配置Microsoft Graph API與Cisco XDR的整合

目錄

簡介

本文檔介紹將Microsoft Graph API與Cisco XDR整合的過程，以及可查詢的資料型別。

必要條件

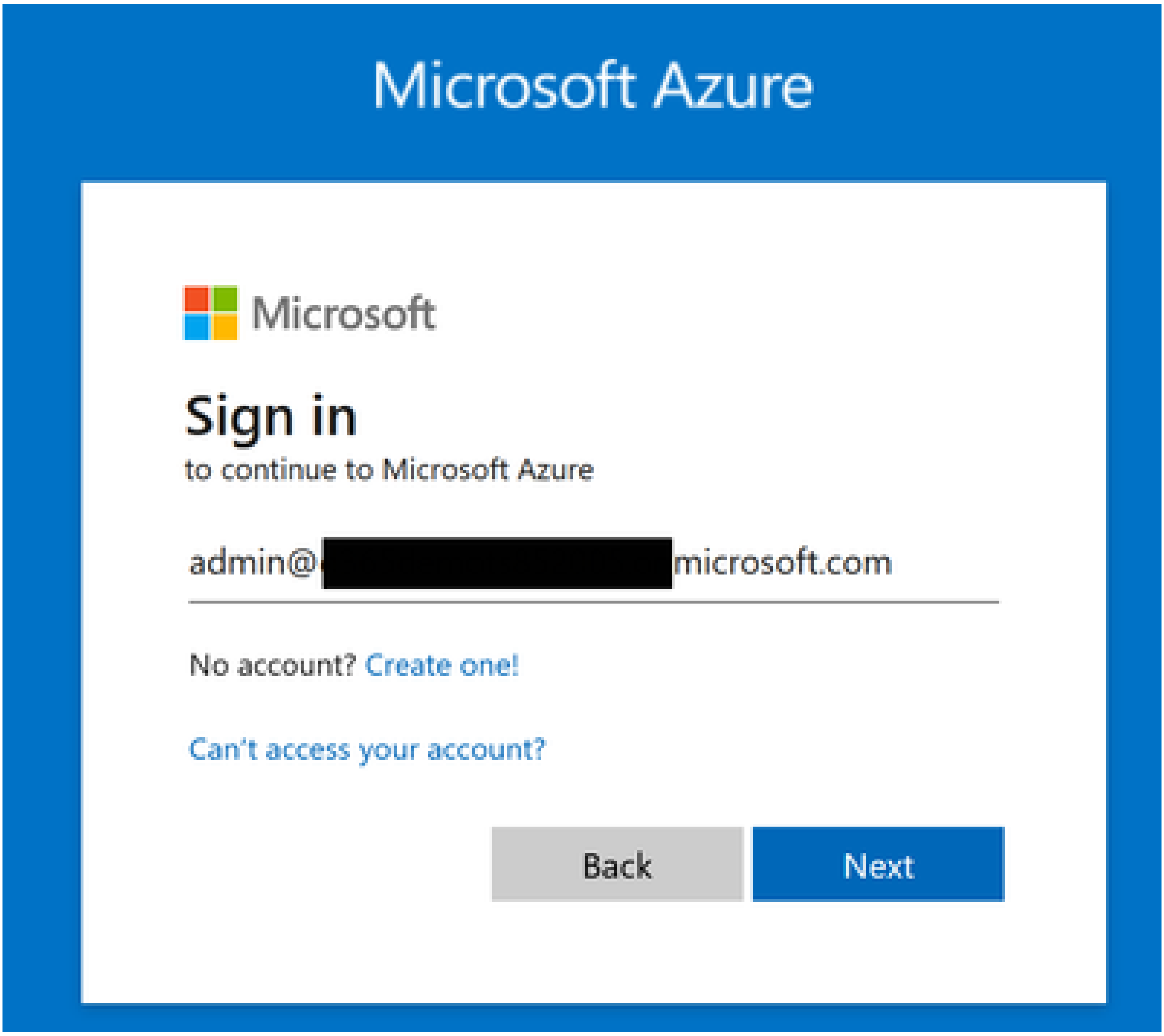
- Cisco XDR管理員帳戶
- Microsoft Azure系統管理員帳戶
- 訪問Cisco XDR

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。

整合步驟

步驟 1.

以系統管理員身份登入Microsoft Azure。



Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

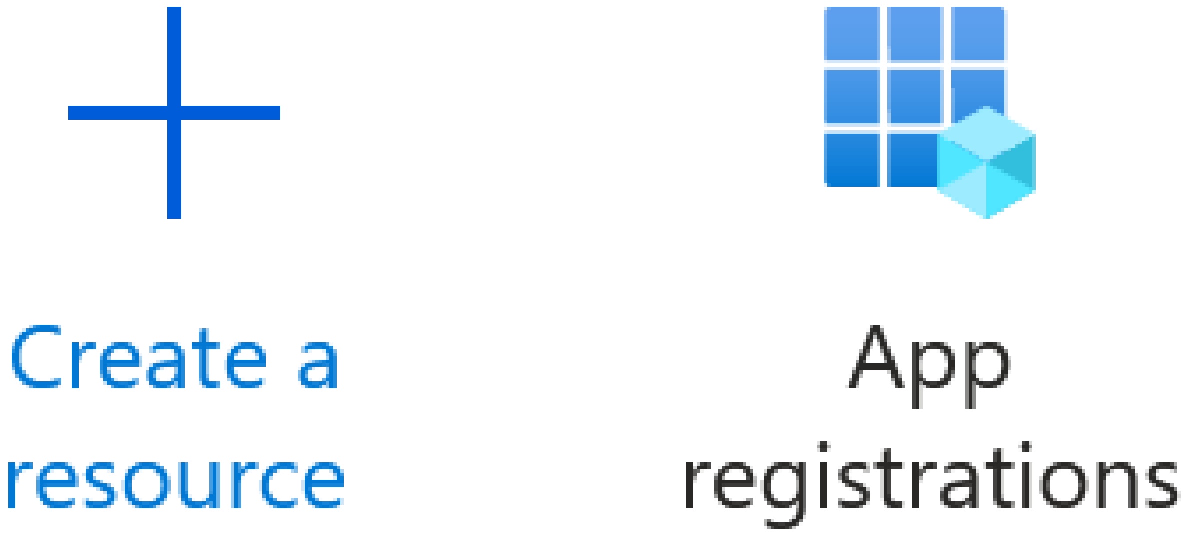
admin@[redacted]microsoft.com

No account? Create one!

Can't access your account?

