Usar a API de relatório Umbrella via Postman

Contents

Introdução

Este documento descreve como usar a API do Cisco Umbrella Reporting no Postman.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

A API Umbrella foi lançada em setembro de 2022, fornecendo uma plataforma fácil de usar e segura que permite que os usuários criem, estendam e integrem com o Umbrella.

Os pontos de extremidade da API Umbrella são hospedados em api.umbrella.com, com caminhos agrupados por caso de uso. As chaves de API podem ser gerenciadas no painel Umbrella, em Admin > chaves de API, e programaticamente com a API KeyAdmin. Cada chave pode ser configurada granularmente com vários escopos agrupados em cinco casos de uso principais:

- Os endpoints de API de administração permitem que você provisione e gerencie chaves e

usuários de API Umbrella, visualize funções e gerencie clientes para provedores e provedores gerenciados.
- Os endpoints de API de autenticação permitem autorizar integrações de outros serviços com a plataforma Umbrella.
- Implantações Os endpoints de API permitem que você provisione, monitore e gerencie redes e outras várias entidades, e as proteja configurando-as em suas políticas Umbrella existentes.
- Os endpoints de API de políticas permitem que você provisione e gerencie listas de destinos e os destinos por lista.
- Os endpoints de API de relatórios permitem que você leia e audite informações de segurança em tempo real sobre suas implantações. A API do Umbrella App Discovery oferece informações sobre seus aplicativos baseados em nuvem.

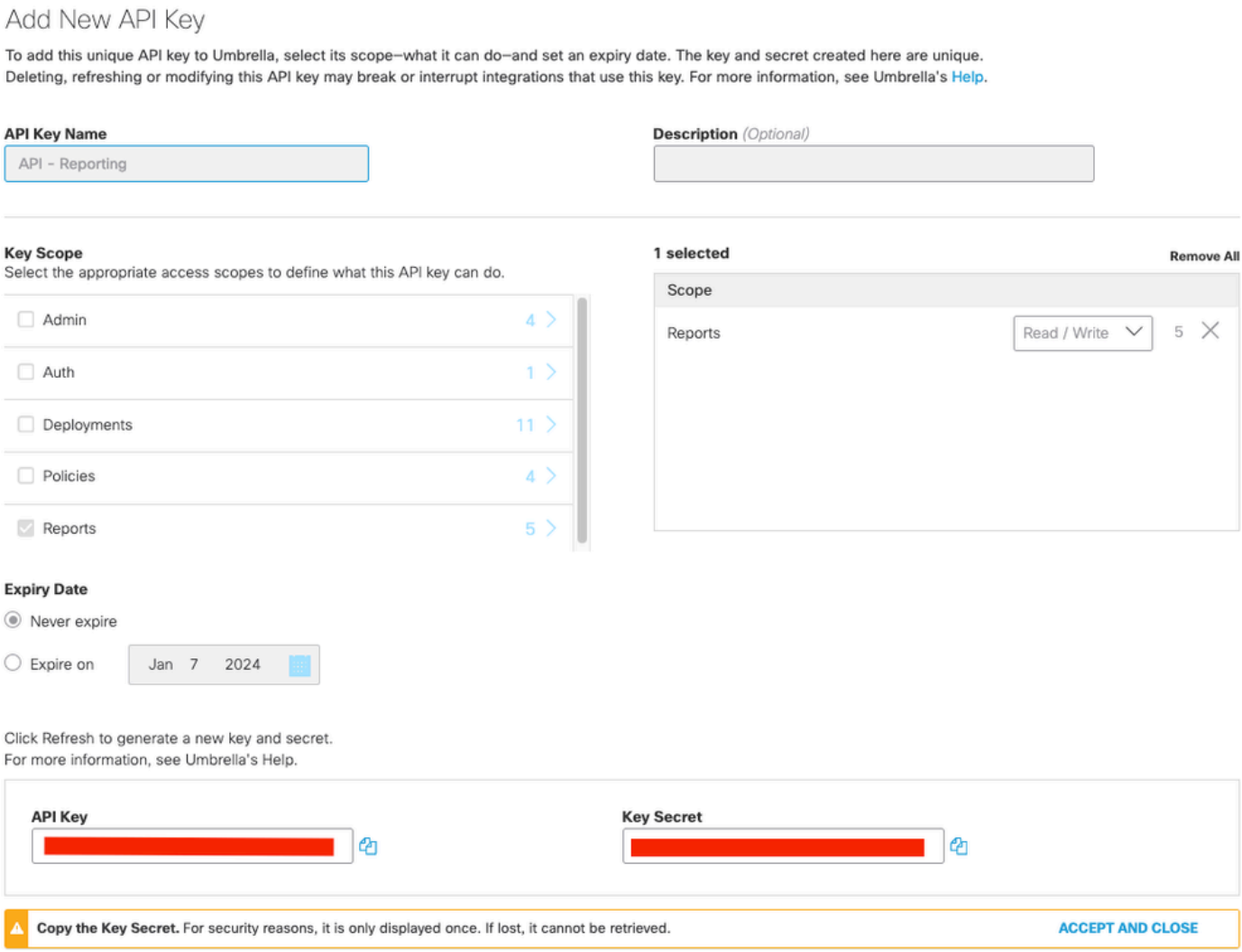
Este artigo demonstra como coletar relatórios de pesquisa de atividades via API.

