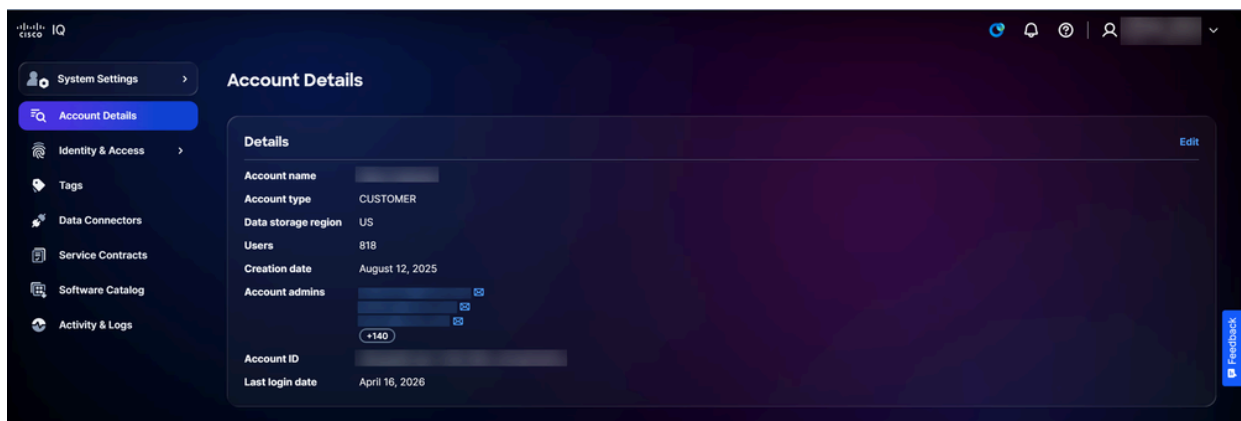
- Administradores de conta
- ID da conta
- Data do último logon

Edição do nome da conta

Somente o nome da conta pode ser alterado na página Detalhes da conta.

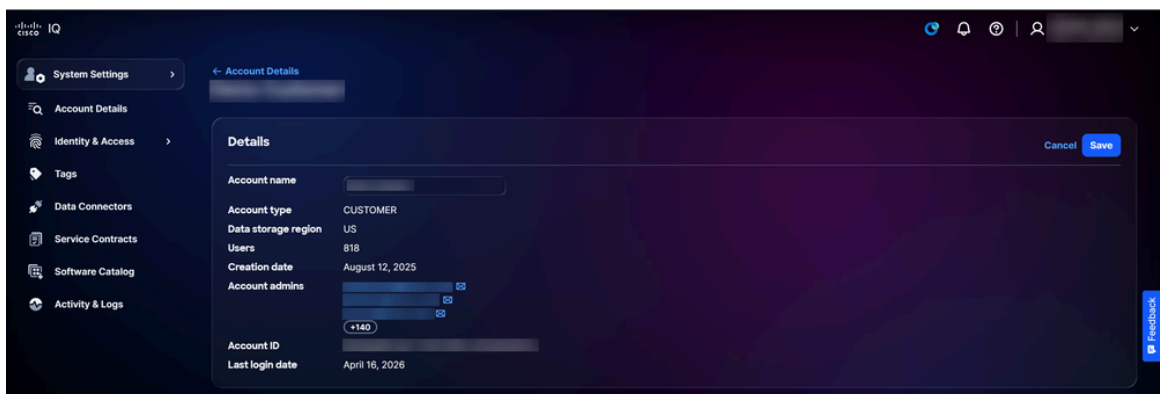
 Note: Para alterar campos, como Região de armazenamento de dados, uma nova conta da empresa deve ser criada.

Para editar um nome de conta:



Detalhes da conta

1. Clique em Editar.



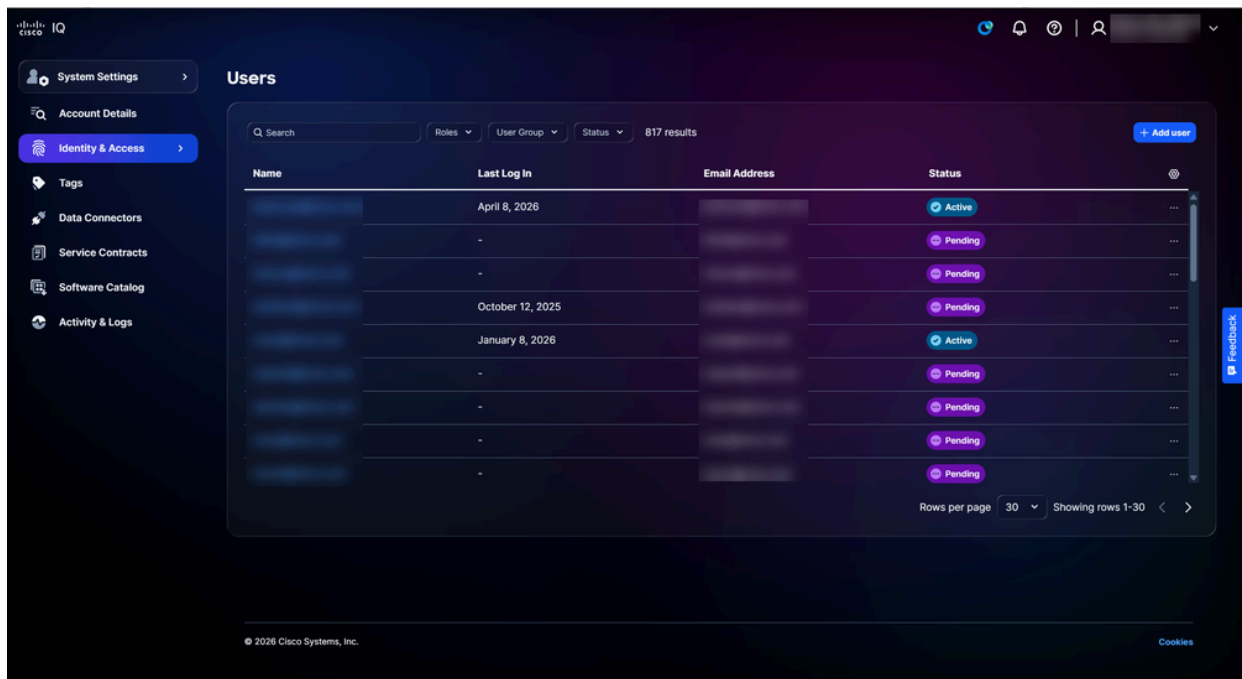
Editar nome da conta

2. Revise o nome da conta.

3. Click Save.

Usuários

As contas de usuário são criadas, modificadas e excluídas na página Usuários. Para navegar até a página Usuários, escolha Configurações do sistema > Identidade e acesso > Usuários. A página Usuários é exibida.




Usuários

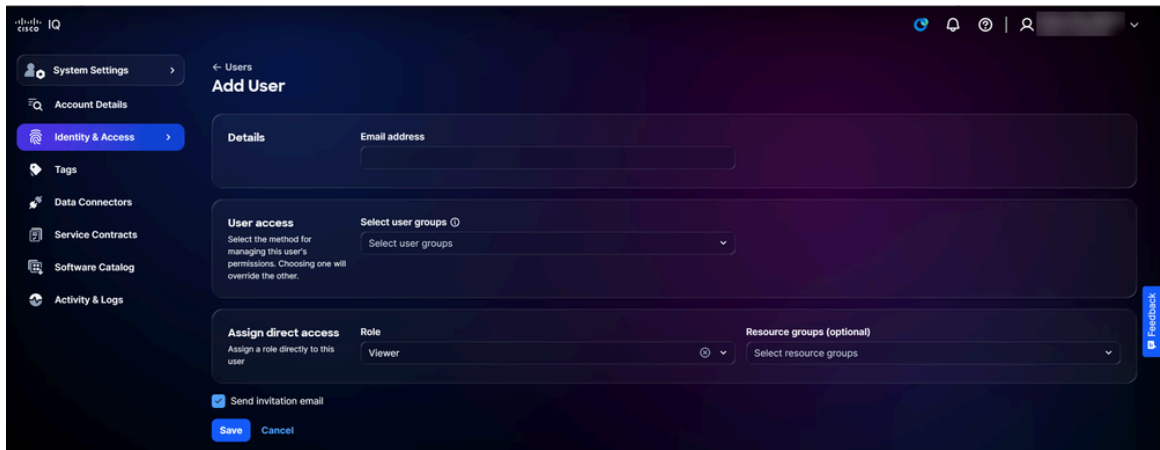
Você pode Pesquisar e Filtrar para restringir a lista usando os campos na parte superior da página.

Adicionando novos usuários

Para adicionar um novo usuário:


 Note: Somente administradores de conta ou outros usuários autorizados podem adicionar novos usuários.

1. Na página Users, clique em Add User. A página Adicionar usuário é exibida.




Adicionar usuário

2. Insira um endereço de e-mail.
3. Opcionalmente, escolha o(s) grupo(s) de usuários na lista suspensa Seleccionar grupos de usuários.
4. Escolha a Função na lista suspensa.

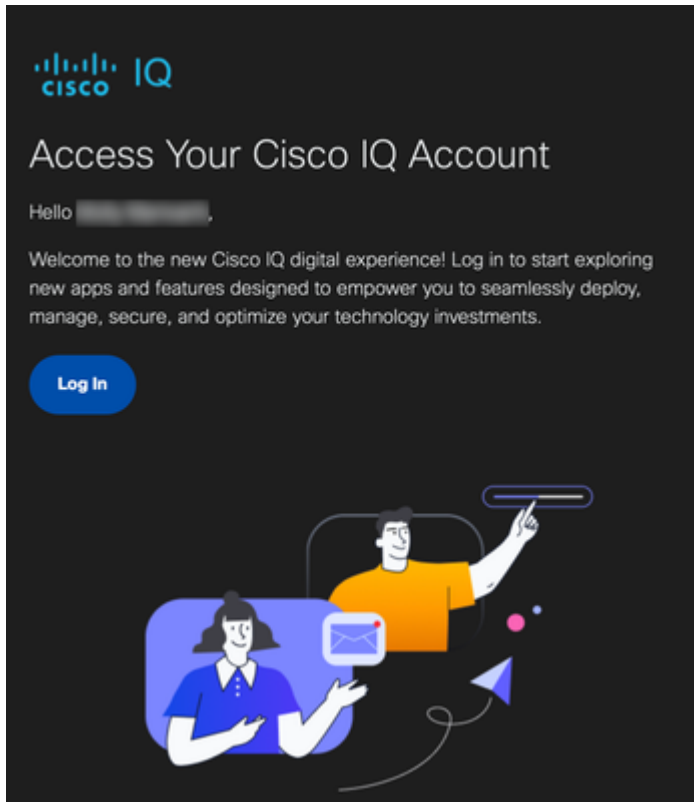
 Note: Os usuários devem pertencer a pelo menos um grupo de usuários com uma função ou receber pelo menos uma função.

5. Opcionalmente, escolha os Grupos de recursos na lista suspensa.

 Note: A lista suspensa Grupos de recursos só é exibida para funções selecionadas.

6. Confirme se a caixa de seleção Enviar e-mail de convite está marcada.
7. Click Save. Uma confirmação é exibida na página Usuários.

Os usuários recebem um e-mail depois de serem convidados por um administrador da conta.

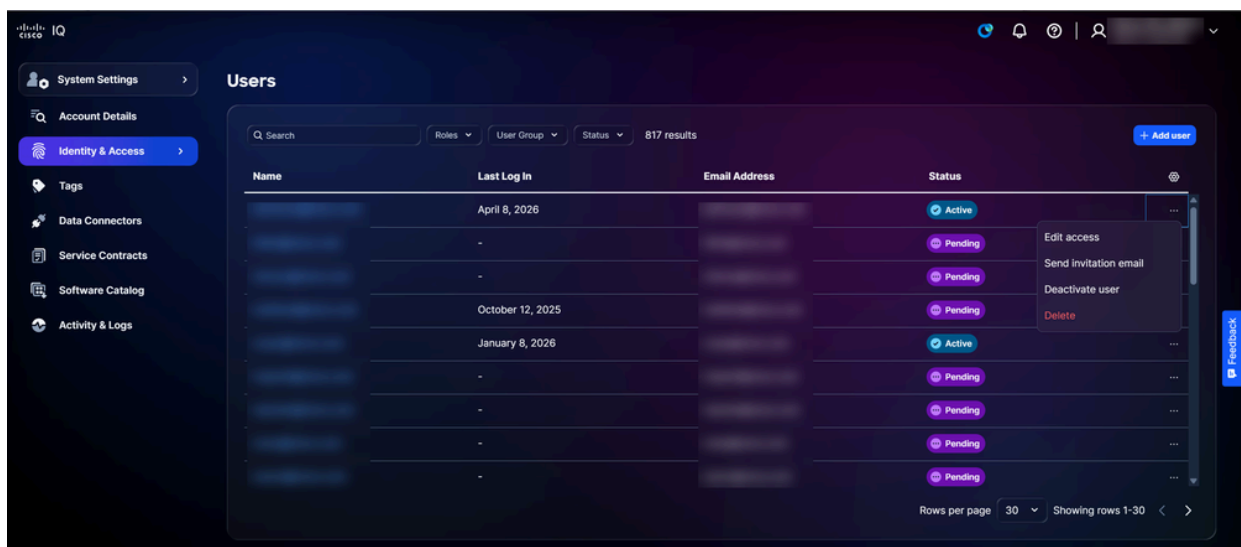


Convite por e-mail

Os usuários convidados podem clicar em Logon no e-mail para fazer login em suas contas. Após fazer login, o status do usuário se torna Ativo.

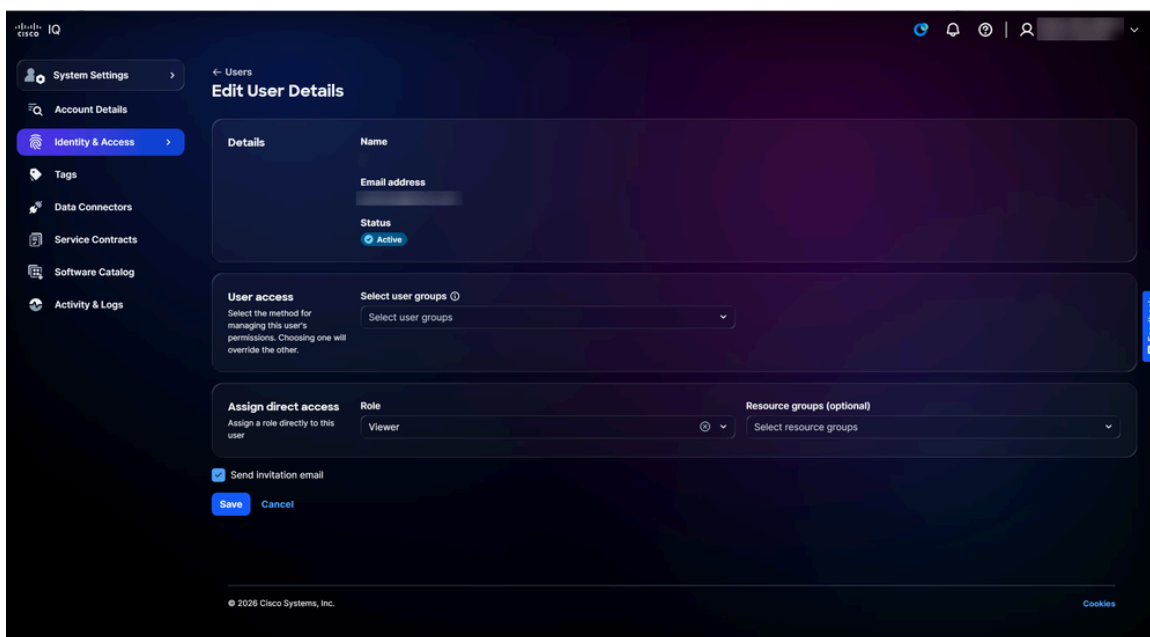
Editando o acesso do usuário

Para editar os grupos de usuários, funções ou grupos de recursos de uma conta de usuário:



Editar acesso

1. A partir de um usuário desejado na página Usuários, escolha o ícone Mais Opções > Editar acesso. A página Editar detalhes do usuário é exibida.



Editar detalhes do usuário

2. Edite os grupos de usuários, funções e grupos de recursos desejados.



Note: Os grupos de recursos só são exibidos para funções selecionadas.

3. Click Save.

Enviando emails de convite

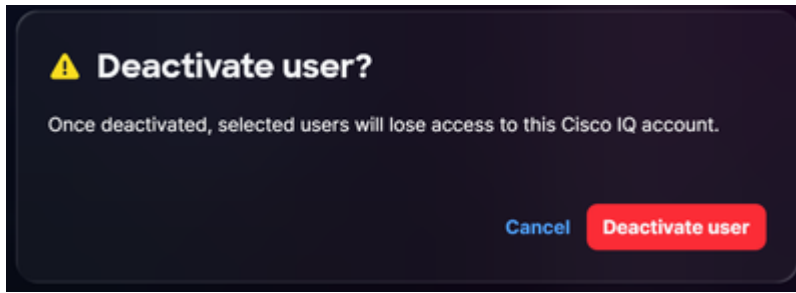
Para enviar um e-mail de convite para uma conta de usuário existente:

1. Navegue até a página Usuários.
2. De um usuário desejado, escolha o ícone Mais Opções > Enviar convite por e-mail. Uma confirmação é exibida.

Desativando usuários

Para desativar uma conta de usuário:

1. A partir de um usuário desejado na página Usuários, escolha o ícone Mais Opções > Desativar usuário. A janela Desativar usuário é aberta.



Desativar confirmação do usuário

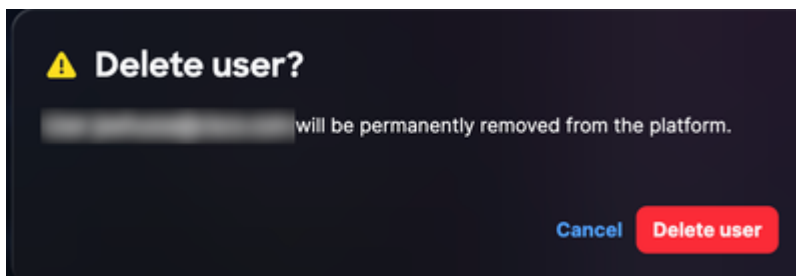
2. Clique em Desativar usuário para confirmar. Uma confirmação é exibida.

Excluindo usuários

 aviso: Não é possível reverter a exclusão de usuários.

Para excluir um usuário:

1. A partir de um usuário desejado na página Usuários, escolha o ícone Mais Opções > Excluir. A janela Excluir usuário é aberta.



Excluir confirmação do usuário

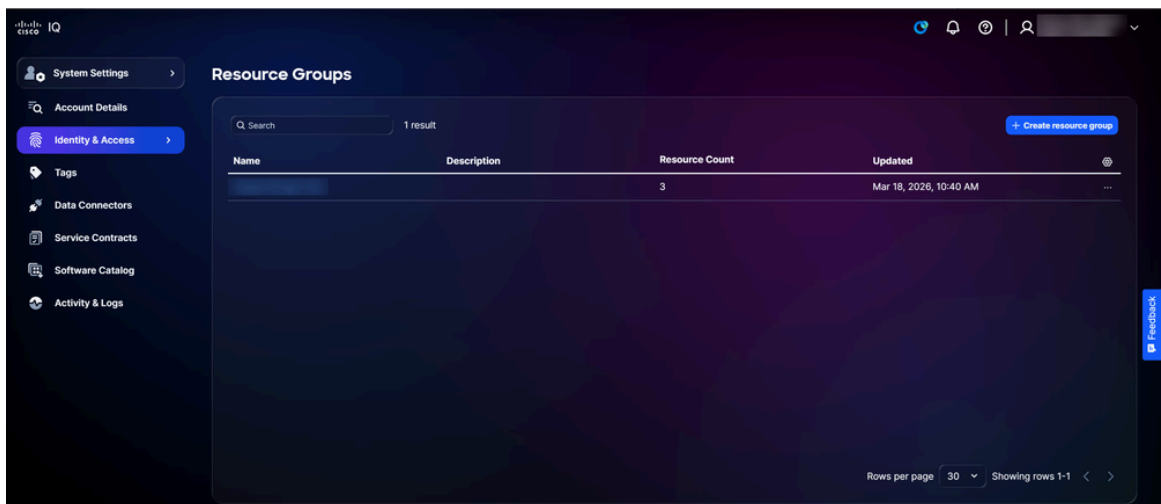
2. Clique em Excluir usuário. O usuário é excluído.

Grupos de recursos

Grupos de recursos são coleções dinâmicas que especificam recursos com base em seu tipo e atributos. A configuração de grupos de recursos permite restringir o acesso a dados de uma função aos recursos que atendem às condições do grupo. Os recursos podem pertencer a vários grupos de recursos. Como um administrador de conta, você pode criar, editar e excluir grupos de recursos.

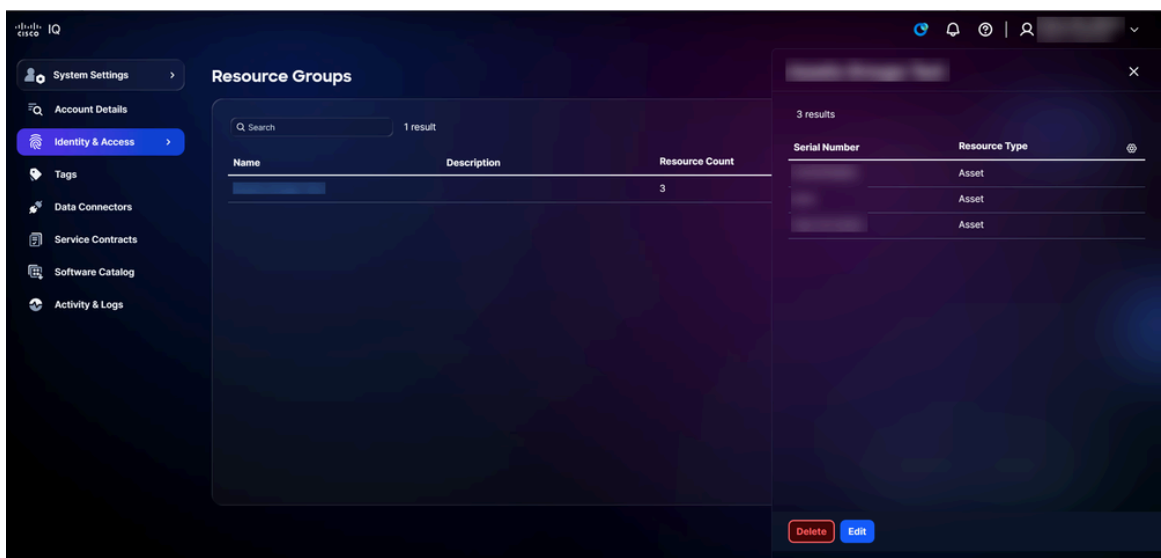
Para exibir grupos de recursos:

1. Escolha Configurações do sistema > Identidade e acesso > Grupos de recursos. A página Grupos de recursos é exibida.



Grupos de recursos

2. Use os campos Pesquisar e Filtro para restringir a lista.
3. Clique no nome de um grupo de recursos para exibir seus detalhes.

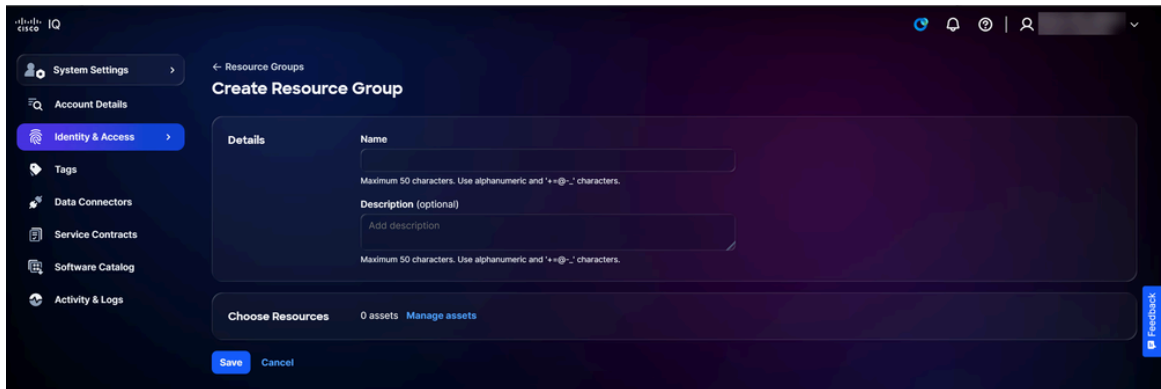


Detalhes do Grupo de Recursos

Criando Grupos de Recursos

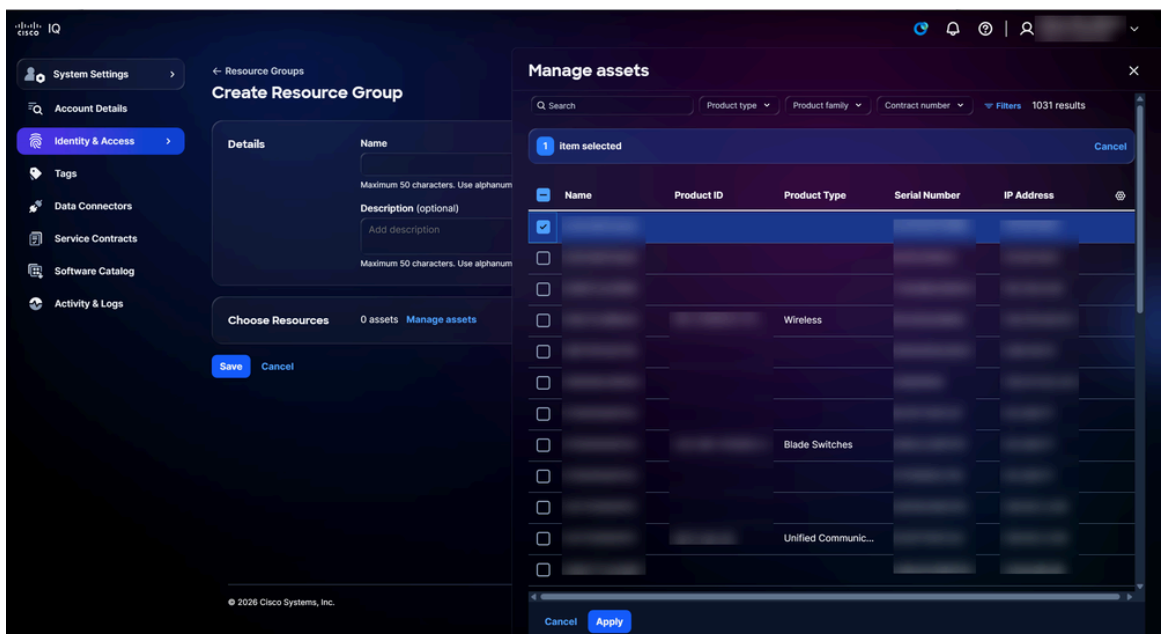
Para criar um novo grupo de recursos:

1. Na página Grupos de Recursos, clique em Criar grupo de recursos. A página Criar Grupo de Recursos é exibida.



Criar grupo de recursos

2. Insira um Nome para o grupo de recursos
3. Opcionalmente, informe uma Descrição.
4. Clique em Gerenciar ativos. A janela Gerenciar ativos é aberta.

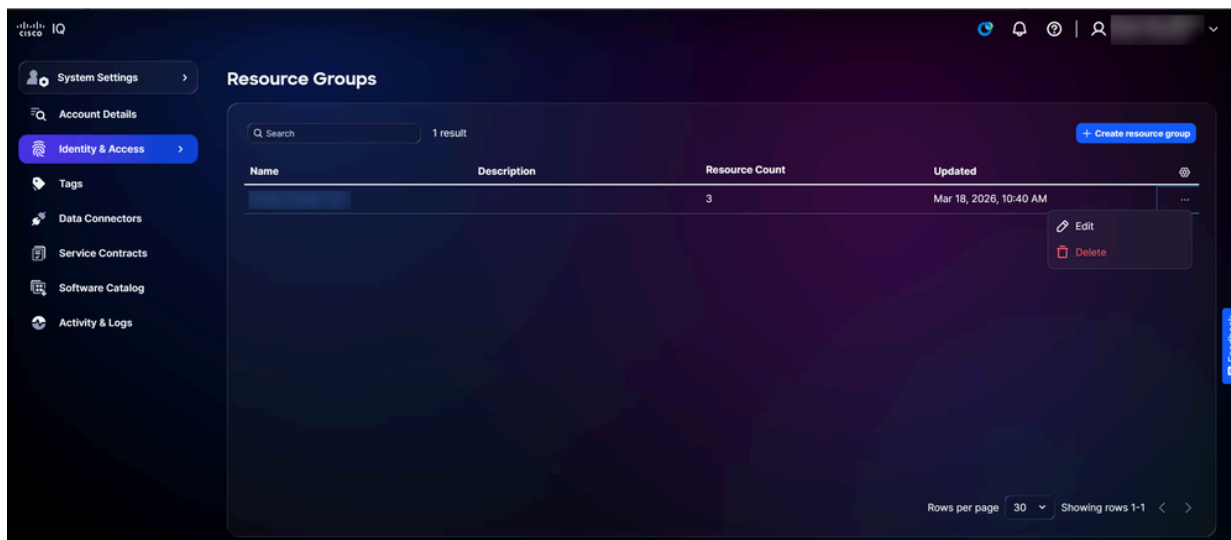


Gerenciar ativos

5. Marque a caixa de seleção dos ativos desejados.
6. Clique em Apply.
7. Click Save.

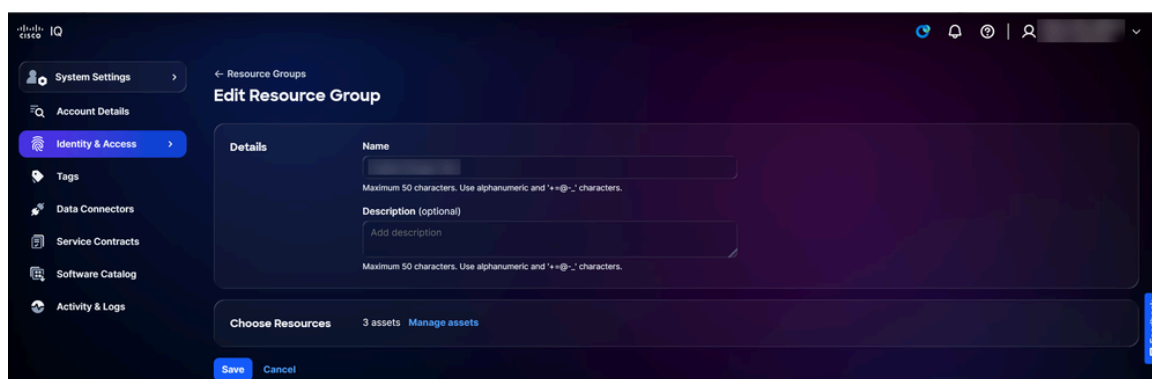
Editando Grupos de Recursos

Para editar um grupo de recursos:



Editar

1. Em um registro na página Grupos de Recursos, escolha o ícone Mais Opções > Editar. A página Editar Grupo de Recursos é exibida.



