

Identificar e solucionar problemas de percepções de dispositivos XDR e integração de guarda-chuva

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

Introdução

Este documento descreve as etapas para configurar a integração e solucionar problemas com o XDR Device Insights e a integração com o Cisco Umbrella.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

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

Componentes Utilizados

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

- XDR

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.

Informações de Apoio

O XDR Device Insights fornece uma visão unificada dos dispositivos em sua organização e consolida inventários 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 uma resposta de

dois cliques para bloquear domínios rapidamente. Várias funções Umbrella são suportadas e vinculadas através de chaves de API que foram geradas na Plataforma Umbrella.

Para saber mais sobre a configuração, consulte os detalhes do módulo de integração.

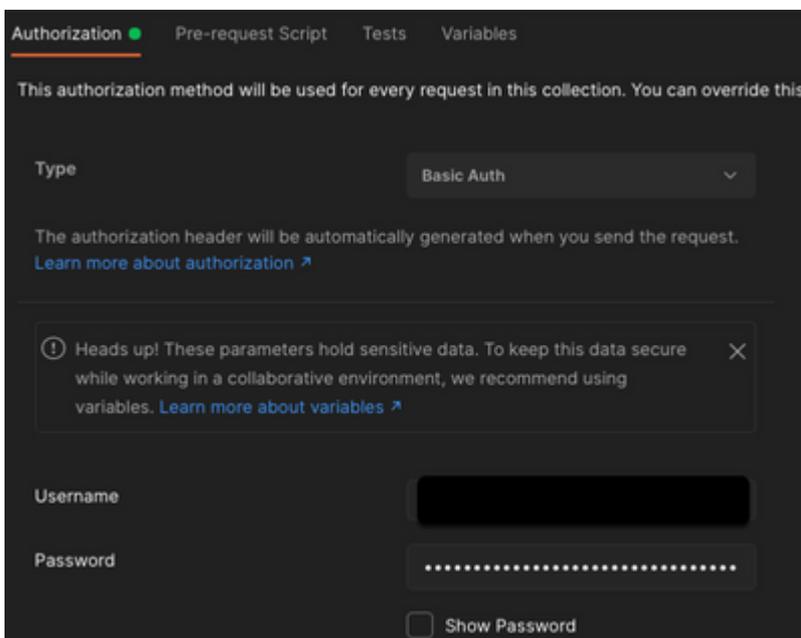
Troubleshooting

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

Teste de conectividade com o XDR Device Insights e Umbrella

Etapa 1. Você pode selecionar **Autenticação Básica** como um método de autorização, 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/`

`/roamingcomputers`

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.

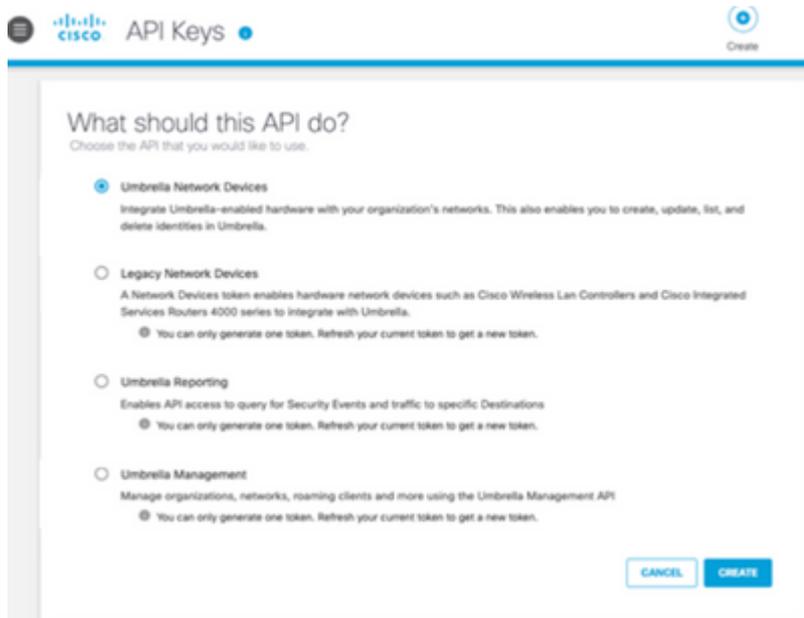
`https://management.api.umbrella.com/v1/organizations/`

`/roamingcomputers?limit=5&page=2`

Chave incorreta

O XDR Device Insights não usa as mesmas chaves que o XDR; em seguida, você precisa verificar e confirmar se as chaves configuradas como chaves da API 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 origem ao XDR Device Insights, você poderá ver um status de conexão da **API REST** bem-sucedida.

- 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, colete os registros 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.