Identificação e solução de problemas de dispositivos XDR e integração DUO

Contents

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

- XDR
- DUO
- 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.

Duo protege sua força de trabalho e leva a segurança de acesso além do perímetro da rede corporativa para proteger seus dados em todas as tentativas de autenticação, de qualquer dispositivo, em qualquer lugar. Com o Duo, você pode confirmar suas identidades rapidamente, monitorar a integridade de dispositivos gerenciados e não gerenciados, definir políticas de segurança adaptáveis personalizadas para sua empresa, proteger o acesso remoto sem um agente de dispositivo e fornecer um Single Sign-On seguro e amigável, de forma rápida e fácil.

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

Troubleshooting

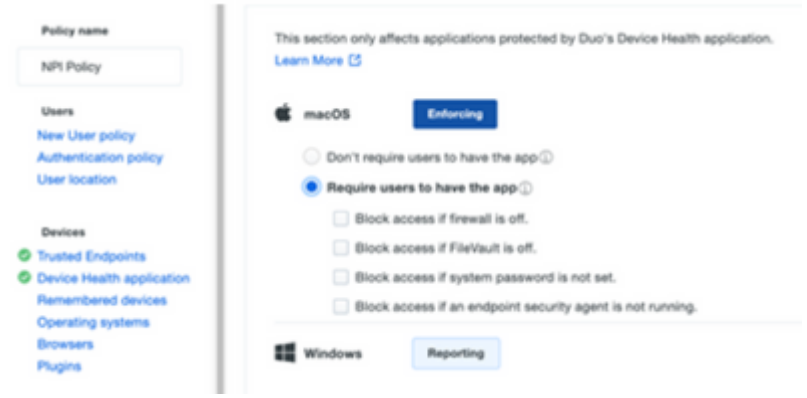
Para solucionar problemas comuns com a integração XDR e DUO, você pode verificar a conectividade e o desempenho da API.

Revisar o nível de licença

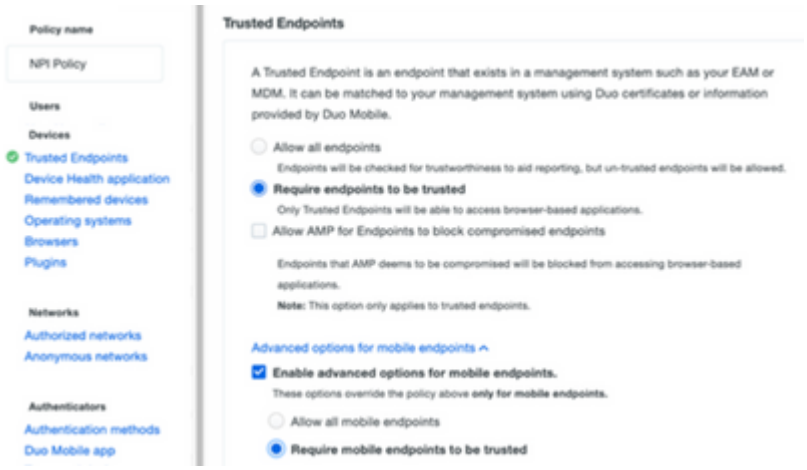
- Verifique a licença no **painel de administração do Duo**
- Duo licenciado para acesso Duo, Duo Beyond (ou qualquer licença de high-end mais recente, apenas MFA ou Free não se aplica), conforme mostrado na imagem

Sem dados do Duo

- Verifique se você usa os dados do **agente de integridade Duo** na **política de autenticação**, como mostrado na imagem



- Verifique se você usa o **ponto de extremidade confiável** na **política de autenticação**, como mostrado na imagem



Teste de conectividade com XDR Device Insights e DUO

Você pode usar a ferramenta Postman para ter uma saída mais visual enquanto testa a conectividade.

> **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.

- O código de erro 40301 "**Acesso proibido**" significa que você não tem o nível correto de licença, como mostrado na imagem

- Você pode selecionar **No Auth** como um método de autorização
- Você pode usar essa chamada de API para obter uma lista dos dispositivos (a API retorna o número máximo suportado de entradas por página) e você pode encontrar a documentação sobre a paginação da API DUO

```
https://
```

```
/admin/v1/endpoints
```

- Em resposta à primeira chamada, o número total de objetos é retornado (os parâmetros offset e limit podem ser usados para obter as próximas páginas), como mostrado na imagem

```
https://
```

```
/admin/v1/endpoints?limit=5&offset=5
```

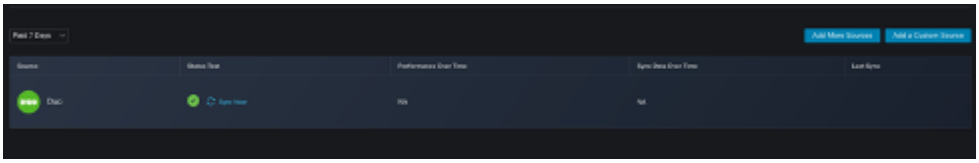

```
"metadata": {
    "total_objects": 64
},
```

```
"metadata": {
    "next_offset": 5,
    "total_objects": 64
},
```


Verificar

Depois que o DUO for adicionado como uma origem para o 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
- Pressione **SYNC NOW** para acionar a sincronização completa inicial, como mostrado na imagem



Caso o problema persista com o XDR Device Insights e a integração DUO, 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.