Editar grupo de recursos

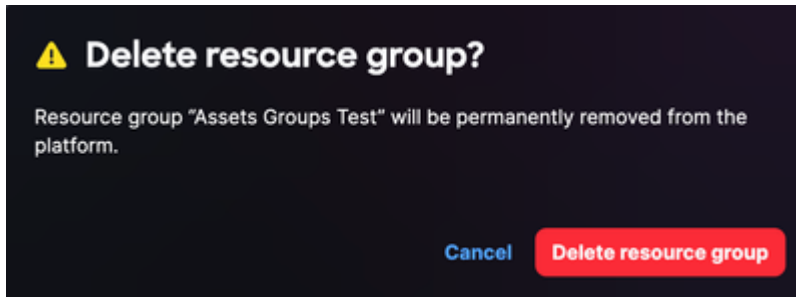
2. Edite os atributos do grupo de recursos, conforme desejado.
3. Click Save.

Excluindo Grupos de Recursos

 aviso: A exclusão de grupos de recursos não pode ser revertida.

Para excluir um grupo de recursos:

1. Em um registro na página Grupos de Recursos, escolha o ícone Mais Opções > Excluir. A janela Excluir grupo de recursos é aberta.




Excluir grupo de recursos

2. Clique em Excluir grupo de recursos. O grupo de recursos foi excluído.

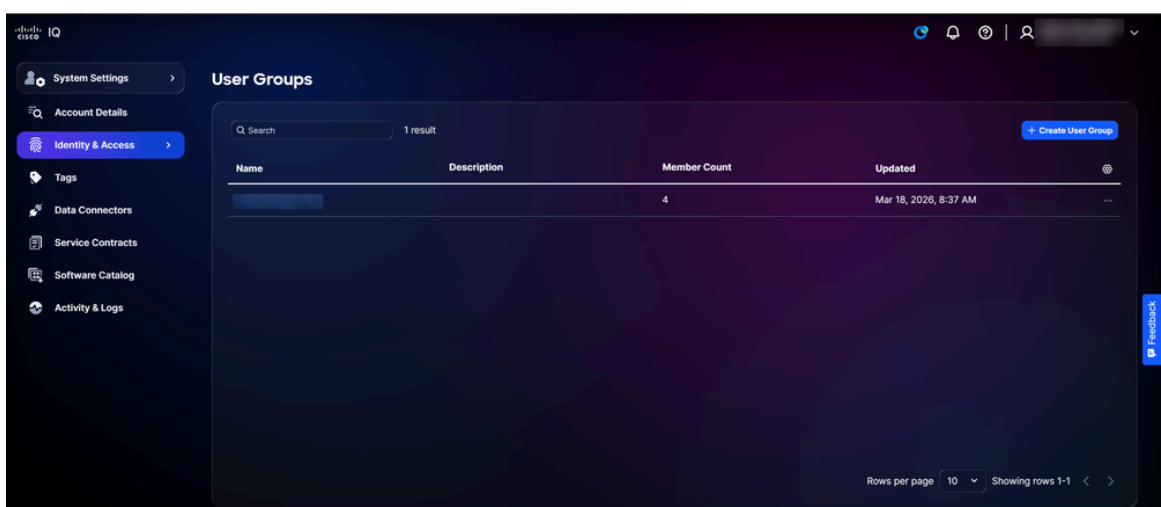
Grupos de usuários

Os grupos de usuários permitem que você controle os usuários efetivamente em toda a conta criando, editando e excluindo grupos de usuários.

 **Note:** O grupo de usuários Todos os usuários da conta existe por padrão em todas as contas no Cisco IQ e não pode ser excluído ou editado. Ele sempre inclui todos os usuários da conta de qualquer tipo específico. Sua finalidade é aplicar funções a todos os usuários na conta.

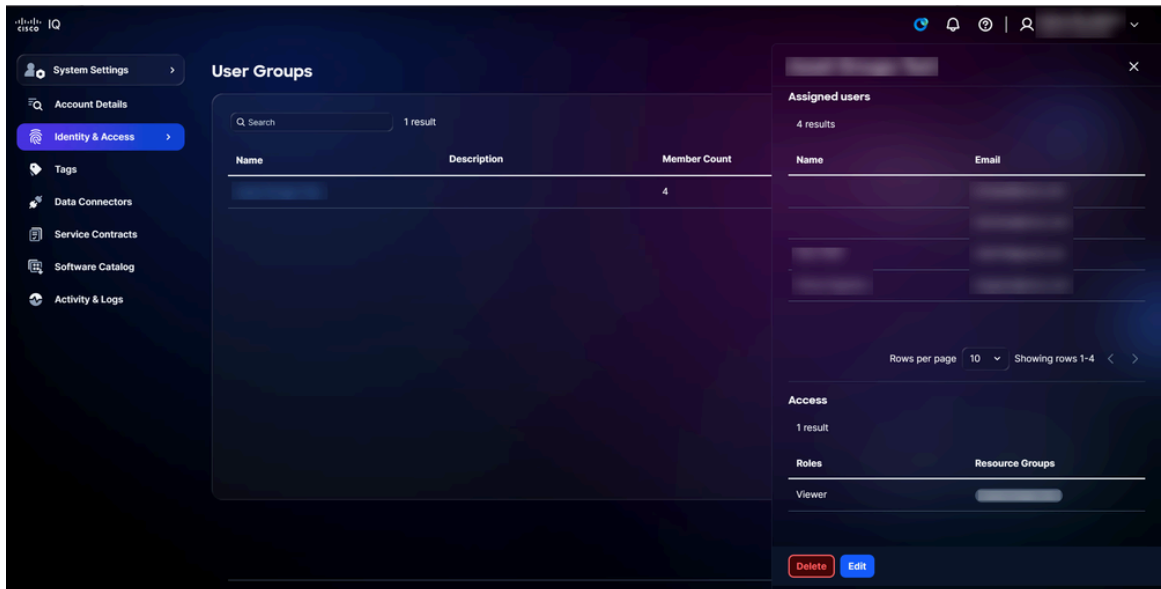
Para exibir grupos de usuários:

1. Escolha Configurações do sistema > Identidade e acesso > Grupos de usuários. A página Grupos de usuários é exibida.



Grupos de usuários

2. Use os campos Pesquisar e Filtro para restringir a lista.
3. Clique em um nome de grupo de usuários para exibir seus detalhes.

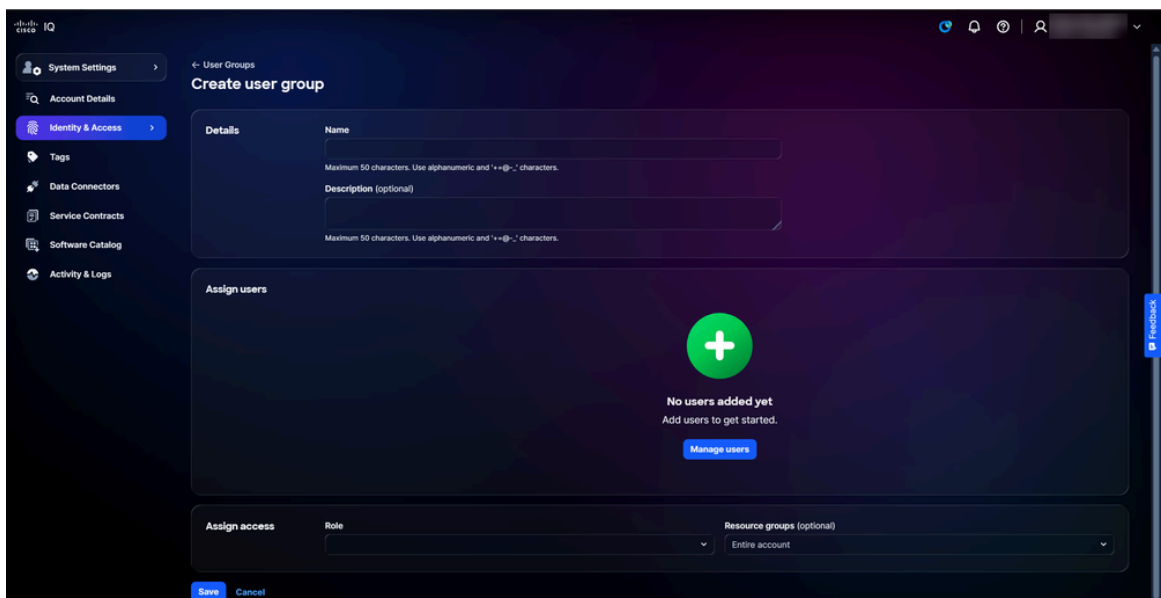


Detalhes do Grupo de Usuários

Criando grupos de usuários

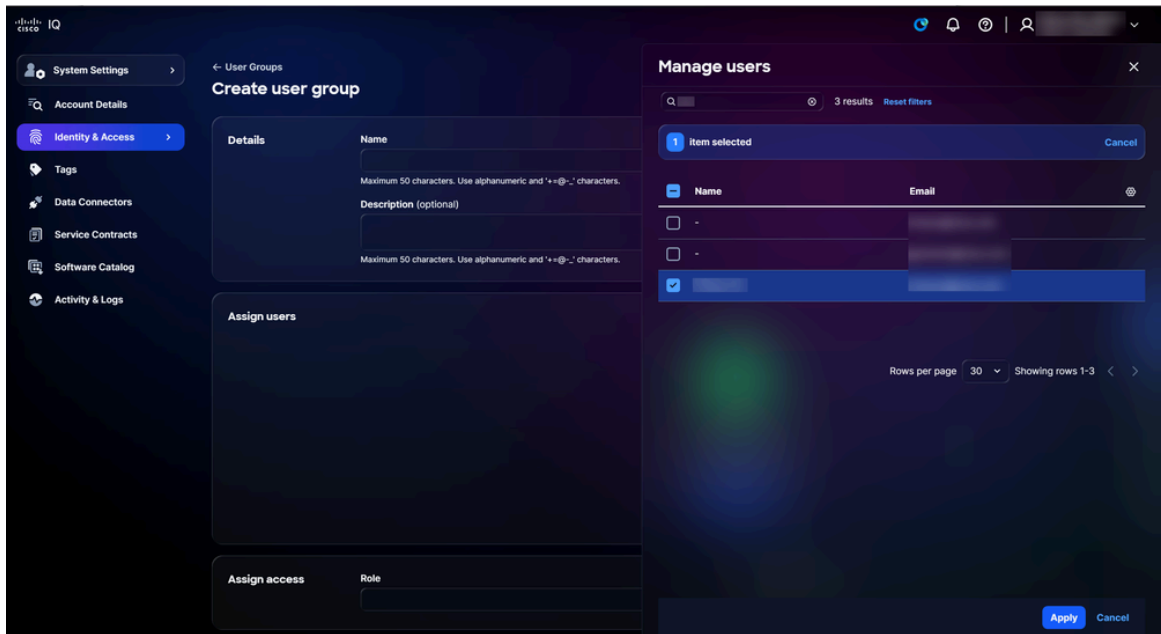
Para criar um novo grupo de usuários:

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




Criar grupo de usuários

2. Insira um Nome para o grupo de usuários.
3. Opcionalmente, informe uma Descrição.
4. Clique em Gerenciar usuários. A janela Gerenciar usuários é aberta.



Gerenciar usuários

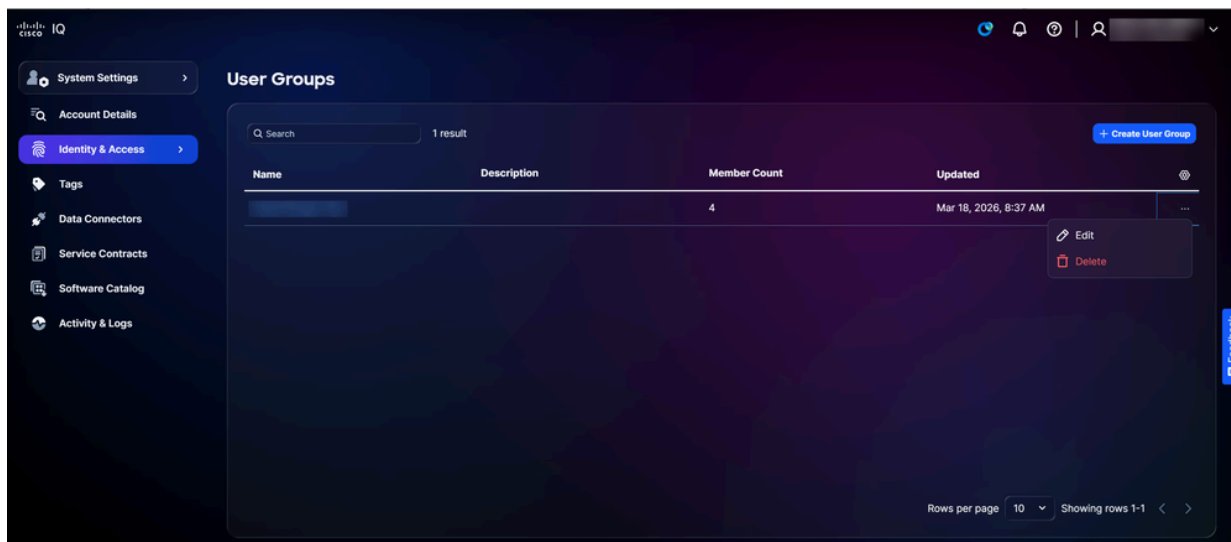
5. Marque as caixas de seleção dos usuários desejados.
6. Clique em Apply.
7. Escolha uma Função na lista suspensa.
8. Opcionalmente, escolha um Grupo de recursos na lista suspensa.

 **Note:** Adicionar grupos de recursos limita os recursos aos quais o grupo de usuários tem acesso. Se uma função for atribuída, mas nenhum grupo de recursos for selecionado, a função será aplicada a todos os recursos relevantes à função na conta.

9. Click Save. O novo grupo de usuários é exibido na tabela Grupos de usuários.

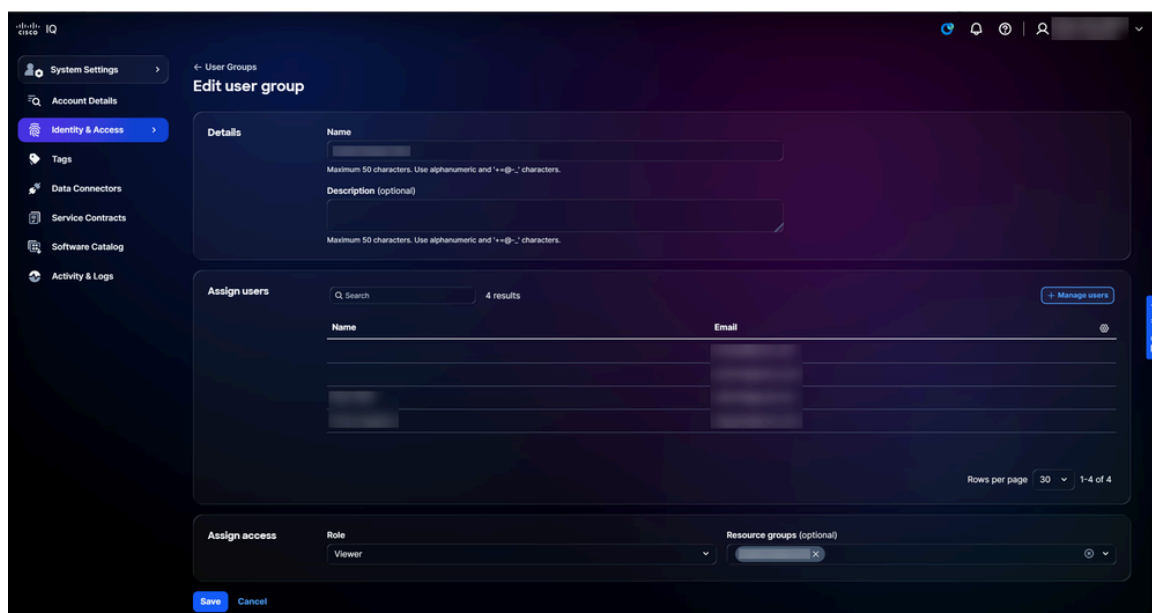
Editando grupos de usuários

Para editar um grupo de usuários:



Editar


1. Em um registro na página Grupos de usuários, escolha o ícone Mais opções > Editar. A página Editar grupo de usuários é exibida.



Editar grupo de usuários

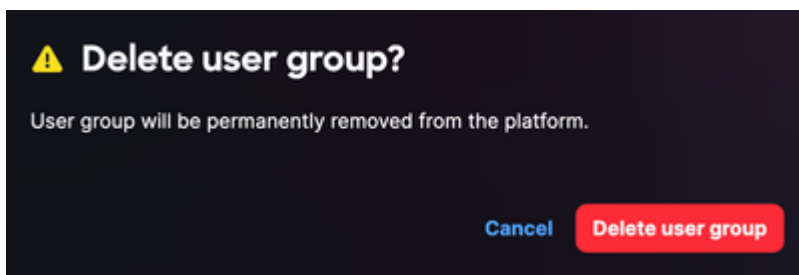
2. Edite os atributos do grupo de usuários conforme desejado.
3. Click Save.

Excluindo grupos de usuários

 aviso: Não é possível reverter a exclusão de grupos de usuários.

Para excluir um grupo de usuários:

1. Em um registro na página Grupos de usuários, escolha o ícone Mais opções > Excluir. A janela Excluir grupo de usuários é aberta.



Excluir grupo de usuários

2. Clique em Excluir grupos de usuários. O grupo de usuários é excluído.

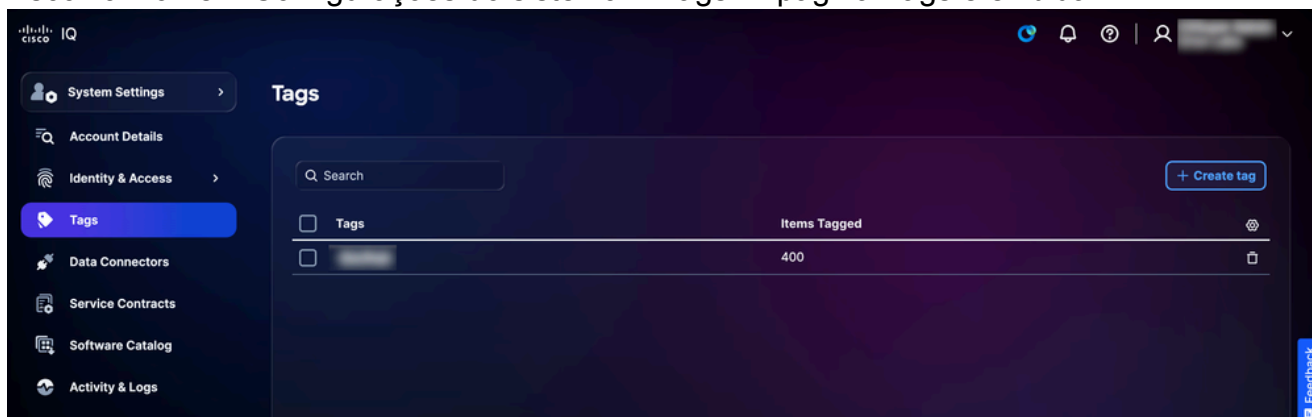
Tags

As etiquetas de inventário são etiquetas personalizadas que você atribui aos ativos de inventário no Cisco IQ. Uma marca é um par `key:value`—por exemplo, `Environment:Prod` ou `Label:Campus`—que você define. Os administradores de contas podem criar e excluir marcas e atribuir usuários a um grupo de recursos, permitindo que eles atribuam marcas de ativos a um dispositivo. Consulte [Grupos de recursos](#) para obter mais informações sobre a atribuição de usuários a um grupo de recursos.

Criando etiquetas de ativo

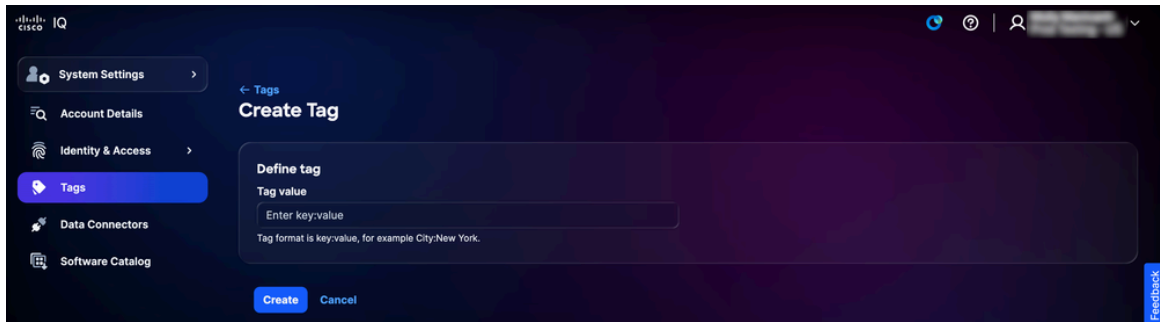
Para criar uma tag:

1. Escolha Home > Configurações do sistema > Tags. A página Tags é exibida.



Tags

2. Clique em Criar tag. A página Criar tag é exibida.



Criar Marca

3. Insira o valor da marca no campo Enter key:value.

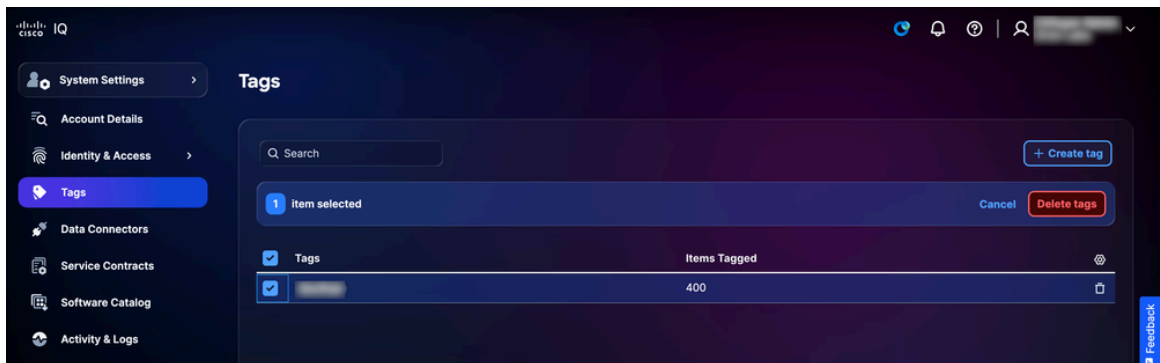
 Note: Os nomes de tag estão no formato key:value (por exemplo, City:NYC).

4. Clique em Criar. A nova marca é exibida na lista de marcas na página Marcas.

Exclusão de marcas de ativo

Para excluir uma marca:

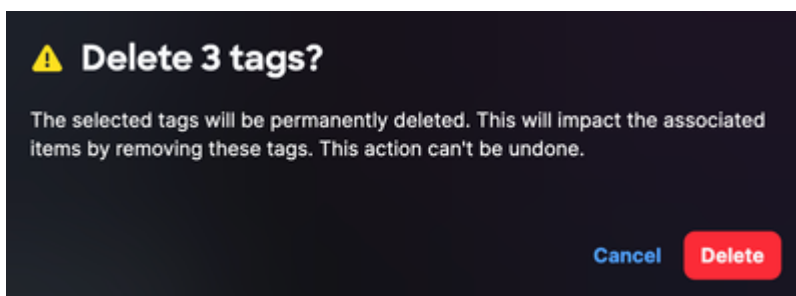
1. Escolha Home > Configurações do sistema > Tags. A página Tags é exibida.



Tags

2. Marque as caixas de seleção das marcas a serem excluídas.

3. Clique em Excluir tags. Uma confirmação é exibida.



Excluir Marca

4. Clique em Excluir para confirmar.

Conectores de dados

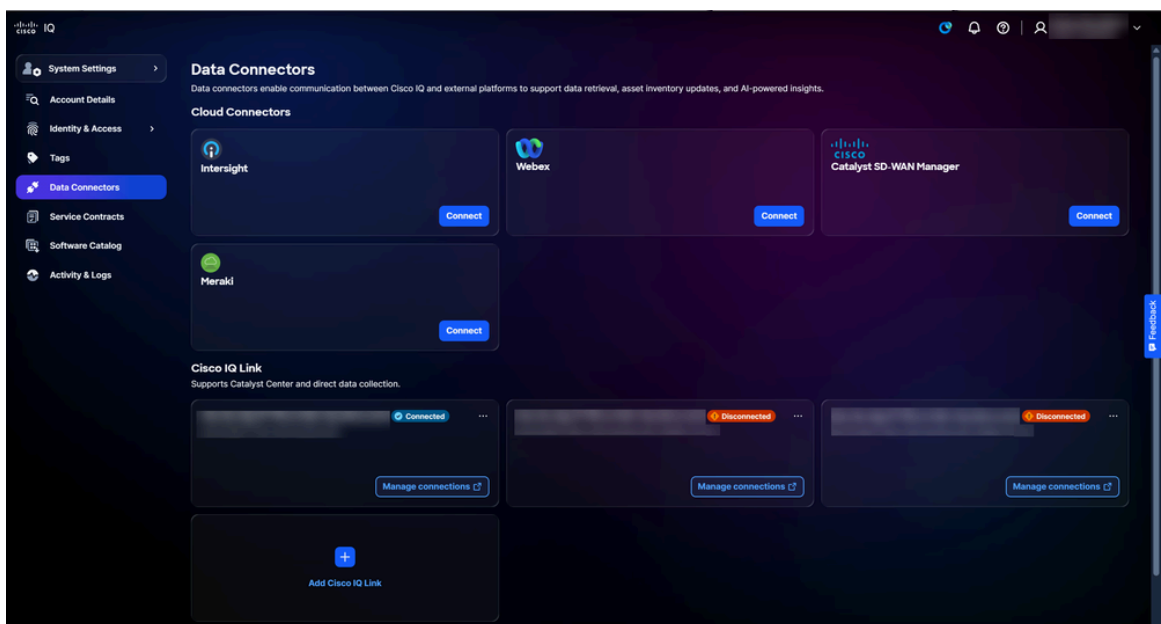
O Cisco IQ usa conectores de dados como parte de uma abordagem de inclusão de dados multicamada para fornecer insights abrangentes sobre a rede. Os conectores de dados coletam telemetria de ativos em sua rede, permitindo que o Cisco IQ forneça informações relevantes e experiência confiável.

Adicionando conectores de nuvem

Conectar os dados de seus produtos em nuvem da Cisco ao Cisco IQ é a maneira mais rápida de começar a usar seus recursos avançados e personalizados. Você pode receber insights personalizados em minutos após configurar suas conexões de dados para os seguintes controladores de produtos: Catalyst Center, Intersight®, painel Meraki, gerenciador SD-WAN, Webex® Control Hub.

Para conectar seus produtos em nuvem da Cisco:

1. Escolha Configurações do sistema > Conectores de dados. A página Conectores de Dados é exibida.

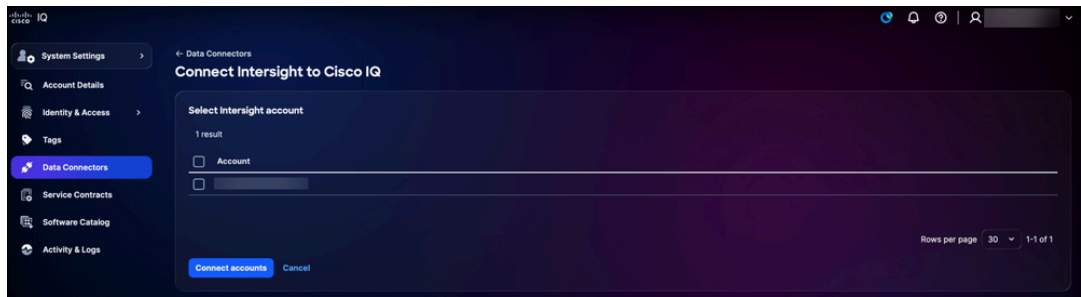


Conectores de nuvem

2. Clique em Connect para obter o conector de nuvem desejado.

3. Conclua as seguintes etapas para o conector de nuvem selecionado:

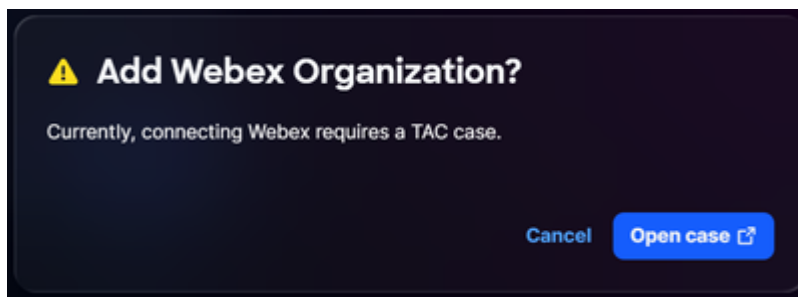
- Intersight



Connect Intersight

1. Marque as caixas de seleção das contas desejadas.
2. Clique em Connect accounts. Você será redirecionado para a página Conectores de Dados e uma confirmação será exibida.