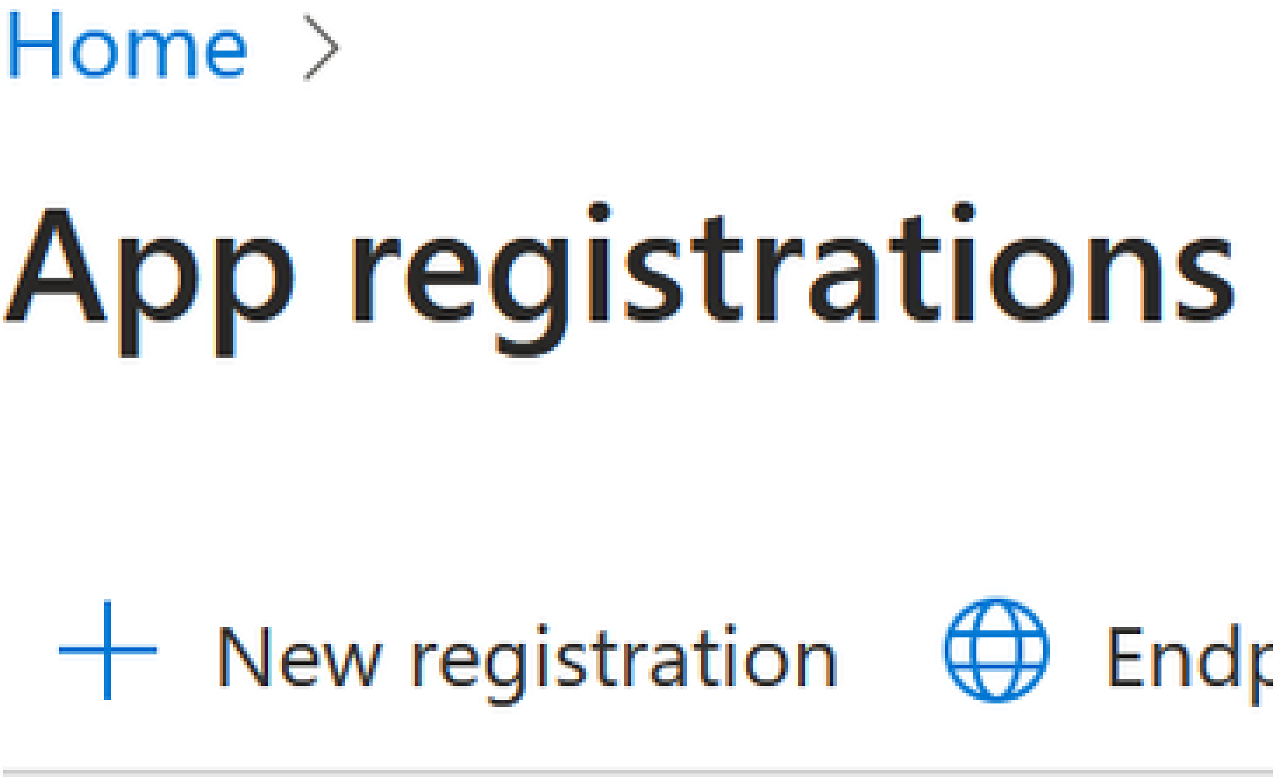
步驟 2.

點選**App Registrations** Azure服務門戶。



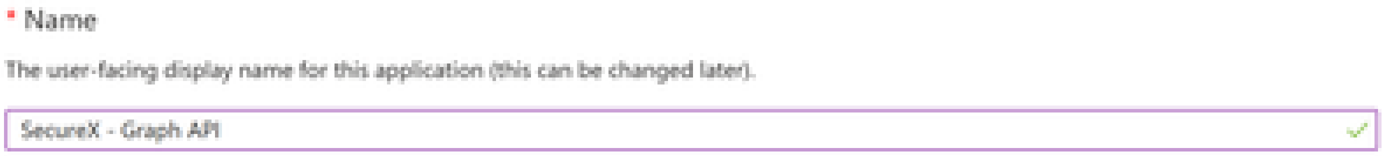
步驟 3.

按一下New registration。



步驟 4.

鍵入名稱以標識您的新應用。



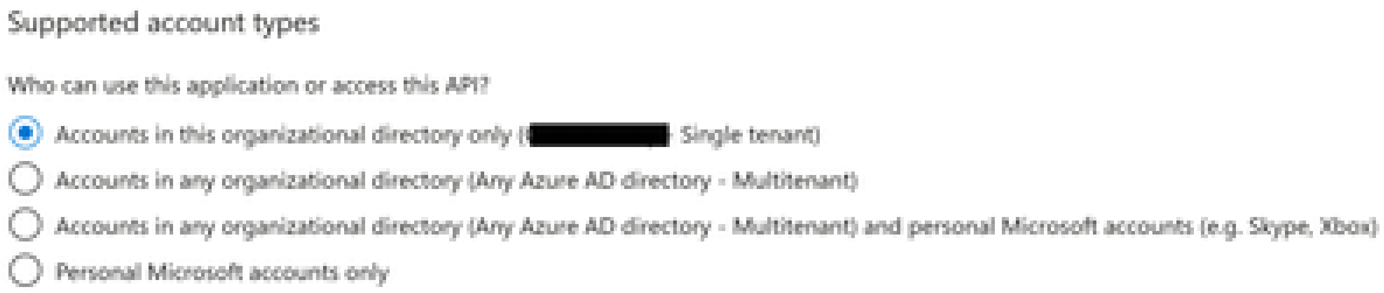
* Name

The user-facing display name for this application (this can be changed later).

SecureX - Graph API ✓

注意：如果名稱有效，會顯示綠色核取記號。

在支援的帳戶型別上，選擇 **Accounts in this organizational directory only**選項。



Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only ([redacted] - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

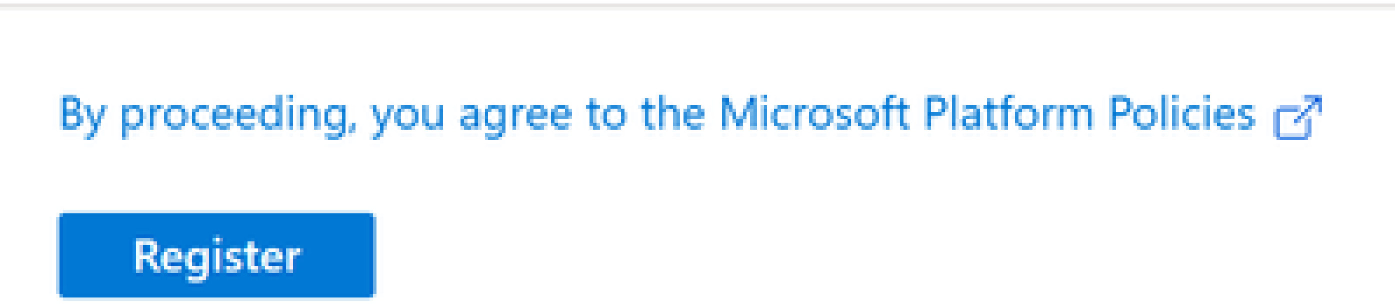
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

注意：您不需要輸入重新導向URI。

步驟 5.

