تكوين تكامل Microsoft Graph API باستخدام Cisco XDR.

المحتويات

المقدمة

يصف هذا المستند إجراء دمج واجهة برمجة تطبيقات Microsoft Graph مع Cisco XDR، ونوع البيانات التي يمكن الاستعلام عنها.

المتطلبات الأساسية

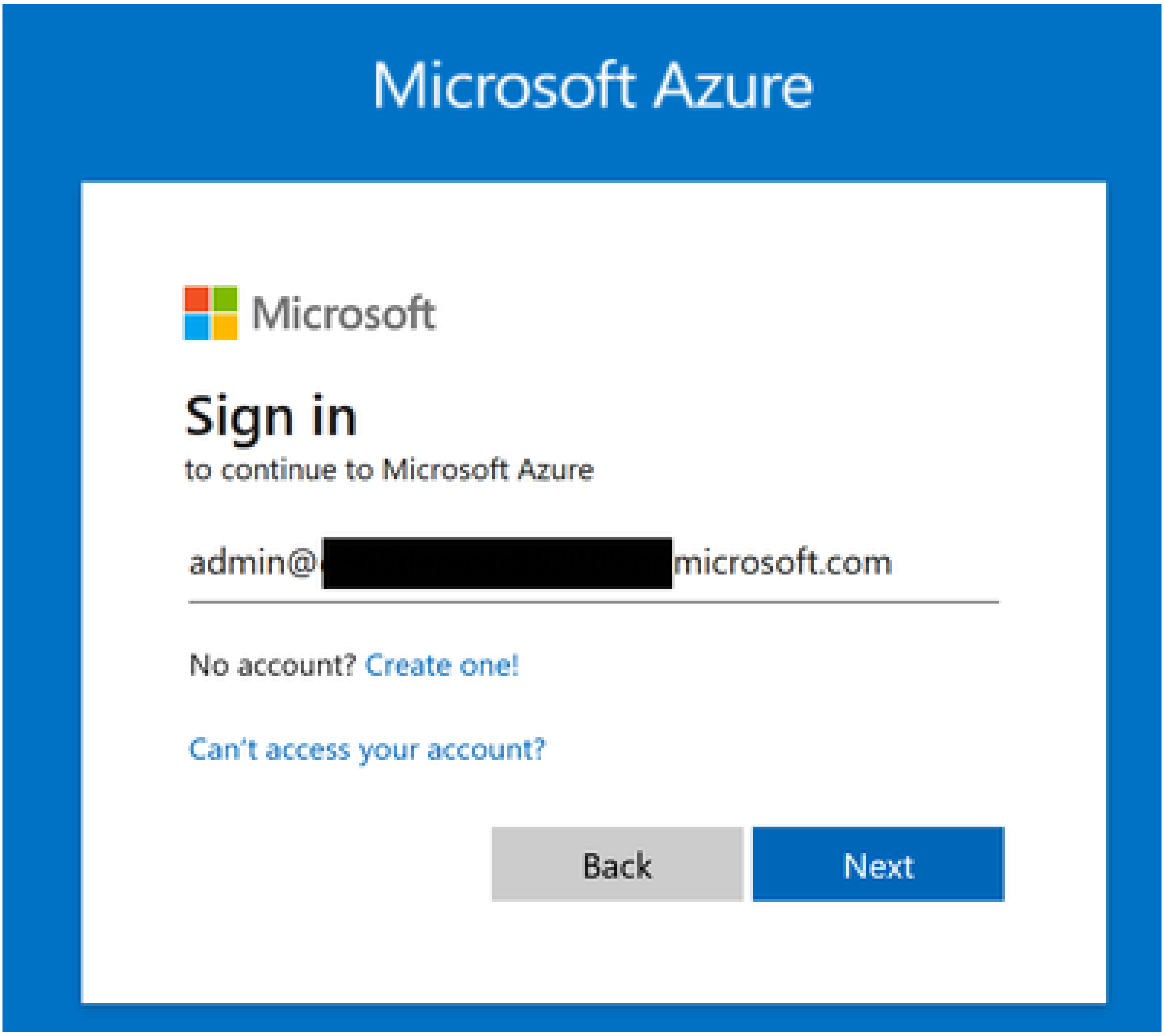
- حساب مسؤول XDR من Cisco
- حساب مسؤول نظام Microsoft Azure
- الوصول إلى Cisco XDR

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

خطوات التكامل

الخطوة 1.