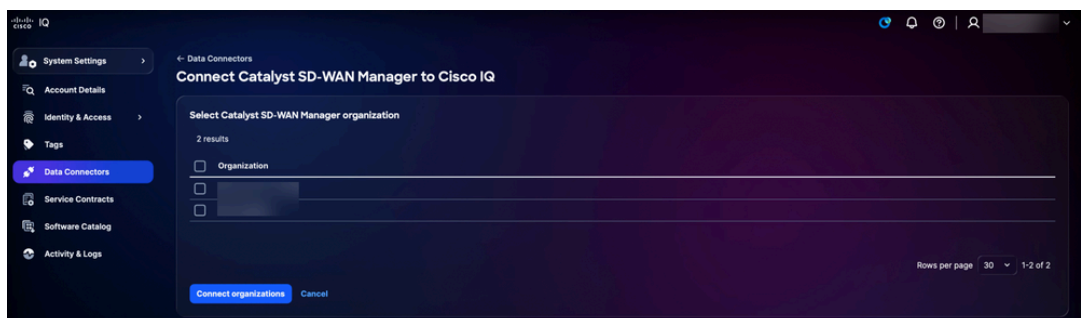
- WebEx



Conecte-se ao Webex

1. Clique em Open case na janela Add Webex Organization. Você é redirecionado para SCM.
2. Crie um caso de suporte no SCM.

- Gerenciador Catalyst SD-WAN

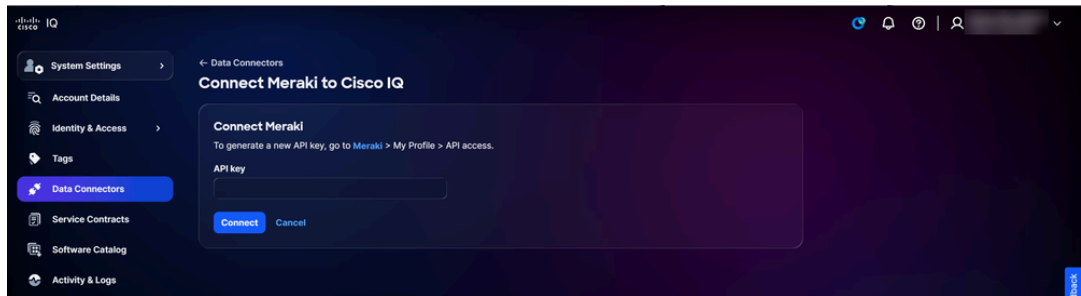


Conectar o Catalyst SD-WAN Manager

1. Marque as caixas de seleção das organizações desejadas.

2. Clique em Conectar organizações. Você será redirecionado para a página Conectores de Dados e uma confirmação será exibida.

- Meraki




Conecte-se à Meraki

1. Siga as instruções na tela.
2. Insira a chave de API.
3. Clique em Conectar. Você será redirecionado para a página Conectores de Dados e uma confirmação será exibida.

Adicionando instâncias de link do Cisco IQ

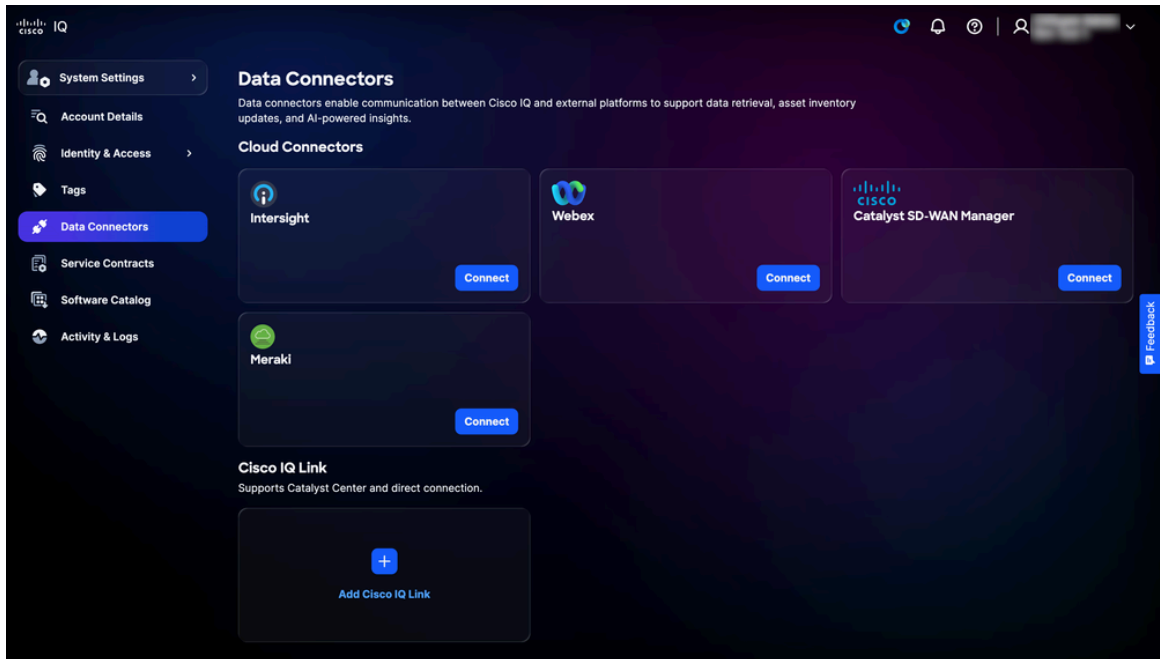
O Cisco IQ Link é um componente local do Cisco IQ projetado para fornecer informações mais completas e inteligentes, como o ciclo de vida de hardware e software e relatórios de inventário. Ele consolida coletores anteriores em um único conector instalado em uma máquina virtual (VM) para coletar dados detalhados de telemetria de seus dispositivos.

O Cisco IQ Link é implantado em sua rede local para executar descoberta automatizada de dispositivos e coleta de telemetria. O Cisco IQ Link suporta a conexão direta e a integração com o Catalyst Center. Além disso, se sua conta tiver sido criada por meio de migração, você poderá aproveitar o CX Agent ou o CSPC para conectar a telemetria.

 **Note:** Para controladores gerenciados em nuvem, o Cisco IQ Link não é necessário, pois os dados necessários podem ser acessados diretamente através do Cisco Cloud.

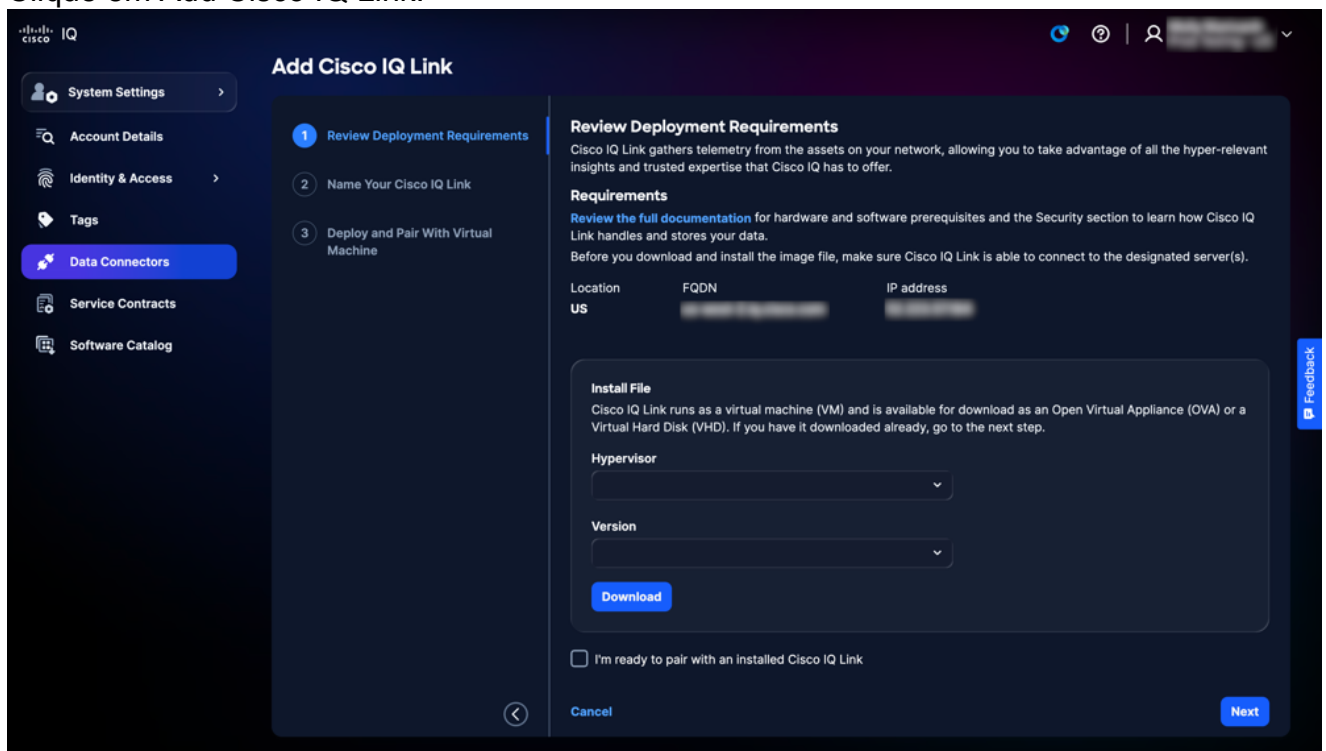
Para adicionar instâncias do Cisco IQ Link ao Cisco IQ:

1. Navegue até a página Conectores de Dados.



Adicionar link do Cisco IQ

2. Clique em Add Cisco IQ Link.



Faça o download do OVA ou VHD

3. Faça o download do Open Virtual Appliance (OVA) ou do Virtual Hard Disk (VHD):

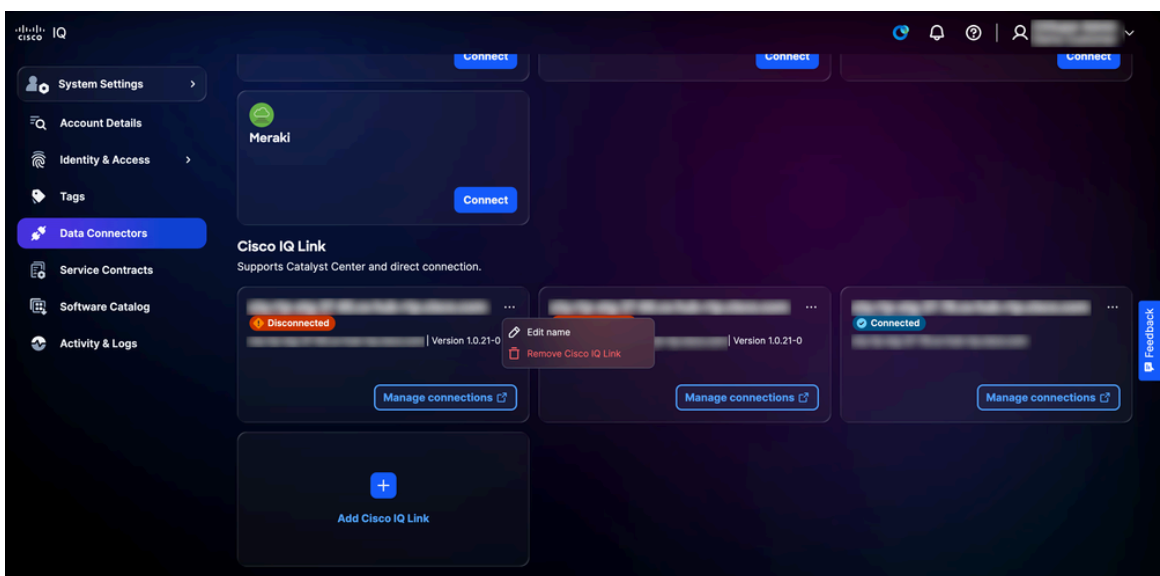
1. Escolha o hipervisor na lista suspensa.
2. Escolha a Versão na lista suspensa.
3. Clique em Download.

4. Clique em Review the full documentation para acessar o [Cisco IQ Link Getting Started Guide](#). Este documento fornece instruções passo a passo abrangentes para instalar o Cisco IQ Link usando o arquivo baixado na etapa anterior. Ele abrange o fluxo de trabalho de implantação completo, incluindo todas as transições necessárias entre a interface Cisco IQ e Cisco IQ Link para finalizar o emparelhamento e a configuração.

Edição de nomes de instância de link do Cisco IQ

Para editar um nome de instância do Cisco IQ Link:

1. Navegue até a instância desejada do Cisco IQ Link na página Data Connectors.



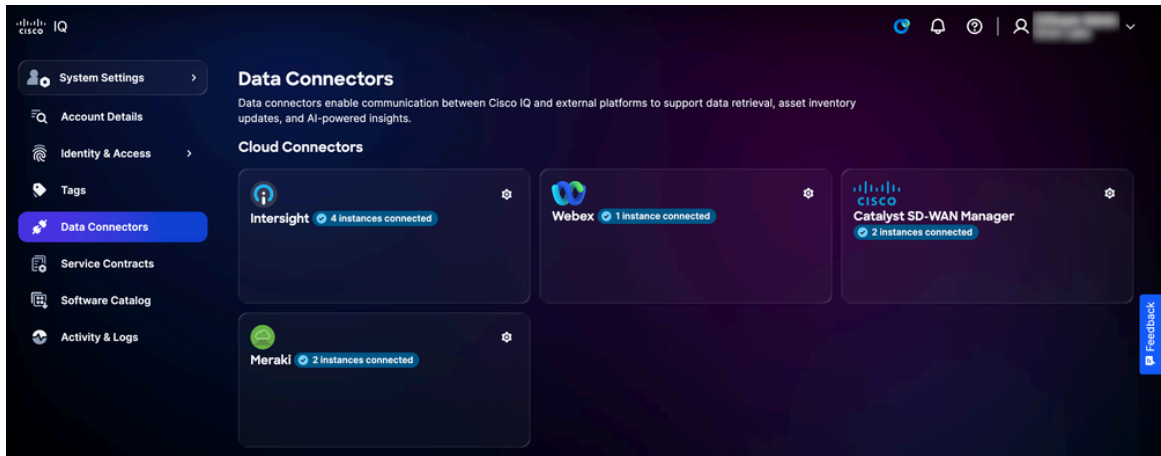
Editar nome

2. Escolha o ícone Mais Opções > Editar nome.
3. Edite o nome conforme desejado.
4. Clique em Update.

Remoção de contas conectadas dos conectores de nuvem

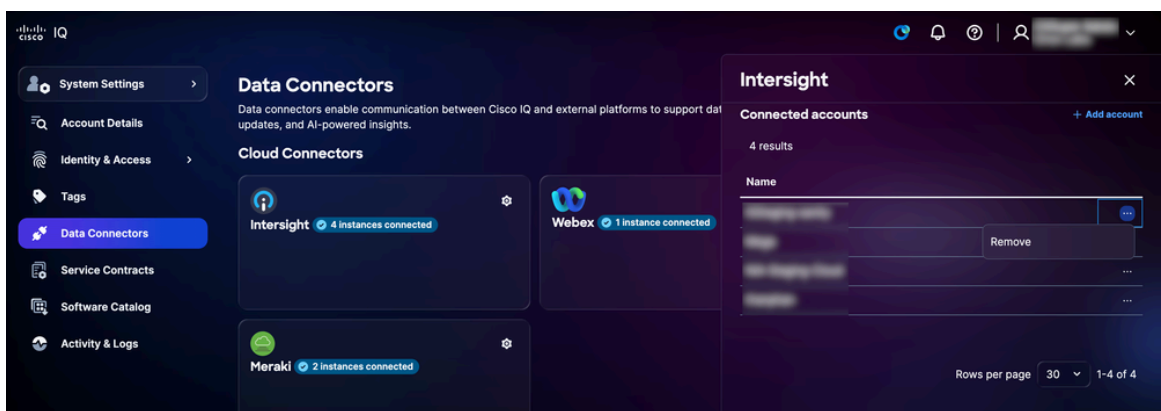
Para remover uma conta conectada dos conectores de nuvem:

1. Navegue até o conector de nuvem desejado na página Conectores de Dados.



Configurações dos conectores de nuvem

2. Clique no ícone Settings. A janela Contas conectadas é aberta.



Remover Conta Conectada do Conector de Nuvem

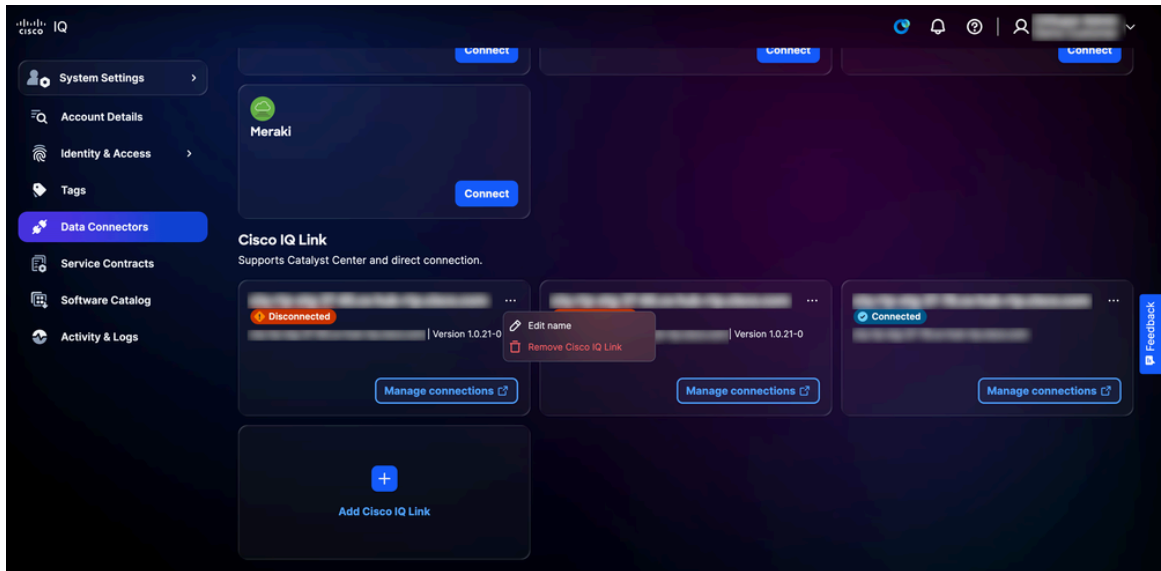
3. Na conta desejada, escolha o ícone Mais Opções > Remove. Uma confirmação é exibida.

4. Clique em Remover para confirmar.

Removendo instâncias de link do Cisco IQ

Para remover uma instância do Cisco IQ Link dos conectores de dados:


1. Navegue até a instância desejada do Cisco IQ Link na página Data Connectors.



Remover link do Cisco IQ

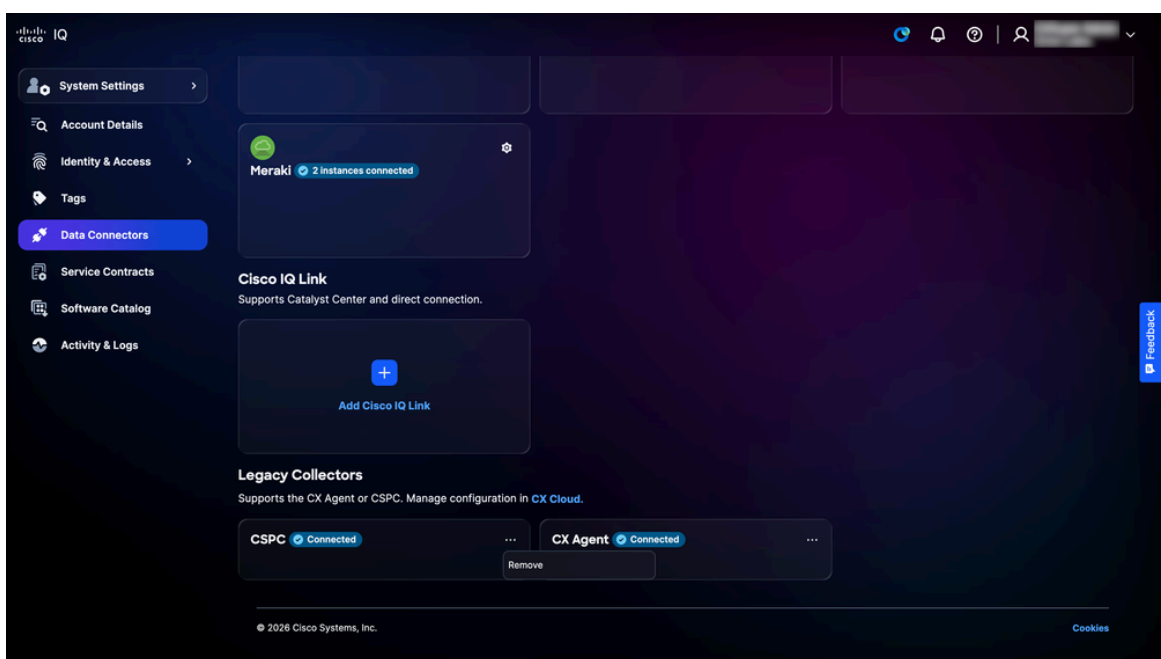
2. Escolha o ícone More Options > Remove Cisco IQ Link. Uma confirmação é exibida.
3. Clique em Open case para abrir um caso de suporte e remover o Cisco IQ Link.

Remoção de coletores legados

 Note: Os coletores legados são exibidos apenas em contas que foram migradas do CX Cloud.

Para remover um conector legado conectado:


1. Navegue até o coletor legado desejado na página Conectores de Dados.



2. Escolha o ícone Mais Opções > Remover. Uma confirmação é exibida.
3. Clique em Abrir caso para abrir um caso de suporte e remover o coletor herdado.

Contratos de serviço

A vinculação de contratos une dados de contratos associados a diferentes membros da equipe e incorpora dispositivos não conectados ao seu inventário por telemetria, centralizando a visibilidade da cobertura de suporte e evitando surpresas de renovação. Vincular contratos exige o número do contrato usado para abrir casos de suporte.

 Note: Para suporte de número de contrato, entre em contato com seu parceiro ou representante de vendas da Cisco.

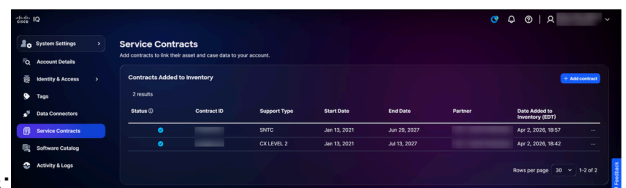
Os principais benefícios dos contratos de serviço incluem:

- Criação de uma visão centralizada da cobertura de suporte da sua organização
- Painéis personalizáveis que permitem que você fique à frente de suas renovações com meses de antecedência
- Expansão da visibilidade do inventário para incluir ativos não conectados à telemetria ou a parte de ambientes "air-gapped"

Vinculando Contratos


Para vincular um contrato na página Service Contracts:

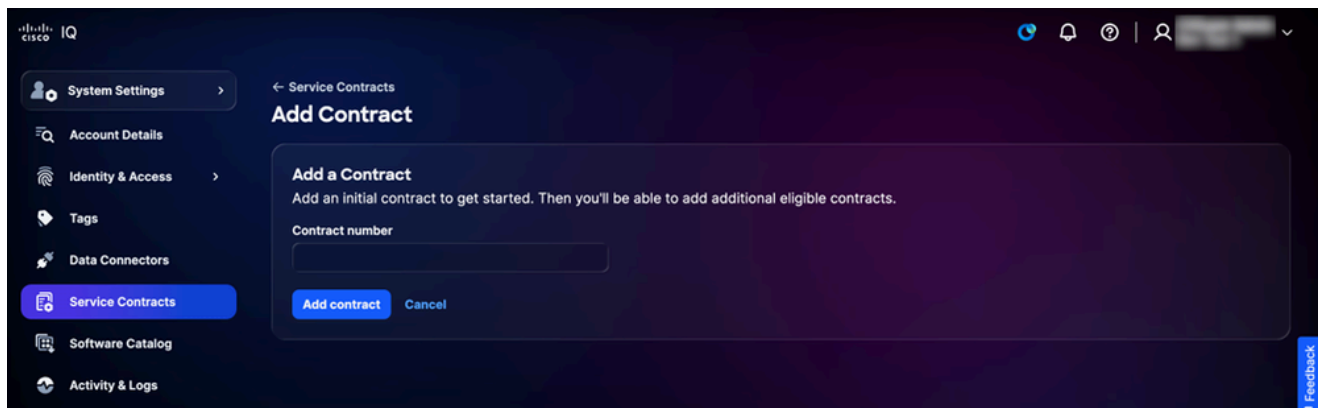
Adicionar contrato



Status	Contract ID	Support Type	Start Date	End Date	Partner	Date Added to Inventory (EST)
✓	10101	SMTC	Jun 13, 2021	Jun 28, 2022		Apr 2, 2020, 18:57
✓	10102	CS LEVEL 2	Jun 13, 2021	Jul 13, 2022		Apr 2, 2020, 18:42

1. Clique em Adicionar contrato. A página Adicionar contrato é exibida.

 Note: Contratos adicionais podem ser adicionados depois que um contrato inicial é adicionado à conta.



Inserir número do contrato

2. Insira o Número do contrato.
3. Clique em Adicionar contrato. O contrato é adicionado à conta.

Catálogo de software

O Catálogo de software 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.

Para acessar o Catálogo de software, navegue para Início > Configurações do sistema > Catálogo de software. A página Catálogo de software é exibida. Nesta página, as instâncias de software disponíveis são exibidas como cartões de disponibilidade do coletor de links. Cada cartão de disponibilidade do coletor de links exibe o nome, a descrição, o editor e a versão de uma instância de software.

Exibindo Detalhes para Instâncias de Software

Para exibir as notas de versão de uma instância de software, clique em Detalhes. Uma janela é aberta com as notas de versão mais recentes da instância. Para exibir as notas de versão anteriores, escolha uma versão na lista suspensa.

Instalando Pacotes para Novas Instâncias de Software

Para fazer download de um instalador para criar uma nova instância:


1. Em uma placa de disponibilidade do coletor de links desejada, escolha Download options > Install packages. A janela do pacote de instalação é aberta.

2. Selecione uma das seguintes opções de hipervisor na lista suspensa:

- ESXi para VMware ESXi
- Hyper-V: para Microsoft Hyper-V
- KVM: para KVM (máquina virtual) baseada em kernel Linux

3. Selecione uma Versão na lista suspensa.

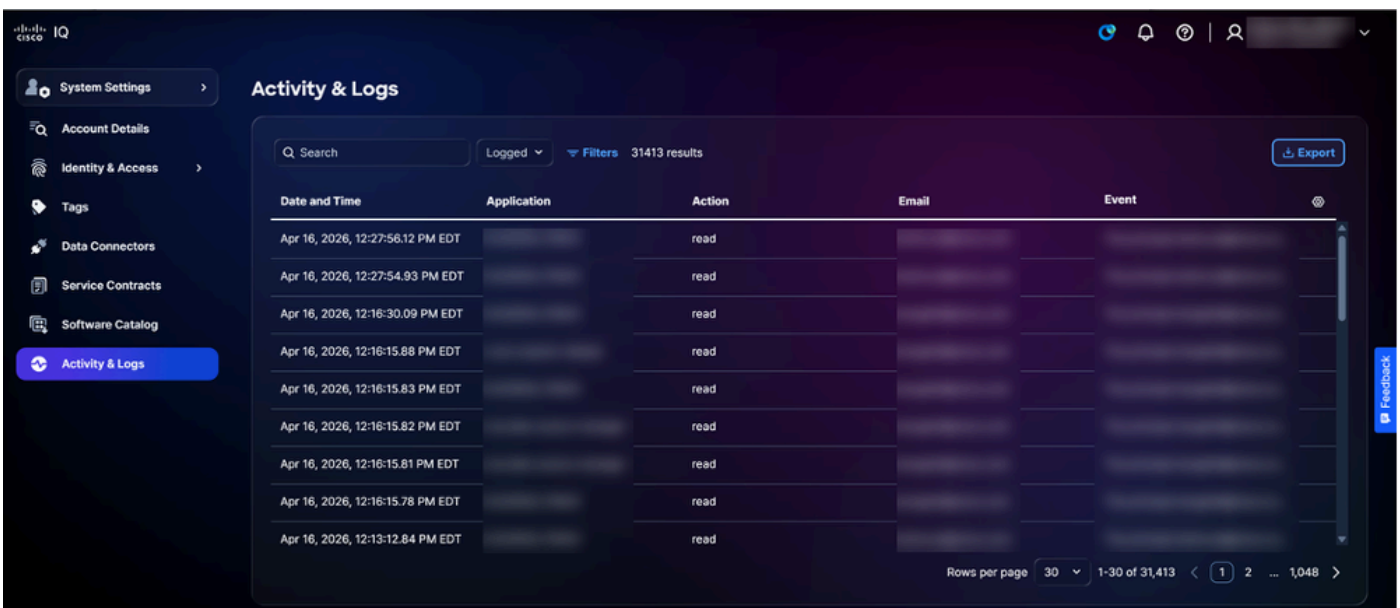
4. Clique em Download para salvar o arquivo localmente.

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

5. Implante o arquivo no seu data center. Consulte o [Guia de Introdução do Cisco IQ Link](#) para obter mais informações.