滾動到螢幕底部並按一下 **Register**。

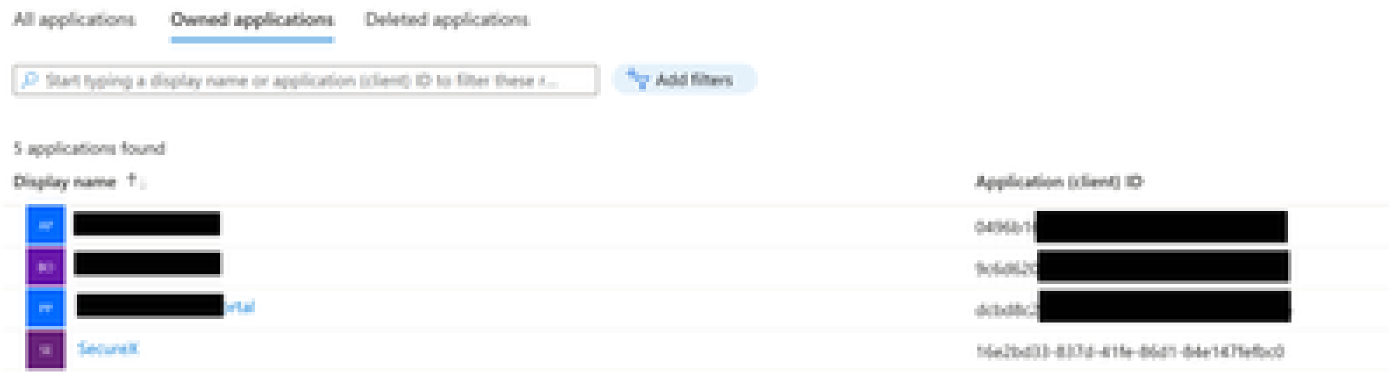


By proceeding, you agree to the Microsoft Platform Policies

步驟 6.

導航回Azure服務頁面，點選App Registrations > Owned Applications。

辨識您的應用程式並按一下名稱。在本例中為SecureX。



All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

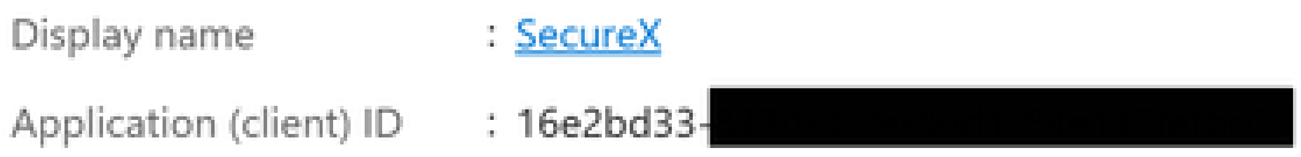
5 applications found

Display name	Application (client) ID
[redacted]	04966b1[redacted]
[redacted]	9c6d62[redacted]
[redacted]rtal	dcbd8c2[redacted]
SecureX	16e2bd33-837d-41fe-86d1-84e147fefbc0

步驟 7.

系統將顯示應用摘要。請確定以下相關詳細資訊：

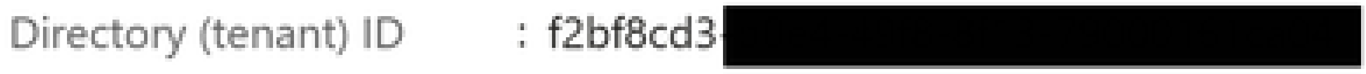
應用程式（使用者端）辨識碼：



Display name : SecureX

Application (client) ID : 16e2bd33-[redacted]