قم بتسجيل الدخول إلى Microsoft Azure كمسؤول نظام.



Microsoft Azure

Sign in

to continue to Microsoft Azure

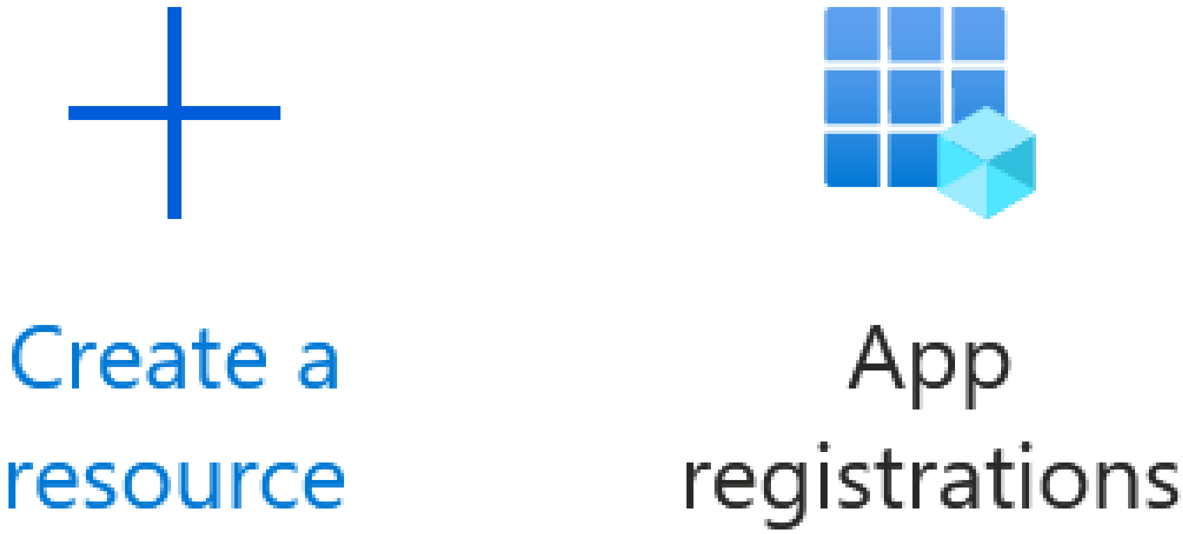
admin@[redacted]microsoft.com

No account? Create one!

Can't access your account?

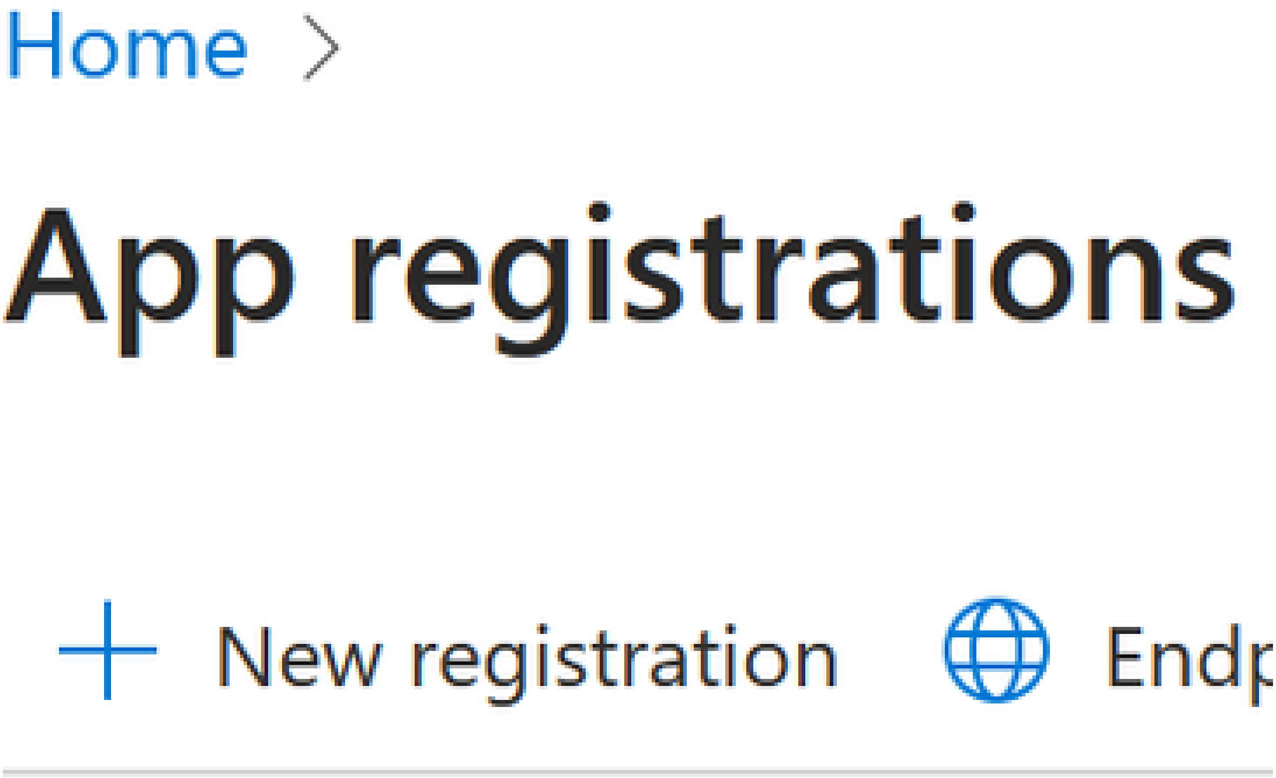
الخطوة 2.