Atividade e registros

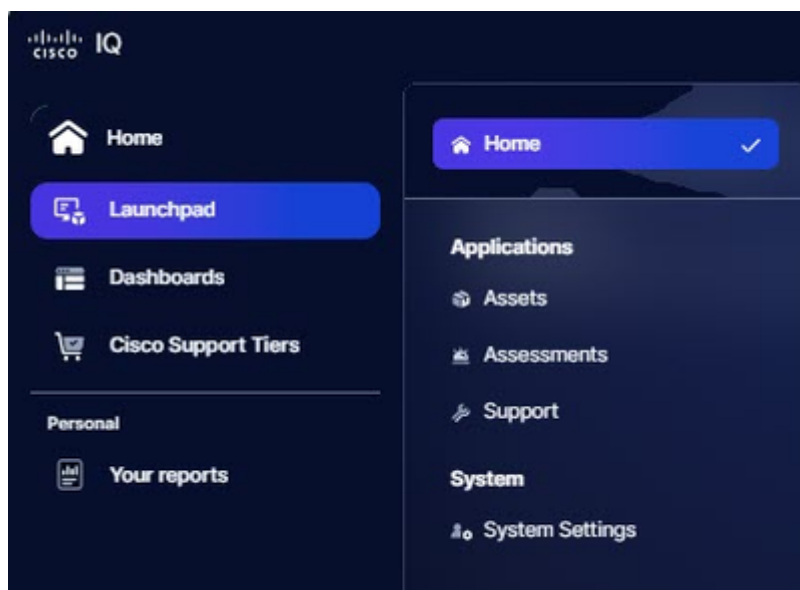
O serviço Activity & Logs centraliza o rastreamento de todas as ações do usuário e eventos do sistema no Cisco IQ para conformidade, solução de problemas e monitoramento. Ele captura registros de auditoria imutáveis para eventos de autenticação, decisões de autorização, acesso a recursos, alterações de configuração e ações administrativas com contexto detalhado, incluindo identidade do usuário, carimbos de data/hora, endereços IP de origem e recursos afetados. A Activity & Logs aplica políticas de retenção e permite consultas flexíveis e filtragem de eventos de auditoria com suporte para pesquisas de intervalo de tempo, filtros baseados no usuário e rastreamento de atividades específicas de recursos.



Date and Time	Application	Action	Email	Event
Apr 16, 2026, 12:27:56.12 PM EDT		read		
Apr 16, 2026, 12:27:54.93 PM EDT		read		
Apr 16, 2026, 12:16:30.09 PM EDT		read		
Apr 16, 2026, 12:16:15.88 PM EDT		read		
Apr 16, 2026, 12:16:15.83 PM EDT		read		
Apr 16, 2026, 12:16:15.82 PM EDT		read		
Apr 16, 2026, 12:16:15.81 PM EDT		read		
Apr 16, 2026, 12:16:15.78 PM EDT		read		
Apr 16, 2026, 12:13:12.84 PM EDT		read		

Aplicativo de Ativos

O aplicativo Assets 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 dentro de 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 aplicativos no Cisco IQ, como o aplicativo de avaliações, dependem desses dados para avaliar a integridade e a segurança de seus dispositivos.



Menu Início

Conceitos principais

O aplicativo 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
- **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

Acesso ao aplicativo Ativos

Para acessar os recursos de gerenciamento de ativos no Cisco IQ, escolha o menu Início > Ativos. 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.

- Assets
- Overview**
- Inventory
- Service Contracts
- End of Life

Overview

Product family ▾ Last signal date ▾ Data source ▾ Asset location ▾ Filters

Ask AI Customize

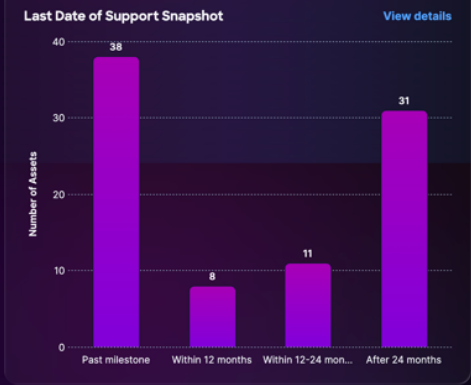
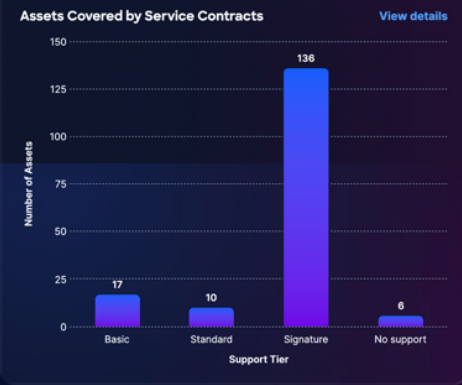
Total Assets **169**
Assets

Covered Assets

163 Covered 96% Of all assets

Uncovered Assets

6 Uncovered 4% Of all assets



Key Asset Metrics

Assets with Telemetry Enabled

169 with telemetry 100% Of all assets

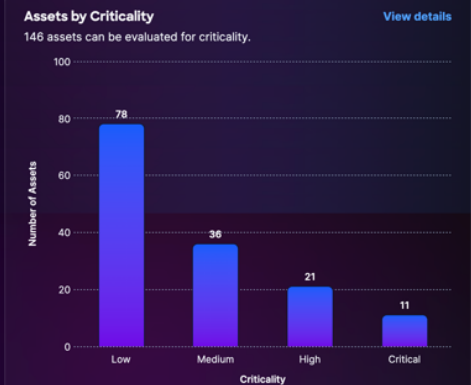
Assets without Telemetry Enabled

0 without telemetry 0% Of all assets

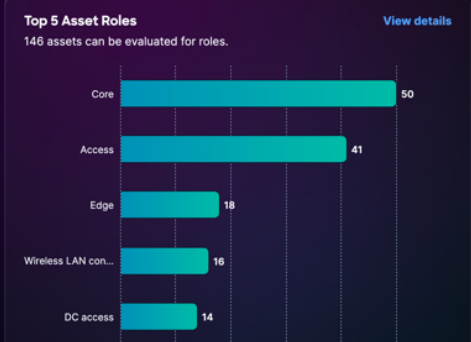
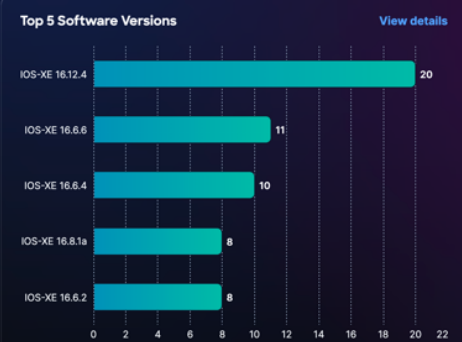
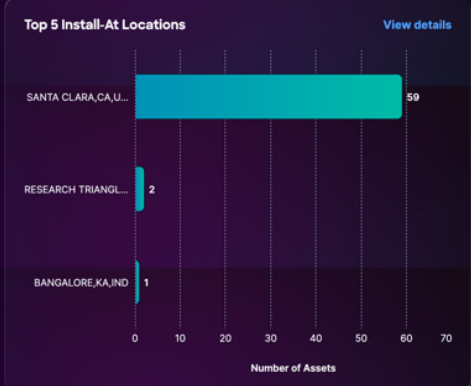
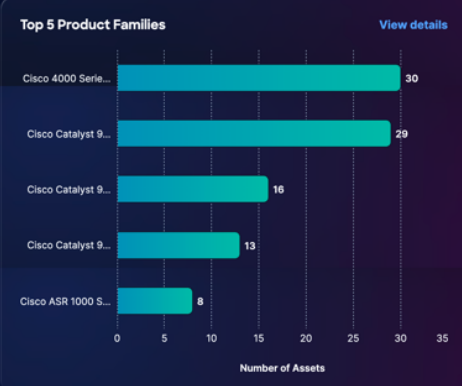
Assets with Critical or High Security Advisories View details

85%

Of the 169 assets with telemetry enabled, 143 have critical or high Security Advisories



Asset Breakdown



O painel exibe as seguintes informações:

- Total de ativos: O número total de ativos na conta do Cisco IQ
- Ativos cobertos: Número total e porcentagem de ativos abrangidos por contratos de serviços
- Ativos não cobertos: Número total e porcentagem 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
- Principais métricas de ativos: Principais métricas adicionais, como status de telemetria, avisos de segurança críticos e informações de LDOS
 - Ativos com telemetria: Número total e percentual de ativos com telemetria habilitada
 - Ativos sem telemetria: 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 com avisos de segurança críticos ou altos
 - Ativos por criticidade: 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.


 Note: 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 aplicativo Assets que prevê a função funcional e a importância comercial dos dispositivos de rede. Analisando as configurações de dispositivos e os recursos habilitados, 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 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

Inventário

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

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 bu...
 175 Cisco Catalyst 9300 Series Switches (49.7% of not covered assets) lack active support contracts, which may limit access to Cisco support resources...


<input type="checkbox"/>	Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milestone	Contract Number	Coverage Status	Telemetry Status	Security
<input type="checkbox"/>			Cloud and ...		End of Ser...	Jun 25, 2028	—	🔒	🟢	0
<input type="checkbox"/>			Switches		End of Ser...	Jan 29, 2027	—	🔒	🟢	4
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23
<input type="checkbox"/>			Switches		—	—		🟢	🟢	23

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.

 Note: 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 Aplicativo para obter mais detalhes.

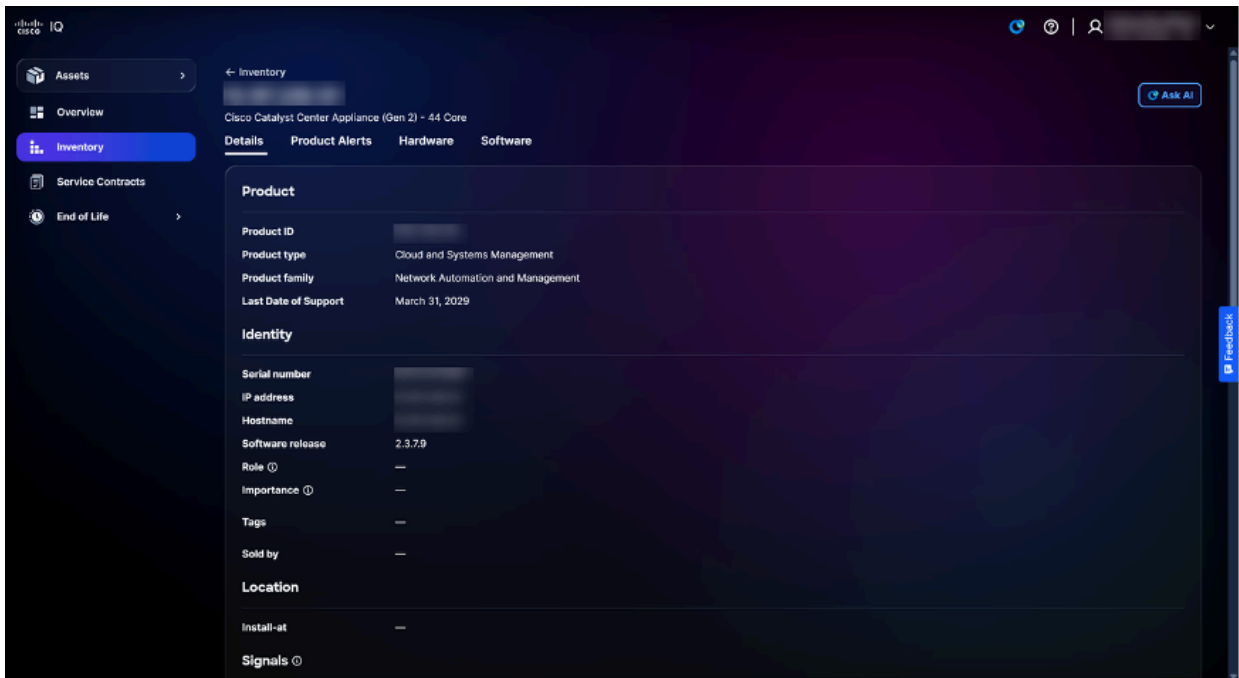
Exportando inventário

Clique em Exportar para salvar uma lista de inventário filtrada no formato .xls ou .csv. Consulte [Exportação de Informações](#) em Recursos Comuns do Aplicativo 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




Detalhes do ativo

- Alertas do produto: Exibe alertas de produtos relacionados, como avisos de segurança e avisos 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 tag é um `key:value` par, por exemplo, `Environment:Prod` ou `Label: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.

Criando e excluindo tags de ativos

Consulte [Marcas](#) em Configurações do sistema para obter mais informações sobre como criar e excluir marcas de ativos.

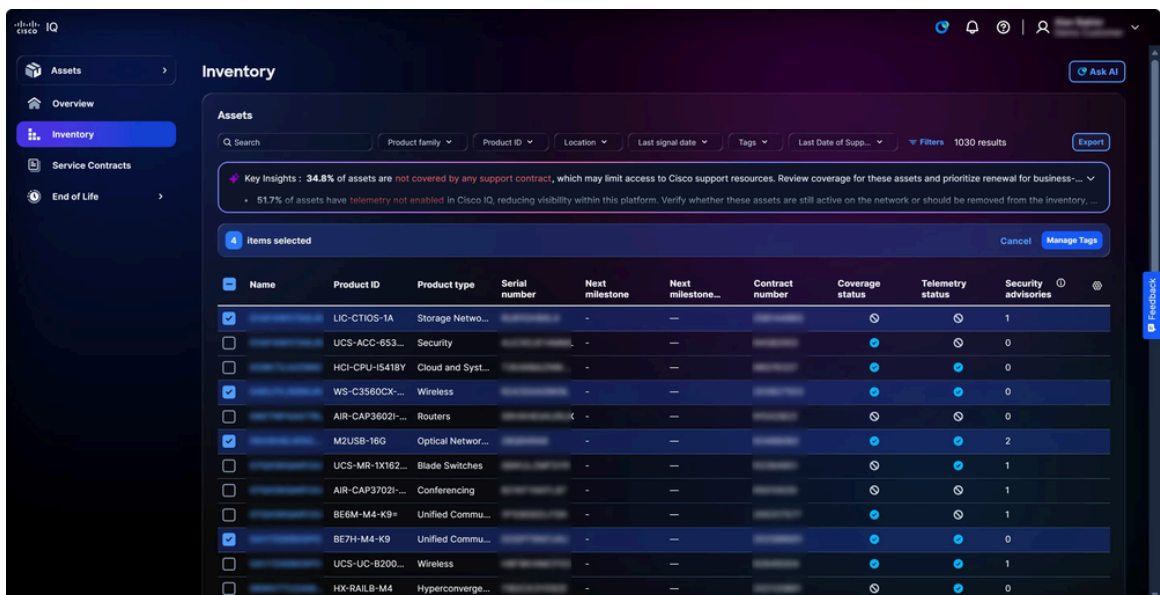
 Note: Somente administradores de conta podem criar e excluir marcas.

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.

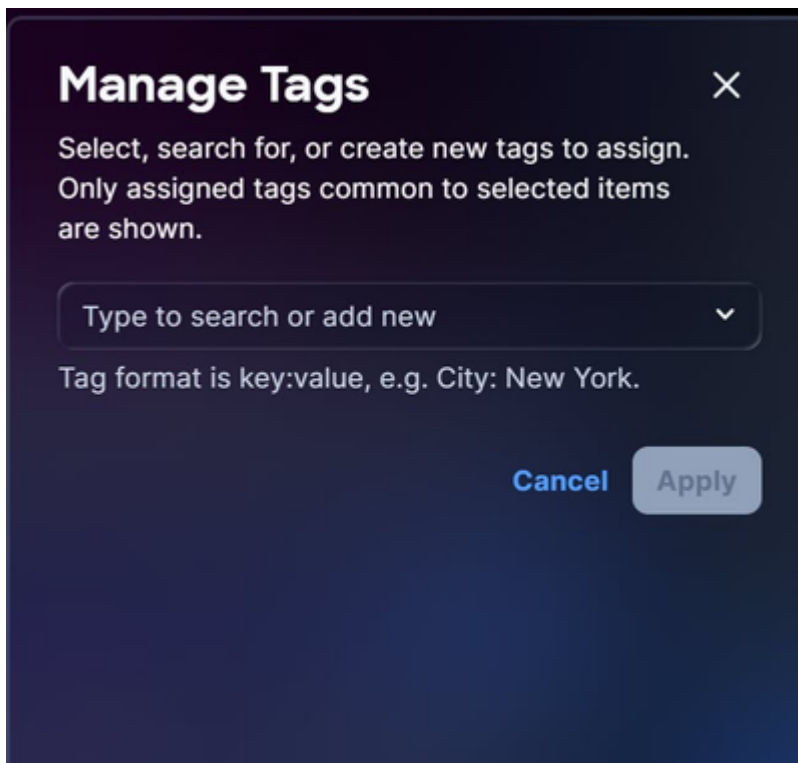
Para atribuir uma etiqueta a um ativo:

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.

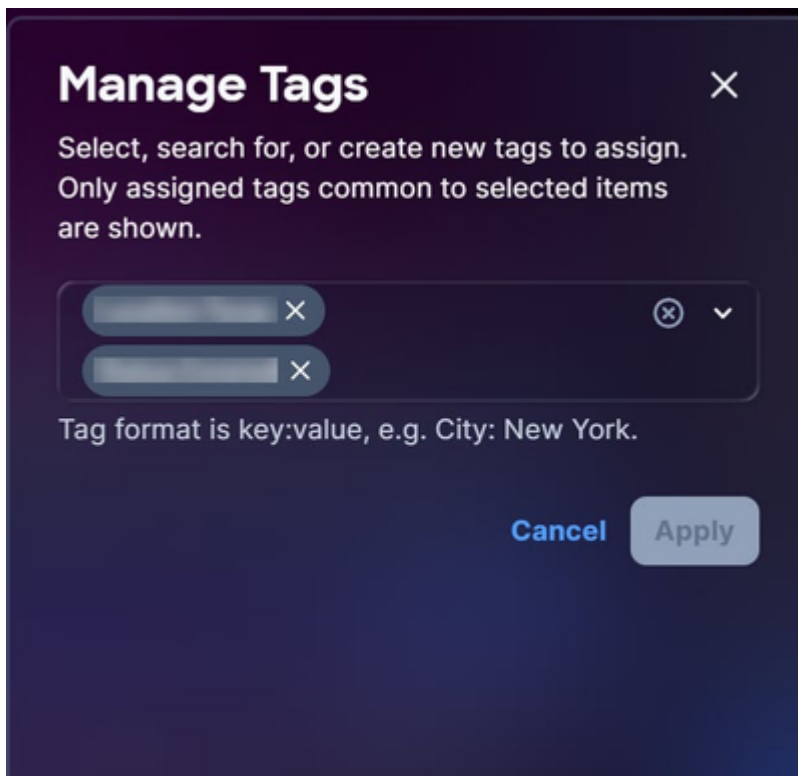
 Note: As marcas estão no `key:value` formato (por exemplo, `City:NYC`).

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

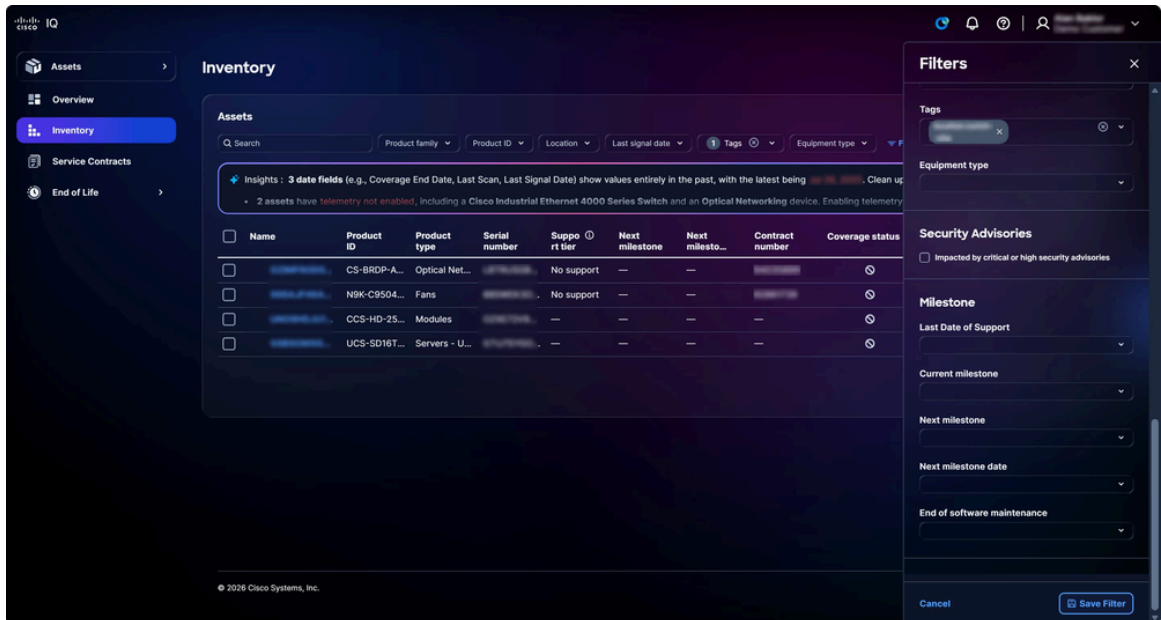
4. Clique no X em qualquer tag para removê-la da seleção.
5. Clique em Apply.

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

3. 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.

The screenshot shows the Cisco IQ Service Contracts page. It features a navigation menu on the left with 'Assets', 'Overview', 'Inventory', 'Service Contracts', and 'End of Life'. The main area displays a table of service contracts with columns: Coverage Status, Contract Number, Support Type, Support Tier, Start Date, End Date, and Partner. Above the table, there are filters for 'All status types', 'All expiration d...', and 'Tags', along with a search bar and an 'Export' button. Insights above the table state: '2 of 4 expired service contracts are linked to 100% impacted assets, representing 50.0% of all expired coverage. Review these contracts to determine if the associated assets r...' and '15 service contracts (9.0%) have start dates within the next 6 months, with the earliest deadline on Apr 16, 2026. Initiate onboarding or renewal processes now to avoid coverage gaps.' A 'Feedback' button is visible on the right side of the table.

Coverage Status	Contract Number	Support Type	Support Tier	Start Date	End Date	Partner
🔍	...	SWSS	No support	May 16, 2025	May 16, 2025	...
🔍	...	TSS	No support	May 28, 2025	May 28, 2025	...
🔍	...	TSS	No support	May 5, 2025	Jul 15, 2025	...
🔍	...		No support	May 21, 2025	Jul 15, 2025	...
🔍	...		No support	May 6, 2025	Jul 28, 2025	...
🔍	...	TSS	No support	Jul 15, 2025	May 28, 2026	...
🔍	...		Basic	May 1, 2024	Aug 29, 2025	...
🔍	...	TSS	No support	Jul 28, 2025	May 11, 2026	...
🔍	...		Basic	Jul 16, 2025	May 11, 2026	...
🔍	...		Basic	May 1, 2024	Apr 11, 2026	...
🔍	...	TSS	No support	May 6, 2025	Aug 16, 2026	...
🔍	...		Basic	Apr 16, 2024	May 1, 2026	...
🔍	...	TSS	No support	May 15, 2025	May 11, 2026	...
🔍	...	TSS	No support	May 16, 2024	Apr 16, 2027	...
🔍	...		Basic	Jul 28, 2025	May 11, 2027	...

Contratos de serviço

gráficos, painéis e gráficos que fornecem informações adicionais. Consulte [Analisando Dados](#) em Recursos Comuns do Aplicativo 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 [Exportação de Informações](#) em Recursos Comuns do Aplicativo para obter mais detalhes.

Aplicativo de avaliações

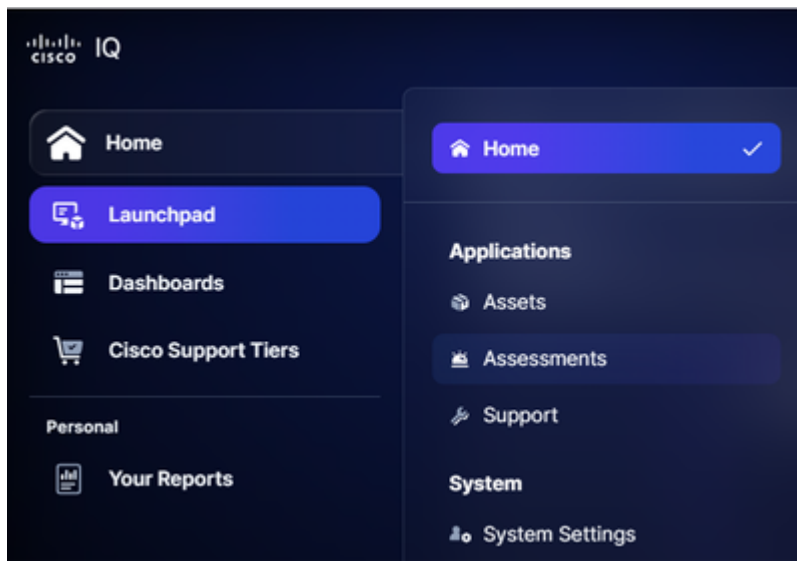
O aplicativo Avaliações fornece uma estrutura de avaliação que permite que os usuários investiguem e reduzam proativamente os riscos relacionados à segurança, estabilidade, capacidade, conformidade e envelhecimento, mantendo as redes seguras, estáveis e confiáveis.

Conceitos principais

O aplicativo Avaliações baseia-se 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 aplicativo de avaliações



Avaliações

Para acessar os recursos de segurança e avaliação no Cisco IQ, escolha o menu Início > Avaliações. A página Visão geral das avaliações é exibida.

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
- Segurança fortalecendo regras com ativos que não foram aprovados: Exibe ativos que falham nas regras de proteção de segurança, categorizados por severidade Alta, Média, Baixa e Informativa
- Regras de configuração com ativos que não foram aprovados: 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 Crítico, Alto, Médio e Sem gravidade

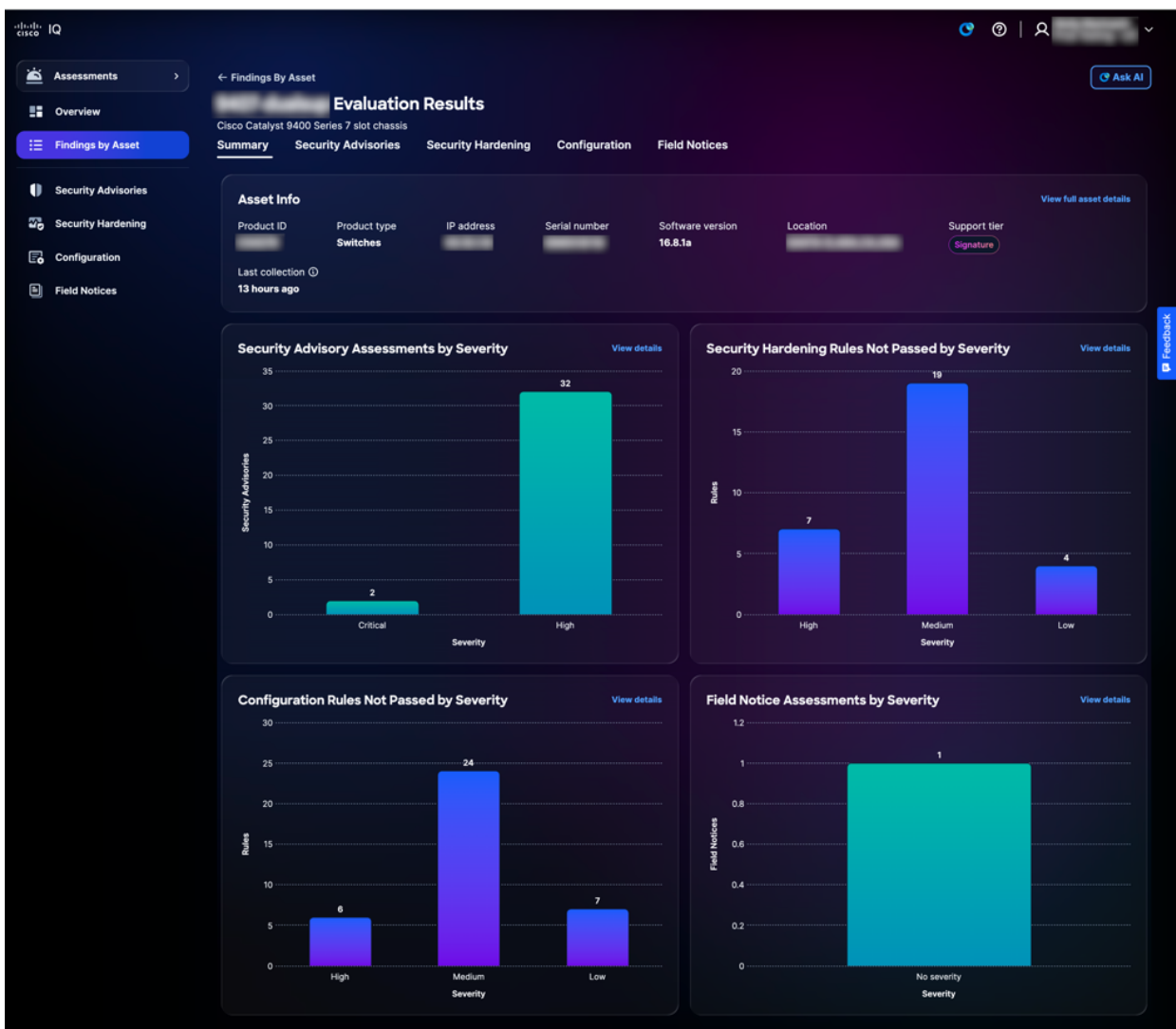
 Note: Os clientes podem apenas visualizar os ativos aos quais têm direito de acesso.

Descobertas por ativo

A página Descobertas por ativo fornece uma lista de ativos que foram avaliados usando pelo

Para exibir as descobertas pelos detalhes do 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

Quando você clica em Exibir detalhes em um bloco, a página é redirecionada para a página relevante no aplicativo.

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


Assessment	Severity	Assets at Risk	Assets Potentially at Risk	CVE	Last Updated
Cisco IOS XE Software ...	High	1009	0		May 7, 2025
Cisco IOS XE Software ...	High	963	0		Nov 2, 2020
Cisco IOS XE Software ...	High	915	10		Sep 24, 2020
Cisco IOS and IOS XE S...	High	915	12		Oct 6, 2025
Cisco IOS XE Software ...	High	915	10		Mar 24, 2021
Multiple Vulnerabilities...	Critical	915	10		Nov 1, 2023
Cisco IOS XE Software ...	High	915	10		Mar 24, 2021
Cisco IOS XE Software ...	High	808	0		Jun 3, 2020


Orientações de Segurança

Pesquisando Views de Filtragem para Recomendações de Segurança

Você pode filtrar a view de lista escolhendo um filtro na lista drop-down. Também é possível pesquisar avaliações de Advertência de Segurança informando o nome da avaliação no campo Pesquisar.