Procedimento de guarda-chuva

1. No painel Umbrella, navegue até Admin > Chaves API.

2. Selecione Chaves de API > Adicionar.

3. Em Escopo de Chave, selecione Relatórios e Criar Chave.



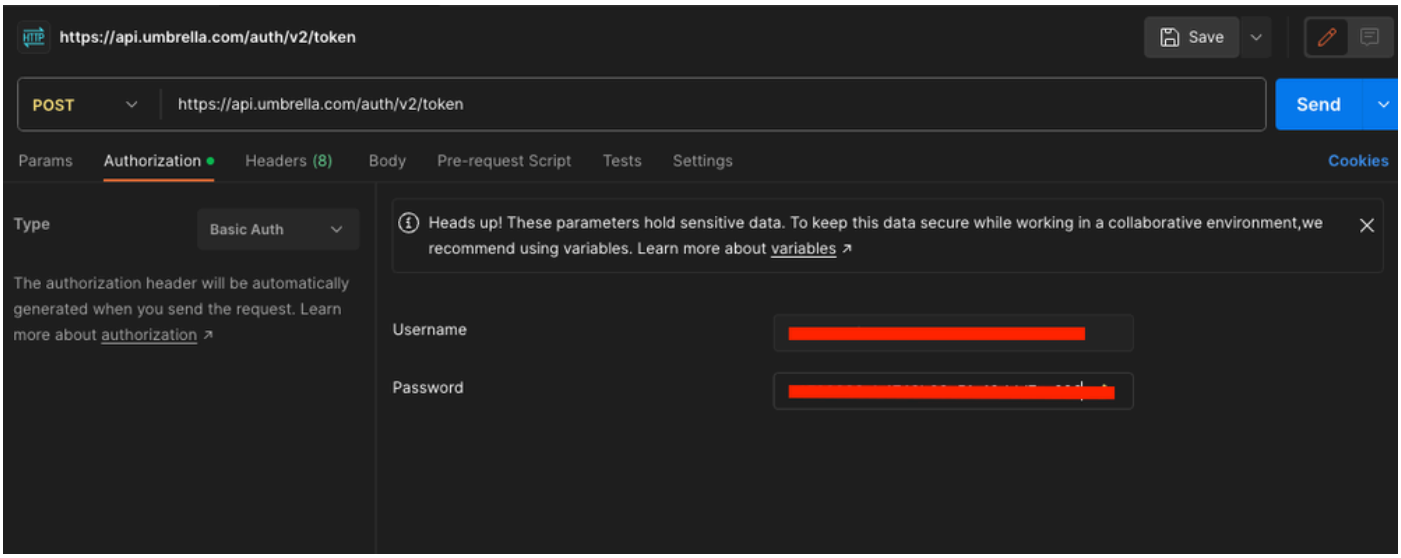
21495050167956

Os administradores podem ajustar o nível de acesso por escopo entre Leitura/Gravação e Somente Leitura, dependendo do uso pretendido de cada chave de API, enquanto as chaves de API podem ser configuradas para expirar em uma data predefinida. Você deve coletar a chave/segredo da API nesta etapa, pois eles estão visíveis no momento e não podem ser exibidos depois.