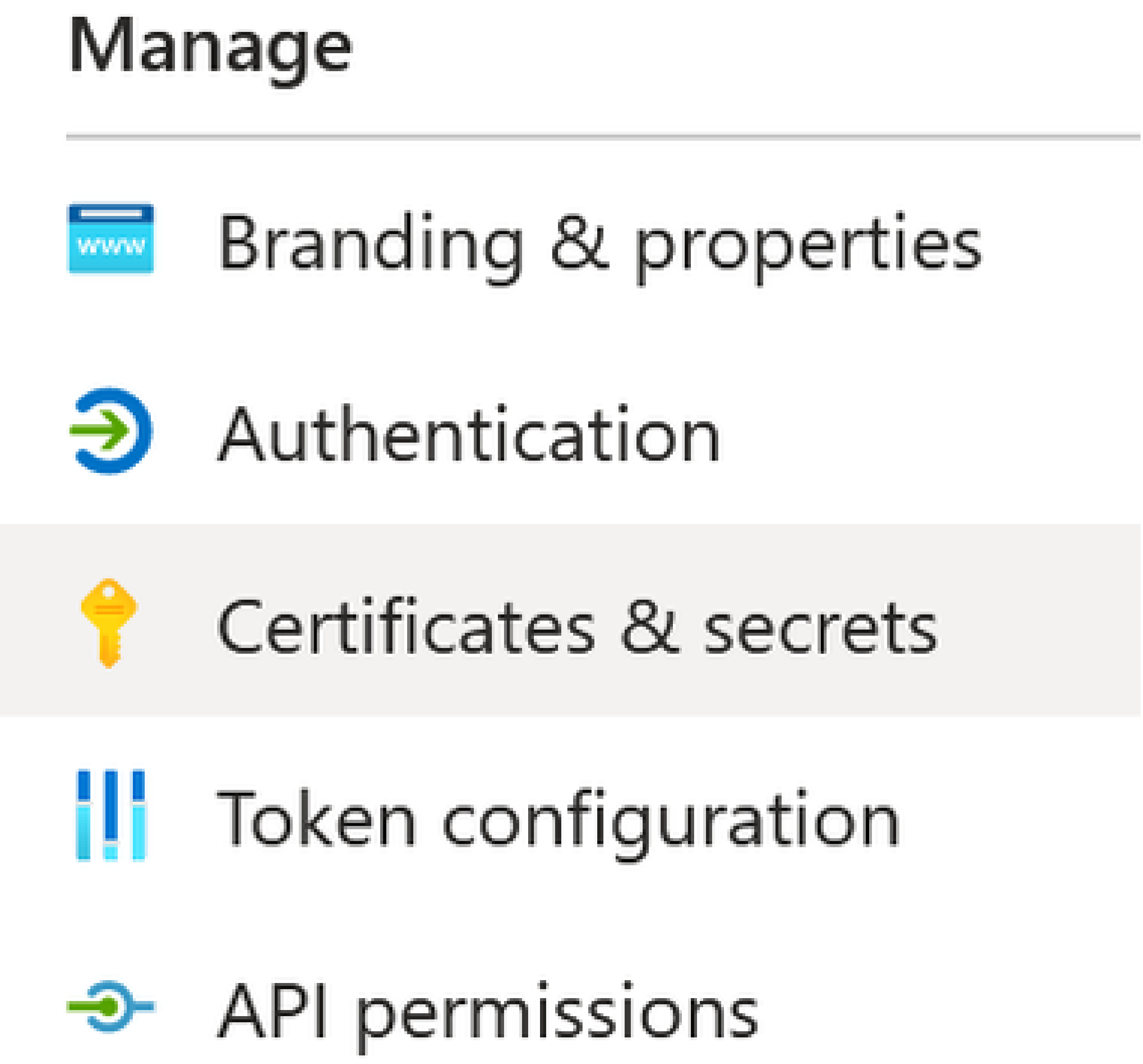
目錄（租戶） ID：



Directory (tenant) ID : f2bf8cd3[redacted]

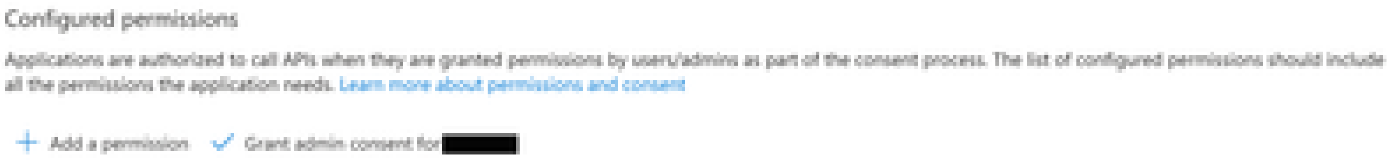
步驟 8.

導航到Manage Menu > API Permissions。



步驟 9.

在「配置的許可權」下，按一下Add a Permission。

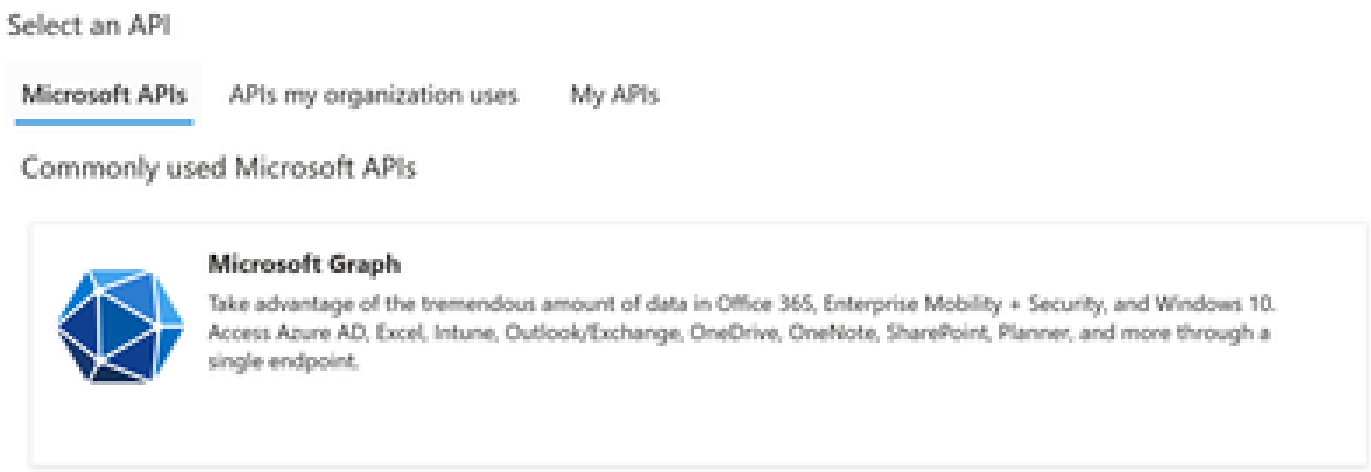


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

步驟 10.

在「請求API許可權」部分中，按一下 **Microsoft Graph**。



Select an API

Microsoft APIs | APIs my organization uses | My APIs

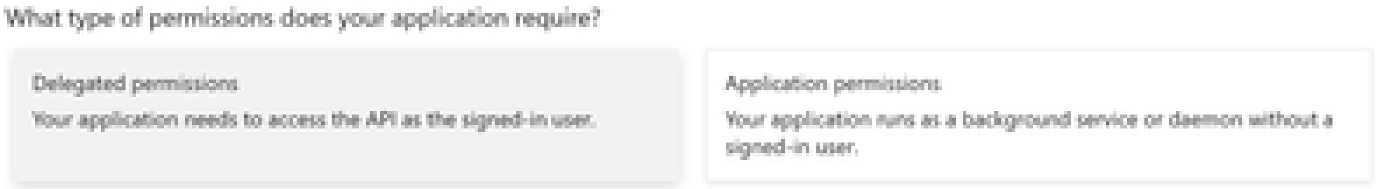
Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

步驟 11.

