

# XDRデバイスの洞察とDUO統合のトラブルシューティング

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

## 概要

このドキュメントでは、統合を設定し、XDR Device InsightsとCisco DUO統合のトラブルシューティングを行う手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- XDR
- DUO
- APIの基礎知識
- Postman APIツール

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- XDR

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

XDR Device Insightsは、組織内のデバイスの統合ビューを提供し、統合されたデータソースのインベントリを統合します。

Duoは従業員の安全を確保し、企業ネットワークの境界を越えたアクセスセキュリティを実現し、認証を試みるたびに、デバイスや場所を問わずデータを保護します。Duoを使用すると、IDの一括確認、管理対象デバイスと管理対象外デバイスの状態の監視、ビジネスに合わせた適応型セキュリティポリシーの設定、デバイスエージェントなしのリモートアクセスの保護、安全で使いやすいシングルサインオンの迅速かつ簡単な提供が可能です。

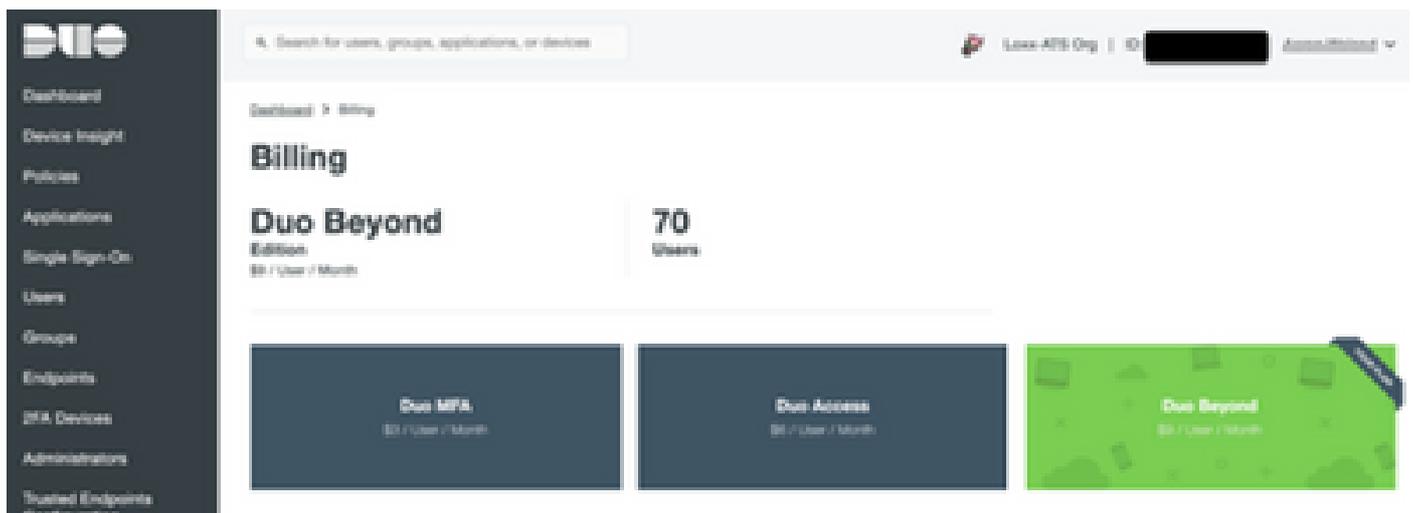
構成の詳細については、統合モジュールの詳細を参照してください。

## トラブルシューティング

XDRとDUOの統合に関する一般的な問題をトラブルシューティングするには、APIの接続性とパフォーマンスを確認します。

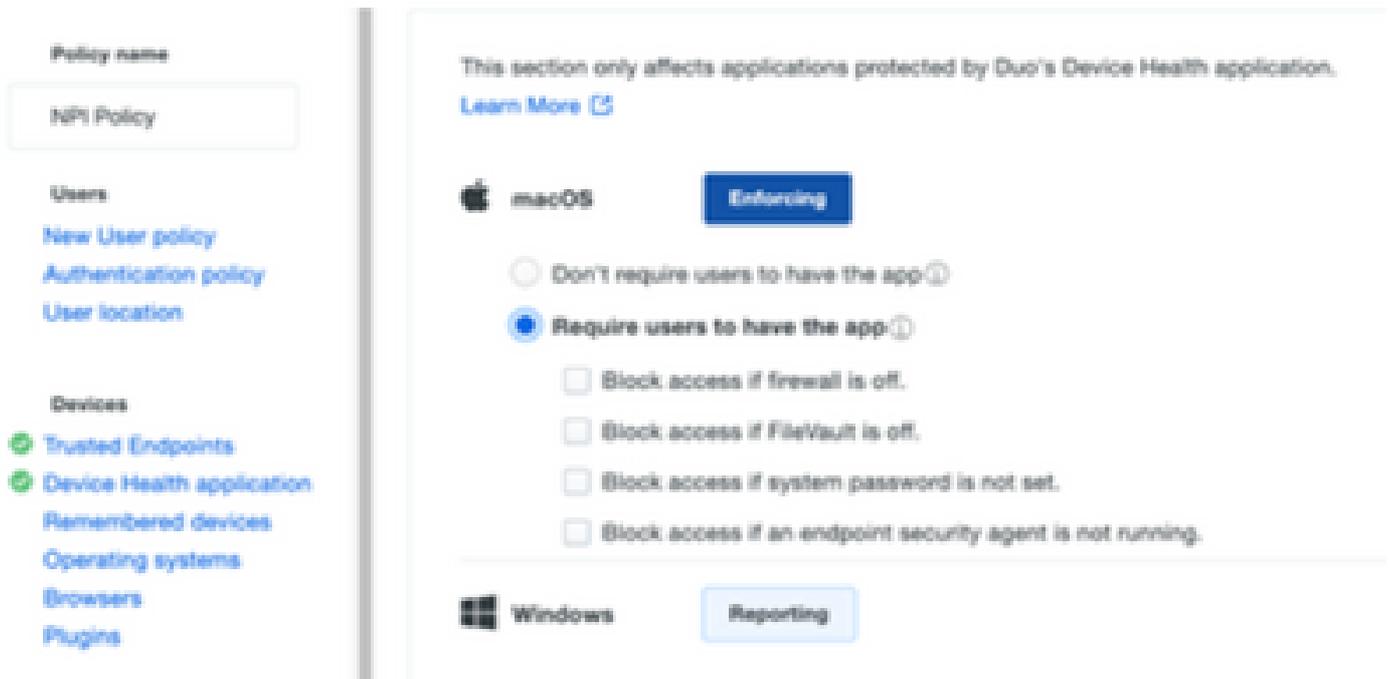
### ライセンスレベルの確認

- Duo Adminパネルでライセンスを確認
- Duo Licensed for Duo Access、Duo Beyond (または新しいハイエンドライセンス、MFAのみまたはFreeは適用されません) (図を参照)