انقر **App Registrations** على مدخل خدمات Azure.



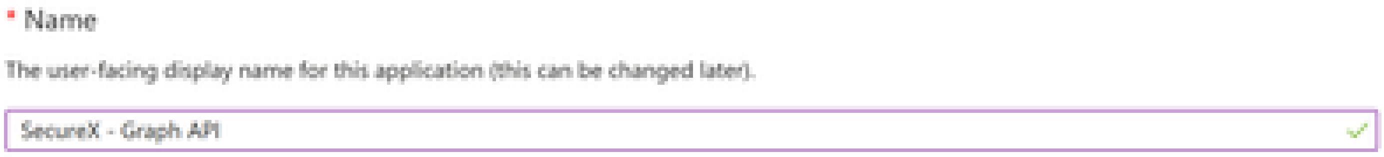
الخطوة 3.

انقر New registration.



الخطوة 4.

اكتب اسما لتعريف التطبيق الجديد.



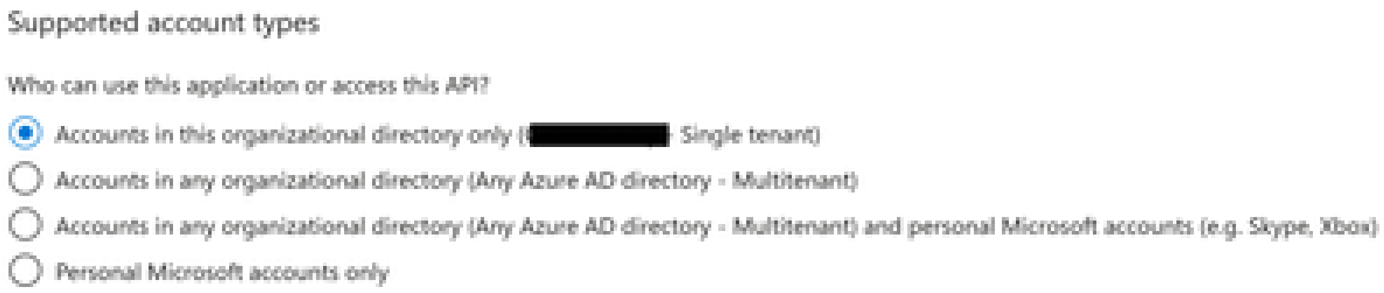
* Name

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

SecureX - Graph API ✓

ملاحظة: تظهر علامة تأشير خضراء إذا كان الاسم صحيحا.

في "أنواع الحساب المدعومة"، أختر الخيار **Accounts in this organizational directory only**.



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)

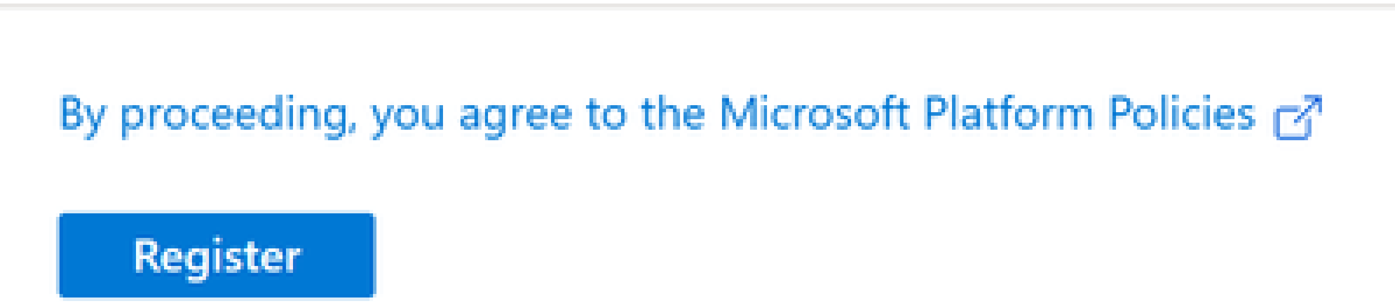
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