As credenciais de API geram tokens de acesso de API válidos por 60 minutos. Este procedimento suporta o fluxo de credenciais do cliente OAuth 2.0. Em ambientes de provedores de serviços ou de várias organizações Umbrella, as credenciais de API pai-organização podem ser usadas para gerar tokens de acesso com os mesmos escopos para uma organização filha especificada durante o processo de autorização.

Procedimento do carteiro

No primeiro momento, é necessário criar um token de acesso OAuth 2.0. Os caminhos de autenticação da API Umbrella começam com https://api.umbrella.com/auth/v2. Após o envio de uma consulta POST e da chave da API do usuário como nome de usuário e senha da API como senha, um Token de Acesso é gerado.

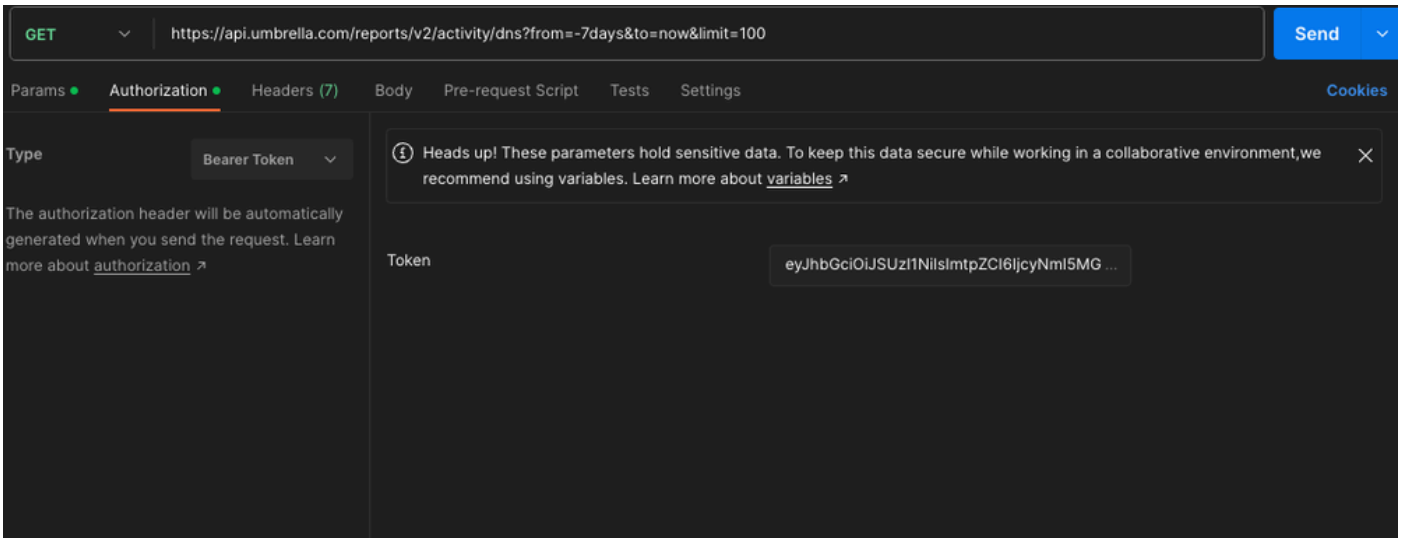


21606708808468

21607051456276

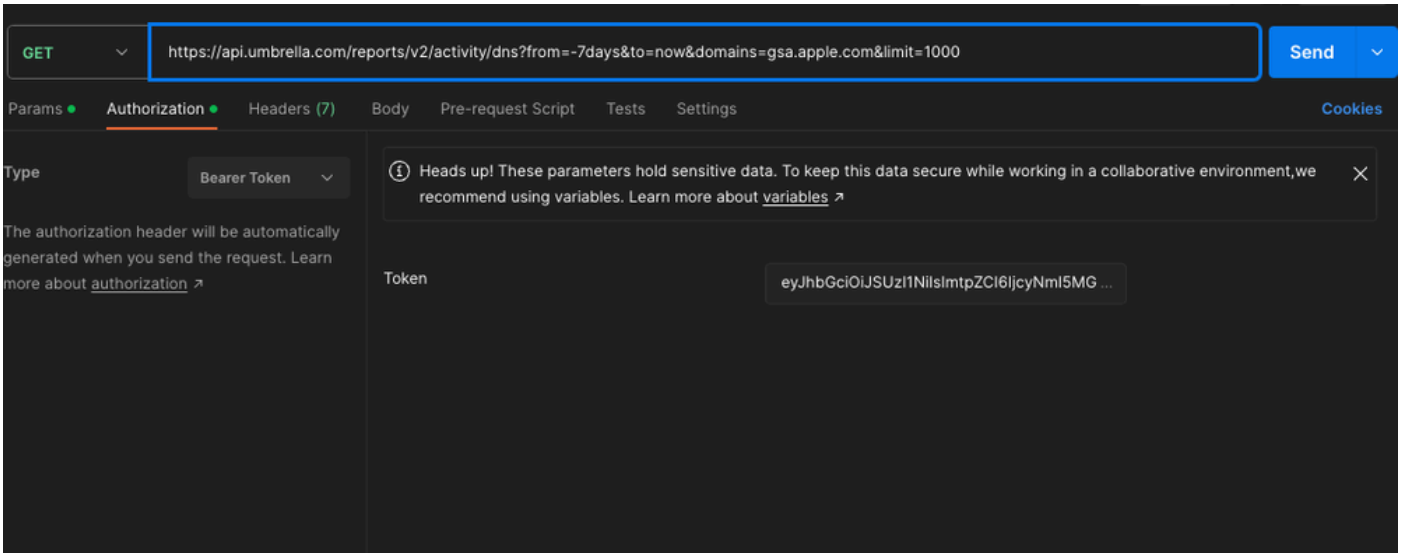
Nesta etapa, você será solicitado a coletar o Token de Acesso. Agora você pode recuperar informações com o Token de acesso.

Você deve selecionar o método GET e inserir o caminho da API (incluindo o parâmetro necessário) e o Token de Acesso. Neste exemplo, você pode recuperar 100 relatórios da atividade de pesquisa exclusivamente para tráfego DNS nos últimos 7 dias.