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

 Note: Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

 Note: 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 sobre exportação.

Exibindo Detalhes da Avaliação da Consultoria de Segurança

Para exibir detalhes adicionais sobre uma avaliação, clique em uma Recomendação. Esta 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 displays the Cisco IQ interface for Security Advisories. The main heading is "Cisco IOS XE Software Privilege Escalation Vulnerabilities". A sidebar on the left contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories (highlighted), Security Hardening, Configuration, and Field Notices. The main content area is divided into two sections: "About the Assessment" and "Assessment Outcome".

About the Assessment

Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration... [Show more](#)

Severity	Assessment ID	CVE	CVSS score
High	[Redacted]	[Redacted] +4	6.7
Version	First published	Last updated	
1.0	May 7, 2025	May 7, 2025	

Source documents: [Security Advisory](#)

Assessment Outcome

Asset Assessment Results

Q Search [] Result [] Product type [] Product family [] Product ID [] Software type [] Filters 1009 results


Asset	Result	Product ID	IP address	Serial number	Support Tier
[Redacted]	Affected	[Redacted]	[Redacted]	[Redacted]	Basic
[Redacted]	Affected	[Redacted]	[Redacted]	[Redacted]	Basic
[Redacted]	Affected	[Redacted]	[Redacted]	[Redacted]	-

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.

 Note: 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 Resultados da avaliação de ativos. A página Detalhes do resultado da avaliação é exibida.


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 sobre exportação.

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 reduzam efetivamente a superfície de ataque e mantenham o alinhamento consistente com as rigorosas práticas recomendadas de segurança da Cisco. Ao centralizar o monitoramento de conformidade e simplificar o processo de fortalecimento, o aplicativo transforma o gerenciamento de segurança de uma tarefa reativa em uma estratégia proativa orientada por dados, garantindo uma rede empresarial resiliente e segura.

 Note: As avaliações de proteção de segurança estão disponíveis exclusivamente para ativos com níveis de suporte Padrão ou Assinatura.

Exibindo Avaliações de Proteção de Segurança

Para exibir detalhes adicionais sobre o Fortalecimento da segurança, clique em uma Avaliação. A



página Avaliação de Fortalecimento da Segurança exibe as seguintes informações:


Fortalecimento da segurança

- Sobre a avaliação: Fornece detalhes adicionais resumindo a finalidade da avaliação
- Resumo 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.

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

 Note: 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 displays the Cisco IQ interface for a Security Hardening Assessment. The main heading is "Security: It is recommended to monitor all channel...". Below this, it states "Evaluated on: Apr 24, 2026, 10:43 AM". The "About the Rule" section explains that the rule evaluates wireless configuration against Cisco best practices. Key details include: Severity: Critical, Software type: AireOS, and Assets evaluated: 25. A "Results Summary" for 25 assets shows 0 Passed, 25 Did not pass, 0 Inconclusive, and 0 Not applicable. The "Asset Results" section features a table with columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The table shows four rows, all with a "Did not pass" result and a "Signature" support tier.


Exibição de Regra

- Sobre a regra: Fornece detalhes sobre a regra, como Severidade, Tipo de software, Versão e Ativos avaliados.
- 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

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.

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

 Note: 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 sobre exportação.

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.

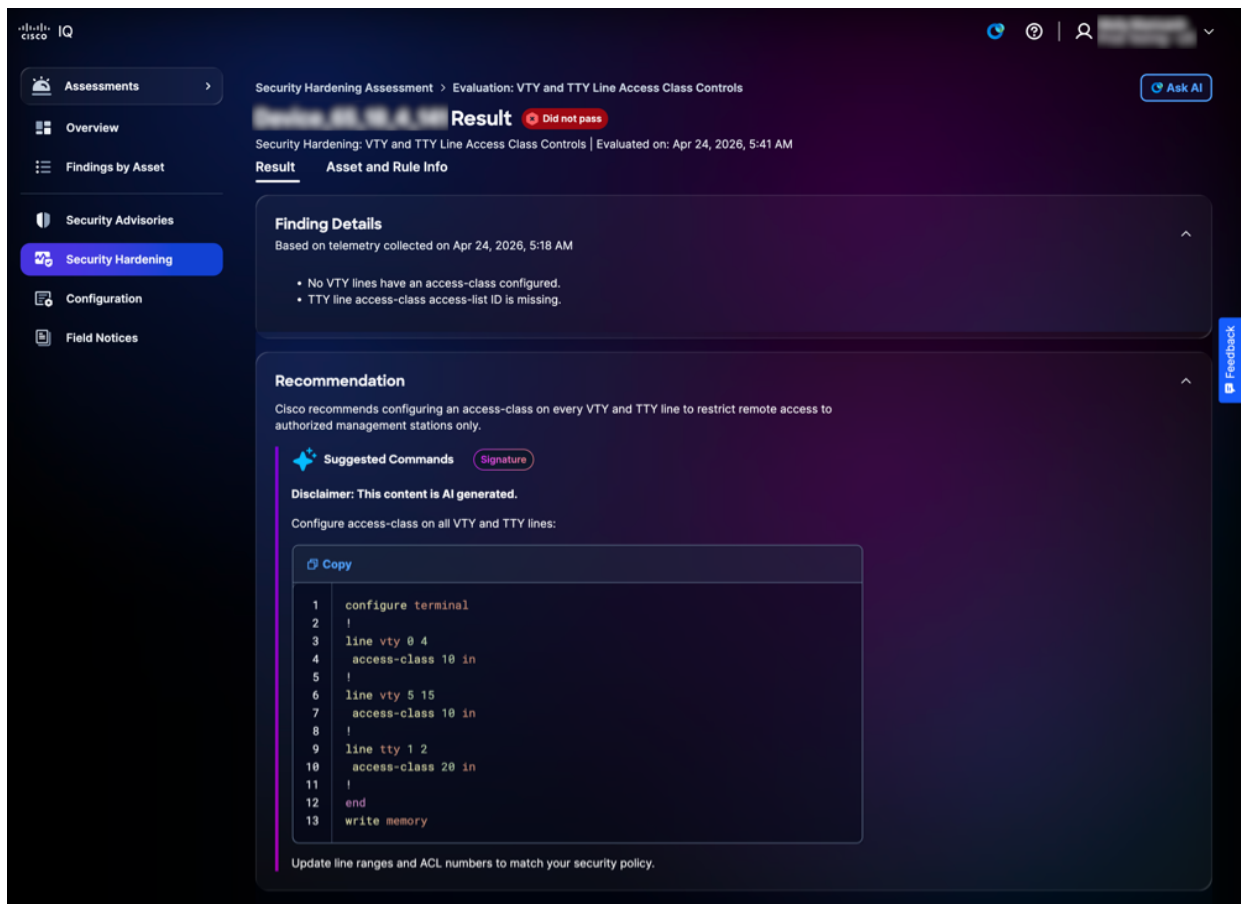
 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

 Note: Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exibindo Resultados de Ativo para Proteção de Segurança

Para exibir os detalhes de um resultado de ativo, clique em um ativo em Resultados de ativos. A página de detalhes do resultado do ativo exibe informações de acordo com seu nível ou nível de direito.

- 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



Camada de Assinatura de Fortalecimento de Segurança

- Camada de Assinatura

- Localizando detalhes: Fornece informações sobre os desvios de configuração identificados durante a avaliação, juntamente com registros de evidências
- Recomendação: Fornece orientação acionável em nível de dispositivo com trecho de código para 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.


The screenshot displays the Cisco IQ Security Hardening Assessment interface. The main content area shows a 'Result' section with a 'Did not pass' status. Below this, there are two main sections: 'About the Asset' and 'About the Rule'. 'About the Asset' includes fields for Product ID, Product type (Switches), IP address, Serial number, Software version (16.11.1), and Location. 'About the Rule' includes a description of the check, a severity level of 'High', and a software type of 'IOS-XE'. There are also links for 'Reference 1' and 'Reference 2'.

Informações sobre ativos e regras

- 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 ou Assinatura.

Exibindo a avaliação da configuração

Para exibir detalhes adicionais sobre a configuração, clique em uma Avaliação. A página Avaliação da configuração exibe as seguintes informações:

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 based on severity. [Show more](#)

Execution Outcome for Apr 24, 2026, 10:45 AM

Summary

Rule evaluations	Assets included
160	327

Insights (Signature)

Based on data from your 312 Signature tier assets.

- Issue:** Critical wireless controllers show widespread baseline security and configuration gaps
- Issue:** Reversible password storage exposes administrative credentials to compromise
- Issue:** Baseline logging, monitoring, and management security controls missing together

Rule Evaluations

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

Q Search | Severity | Category | Software type | Evaluation result | Filters 160 results | Export

Insights: Only 3 of 160 rules are classified as **Critical severity**, including rules for monitoring channel utilization, WLAN management VLAN usage, and con...
 29 rules under the Wireless category apply exclusively to AireOS software, representing 100% of rules in this software type. Prioritize wireless-specific co...

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Applicable	Category	Software Type
Version: Controller with not recommended...	Critical	25	25	0	0	0	Wireless	+1
Security: It is recommended to monitor...	Critical	25	25	0	0	0	Wireless	+1
Security: WLAN may be using management...	Critical	25	25	0	0	0	Wireless	+1
NTP: NTP Polling Interval is set, but no...	High	25	25	0	0	0	Wireless	+1
COMMON Password-Recovery Configuration...	High	302	4	0	17	281	Security a...	+1

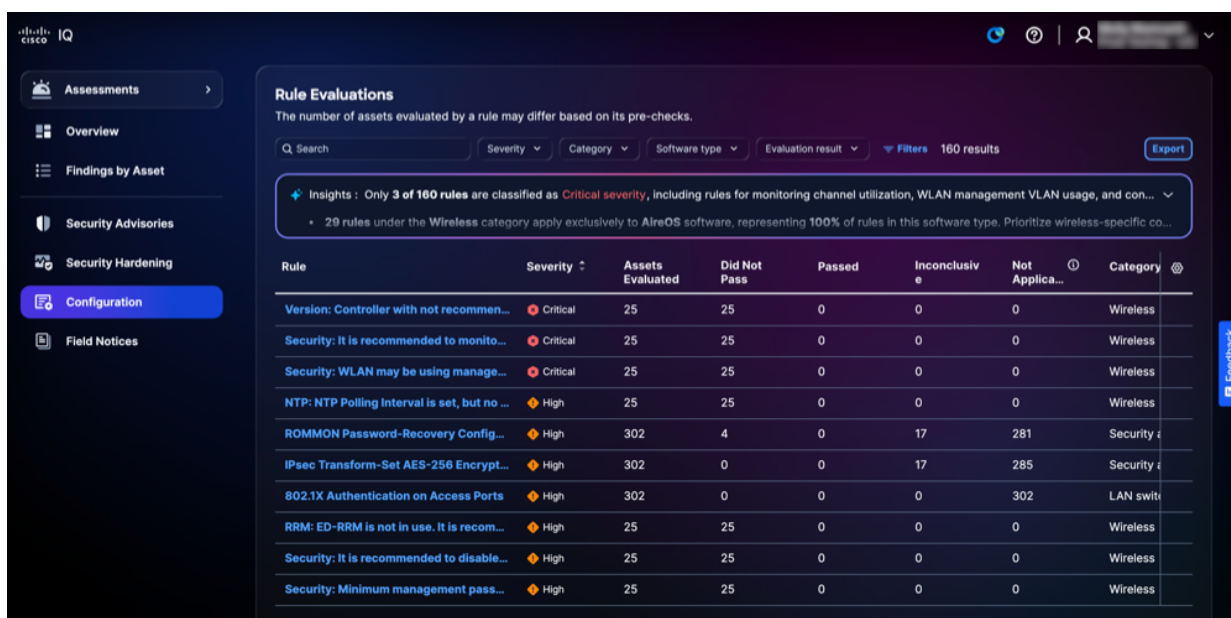
Avaliação da configuração

- 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: Fornecer a área de domínio à qual a regra pertence
- Tipo de software: Indique o tipo de ativos de software aos quais a regra se aplica

Pesquisando e Filtrando Views para Regras




The screenshot shows the Cisco IQ interface for Rule Evaluations. It features a sidebar with navigation options like Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices. The main content area displays a table of rule evaluations with the following data:

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Applicable	Category
Version: Controller with not recommen...	Critical	25	25	0	0	0	Wireless
Security: It is recommended to monito...	Critical	25	25	0	0	0	Wireless
Security: WLAN may be using manage...	Critical	25	25	0	0	0	Wireless
NTP: NTP Polling Interval is set, but no ...	High	25	25	0	0	0	Wireless
ROMMON Password-Recovery Config...	High	302	4	0	17	281	Security
IPsec Transform-Set AES-256 Encrypt...	High	302	0	0	17	285	Security
802.1X Authentication on Access Ports	High	302	0	0	0	302	LAN swit
RRM: ED-RRM is not in use. It is recom...	High	25	25	0	0	0	Wireless
Security: It is recommended to disable...	High	25	25	0	0	0	Wireless
Security: Minimum management pass...	High	25	25	0	0	0	Wireless

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.

 Note: 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 displays the Cisco IQ Configuration Assessment interface. The top navigation bar includes the Cisco IQ logo and user profile. The left sidebar contains menu items: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Configuration Assessment' and shows a rule titled 'Version: Controller with not recommended code ver...'. Below the title, it indicates the rule was evaluated on 'Apr 24, 2026, 10:41 AM'. The 'About the Rule' section provides a description and key metrics: Severity (Critical), Category (Wireless), Software type (AireOS), and Assets evaluated (25). A 'Results Summary' section shows 0 Passed, 25 Did not pass, 0 Inconclusive, and 0 Not applicable. The 'Asset Results' section features a search bar, filters, and a table with columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The table shows three rows, all with a 'Did not pass' result.

Avaliação

- Sobre a regra: Fornece detalhes sobre uma regra como Severidade, Categoria, Tipo de software e Ativos avaliados e inclui links para documentação relevante da origem
- 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


Exportação de Resultados de Ativo

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

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.

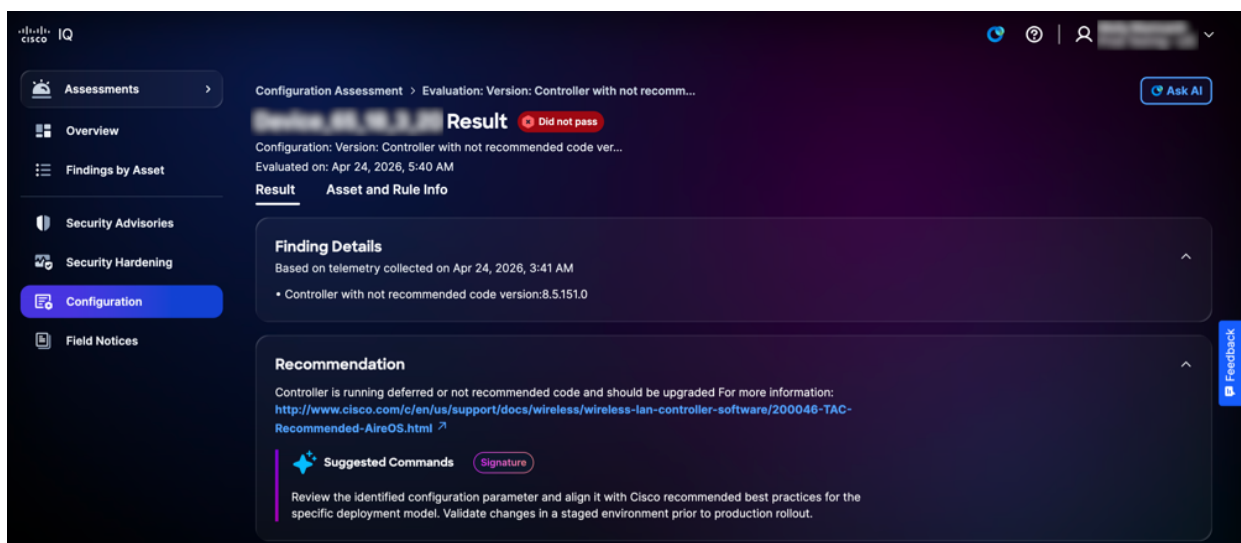
 Note: Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

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.

- 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

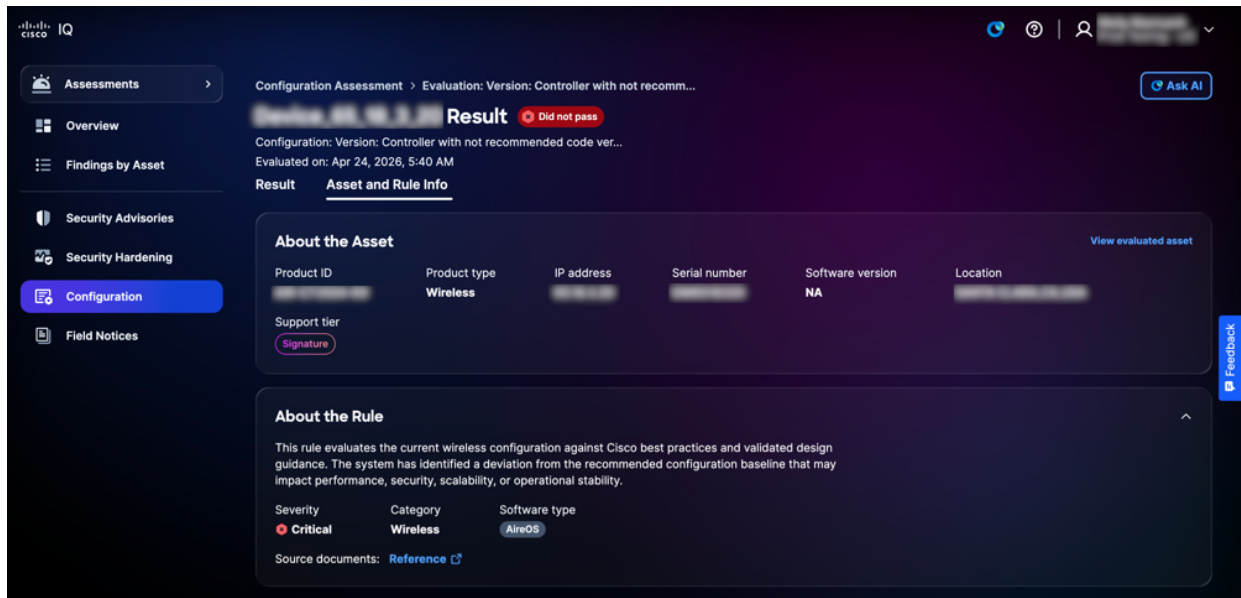


Camada de Assinatura de Configuração

- Camada de Assinatura
 - Localizando detalhes: Fornece informações sobre os desvios de configuração identificados durante a avaliação, juntamente com registros de evidências
 - Recomendação: Fornece orientação acionável em nível de dispositivo com trechos de código 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.



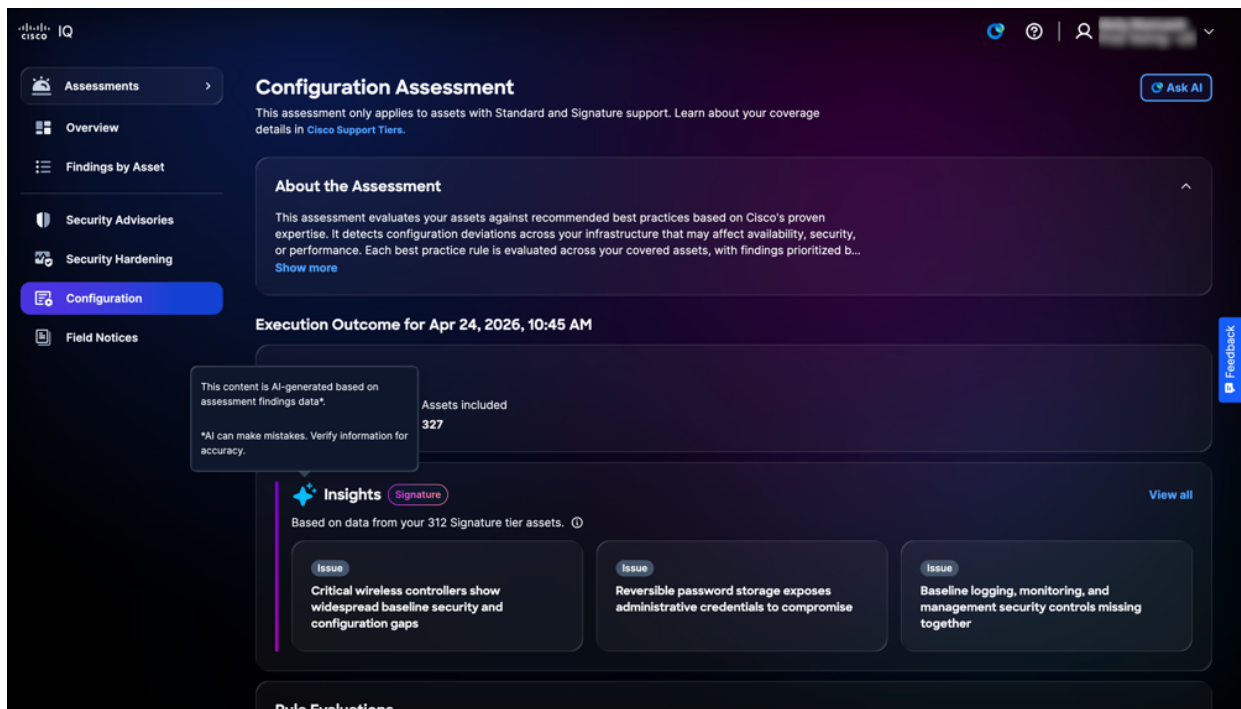
Informações sobre ativos e regras

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

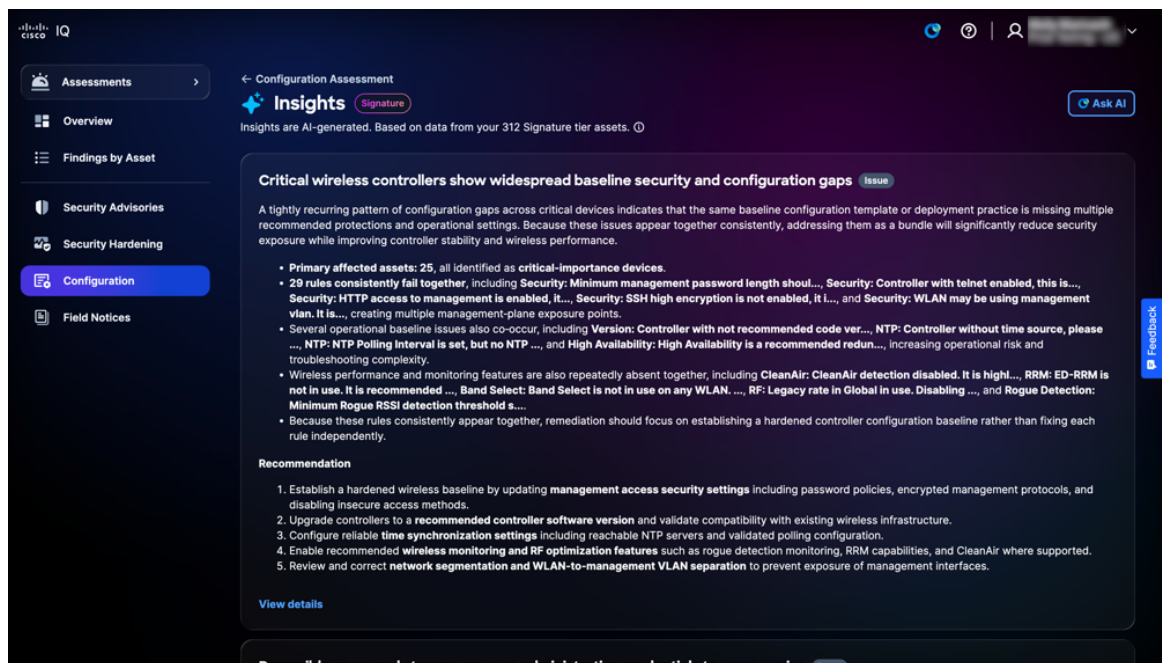
Os insights são gerados por IA e servem como um painel inteligente que sintetiza dados de avaliação em cartões-chave priorizados, destacando as disparidades de configuração críticas em várias descobertas. Ele permite que você enfrente com eficiência os riscos de infraestrutura mais impactantes, concentrando-se 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

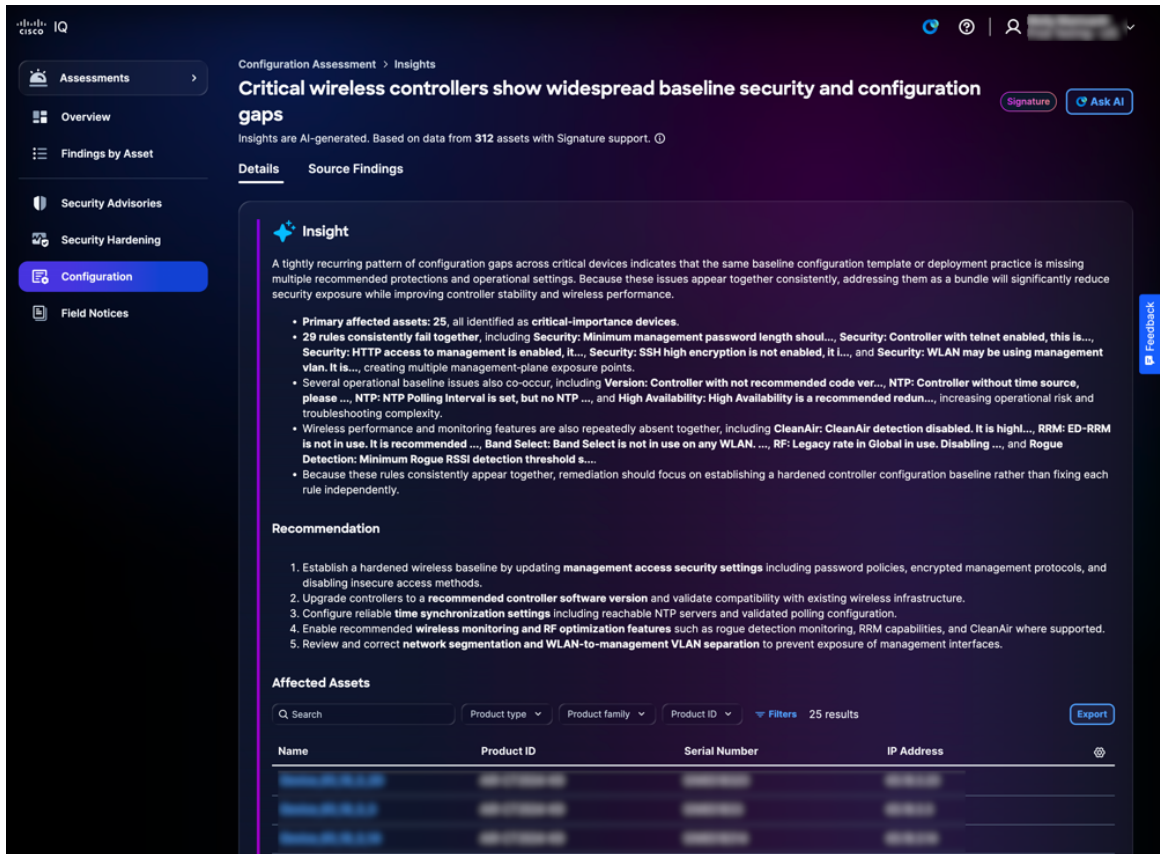
Para exibir detalhes do Insights:

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



Página Insights

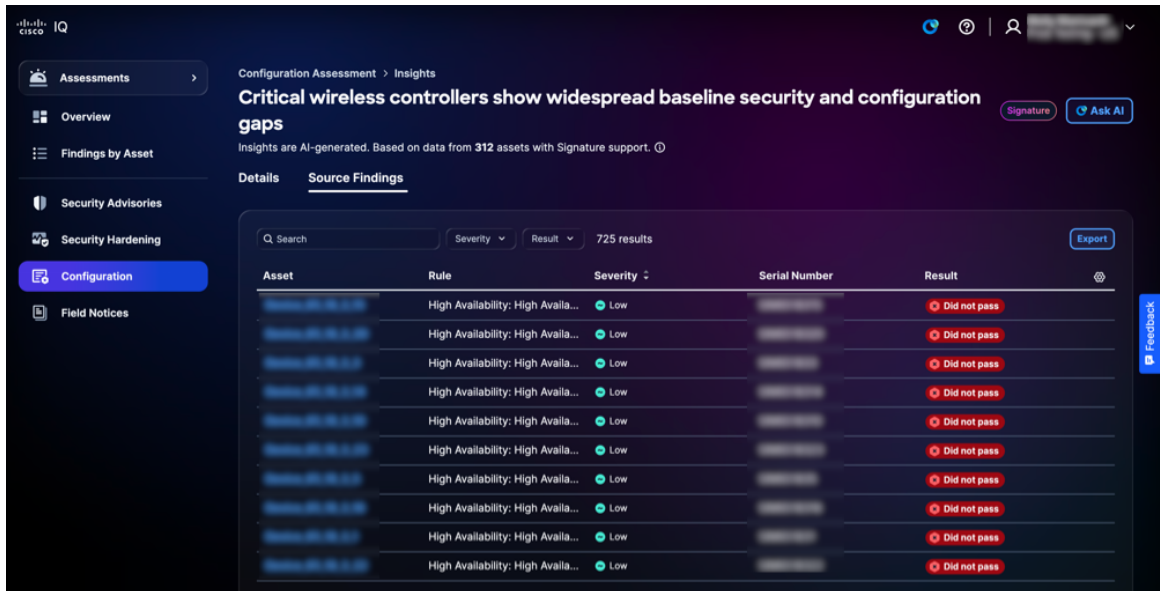
2. Clique em Exibir detalhes. A página de detalhes Insights é exibida com as seguintes informações: Você também pode clicar em qualquer cartão para abrir a página detalhada.



