Solución de problemas de XDR Device Insights y DUO Integration

Contenido

Introducción

Este documento describe los pasos para configurar la integración y resolver problemas de XDR Device Insights y la integración de Cisco DUO.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- XDR
- DUO
- Conocimiento básico de las API
- herramienta API Postman

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- XDR

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

XDR Device Insights proporciona una vista unificada de los dispositivos de su organización y consolida inventarios a partir de fuentes de datos integradas.

Duo protege a su personal y lleva la seguridad de acceso más allá del perímetro de la red corporativa para proteger sus datos en cada intento de autenticación, desde cualquier dispositivo y en cualquier lugar. Con Duo, puede confirmar sus identidades en un instante, supervisar el estado de los dispositivos administrados y no administrados, establecer políticas de seguridad adaptables adaptadas a su empresa, proteger el acceso remoto sin un agente de dispositivos y proporcionar un inicio de sesión único seguro y fácil de usar de forma rápida y sencilla.

Si desea obtener más información sobre la configuración, revise los detalles del módulo de integración.

Troubleshoot

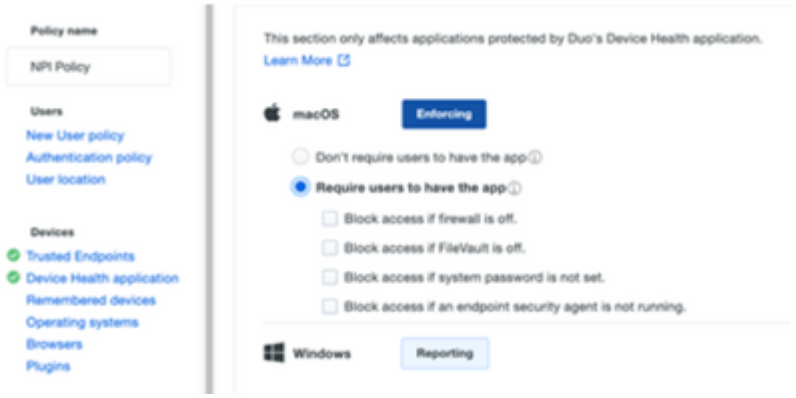
Para resolver problemas comunes con la integración XDR y DUO, puede verificar la conectividad y el rendimiento de la API.

Revisar el nivel de licencia

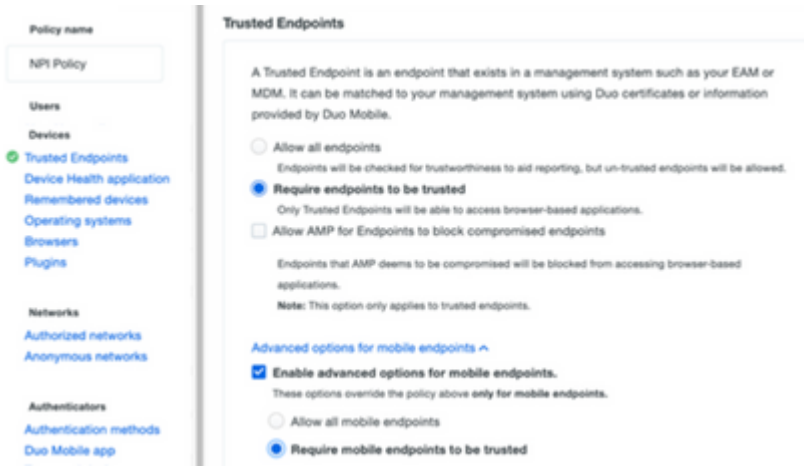
- Comprobación de la licencia en el **panel Duo Admin**
- Duo Licensed for Duo Access, Duo Beyond (o cualquier licencia de gama alta más reciente, solo MFA o gratuito no se aplica), como se muestra en la imagen

No hay datos de Duo

- Verifique que utiliza los datos de **Duo Health Agent** en la **Política de autenticación**, como se muestra en la imagen



- Verifique que utiliza **Trusted Endpoint** en **Auth Policy**, como se muestra en la imagen



Prueba de conectividad con XDR Device Insights y DUO

Puede utilizar la herramienta Postman para obtener una salida más visual mientras prueba la conectividad.

> **Nota**: Postman no es una herramienta de Cisco. Si tiene alguna pregunta sobre la funcionalidad de la herramienta Postman, póngase en contacto con el servicio de asistencia de Postman.

- El código de error 40301 "**Acceso prohibido**" significa que no tiene el nivel correcto de licencia, como se muestra en la imagen

- Puede seleccionar **No Auth** como método de autorización
- Puede utilizar esta llamada API para obtener una lista de los dispositivos (API devuelve el número máximo admitido de entradas por página), y puede encontrar documentación sobre la paginación de la API DUO

```
https://
```

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

- En respuesta a la primera llamada, se devuelve el número total de objetos (los parámetros offset y limit se pueden utilizar para obtener las páginas siguientes), como se muestra en la imagen

```
https://

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

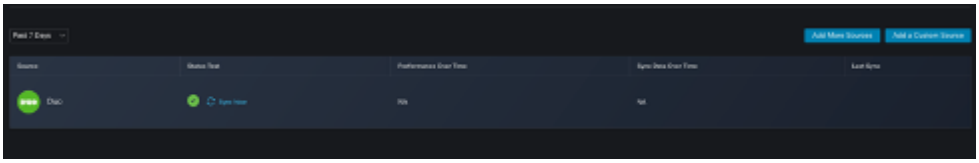
```
"metadata": {
    "total_objects": 64
},
```

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

Verificación

Una vez que se agrega DUO como fuente a XDR Device Insights, puede ver un estado de conexión **REST API** exitoso.

- Puede ver la conexión **API REST** con un estado verde
- Presione en **SYNC NOW** para activar la sincronización completa inicial, como se muestra en la imagen



En caso de que el problema persista con la integración de XDR Device Insights y DUO, recopile los registros HAR del navegador y póngase en contacto con el soporte del TAC para realizar un análisis más profundo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).