

Solucionar problemas de insights de dispositivos e integração de guarda-chuva

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshoot](#)

[Teste de conectividade com Device Insights e Umbrella](#)

[Chave incorreta](#)

[Verificar](#)

Introduction

Este documento descreve as etapas para configurar a integração e solucionar problemas do Device Insights e da integração do Cisco Umbrella.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos.

- SecureX
- Umbrella
- Conhecimento básico de APIs
- ferramenta de API Postman

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- SecureX 1.103

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O SecureX Device Insights fornece uma visão unificada dos dispositivos em sua organização e consolida inventários a partir de fontes de dados integradas.

A Umbrella detecta automaticamente a infraestrutura do invasor preparada para as ameaças atuais e bloqueia proativamente solicitações mal-intencionadas antes que elas atinjam a rede ou os endpoints de uma empresa. Com a integração, você pode interromper as infecções por malware mais cedo, identificar dispositivos já infectados mais rapidamente e evitar a extração de dados. A integração oferece visibilidade completa da atividade da Internet em todos os locais e usuários e permite que você tome medidas com dois cliques para bloquear domínios rapidamente. Várias funções Umbrella são suportadas e vinculadas através de chaves de API que foram geradas na Plataforma Umbrella.

Se você quiser saber mais sobre a configuração, leia este artigo [aqui](#) para obter os detalhes do módulo de integração.

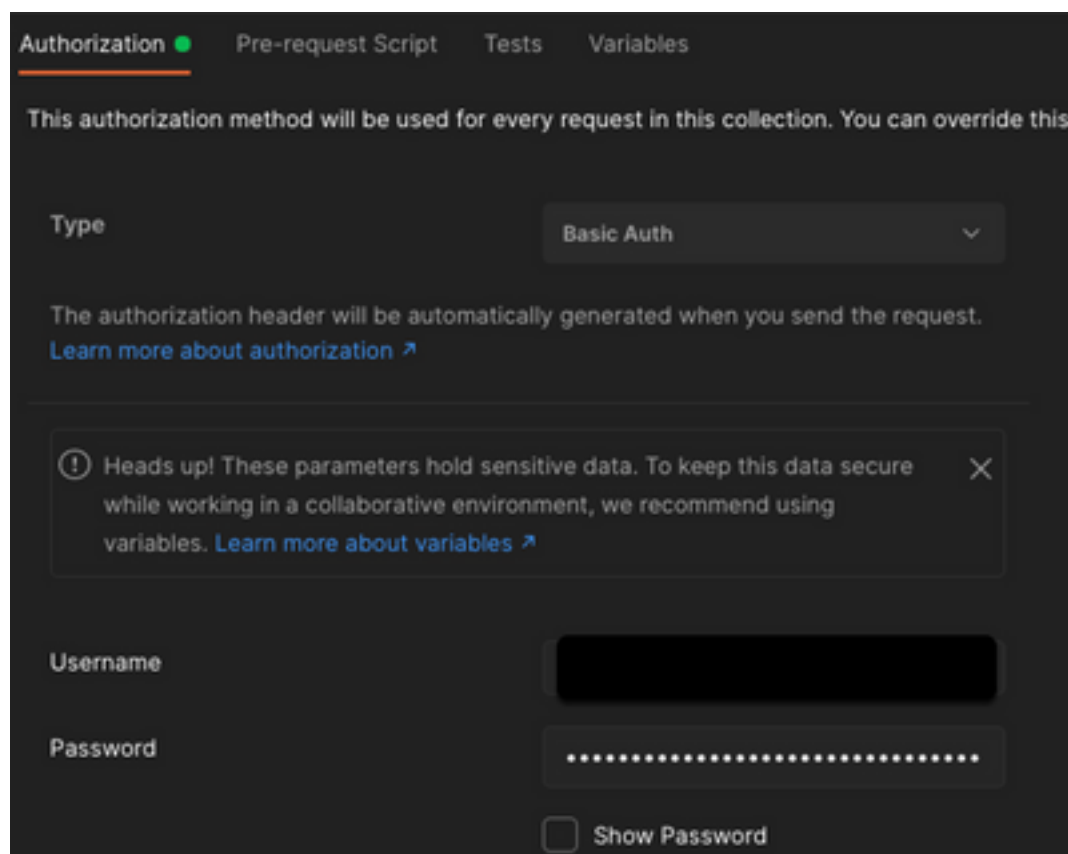
Troubleshoot

Para solucionar problemas comuns com a integração do SecureX e Umbrella, você pode verificar a conectividade e o desempenho da API.