選擇Application permissions。



What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

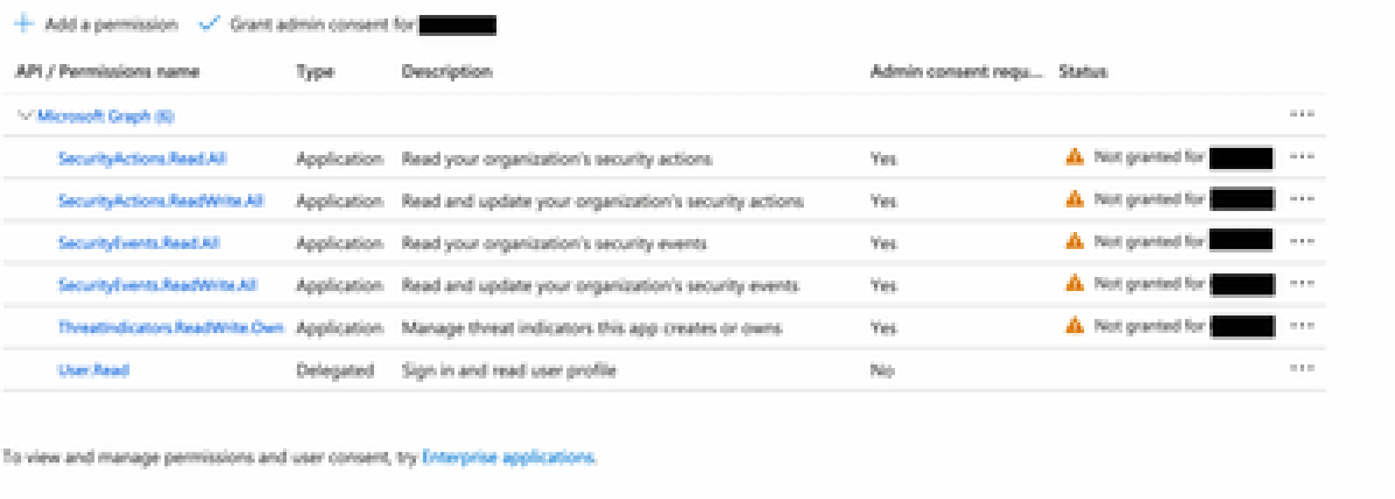
在搜尋欄中查詢Security。展開 **Security Actions** 並選取

- **全部讀取**
- **全部讀取**
- **安全事件並選擇**
  - **全部讀取**
  - **全部讀取**
- **威脅指示器並選擇**
  - **ThreatIndicators.ReadWrite.OwnedBy**

按一下Add permissions。

步驟 12.

檢閱您選取的許可權。

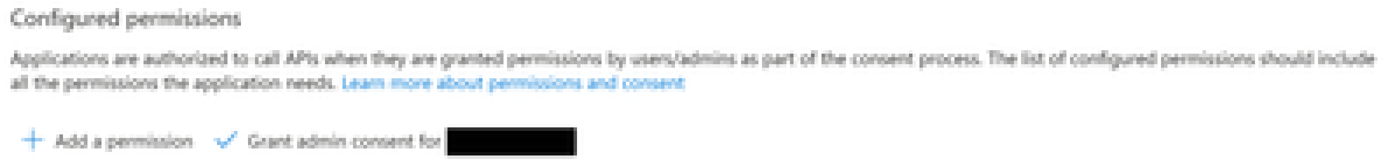


＋ Add a permission ✓ Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent requ...	Status	
∨ Microsoft Graph (6)					···
SecurityActions.Read.All	Application	Read your organization's security actions	Yes	⚠ Not granted for [redacted]	···
SecurityActions.ReadWrite.All	Application	Read and update your organization's security actions	Yes	⚠ Not granted for [redacted]	···
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	⚠ Not granted for [redacted]	···
SecurityEvents.ReadWrite.All	Application	Read and update your organization's security events	Yes	⚠ Not granted for [redacted]	···
ThreatIndicators.ReadWrite.Own	Application	Manage threat indicators this app creates or owns	Yes	⚠ Not granted for [redacted]	···
User.Read	Delegated	Sign in and read user profile	No		···

To view and manage permissions and user consent, try Enterprise applications.

按一下 **Grant Admin consent** 以取得您的組織。



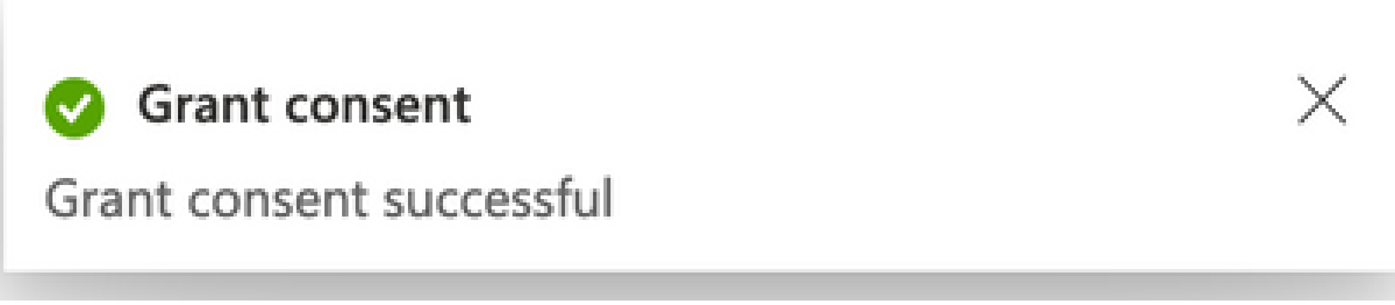
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

＋ Add a permission ✓ Grant admin consent for [redacted]

出現一個提示，提示您選擇是否要同意所有許可權。按一下Yes。

將會顯示類似快顯視窗，如下圖所示：



Grant consent

Grant consent successful

步驟 13.