Detalhes dos Insights


- **Informações:** Fornecer um resumo que destaque os padrões recorrentes de desvios de configuração identificados por meio de uma análise abrangente em várias descobertas, bem como as áreas de excelência em sua infraestrutura em que 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 fonte exibe as descobertas individuais detalhadas que suportam suas percepções.



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.

Field Notices

About the Assessments

These assessments evaluate your assets against Cisco Field Notices published for significant non-security related product issues to prevent or mitigate incidents.

Field Notice Assessments With Vulnerabilities Detected

Search: [] Severity: [] Last updated: [] Tags: [] 54 results [Export]

Insights: 5 field notices are classified as **Critical impact**, signaling a risk of service downtime if unaddressed. Review these notices to apply recommended ...

3 field notices are rated **High impact**, indicating potential product degradation. Schedule maintenance to apply available fixes and mitigate operational risk.

Assessment	Severity	Assets at Risk	Assets Potentially at Risk
FN72464 - Cisco Nexus 9300 Switches an...	Critical	3	0
FN74267 - Cisco NCS-55A2 and NCS-57C...	Critical	0	1
FN74350 - Cisco Unified Border Element: L...	Critical	0	214
FN74222 - Full or Partial Cisco 9800 Serie...	Critical	0	5
FN74223 - Some Cisco NCS 540 Series Me...	Critical	0	3
FN63942 - Cisco Wireless Lightweight Ac...	High	0	54
FN74287 - New Memory Component Intro...	High	0	1
FN74353 - Cisco Network Convergence Sy...	High	0	1
FN74148 - PAK and RTU Licenses Cannot ...	Medium	0	6

Field Notices

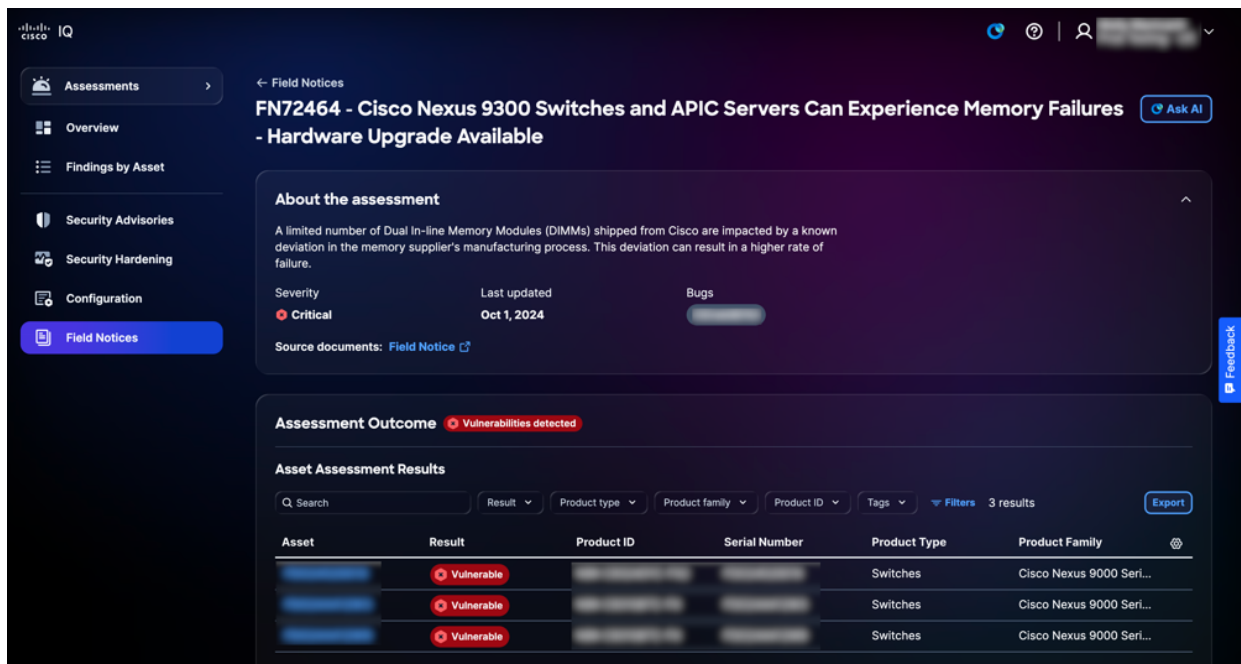
Pesquisando e Filtrando Views para Avisos de Campo

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 de ativos são exibidos:

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




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.

 Note: Há filtros diferentes disponíveis, dependendo de suas funções e permissões.

Exportando Resultados de Ativo de Avaliação 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 sobre exportação.

Exibindo Resultados de Ativo de Avaliação para Avisos de Campo

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

Aplicativo de suporte

O aplicativo Suporte oferece uma visão consolidada dos casos de atendimento ao cliente. 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 acessar o aplicativo Support no Cisco IQ, selecione Home > Support. A página Visão geral do suporte é exibida.

Visão geral do suporte



Visão geral do suporte

A página Visão geral do suporte é um painel interativo de gráficos com as seguintes informações:

- Casos abertos por gravidade: Todos os casos abertos nos últimos 90 dias categorizados por

gravidade de S1 a S4

- Casos abertos por status de caso: Todos os casos abertos nos últimos 90 dias categorizados por status do caso
- RMAs por status: Todas as RMAs dos últimos 90 dias categorizadas por seu status
- Casos fechados por gravidade: O número total de casos fechados dos últimos 90 dias categorizados por gravidade

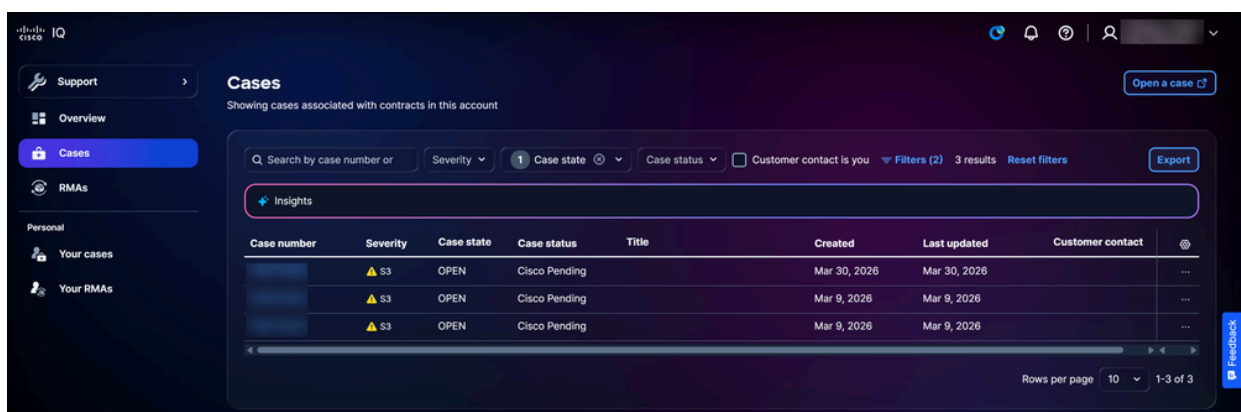
Exibindo detalhes de casos

Clicar em Exibir detalhes redireciona a página para a página Casos da conta. Clicar em uma barra de um gráfico na página Visão geral redireciona a página para a página Casos da conta com filtros relevantes aplicados. Por exemplo, clicar na barra de gravidade S1 no gráfico Open Cases by Severity redireciona para a página Cases da conta com Case status definido como "Open" e Severity definido como "S1". Consulte [Casos](#) para obter mais informações.

Casos

Casos de conta

Navegue até a página Cases clicando em Cases no painel esquerdo.



The screenshot shows the Cisco IQ interface for the 'Cases' page. The page title is 'Cases' and it indicates 'Showing cases associated with contracts in this account'. There is a search bar and several filters: Severity (set to S3), Case state (set to OPEN), Case status (set to Cisco Pending), and Customer contact is you (unchecked). The table below shows 3 results. The table has columns for Case number, Severity, Case state, Case status, Title, Created, Last updated, and Customer contact. The first row shows a case with Severity S3, Case state OPEN, Case status Cisco Pending, and Created on Mar 30, 2026. The second and third rows show cases with Severity S3, Case state OPEN, Case status Cisco Pending, and Created on Mar 9, 2026. The page also includes an 'Export' button and a 'Feedback' button.

Case number	Severity	Case state	Case status	Title	Created	Last updated	Customer contact
	▲ S3	OPEN	Cisco Pending		Mar 30, 2026	Mar 30, 2026	
	▲ S3	OPEN	Cisco Pending		Mar 9, 2026	Mar 9, 2026	
	▲ S3	OPEN	Cisco Pending		Mar 9, 2026	Mar 9, 2026	

Casos

A página Casos exibe uma lista consolidada de todos os casos associados aos contratos em sua conta do Cisco IQ. Você pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar. As colunas Case number, Severity, Case state, Case status, Title e Created sempre são exibidas e não podem ser desmarcadas.

Ações disponíveis

As ações a seguir podem ser executadas na página Casos:

- Abra um caso: Clique em Abrir um caso para abrir o [SCM](#) e criar um caso
- Exportar dados: Clique em Exportar para baixar todos os dados exibidos atualmente no painel como um arquivo CSV
- Exibir detalhes do caso: Clique em um número de caso ou em uma linha de tabela para abrir a visualização detalhada de um caso (consulte [Visualizações de detalhes do caso](#) para obter mais informações)
- Fechar um caso: Escolha o ícone More Options de um caso aberto > Close case para abrir a janela Close case, onde você pode fornecer um motivo para o fechamento e fechar o caso
- Reabrir um caso: Escolha o ícone More Options de um caso fechado > Reopen case para abrir a janela Reopen case, onde você pode fornecer um motivo para a reabertura e abrir o caso

 Note: Os casos encerrados podem ser reabertos no prazo de 14 dias após o encerramento.

Filtrando exibições de casos

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou marcando a caixa de seleção Contato do cliente é você. Opcionalmente, clique em Filtros e escolha na lista de opções de filtro disponíveis. Os filtros e as seleções persistem nas sessões e nos logons para personalizar o painel. Os filtros padrão aplicados são:

- Estado do caso: Aberto
- Criado: Criado em 90 dias

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

Seus casos

Navegue até a página Your Cases (Seus casos) clicando em Your cases (Seus casos) no painel esquerdo.

The screenshot shows the 'Your cases' page in Cisco IQ. The page title is 'Your cases' and it includes a sub-header 'Includes all cases you are authorized to view.' There is a search bar and several filters: 'Severity', 'Case state' (set to 1), 'Case status', and 'Customer contact is you'. There are 9 results and a 'Reset filters' button. An 'Export' button is also present. The table below shows the details of the cases.

Case number	Severity	Case state	Case status	Title	Created	Last updated	Customer contact	
	▲ S3	OPEN	Cisco Pending		Apr 11, 2026	Apr 13, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 8, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 29, 2026	Apr 2, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 27, 2026	Mar 4, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Jan 30, 2026		...

At the bottom right of the table, it says 'Rows per page 30' and '1-9 of 9'.

Seus casos

A página Your Cases (Seus casos) exibe uma lista consolidada de casos que você está autorizado a visualizar e gerenciar. Você pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar. As colunas Case number, Severity, Case state, Case status, Title e Created sempre são exibidas e não podem ser desmarcadas.

Ações disponíveis

As ações a seguir podem ser executadas na página Seus casos:

- Abra um caso: Abra um caso: Clique em Abrir um caso para abrir o SCM e criar um caso
- Exportar dados: Clique em Exportar para baixar todos os dados exibidos atualmente no painel como um arquivo CSV
- Exibir detalhes do caso: Clique em um número de caso ou em uma linha de tabela para abrir a visualização detalhada de um caso (consulte [Visualizações de detalhes do caso](#) para obter mais informações)
- Fechar um caso: Escolha o ícone More Options de um caso aberto > Close case para abrir a janela Close case, onde você pode fornecer um motivo para o fechamento e fechar o caso
- Reabrir um caso: Escolha o ícone More Options de um caso fechado > Reopen case para abrir a janela Reopen case, onde você pode fornecer um motivo para a reabertura e abrir o caso

 Note: Os casos encerrados podem ser reabertos no prazo de 14 dias após o encerramento.

Filtrando exibições para seus casos

Você pode filtrar a exibição de lista escolhendo um filtro nas listas suspensas ou marcando a caixa de seleção Contato do cliente é você. Opcionalmente, clique em Filtros e escolha na lista de opções de filtro disponíveis. Os filtros e as seleções persistem nas sessões e nos logons para personalizar o painel. Os filtros padrão aplicados são:

- Estado do caso: Aberto
- Caixa de seleção O contato do cliente é você
- Criado: Criado em 90 dias

 Note: Alguns filtros podem ficar ocultos, dependendo das configurações de zoom da tela.

Exibições de detalhes do caso

Para visualizar os detalhes de um caso, clique em um caso na lista.

Exibição de detalhes do caso

A visualização de detalhes do caso é exibida e fornece uma visualização centralizada de um caso de suporte, permitindo que você revise as informações do caso, as informações de ativos afetados, rastreie o progresso do TAC e acesse as ações de caso disponíveis. As ações disponíveis incluem reabrir um caso fechado clicando em Reabrir caso, fechar um caso aberto clicando em Fechar caso e iniciar o AI Assistant com o contexto do caso clicando em Perguntar IA. As guias disponíveis estão descritas nas seções abaixo.

 Note: Os campos que são gerados por AI são rotulados com um ícone Estrela quando aplicável.

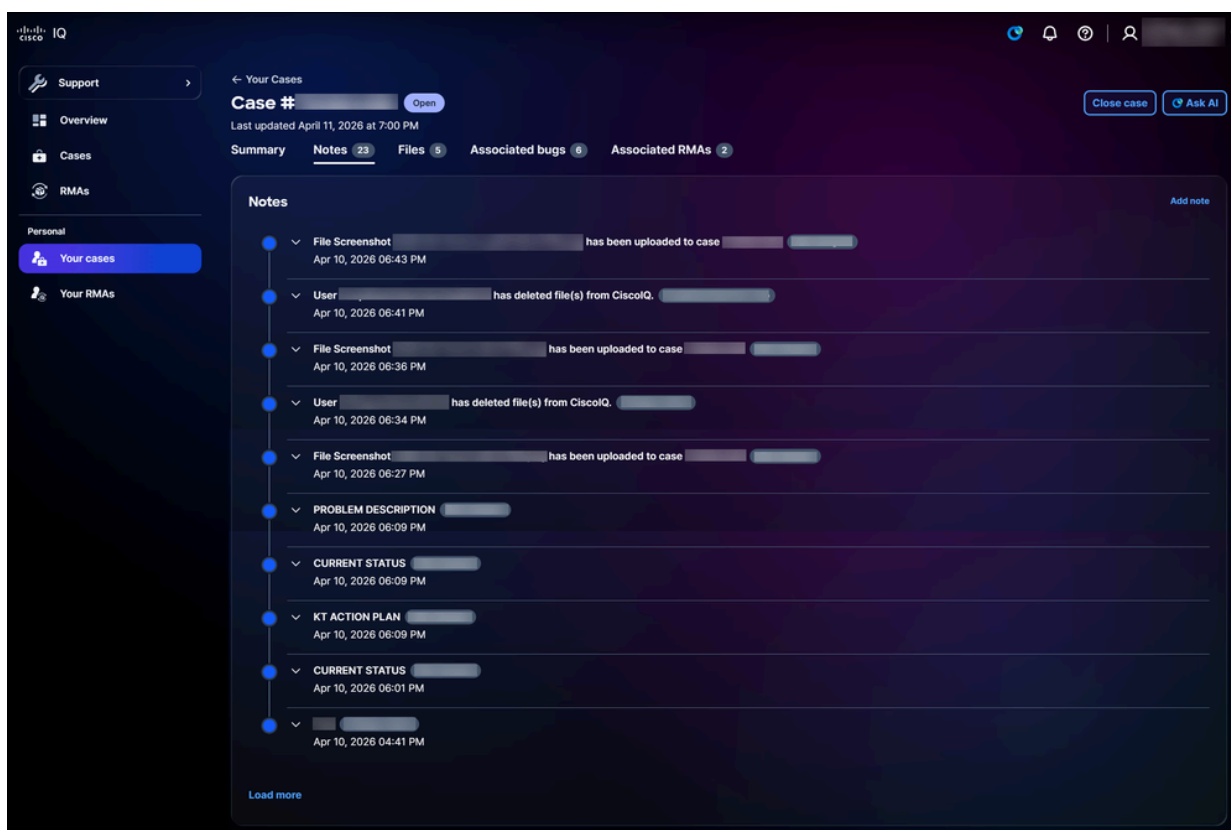
Insights : For 11 entitled cases with Severity 4, configuration assistance is the leading issue, accounting for 6 instances (54.5%). Prioritize training or documentation updates to reduce...
 • Among 9 open entitled cases, installation, uninstallation, or upgrade issues represent 33.3% (3 cases) of the workload. Review deployment workflows to streamline these processes.

Ícone de estrela

Summary

A guia Resumo exibe informações importantes sobre o caso, permitindo que você compreenda rapidamente o estado atual, o contexto e o progresso de um caso de suporte individual. Você pode revisar os detalhes do caso e os ativos afetados, monitorar o ciclo de vida do seu caso por meio dos detalhes do progresso do TAC, modificar as informações de contato e especificar endereços de e-mail para receber notificações de atualização do caso. Somente os campos selecionados são editáveis.


Notas



Notas

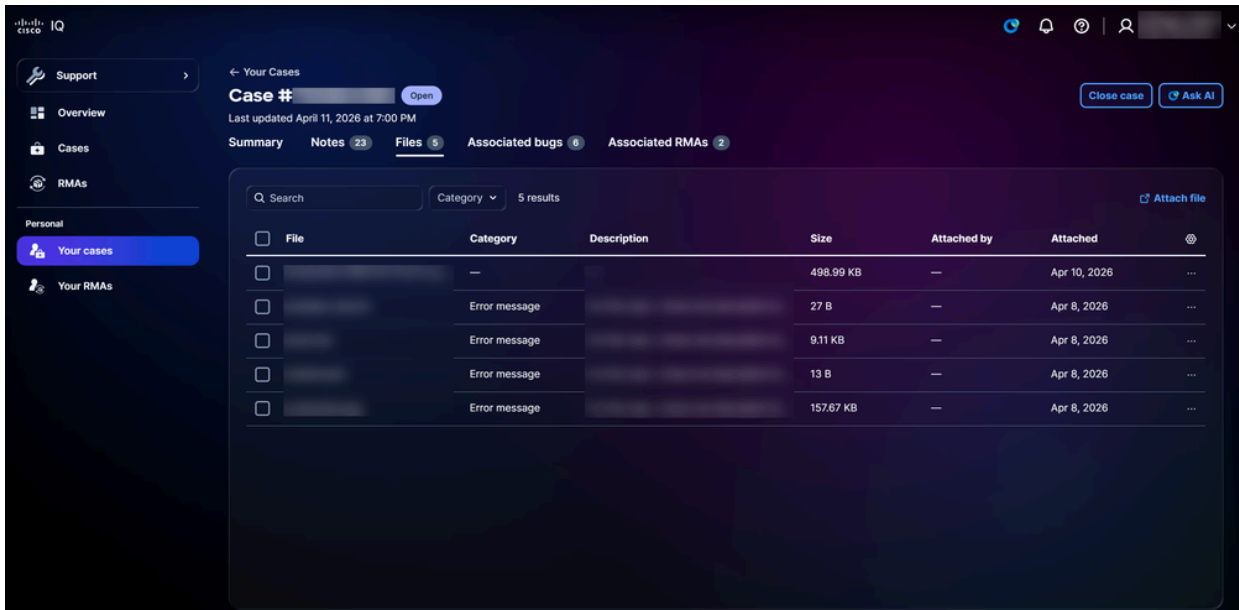
Clicar na guia Notas abre a página Notas. Você pode visualizar todas as notas associadas a um caso, independentemente de terem sido enviadas por um cliente ou por um engenheiro da Cisco.

Para adicionar uma nova nota:

 aviso: As notas não podem ser excluídas.

1. Clique em Add note. A janela Adicionar nota é aberta.
2. Insira um Título.
3. Insira os Detalhes.
4. Clique em Add.

Arquivos




Arquivos

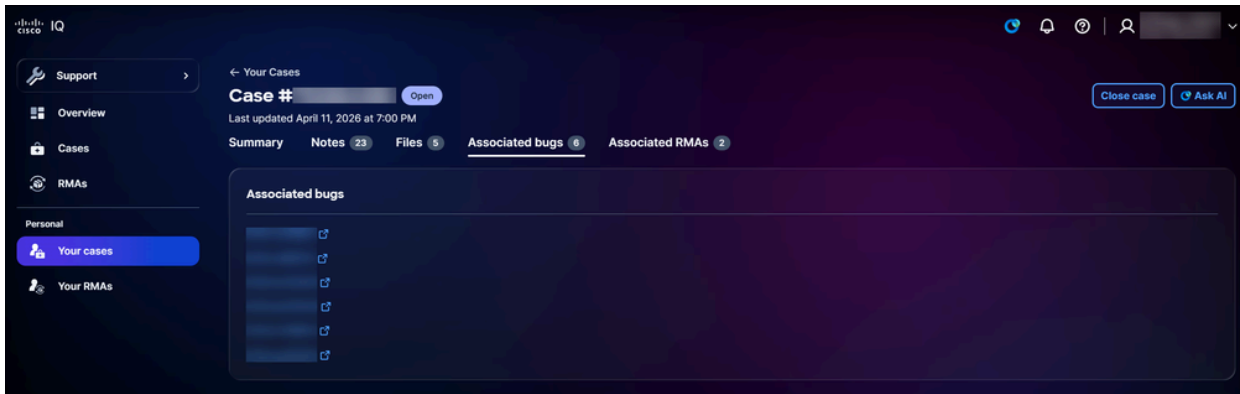
Clicar na guia Arquivos abre a página Arquivos. Você pode visualizar o nome, o tamanho e a data dos arquivos de um caso, bem como adicioná-los ou excluí-los. Filtre arquivos selecionando uma opção na lista suspensa Categoria. Opcionalmente, clique em Filtros e escolha entre as opções de filtro disponíveis. Você também pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar.

Para adicionar um arquivo, clique em Anexar arquivo. Você é redirecionado para o SCM, onde pode carregar um arquivo para o caso.

Para excluir um arquivo, marque as caixas de seleção dos arquivos desejados e clique em Excluir. A janela Excluir arquivo(s) se abre. Clique em Excluir arquivo(s).

 Note: Não há suporte para downloads de arquivo.

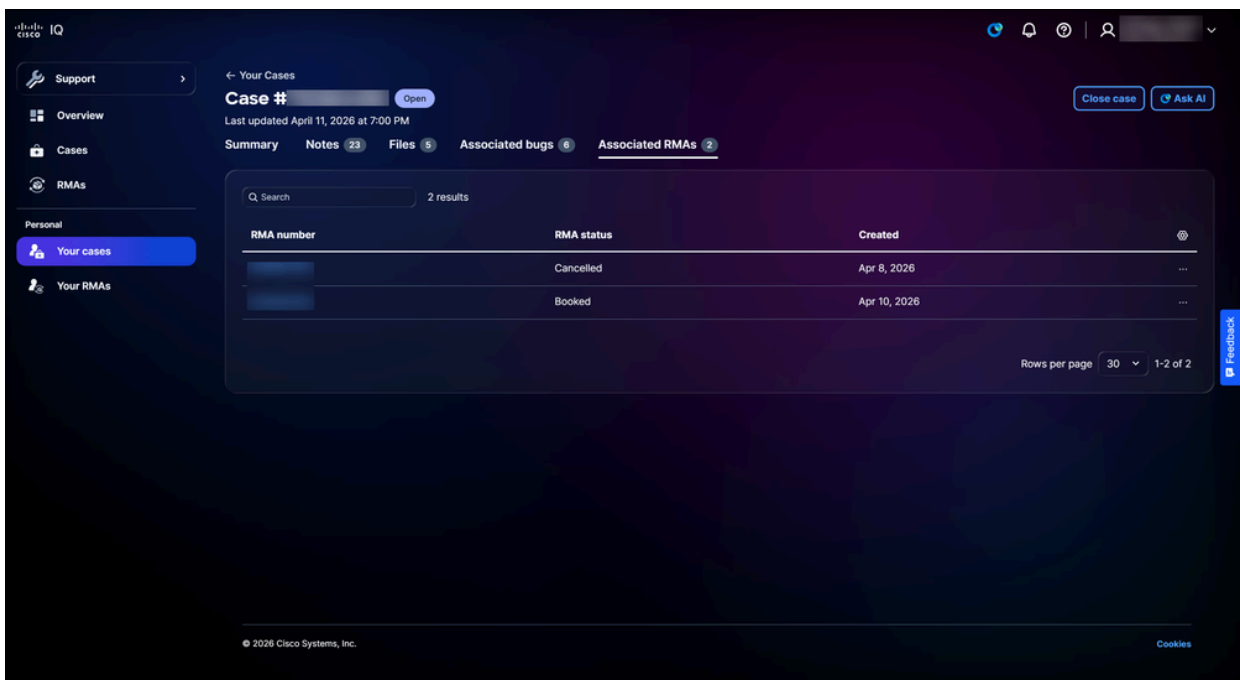
Bugs associados



Bugs associados

Clicar na guia bugs associados abre a página bugs associados. Você pode clicar na ID de um bug para executar o lançamento cruzado de informações detalhadas de bug na [Bug Search Tool](#) do Cisco.com.

RMAs associadas



RMAs associadas

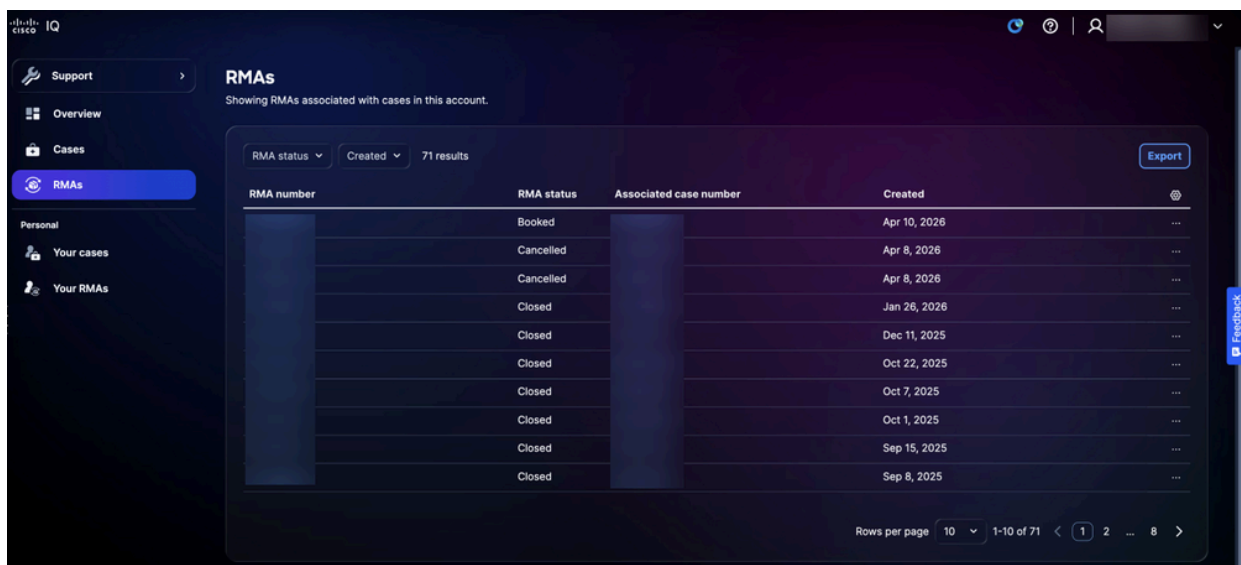
Clicar na guia RMAs Associadas abre a página RMAs Associadas. Você pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar. As ações a seguir podem ser executadas na página RMAs Associadas:

- Fechar um caso: Clique em Fechar caso para abrir a janela Fechar caso, onde você pode fornecer um motivo para o fechamento e fechar o caso

- Exibir detalhes da RMA: Clique em um número de RMA ou na linha da tabela para abrir uma visualização detalhada da RMA (consulte [Visualizações dos detalhes da RMA](#) para obter mais informações)
- Entre em contato com a Cisco Logistics: Escolha o ícone Mais Opções de uma linha > Entre em contato com a logística da Cisco para entrar em contato com a equipe de logística da Cisco

RMA's

RMA's da conta



The screenshot shows the Cisco IQ interface for RMA's. The left sidebar has a navigation menu with 'Support', 'Overview', 'Cases', and 'RMA's' (highlighted). The main content area is titled 'RMA's' and shows 'Showing RMA's associated with cases in this account.' Below this, there are filters for 'RMA status' and 'Created', and a count of '71 results'. An 'Export' button is visible in the top right. The table below has the following columns: 'RMA number', 'RMA status', 'Associated case number', and 'Created'. The table contains 10 rows of data.

RMA number	RMA status	Associated case number	Created
	Booked		Apr 10, 2026
	Cancelled		Apr 8, 2026
	Cancelled		Apr 8, 2026
	Closed		Jan 26, 2026
	Closed		Dec 11, 2025
	Closed		Oct 22, 2025
	Closed		Oct 7, 2025
	Closed		Oct 1, 2025
	Closed		Sep 15, 2025
	Closed		Sep 8, 2025

At the bottom of the table, there is a pagination control showing 'Rows per page' set to 10, and '1-10 of 71' results, with page numbers 1 and 2 visible.

Lista de RMA's

Navegue até a página RMA's clicando em RMA's no painel esquerdo. A página RMA's exibe uma lista consolidada de todas as RMA's associadas aos casos em sua conta do Cisco IQ. Você pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar.