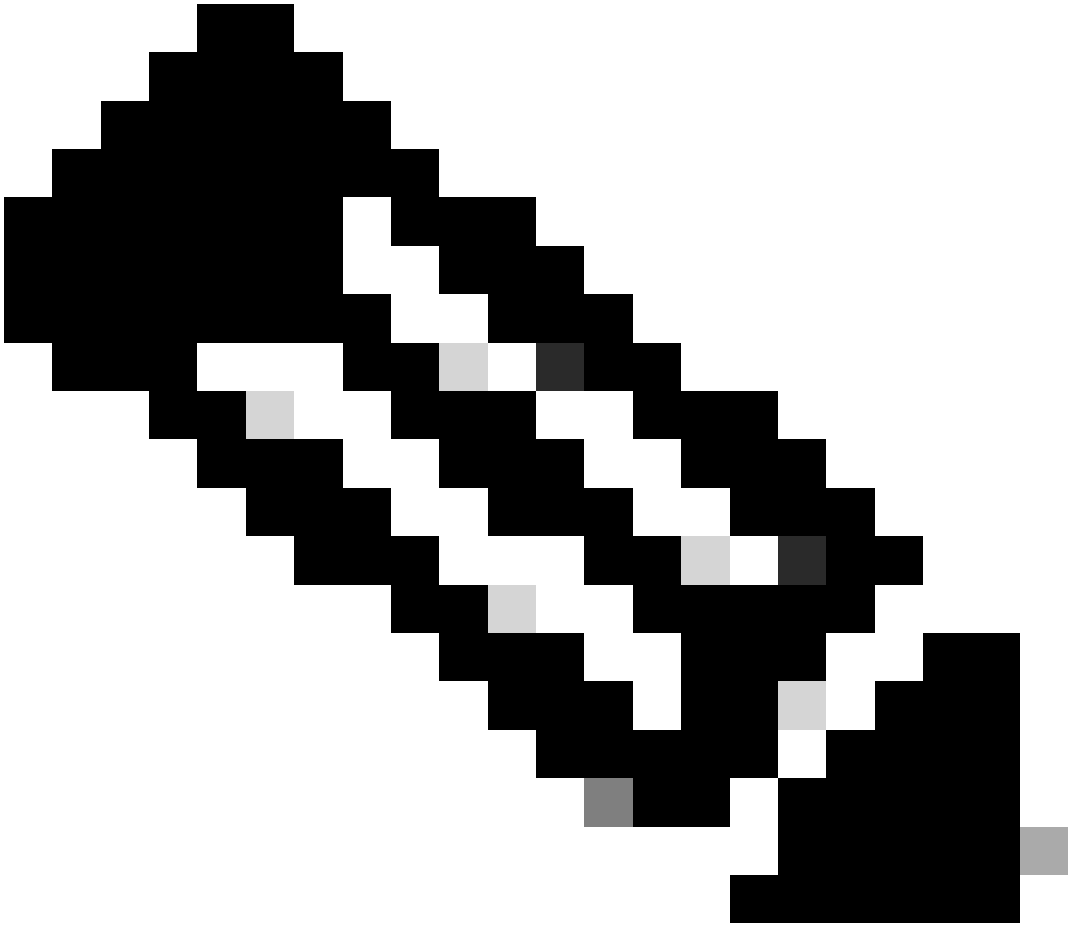
21607952074772

Em outro exemplo, você pode tentar extrair 1000 relatórios da pesquisa de atividades, exclusivamente para tráfego DNS nos últimos 7 dias, especificamente para o domínio "gsa.apple.com".



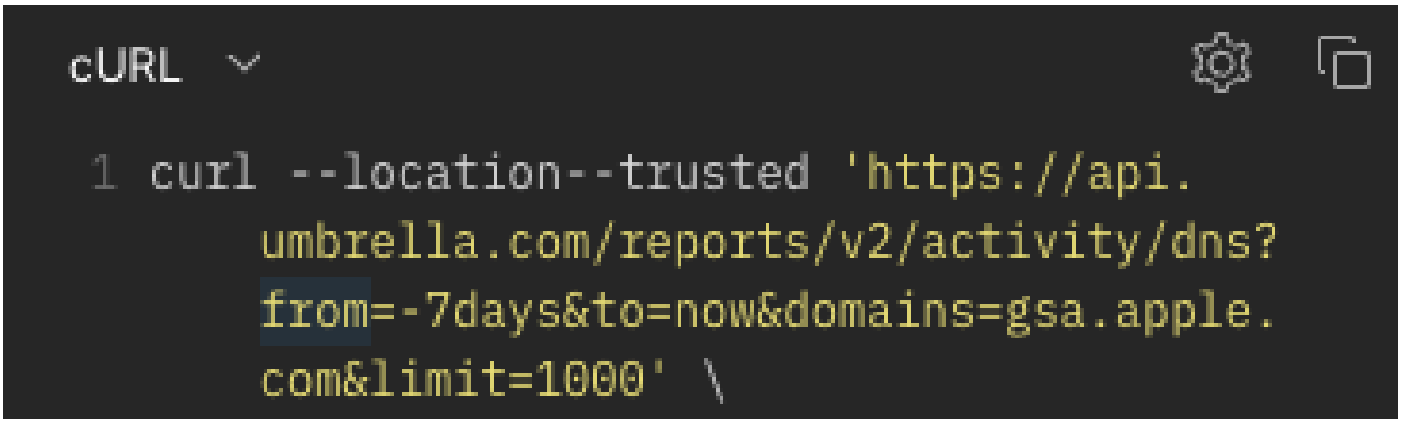
21607927544468

Você pode consultar Parâmetros de consulta de solicitação para descobrir parâmetros adicionais que podem ser usados na consulta de API.



