

排除XDR裝置洞察和DUO整合故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

簡介

本文檔介紹配置XDR裝置洞察和Cisco DUO整合以及對其進行故障排除的步驟。

必要條件

需求

思科建議您瞭解這些主題。

- XDR
- DUO
- API基礎知識
- Postman API工具

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據。

- XDR

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

XDR Device Insights提供組織中裝置的統一檢視，並整合來自整合資料來源的清單。

Duo可以保護您的員工安全，並在每次身份驗證嘗試時，從任何裝置、任何地點獲取企業網路邊界之外的訪問安全，以保護您的資料。藉助Duo，您可以在快照中確認您的身份、監控受管和非受管裝置的運行狀況、設定為您的企業量身定製的自適應安全策略、無需裝置代理即可確保遠端訪問的安全性，以及快速輕鬆地提供安全、使用者友好的單點登入。

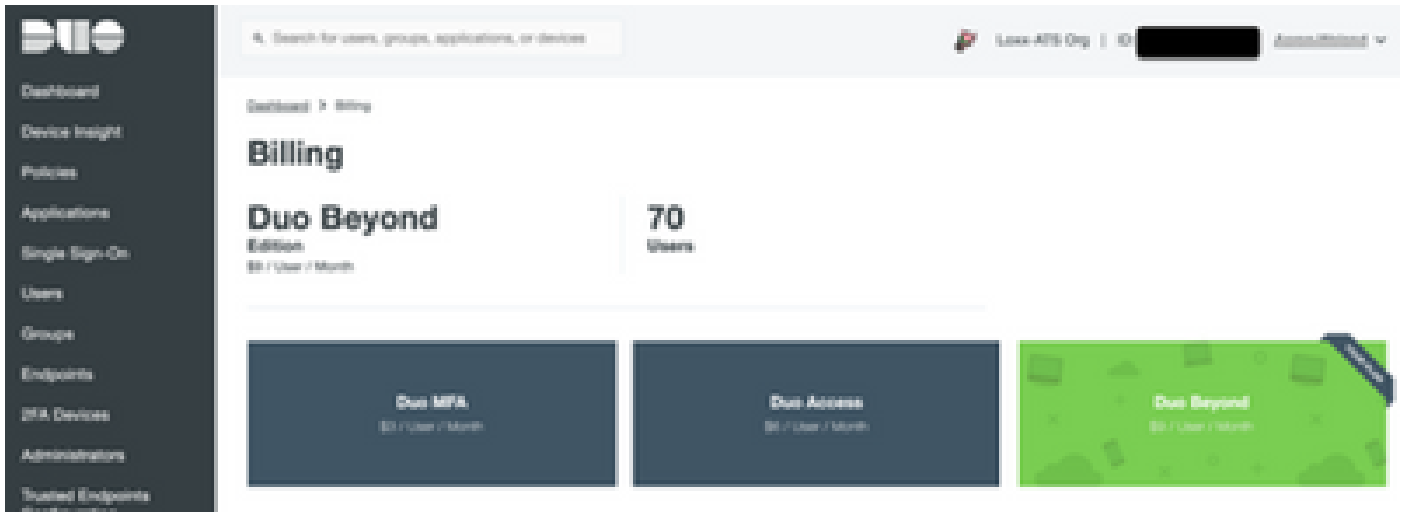
如果您想瞭解有關配置的更多資訊，請檢視整合模組的詳細資訊。

疑難排解

為了解決XDR和DUO整合的常見問題，您可以驗證API的連線和效能。

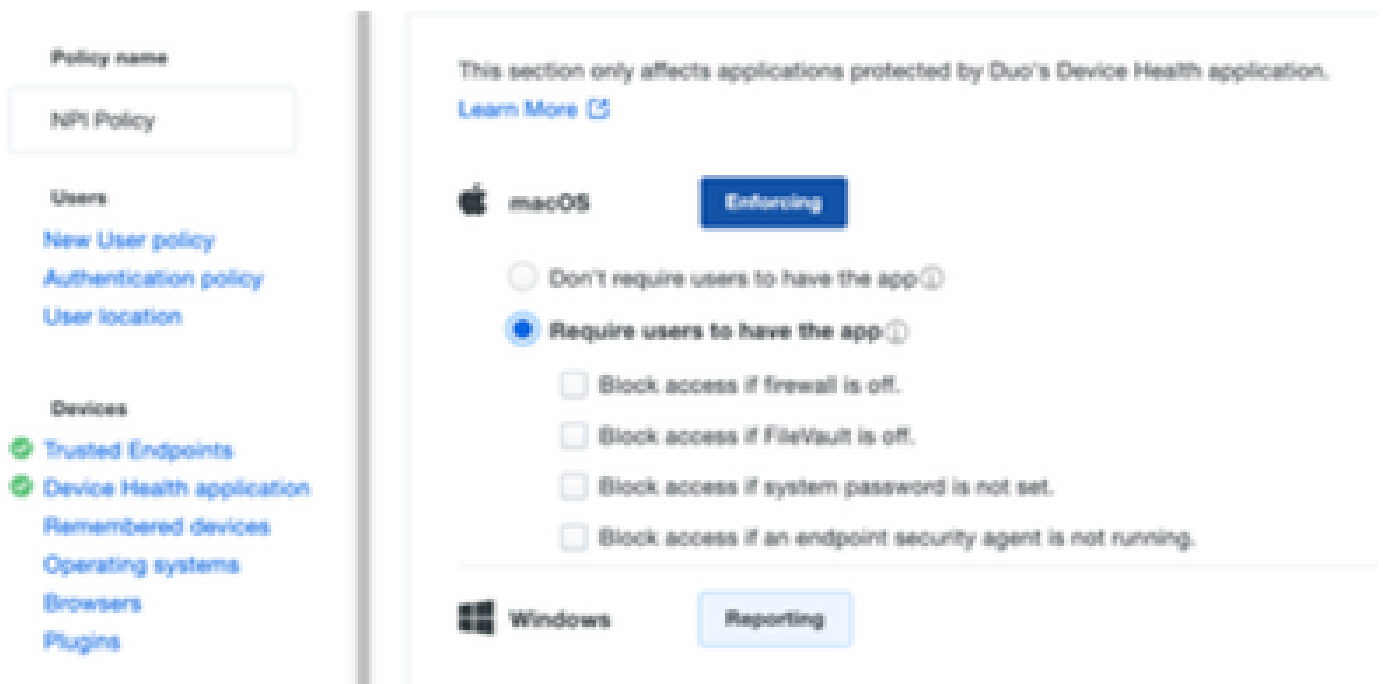
檢視許可證級別

- 在Duo Admin面板中檢查許可證
- Duo Licensed for Duo Access，Duo Beyond（或任何更新的高端許可證，僅MFA或免費不適用），如下圖所示



沒有來自Duo的資料

- 驗證是否在Auth Policy中使用Duo Health Agent資料，如下圖所示



- 驗證您是否在Auth Policy中使用Trusted Endpoint，如下圖所示

Policy name
NPI Policy

Users

Devices

Trusted Endpoints

Device Health application

Remembered devices

Operating systems

Browsers

Plugins

Networks

Authorized networks

Anonymous networks

Authenticators

Authentication methods

Duo Mobile app

Trusted Endpoints

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

- Allow all endpoints
Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.