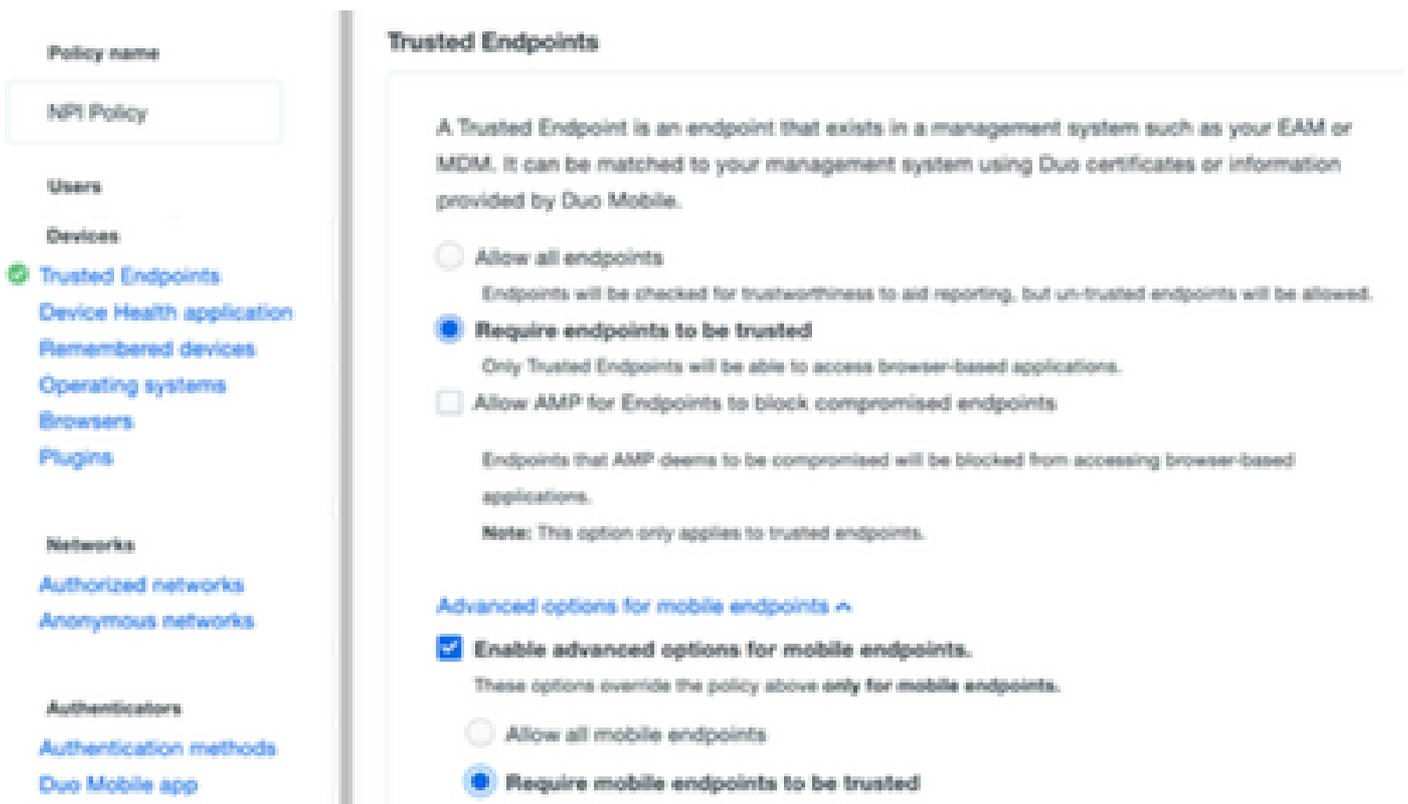


### Duoからデータなし

- 次の図に示すように、認証ポリシーでDuo Health Agentデータを使用していることを確認します



- 次の図に示すように、認証ポリシーで信頼できるエンドポイントを使用していることを確認します



## XDR Device InsightsとDUOによる接続テスト

Postmanツールを使用すると、接続をテストしながら、より視覚的な出力を得ることができます。

注:Postmanはシスコが開発したツールではありません。Postmanツールの機能について質

---

問がある場合は、Postmanサポートにお問い合わせください。

---

- エラーコード40301「Access Forbidden」は、図に示すように、適切なレベルのライセンスがないことを意味します



```
"code": 40301,  
"message": "Access forbidden",  
"stat": "FAIL"
```

- 認可方式としてNo Authを選択できます
- このAPI呼び出しを使用してデバイスのリストを取得できます ( APIは1ページ当たりのサポートされる最大エントリ数を返します )。また、DUO APIのページネーションに関する[ドキュメント](#)も参照できます

https://

/admin/v1/endpoints

- 最初の呼び出しに応答して、図に示すように、オブジェクトの合計数が返されます ( offsetおよびlimitパラメータを使用して次のページを取得できます )

https://

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

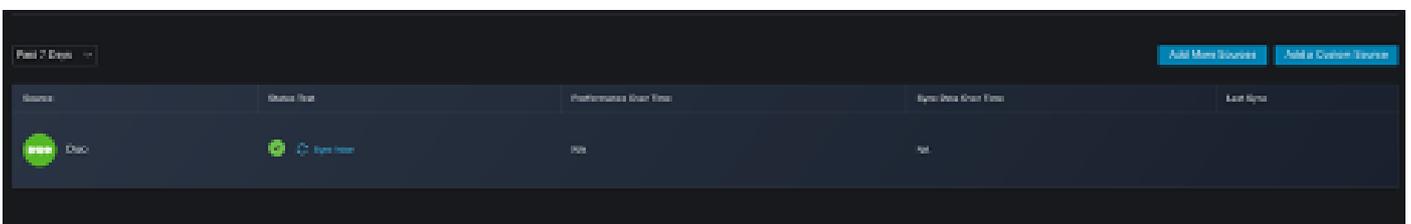
```
"metadata": {  
  "total_objects": 64  
},
```

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

## 確認

XDR Device InsightsのソースとしてDUOが追加されると、正常なREST API接続ステータスが表示されます。

- 緑色のステータスでREST API接続を確認できます
- 図に示すように、SYNC NOWを押して最初の完全同期をトリガーします



XDR Device InsightsとDUOの統合でも問題が解決しない場合は、ブラウザからHARログを収集し、TACサポートに連絡して、より詳細な分析を実行してください。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。