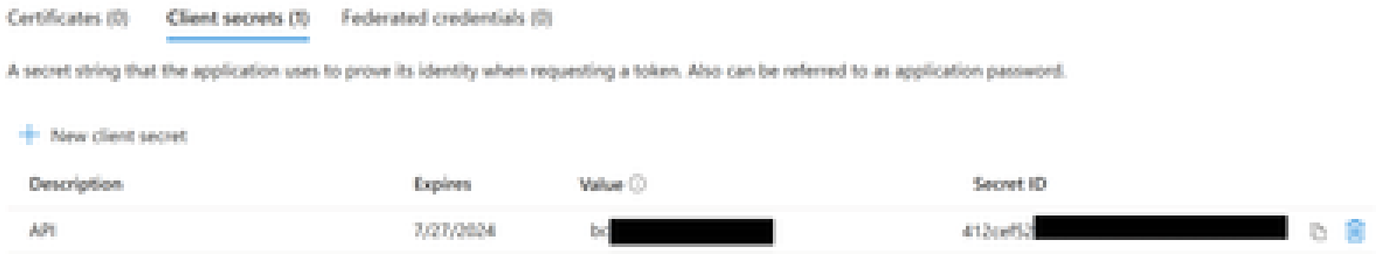
導航到Manage > Certificates & Secrets。

按一下Add New Client Secret。

撰寫簡短描述並選取有效的日期Expires。建議選擇6個月以上的有效日期，以防止API金鑰過期。

建立後，將說明 **Value**的部分複製並儲存在安全位置，因為它可用於整合。

警告：此欄位無法恢復，您必須建立新金鑰。



Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

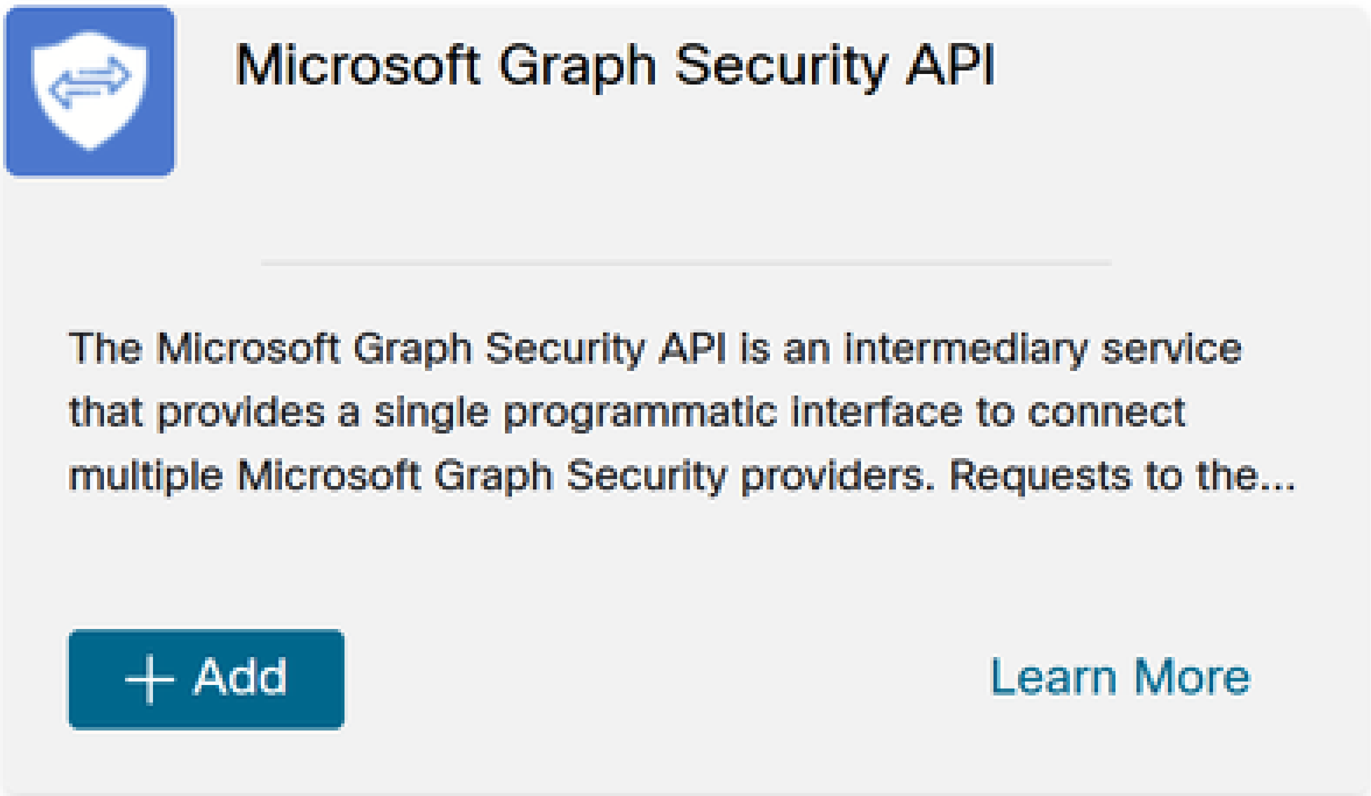
Description	Expires	Value ⓘ	Secret ID
API	7/27/2024	[redacted]	[redacted]

警告：此欄位無法恢復，您必須建立新金鑰。

獲取所有資訊後，導航回 **Overview** 並複製應用的值。然後導航到SecureX。

步驟 14.

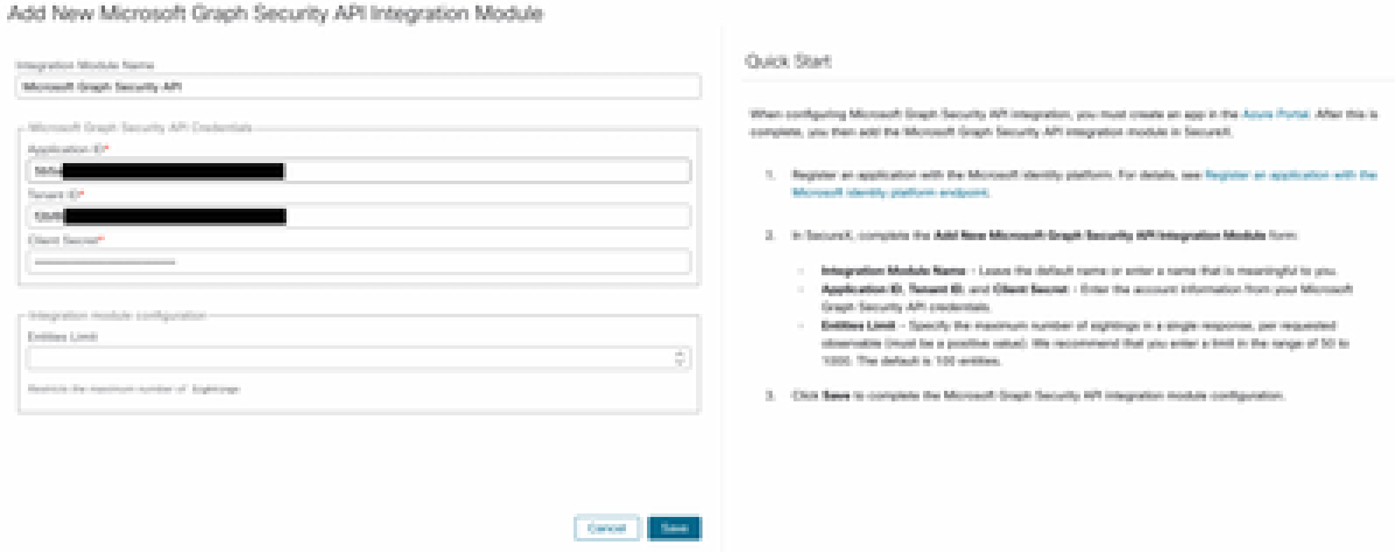
導航到Integration Modules > Available Integration Modules > 選擇Microsoft Security Graph API，點選Add。



Microsoft Graph Security API

The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers. Requests to the...