- Require endpoints to be trusted**
Only Trusted Endpoints will be able to access browser-based applications.
- Allow AMP for Endpoints to block compromised endpoints
Endpoints that AMP deems to be compromised will be blocked from accessing browser-based applications.
Note: This option only applies to trusted endpoints.

Advanced options for mobile endpoints

- Enable advanced options for mobile endpoints.**
These options override the policy above only for mobile endpoints.
- Allow all mobile endpoints
- Require mobile endpoints to be trusted**

使用XDR Device Insights和DUO進行連線測試

測試連通性時，您可以使用Postman工具獲得更直觀的輸出。

注意:Postman不是思科開發的工具。如果您對Postman工具功能有任何疑問，請聯絡Postman支援。

- 錯誤代40301「Access Forbidden」表示您沒有適當級別的許可證，如下圖所示



- 您可以選擇No Auth作為授權方法
- 您可以使用此API呼叫獲取裝置清單（API返回每頁支援的最大條目數），還可以找到有關[DUO API分頁的文檔](#)

https://

/admin/v1/endpoints

- 響應第一個呼叫，返回對象的總數（偏移和限制引數可用於獲取下一頁），如下圖所示

https://

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

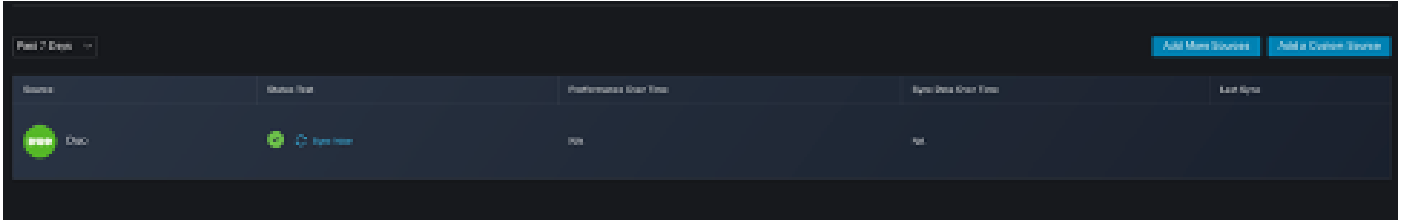
```
"metadata": {  
  "total_objects": 64  
},
```

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

驗證

將DUO新增為XDR裝置洞察的源後，您可以看到成功的REST API連接狀態。

- 您可以看到REST API連接處於綠色狀態
- 按SYNC NOW以觸發初始完全同步，如下圖所示



如果XDR裝置洞察和DUO整合問題仍然存在，請從瀏覽器收集HAR日誌，並聯絡TAC支援以執行更深入的分析。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。