Teste de conectividade com Device Insights e Umbrella

Etapa 1. Você pode selecionar **Basic Auth** como um método de autorização, já que o MobileIron o utiliza, como mostrado na imagem.

Observação: Postman não é uma ferramenta desenvolvida pela Cisco. Se você tiver alguma dúvida sobre a funcionalidade da ferramenta Postman, entre em contato com o suporte do Postman.



Etapa 2. Você pode obter **computadores em roaming**, com essa chamada de API (o limite de

página padrão é de 100 entradas).

<https://management.api.umbrella.com/v1/organizations/>

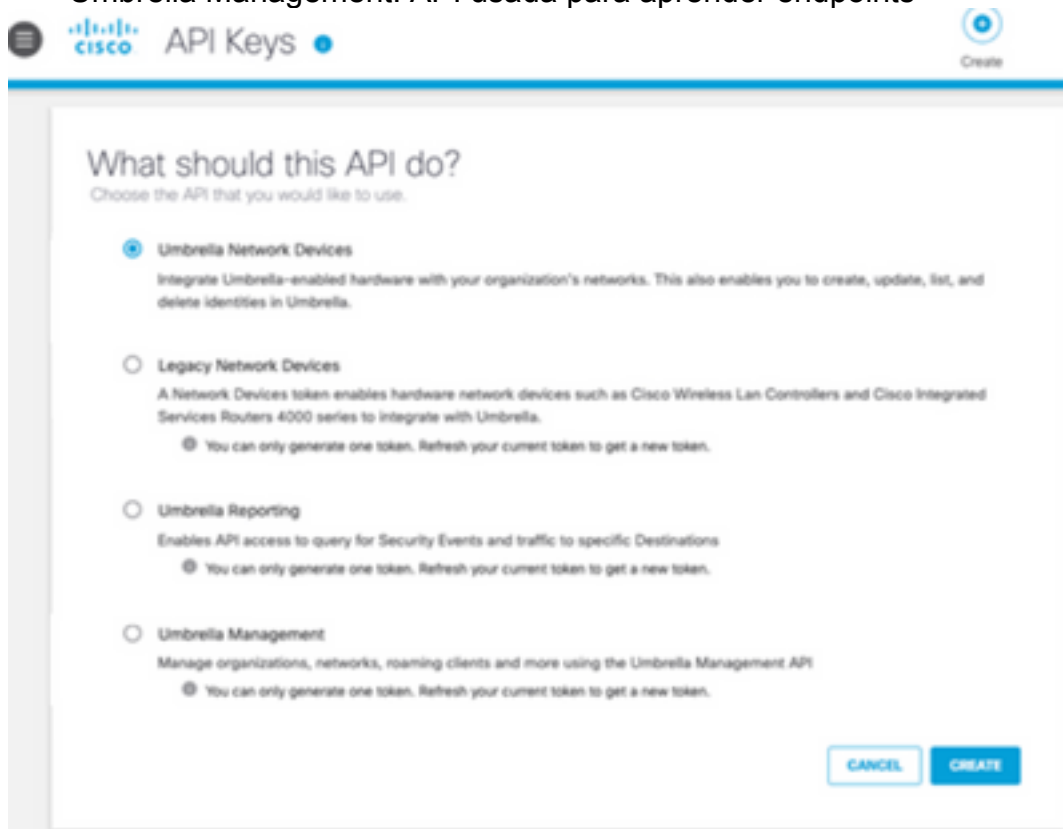
Etapa 3. Em resposta à primeira chamada, o número total de objetos é retornado. Você pode usar parâmetros de limite e de página para obter as próximas páginas.

<https://management.api.umbrella.com/v1/organizations/>

Chave incorreta

O Device Insights não usa as mesmas chaves que o SecureX, então você precisa verificar e confirmar se as chaves configuradas como chaves da API do Umbrella estão corretas, como mostrado na imagem.

- Umbrella Network Devices: API usada para saber quais políticas de DNS
- Umbrella Management: API usada para aprender endpoints



Verificar

Depois que o Umbrella for adicionado como uma fonte para o Device Insights, você poderá ver um status de conexão **REST API** bem-sucedido.

- Você pode ver a conexão da **API REST** com um status verde
- Clique em **SYNC NOW** para disparar a sincronização completa inicial, como mostrado na imagem



Caso o problema persista com a integração do Device Insights e Umbrella, consulte este [artigo](#) para coletar logs HAR do navegador e entre em contato com o suporte do TAC para executar uma análise mais profunda.

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.