分配名稱並貼上您從Azure門戶獲得的值。



Add New Microsoft Graph Security API Integration Module

Integration Module Name: Microsoft Graph Security API

Microsoft Graph Security API Credentials

Application ID*: [redacted]

Tenant ID*: [redacted]

Client Secret*: ••••••••••••••••••••

Integration module configuration

Entities Limit:

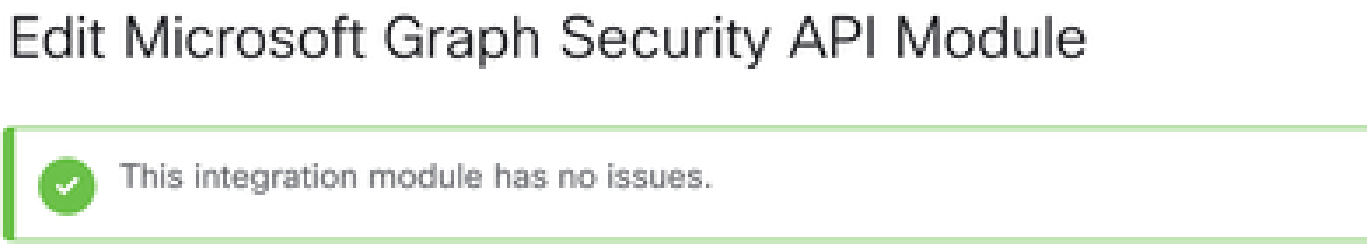
Restrict the maximum number of Sightings

Quick Start

When configuring Microsoft Graph Security API integration, you must create an app in the Azure Portal. After this is complete, you then add the Microsoft Graph Security API integration module in SecureX.

1. Register an application with the Microsoft identity platform. For details, see Register an application with the Microsoft identity platform endpoint.
2. In SecureX, complete the **Add New Microsoft Graph Security API Integration Module** form:
   - **Integration Module Name** - Leave the default name or enter a name that is meaningful to you.
   - **Application ID, Tenant ID**, and **Client Secret** - Enter the account information from your Microsoft Graph Security API credentials.
   - **Entities Limit** - Specify the maximum number of sightings in a single response, per requested observable (must be a positive value). We recommend that you enter a limit in the range of 50 to 1000. The default is 100 entities.
3. Click **Save** to complete the Microsoft Graph Security API integration module configuration.

按一下Save，然後等待運行狀況檢查成功。



Edit Microsoft Graph Security API Module

This integration module has no issues.

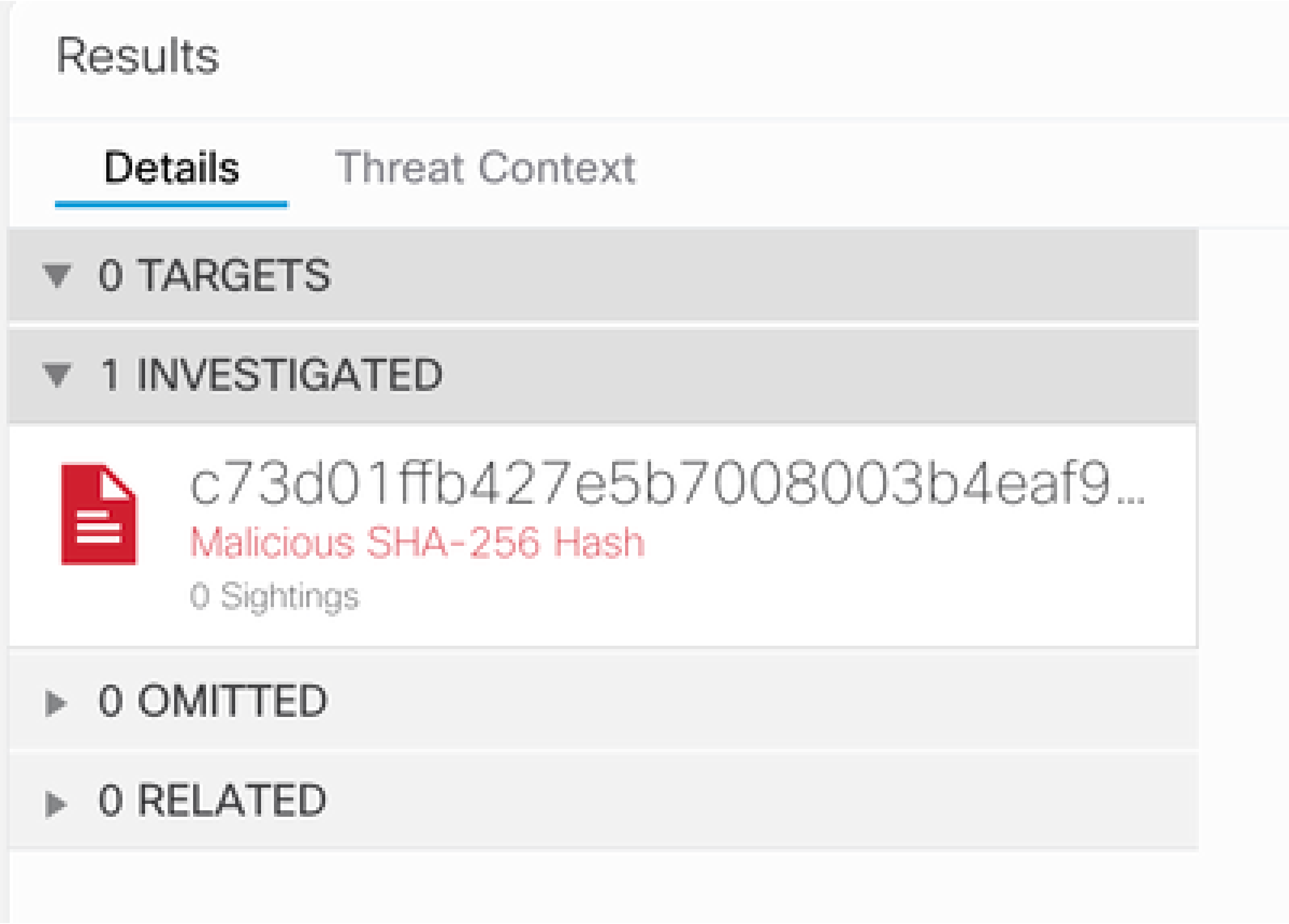
執行調查

目前，Microsoft Security Graph API未在Cisco XDR Dashboard中填充磁貼。相反，可以使用調查來查詢Azure門戶中的資訊。