Ações disponíveis

As seguintes ações podem ser executadas na página RMA's:

- Exportar dados: Clique em Exportar para fazer download de todos os dados exibidos atualmente como um arquivo CSV
- Exibir detalhes da RMA: Clique em um número de RMA ou na linha da tabela para abrir uma visualização detalhada da RMA (consulte [Visualizações dos detalhes da RMA](#) para obter

mais informações)

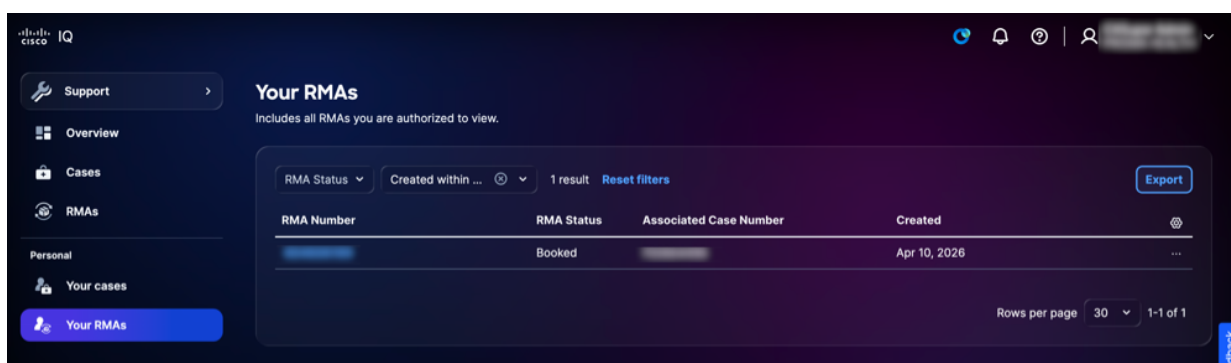
- Entre em contato com a Cisco Logistics: Escolha o ícone Mais Opções de uma linha > Entre em contato com a logística da Cisco para entrar em contato com a equipe de logística da Cisco

Filtragem de exibições para RMAs de conta

Você pode filtrar a exibição de lista escolhendo filtros nas listas suspensas.

Seus RMAs

Navegue até a página Suas RMAs clicando em Suas RMAs no painel à esquerda.



Seus RMAs

A página Suas RMAs exibe uma lista consolidada de RMAs que você tem os direitos necessários para visualizar e gerenciar. Você pode configurar as colunas exibidas na lista clicando no ícone Configurações, marcando as caixas de seleção das colunas desejadas e clicando em Aplicar.

Ações disponíveis

As seguintes ações podem ser executadas na página Suas RMAs:

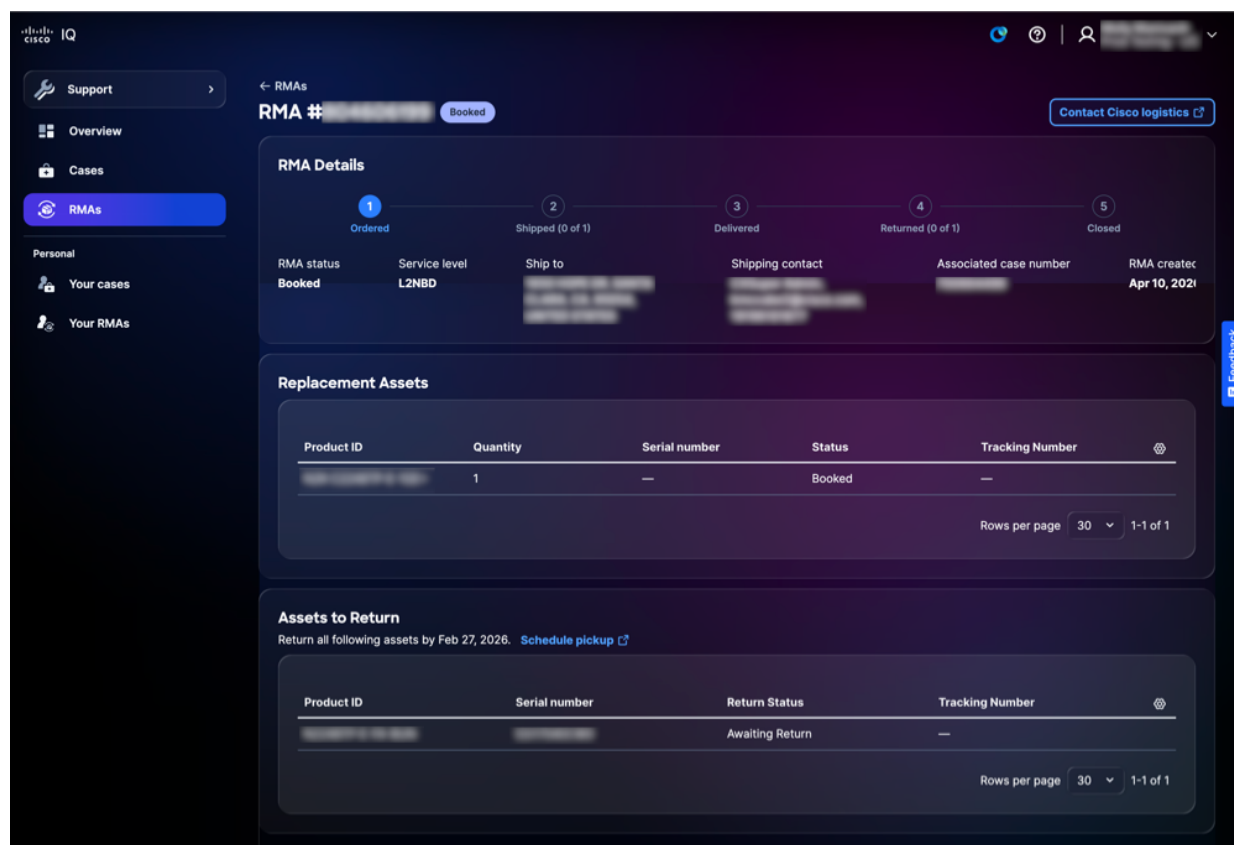
- Exportar dados: Clique em Exportar para fazer download de todos os dados exibidos atualmente como um arquivo CSV
- Exibir detalhes da RMA: Clique em um número de RMA ou na linha da tabela para abrir uma visualização detalhada da RMA (consulte [Visualizações dos detalhes da RMA](#) para obter mais informações)
- Entre em contato com a Cisco Logistics: Escolha o ícone Mais Opções de uma linha > Entre em contato com a logística da Cisco para entrar em contato com a equipe de logística da

Cisco

Filtragem de exibições para suas RMAs

Você pode filtrar a exibição de lista escolhendo uma opção na lista suspensa Criado.

Exibições de detalhes da RMA



Exibição de detalhes da RMA


A visualização dos detalhes da RMA oferece uma visualização centralizada de uma RMA, permitindo que você revise as informações da RMA, rastreie o progresso e acesse as ações de RMA disponíveis. As ações disponíveis incluem entrar em contato com a equipe de logística da Cisco, acessar números de rastreamento e agendar captações de ativos.

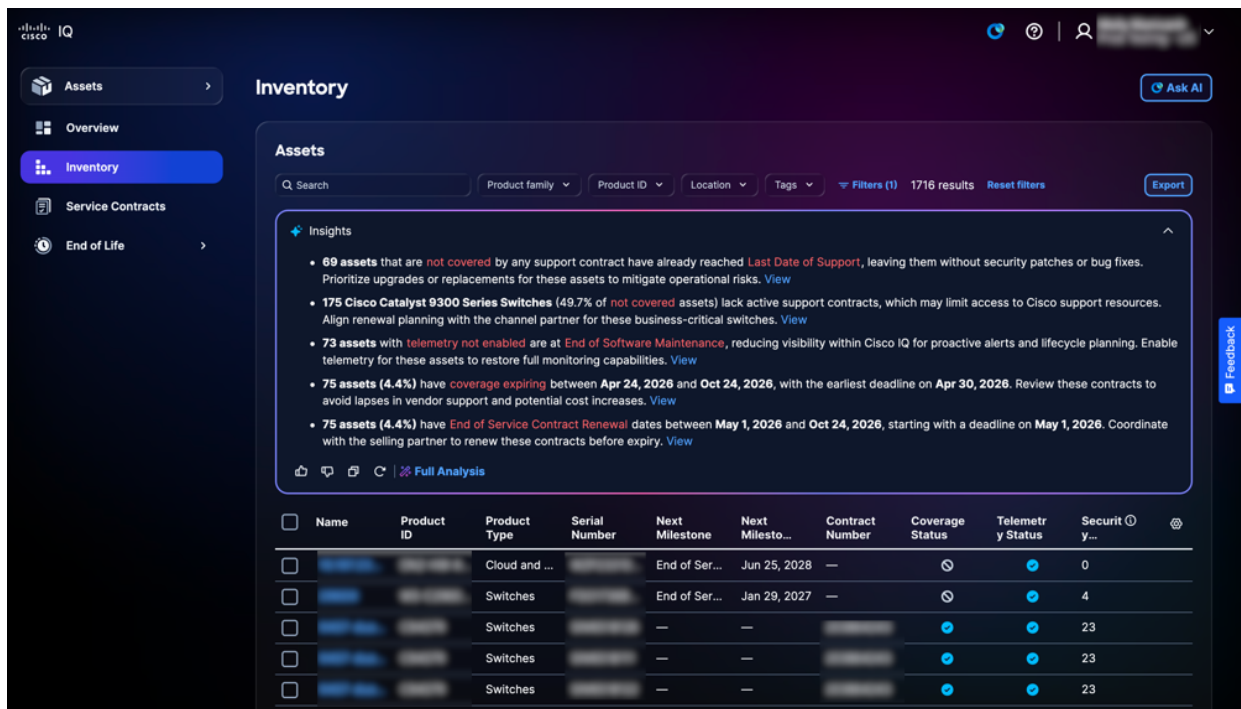
Recursos comuns de aplicativos

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.



The screenshot displays the Cisco IQ Inventory Insights panel. The top section, titled 'Insights', contains five bullet points detailing asset issues: 69 assets not covered by support contracts, 175 Cisco Catalyst 9300 Series Switches lacking active support contracts, 73 assets with telemetry not enabled, 75 assets with coverage expiring between Apr 24, 2026 and Oct 24, 2026, and 75 assets with End of Service Contract Renewal dates between May 1, 2026 and Oct 24, 2026. Below the insights is a table with columns: Name, Product ID, Product Type, Serial Number, Next Milestone, Next Milestone Date, Contract Number, Coverage Status, Telemetry Status, and Security. The table lists several assets, including Cloud and Switches, with their respective details.

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

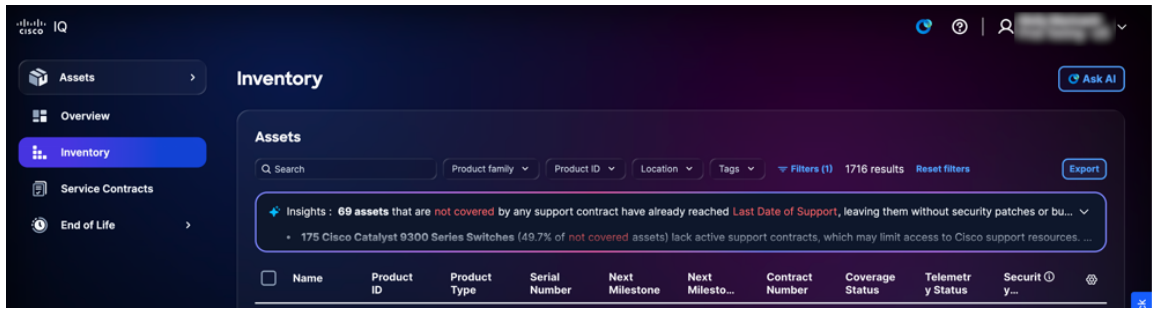
Exportando informações

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.

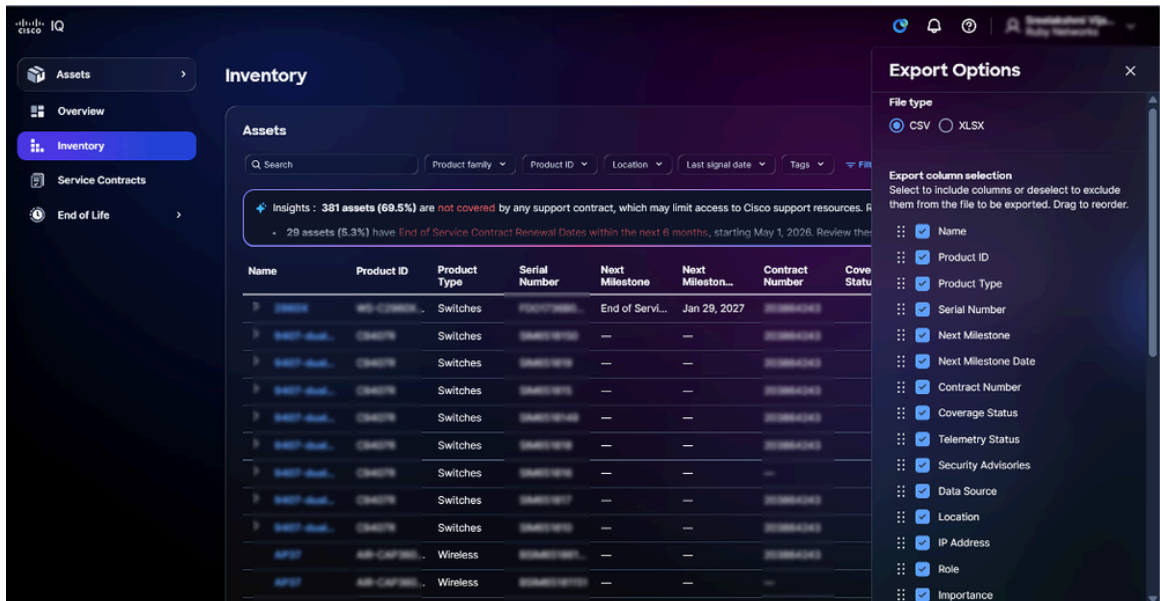
Para exportar informações de uma página:

1. Navegue até a página.



Exportação de Inventário no Aplicativo Ativos

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



Opções de exportação

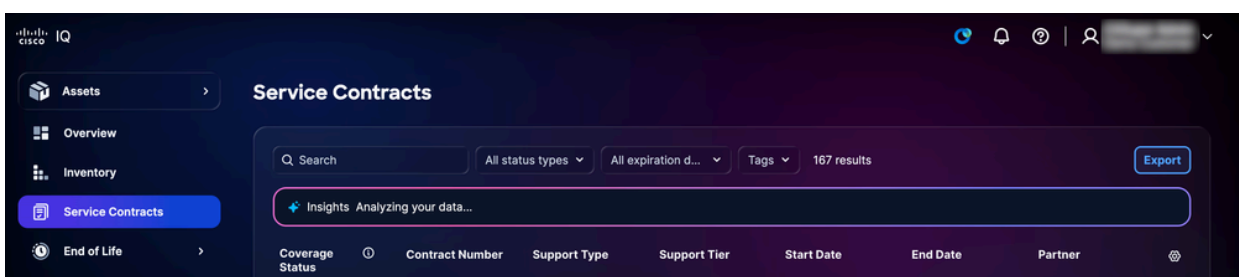
3. Selecione um tipo de arquivo.

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.

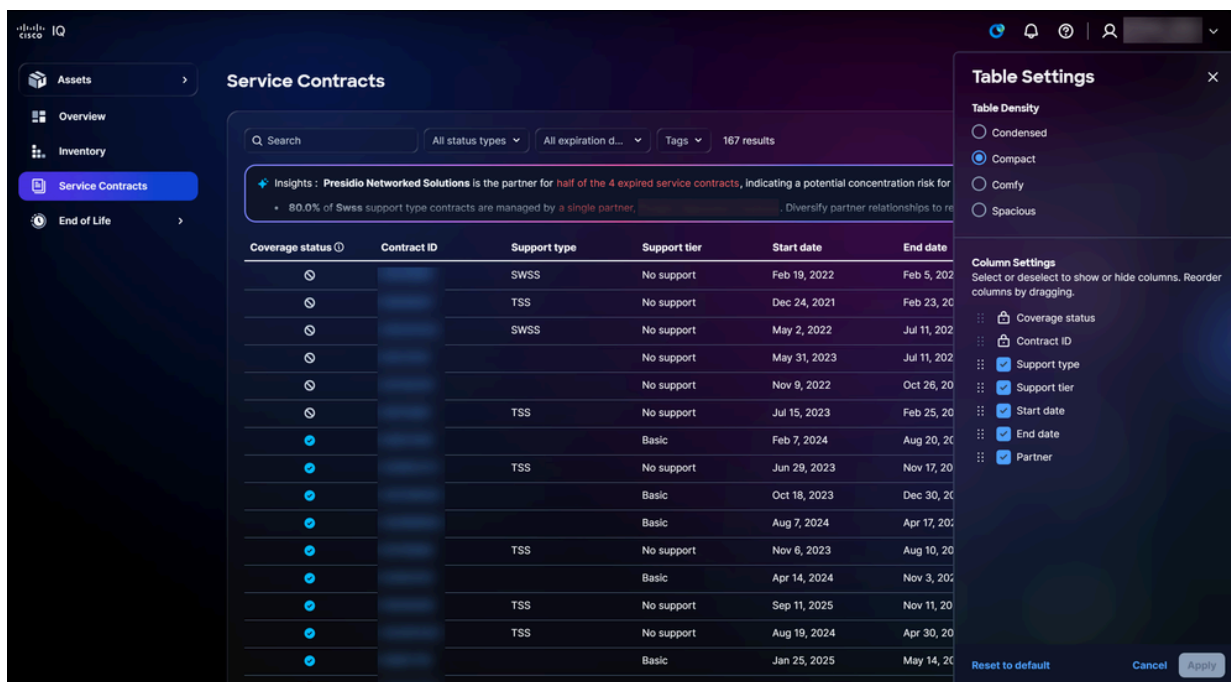
Configurações da tabela

Você pode definir configurações de tabela para criar exibições personalizadas e refinadas para diferentes recursos do aplicativo.



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.

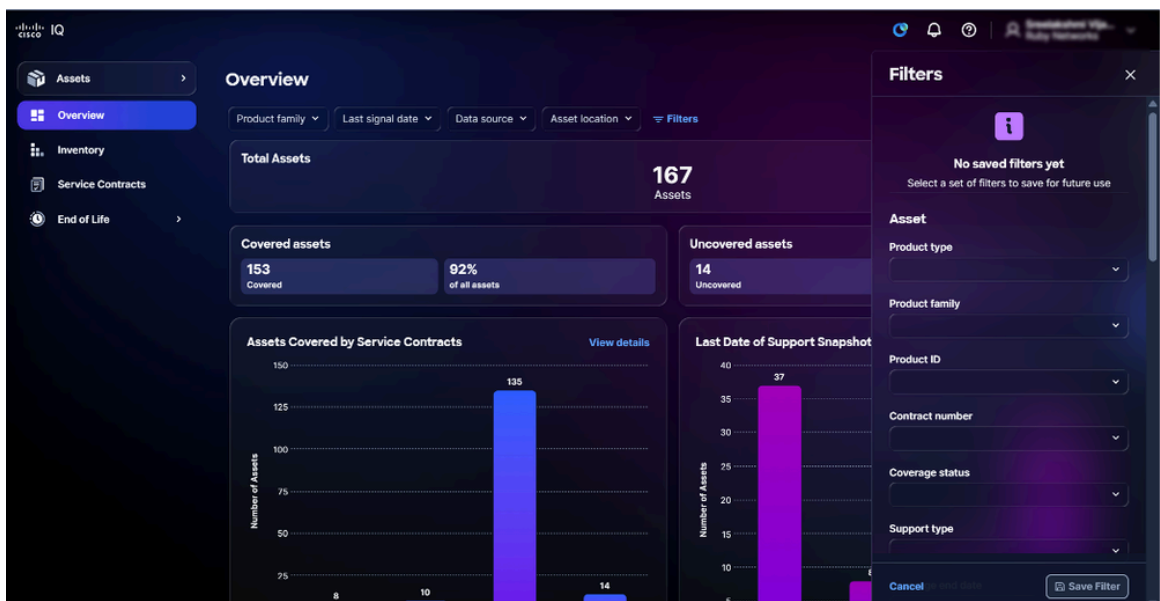
Personalização de filtros

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

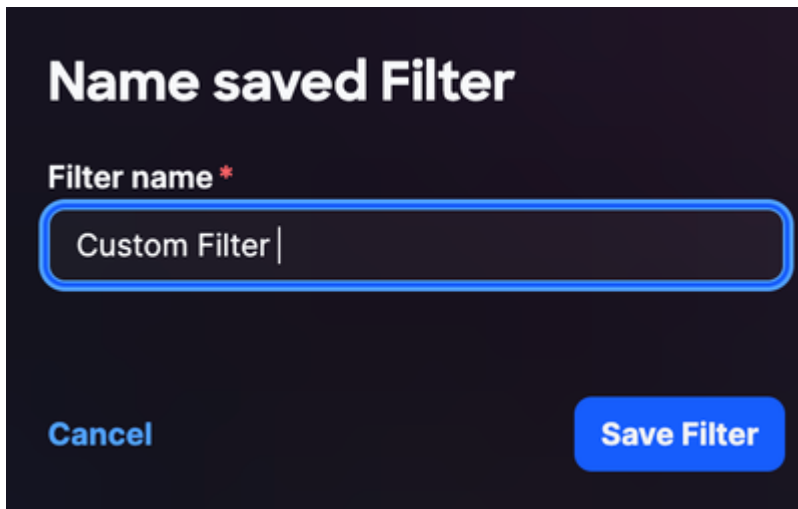
Para criar um filtro personalizado:

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



Filtros

- Escolha os filtros desejados nas listas suspensas.
- Clique em Save Filter. A janela Filtro de nome salvo é aberta.



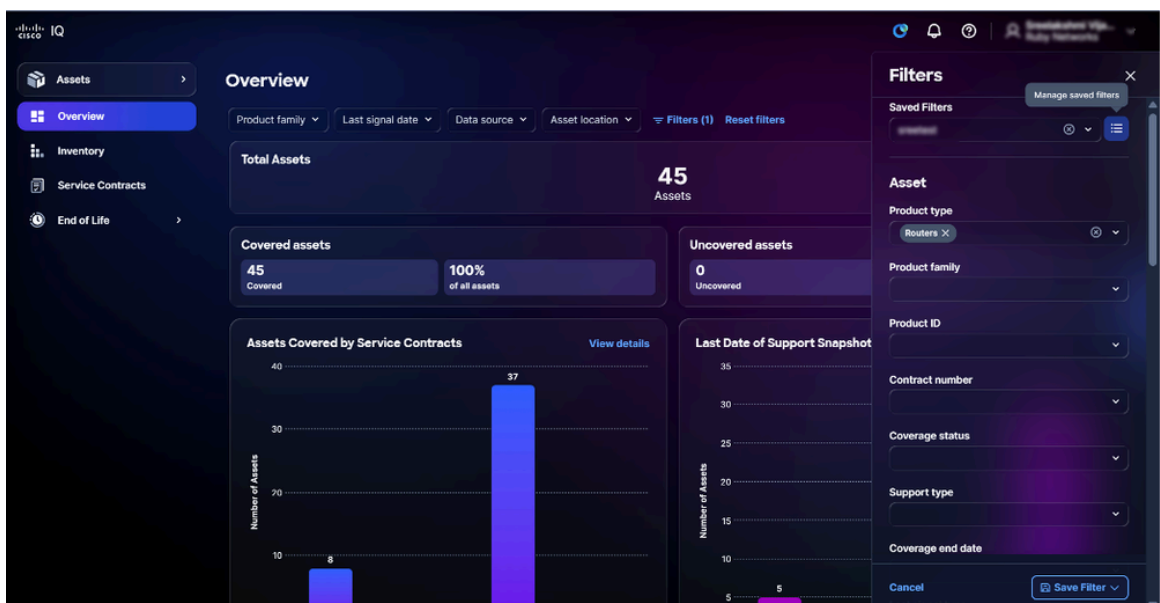
Nome do filtro

- Insira um nome de filtro.
- Clique em Save Filter para confirmar.

Edição de um nome de filtro

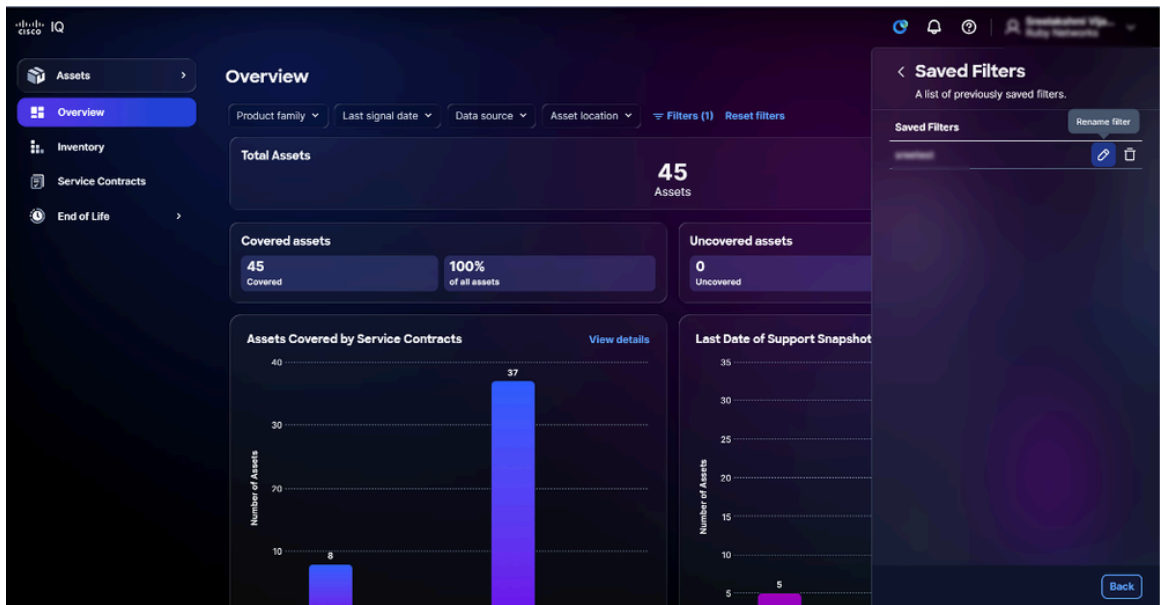
Para editar um filtro personalizado:

- Clique em Filtros.



Gerenciar filtros salvos

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



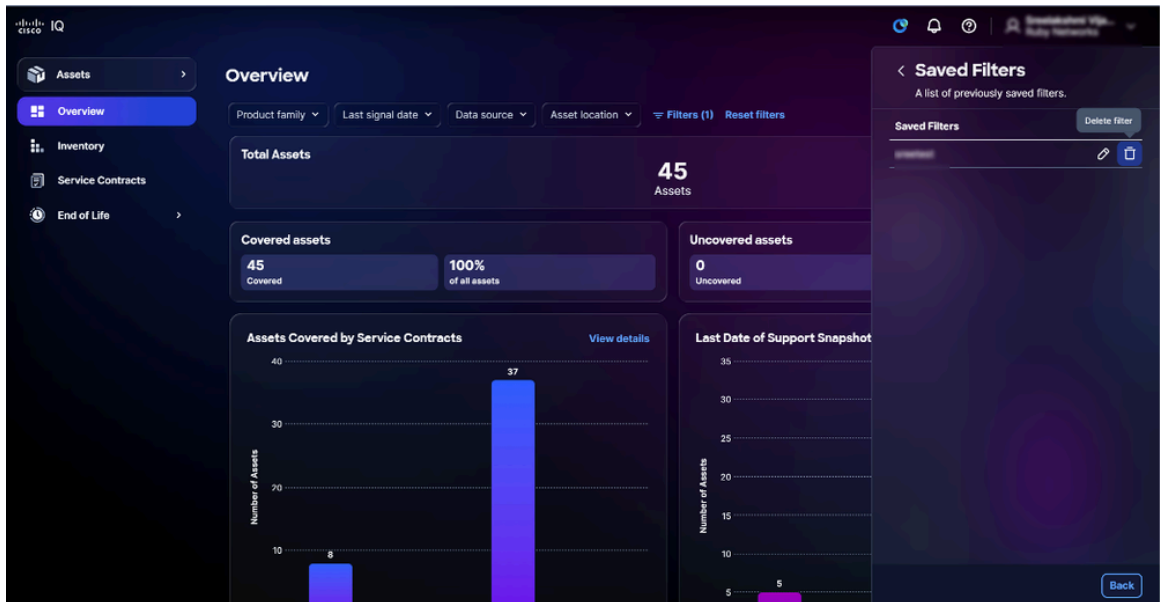
Editar filtro

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.
5. Clique em Sim, excluir para confirmar.

Assistente de AI


Overview

O Cisco IQ AI Assistant foi projetado para melhorar a compreensão e o uso do Cisco IQ, transformando dados brutos em insights práticos, recomendações e ações guiadas. Ele se integra a ferramentas existentes, onde aproveita fontes de dados individuais e sintetiza inteligência em vários fluxos de dados para fornecer sugestões em tempo real. Ao fornecer compreensão contextual que capacita os usuários a tomar decisões proativas e informadas e simplificar processos para o envolvimento e o sucesso do cliente, o Cisco IQ AI Assistant otimiza os resultados operacionais e melhora a experiência do usuário do Cisco IQ.