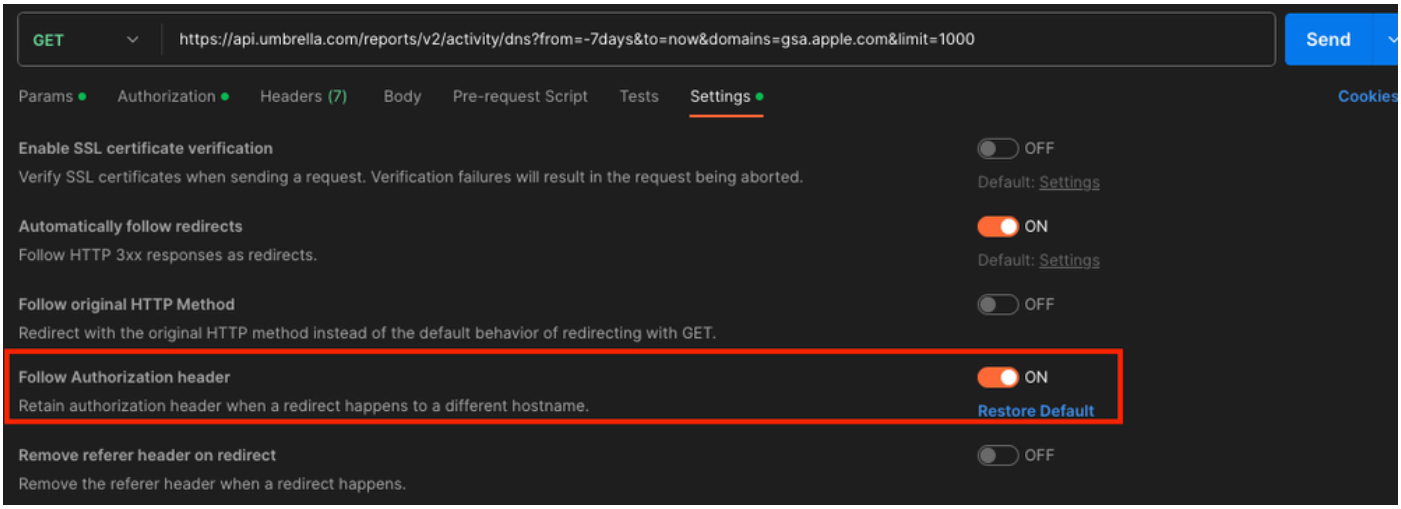
Note: Se uma solicitação de cliente HTTP não se origina do mesmo continente que o local do data warehouse do Umbrella, o servidor Umbrella responde com 302 Achados. Para redirecionar automaticamente solicitações HTTP e preservar o cabeçalho de Autorização HTTP, você pode definir sinalizadores adicionais ou habilitar uma configuração de redirecionamento.

curva: Você deve passar os sinalizadores -L ou —location e —location-trusted para redirecionar a solicitação HTTP curl e reter o cabeçalho de Autorização.



21608126036628

POSTMAN: No ambiente Postman, navegue até uma API e selecione um método GET. Navegue até Configurações > Ativar cabeçalho Seguir autorização para preservar o cabeçalho de autorização para solicitações de redirecionamento.



21608126042388

Respostas

Depois de enviar a ação GET para o URL, você pode receber vários códigos de status:

- Status:200: A solicitação obteve as informações solicitadas com êxito.
- Status: 400: solicitação inválida. Pode estar relacionado à URL que você enviou para consulta. Um ou mais parâmetros não estão corretos.
- Status: 401: Não autorizado. O cabeçalho de autorização está ausente ou o token não está autorizado.
- Status:403: Proibido. Token inválido.

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.