請記住，Graph API只能查詢：

- ip
- 網域
- 主機名
- url
- 檔案名稱
- file_path
- sha256

在本示例中，調查使用了此SHAc73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148。



Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED

c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

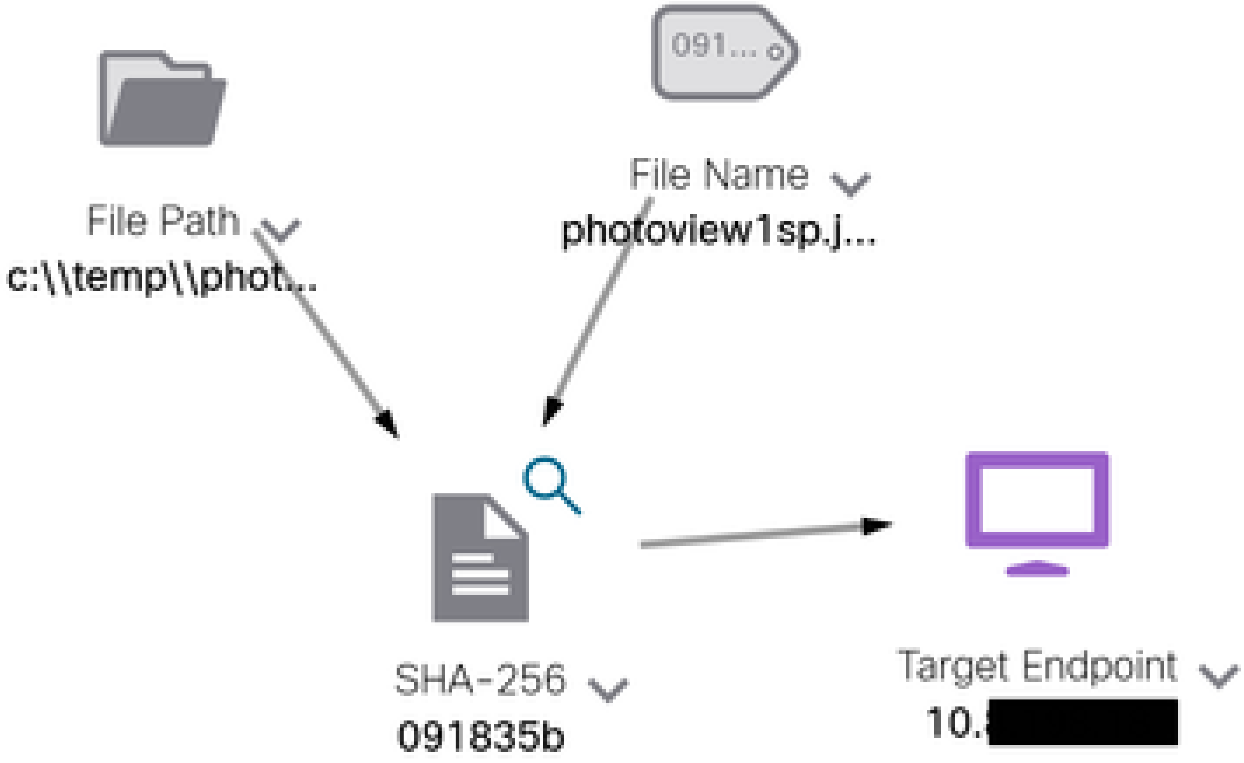
如您所見，它在實驗室環境中有0次發現，那麼如何測試Graph API是否有效？

打開WebDeveloper工具，運行調查，然後找到名為Observables的檔案並發佈到**visibility.amp.cisco.com**的事件。

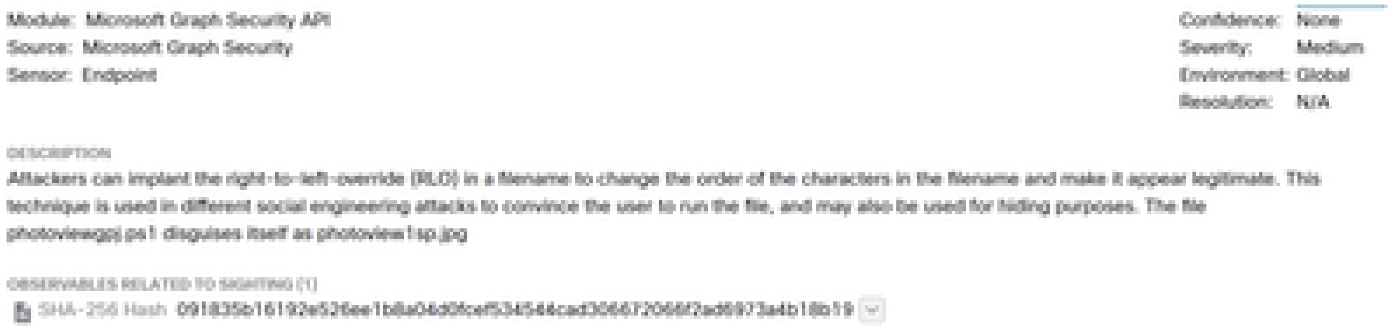
驗證

您可以使用此連結：[Microsoft graph security Snapshots]()獲取快照清單，可幫助您瞭解可以從每種型別的可觀察得到的響應。

您可以看到如下圖所示的範例：



展開視窗，您可以看到整合所提供的資訊：


Module: Microsoft Graph Security API
Source: Microsoft Graph Security
Sensor: Endpoint

Confidence: None
Severity: Medium
Environment: Global
Resolution: N/A

DESCRIPTION

Attackers can implant the right-to-left-override (RLO) in a filename to change the order of the characters in the filename and make it appear legitimate. This technique is used in different social engineering attacks to convince the user to run the file, and may also be used for hiding purposes. The file photoviewgpj.ps1 disguises itself as photoview1sp.jpg

OBSERVABLES RELATED TO SIGHTING (1)

SHA-256 Hash 091835b16192e526ee1b8a04d0fcef534544cad306672066f2ad6973a4b18b19

請記住，資料必須存在於Azure門戶中，當與其他Microsoft解決方案一起使用時，Graph API的運行效果更好。但是，這必須由Microsoft支援部門進行驗證。

疑難排解

- 授權失敗的訊息：
  - 確保 **Tenant ID** 和Client ID的值正確並且仍然有效。

- 調查中未顯示任何資料：

  - 確保複製並貼上了 **Tenant ID** 和 **Client ID**的適當值。

    - 確保使用了Certificates & Secrets部分 **Value** 的欄位資訊。

    - 使用WebDeveloper工具確定調查發生時是否查詢圖形API。

    - 當Graph API合併來自各種Microsoft警報提供者的資料時，請確保查詢過濾器支援OData。（例如，Office 365安全與合規性和Microsoft Defender ATP）。

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）。