Os recursos do Cisco IQ AI Assistant incluem:

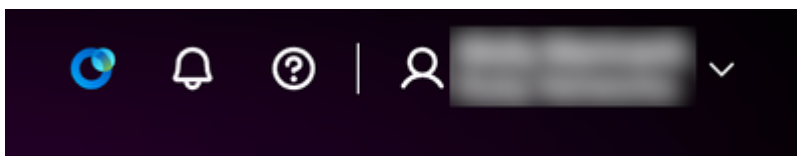
- Manipulação robusta de gabinetes de borda: Receber explicações transparentes e redirecionamento claro, garantindo uma experiência de suporte contínua e maior satisfação do usuário
- Capacidade de transmissão contínua: Exibir respostas à medida que forem geradas
- Dados contextuais aprimorados: O contexto dinâmico permite interações perfeitas entre aplicativos, páginas e sessões

- Suporte ao gerenciamento de casos: Crie, exiba e gerencie casos exibidos na exibição de Lista de casos
- Gerenciamento de inventário de ativos: Rastrear, gerenciar e gerar relatórios para os ativos ou recursos de uma organização
- Criticalidade do ativo: Priorizar ativos para atividades de mitigação de riscos com base em sua função e importância na rede
- Avaliação e gerenciamento de riscos: Avalie e gerencie os riscos potenciais associados aos ativos de uma organização
- Fortalecimento da segurança: Comparar as configurações dos dispositivos suportados do cliente com as diretrizes de proteção da Cisco e da CISA (Cybersecurity and Infrastructure Security Agency)
- Configuração: Avaliar as configurações em execução no dispositivo do cliente em relação às práticas recomendadas, identificar desvios de configuração e fornecer recomendações acionáveis

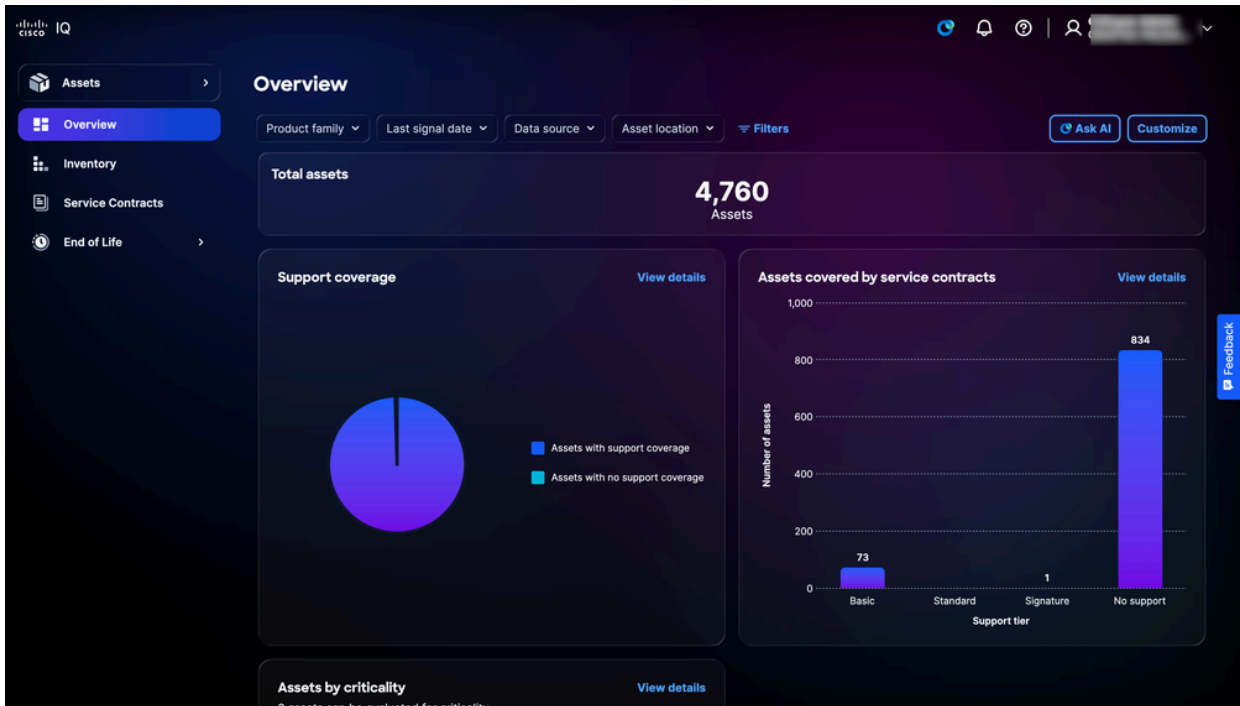
 Note: O Cisco IQ AI Assistant pode ser iniciado de qualquer lugar dentro do Cisco IQ. Ele está disponível para todos os usuários, mas os recursos oferecidos diferem com base no nível de suporte (básico, padrão ou assinatura).

Acesso ao Cisco IQ AI Assistant

Para usar o Cisco IQ AI Assistant:




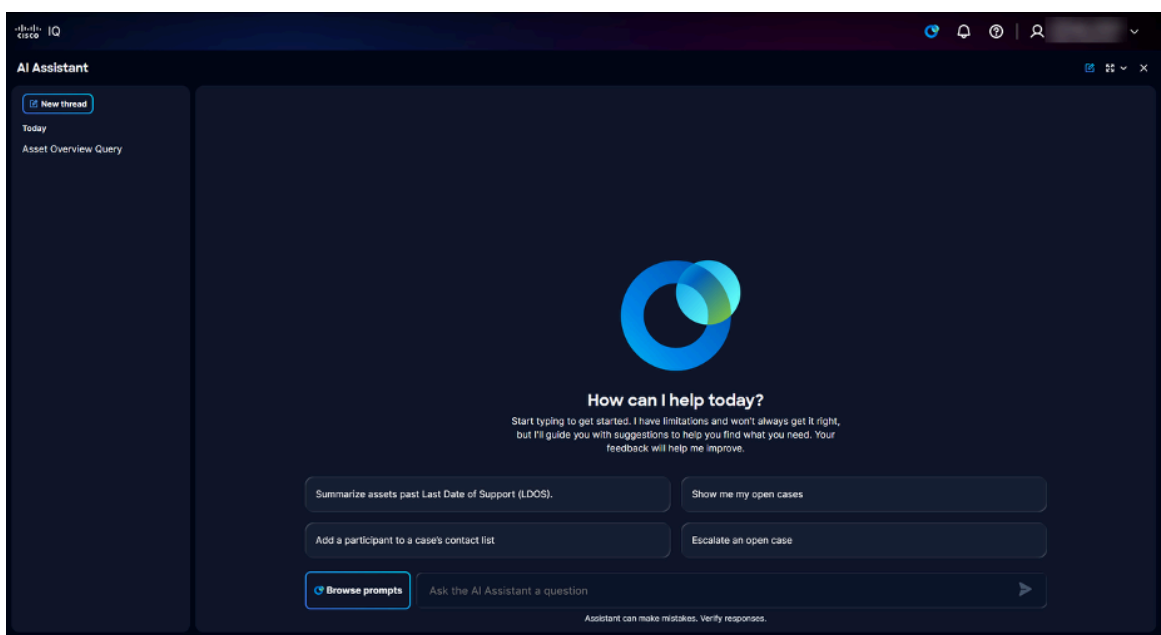
Ícone do assistente do AI




Pergunte à IA

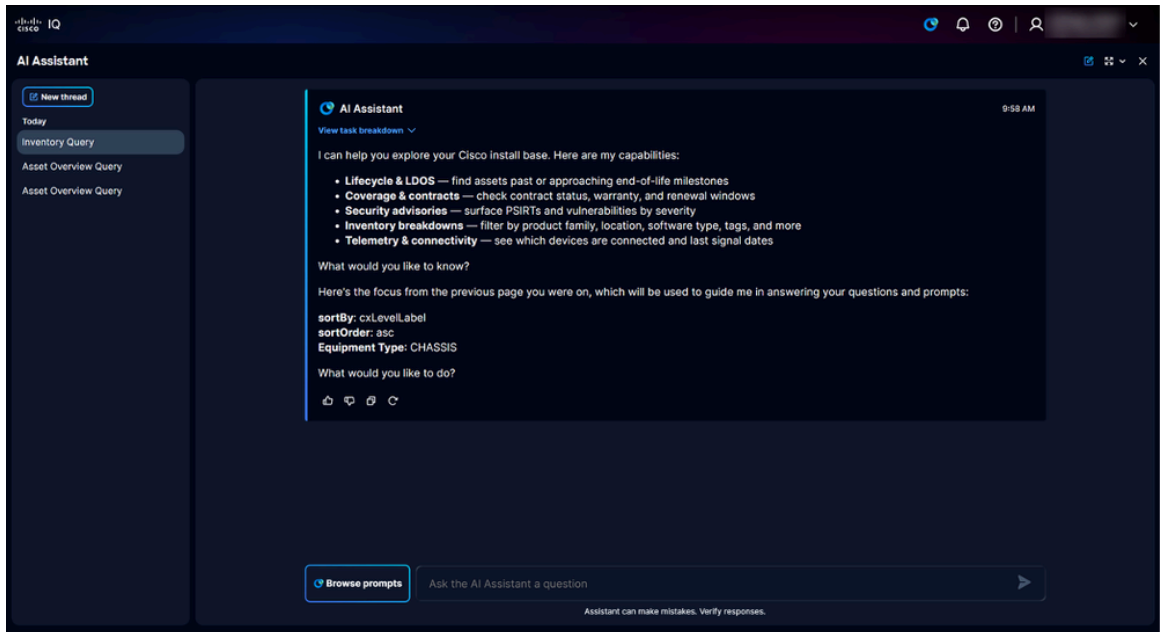
1. Inicie o Cisco IQ AI Assistant clicando no ícone do AI Assistant ou clicando em Ask AI.

 Note: O Cisco IQ AI Assistant pode ser acessado de qualquer lugar dentro do Cisco IQ clicando nessas duas (2) opções. Ele utiliza dados e contexto da página específica onde os usuários os lançam, permitindo que forneçam informações e recomendações altamente relevantes. Ao compreender sua tarefa atual, ele oferece orientação personalizada, etapas de solução de problemas e maior eficiência.




Página inicial

 Note: Você pode digitar um novo prompt ou procurar a biblioteca de prompts pré-fabricados.



Página inicial com contexto de aplicação

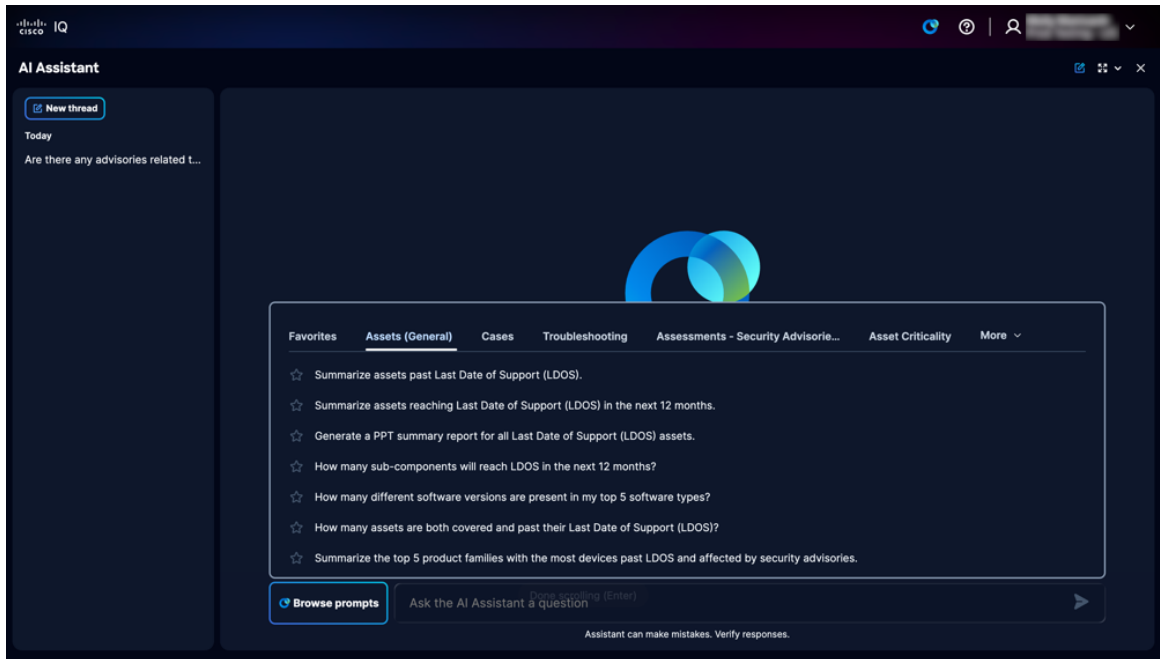
 Note: Por padrão, a visualização do Cisco IQ AI Assistant é definida como tela inteira. Quando você seleciona uma nova exibição, o Cisco IQ AI Assistant mantém a exibição selecionada anteriormente.

O Cisco IQ AI Assistant exibe as seguintes opções disponíveis:

- Threads anteriores: fornece 30 dias de histórico de prompt
- Procurar Prompts: Abre a biblioteca de prompts; consulte o Apêndice A: [O Cisco IQ AI Assistant solicita](#) uma lista de todas as perguntas disponíveis na biblioteca de prompts
- Faça ao Assistente do AI um campo de pergunta: Campo de texto para fazer uma pergunta ao Assistente do AI; use frases completas e descritivas para receber melhores respostas

2. Escolha um prompt usando um dos seguintes métodos:

- Procure prompts inserindo uma (1) ou mais palavras-chave no campo Ask the AI Assistant a question e clique no prompt
- Insira uma pergunta de forma livre usando frases descritivas e completas no campo Ask the AI Assistant a question (Faça uma pergunta ao assistente do AI)



Biblioteca de Prompts

- Clique em Procurar prompts para abrir a biblioteca de prompts e escolha qualquer uma das seguintes guias de categoria de prompt:
 - Ativos (Geral): Avisos relacionados ao ciclo de vida do ativo, incluindo consultas de LDOS e inventário geral
 - Casos: Avisos para apoiar ações de gerenciamento de casos, como visualização, atualização, encaminhamento e fechamento de casos, permitindo um controle eficiente e a conexão com o engenheiro de suporte da Cisco
 - Troubleshooting: Prompts para ajudar com mensagens de erro do syslog ou perguntas sobre configuração
 - Avaliações - Avisos de segurança: Avisos relacionados à avaliação da postura geral de segurança da rede, identificação de vulnerabilidades críticas e listagem de ativos específicos afetados por ameaças de segurança de alta gravidade ou pontos fracos na configuração
 - Criticalidade do ativo: Prompts relacionados à priorização de ativos para atividades de mitigação de riscos com base em sua função e importância na rede
 - Avaliações - Configuração: Prompts relacionados ao resumo dos resultados da avaliação da configuração, à identificação de desvios de configuração em relação às práticas recomendadas e à geração de recomendações acionáveis
 - Avaliações - Fortalecimento da segurança: Prompts relacionados à identificação das configurações básicas de segurança recomendadas,

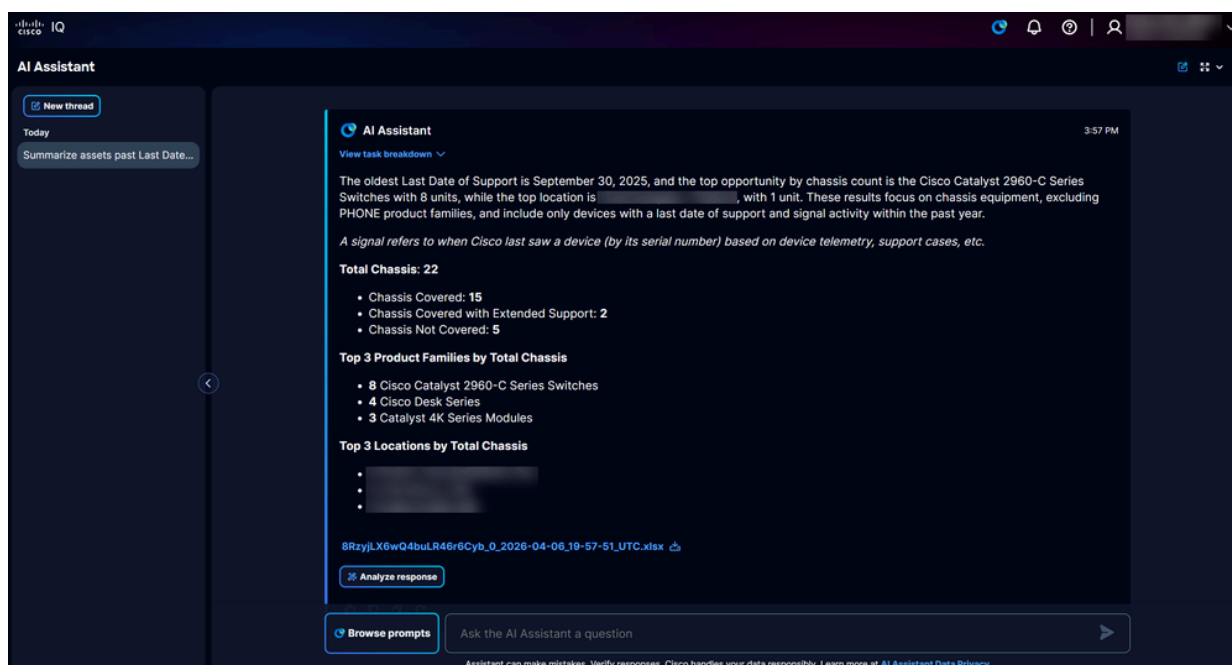
práticas recomendadas para proteção de dispositivos e procedimentos passo a passo para proteção da infraestrutura de rede da Cisco

3. Clique em um prompt. Uma resposta é gerada.

Dados contextuais aprimorados para o assistente do AI

O Cisco IQ AI Assistant garante que o contexto seja dinâmico, permitindo interações perfeitas entre aplicativos, páginas e sessões. Isso garante que cada resposta utilize dados contextuais para fornecer respostas altamente relevantes personalizadas para a sua pergunta.

Sumarização e Priorização de LDOS



Relatório LDOS

O recurso de sumarização e priorização do LDOS permite que você identifique e trate rapidamente os riscos associados aos ativos de rede. Esse recurso classifica os ativos por suas funções de rede esperadas e status de vulnerabilidade de segurança, permitindo a correção de vulnerabilidades e melhorando a qualidade geral do serviço.

Principais benefícios

Os principais benefícios do recurso de sumarização e priorização do LDOS incluem:

- Exibição de risco priorizada

- Análise de impacto operacional
- Insights práticos

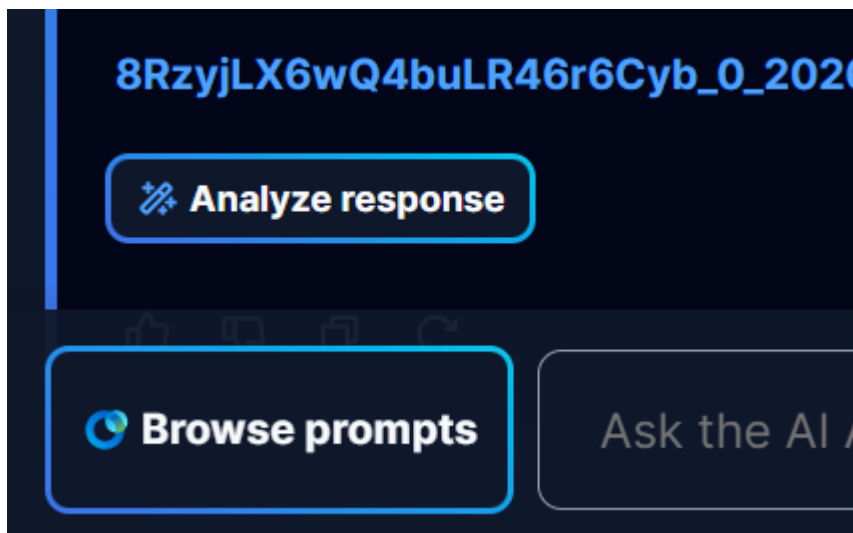
Como parte desse recurso, você pode visualizar um conjunto limitado de perguntas pré-implantadas (marcadas por "**") na interface do usuário ou ao visualizar informações do LDOS.

Relatórios

Geração de relatório LDOS

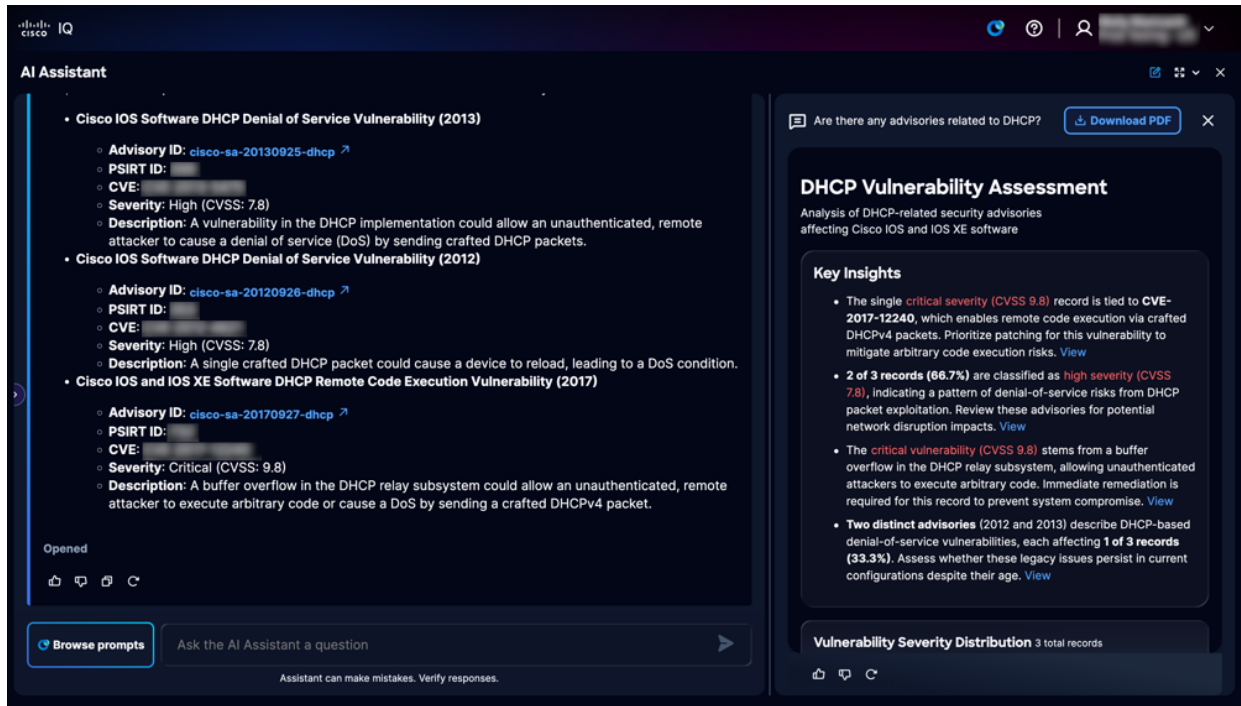
Relatórios LDOS com curadoria gerados por AI fornecem resumos de ativos que se aproximam ou ultrapassam seu LDOS. Os relatórios também destacam opções de atualização, bem como identificam recomendações de segurança e vulnerabilidades para ajudá-lo a entender rapidamente o cenário de risco da sua rede.

Analisar resposta



Analisar resposta

Ao clicar em Analisar resposta, você recebe um resumo acionado por IA que resume dados e gera várias visualizações, como gráficos, painéis e gráficos, fornecendo informações úteis.



Resumo da IA

O resumo acionado por IA contém um botão Download PDF para fazer o download do relatório como PDF.

Fontes de dados para resumo e geração de relatório do LDOS

As principais fontes de dados a seguir são aproveitadas pelo recurso de sumarização e priorização do LDOS:

- Ativos e contratos da base instalada
- Ativos e contratos de telemetria
- Dados de Sinal CX
- Etapas do EOL para ativos de hardware e software

Solução de problemas com o Cisco IQ AI Assistant

O Cisco IQ permite que você resolva problemas de dispositivo de forma independente com o Cisco IQ AI Assistant. Desenvolvido com base em ferramentas de solução de problemas certificadas da Cisco e em uma base de conhecimento comprovada, este assistente intuitivo e interativo fornece recomendações contextuais em tempo real.


Ele é projetado para cenários de solução de problemas diários e ajuda os engenheiros de rede a

investigar problemas de produtos da Cisco, analisar sintomas e identificar as próximas etapas úteis. Ele interpreta detalhes técnicos, como mensagens de erro, syslogs, defeitos de software, orientações de versão e perguntas relacionadas à configuração. Ao enfrentar os desafios instantaneamente, você pode manter o desempenho ideal e economizar tempo resolvendo problemas sem a necessidade de abrir um caso de suporte.

Melhores práticas

Ao usar o Cisco IQ AI Assistant para solução de problemas, use as seguintes práticas recomendadas:

- Ser o mais específico possível; inclua a plataforma, a família de produtos e a versão do software em sua primeira mensagem

 Note: Ao iniciar o Cisco IQ AI Assistant a partir de um ativo, ele já tem essas informações.

- Cole o erro exato, o alarme ou o texto do syslog em vez de parafraseá-lo
- Descreva o que mudou antes do início do problema, como uma atualização, atualização de configuração ou alteração de topologia
- Compartilhe o impacto claramente, como se o problema afeta um (1) dispositivo, um (1) local ou vários usuários


Casos

O recurso Gerenciamento de casos permite que os usuários gerenciem seus casos de suporte por meio do autoatendimento, garantindo que os aplicativos e serviços comerciais sejam restaurados imediatamente. Esse recurso ajuda a gerenciar casos com eficiência e a simplificar a experiência de suporte. Consulte [Aplicativo de Suporte](#) para obter mais informações sobre o Gerenciamento de Casos.

Com o Gerenciamento de casos, os usuários podem visualizar e rastrear rapidamente seus casos de suporte em um único local. Ele ajuda a verificar o status do caso, revisar atualizações, acompanhar o progresso e manter-se informado sobre as próximas etapas, facilitando o gerenciamento de problemas e a obtenção de suporte mais rápido.

Apêndice A: Prompts do Cisco IQ AI Assistant

Este apêndice fornece uma visão geral detalhada dos prompts disponíveis no Cisco IQ AI Assistant, organizados em listas de marcadores por temas de pergunta.

 Note: Você pode procurar os prompts disponíveis selecionando sugestões relevantes à medida que a biblioteca de prompts restringe as opções com base na sua entrada, ou pode enviar seu próprio prompt personalizado. O Cisco IQ AI Assistant conta com a entrada de linguagem natural e não inclui formulários de entrada, como menus suspensos, garantindo uma experiência de usuário perfeita.

Os prompts a seguir estão disponíveis na guia Ativos (Geral):

- Resuma os ativos após a última data de suporte (LDOS).
- Resuma os ativos que atingirão a última data de suporte (LDOS) nos próximos 12 meses.
- Gere um relatório resumido de PPT para todos os ativos de LDOS (Última data de suporte).
- Quantos subcomponentes alcançarão o LDOS nos próximos 12 meses?
- Quantas versões diferentes de software estão presentes nos meus 5 principais tipos de software?
- Quantos ativos estão cobertos e ultrapassaram sua última data de suporte (LDOS)?
- Resuma as 5 principais famílias de produtos com a maioria dos dispositivos anteriores ao LDOS e afetadas por avisos de segurança.
- Resuma as placas e os módulos depois do LDOS e afetados pelas recomendações de segurança.
- Quantos subcomponentes estão atingindo marcos de fim de vida útil antes do chassi pai?

Os prompts a seguir estão disponíveis na guia Cases:

- Mostrar meus casos abertos
- Resumir um caso
- Mostrar o status de uma RMA
- Mostrar o status de um bug
- Dê-me uma atualização sobre um caso
- Fornecer a atualização mais recente e quaisquer itens de ação pendentes para um caso
- Fechar um caso aberto
- Adicionar um participante à lista de contatos de um caso
- Criar uma comunicação do espaço Webex sobre um caso
- Entre em contato comigo com o engenheiro responsável pelo caso
- Aumentar o nível de gravidade de um caso aberto
- Escalonar um caso aberto
- Solicitar um novo engenheiro para um caso
- Recolocar um caso em aberto na fila
- Adicionar nota a um caso

Os prompts a seguir estão disponíveis na guia Troubleshooting:

- Como soluciono problemas de erro de Syslog [Erro] e identifico a causa raiz?
- Como soluciono problemas de configuração e identifico a causa raiz do [ABCD]?
- Como configuro [XYZ] na ID do produto [ABCD]?

Os prompts a seguir estão disponíveis na guia Avaliações - Avisos de Segurança:

- Há alguma recomendação relacionada ao DHCP?
- Há um aviso de segurança para verificar se há vulnerabilidades de escalonamento de privilégios da interface do usuário da Web relacionadas ao tífão de sal?
- Antes de habilitar o HTTP, você pode verificar se há avisos de segurança conhecidos ou vulnerabilidades relacionadas à habilitação do HTTP?
- Quantas recomendações de segurança estão vulneráveis na minha rede?
- Quantos dispositivos são vulneráveis a avisos de segurança?

Os prompts a seguir estão disponíveis na guia Criticidade do ativo:

- Quais são meus ativos mais importantes por função e importância?
- Quantos dispositivos principais são afetados pelas recomendações de segurança?
- Resuma os dispositivos essenciais e de alta importância com cobertura que expirará nos próximos 12 meses
- Priorizar ativos LDOS para atualização com base na função e importância.
- Priorize ativos sem cobertura ou a serem descobertos em breve para renovação com base na função e na importância.
- Priorize contratos prestes a expirar para renovação com base na função e na importância desses ativos cobertos.
- Priorizar vulnerabilidades de PSIRT com base na gravidade, função e importância dos ativos afetados.

Os prompts a seguir estão disponíveis na guia Avaliações - Configuração:

- Você pode fornecer um resumo da minha avaliação de configuração recente?
- Quantas regras de práticas recomendadas de configuração foram avaliadas e quantas resultaram em pelo menos um ativo que não foi aprovado?
- Quais são os desvios de configuração mais comuns na minha rede?
- Quais famílias de produtos da Cisco apresentam a maioria dos desvios das práticas recomendadas de configuração?
- Quantos ativos foram avaliados e qual porcentagem não passou?
- Quais categorias apresentam a maioria dos desvios das práticas recomendadas de

configuração?

- Quais desvios de configuração representam o maior risco para minha rede e quais ações corretivas são recomendadas?
- Quais ativos têm o máximo de desvios de configuração críticos e de alta gravidade? Que ações corretivas são recomendadas?
- Mostrar a divisão dos desvios de configuração críticos e de alta gravidade por criticidade de ativo
- Mostrar detalhamento dos desvios das regras de práticas recomendadas de configuração por gravidade, categoria e tipo de software

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?

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.