ملاحظة: لا تحتاج إلى كتابة URI لإعادة التوجيه.

الخطوة 5.

قم بالتمرير إلى أسفل الشاشة وانقر **Register**.

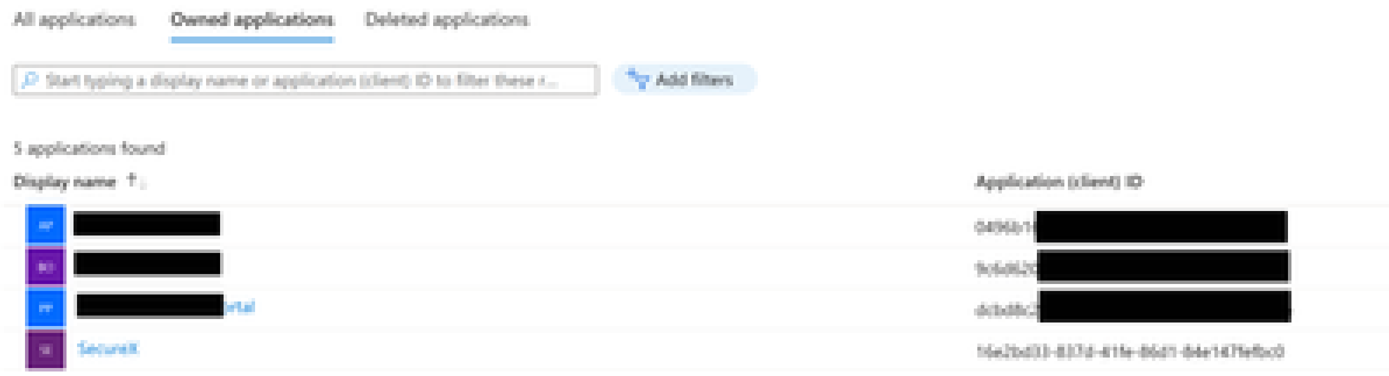


By proceeding, you agree to the Microsoft Platform Policies

الخطوة 6.

انتقل للخلف إلى صفحة خدمات Azure، انقر App Registrations > Owned Applications.

تعرف على التطبيق وانقر فوق الاسم. في هذا المثال، SecureX.



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

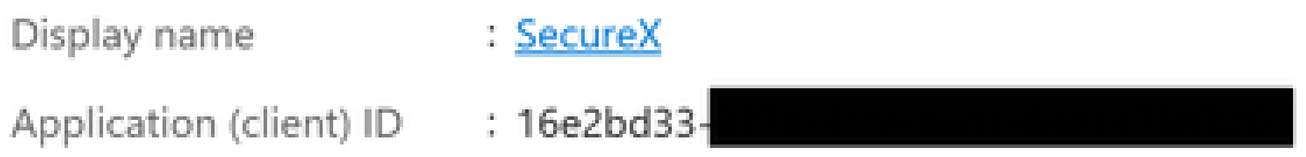
5 applications found

Display name	Application (client) ID
[redacted]	04f96b1[redacted]
[redacted]	9c6d62[redacted]
[redacted]ortal	dcbd8c2[redacted]
SecureX	16e2bd33-837d-41fe-86d1-84e147fefbc0

الخطوة 7.

يظهر ملخص للتطبيق الخاص بك. يرجى تحديد هذه التفاصيل ذات الصلة:

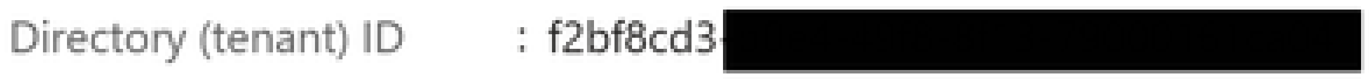
معرف التطبيق (العميل):



Display name : SecureX

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

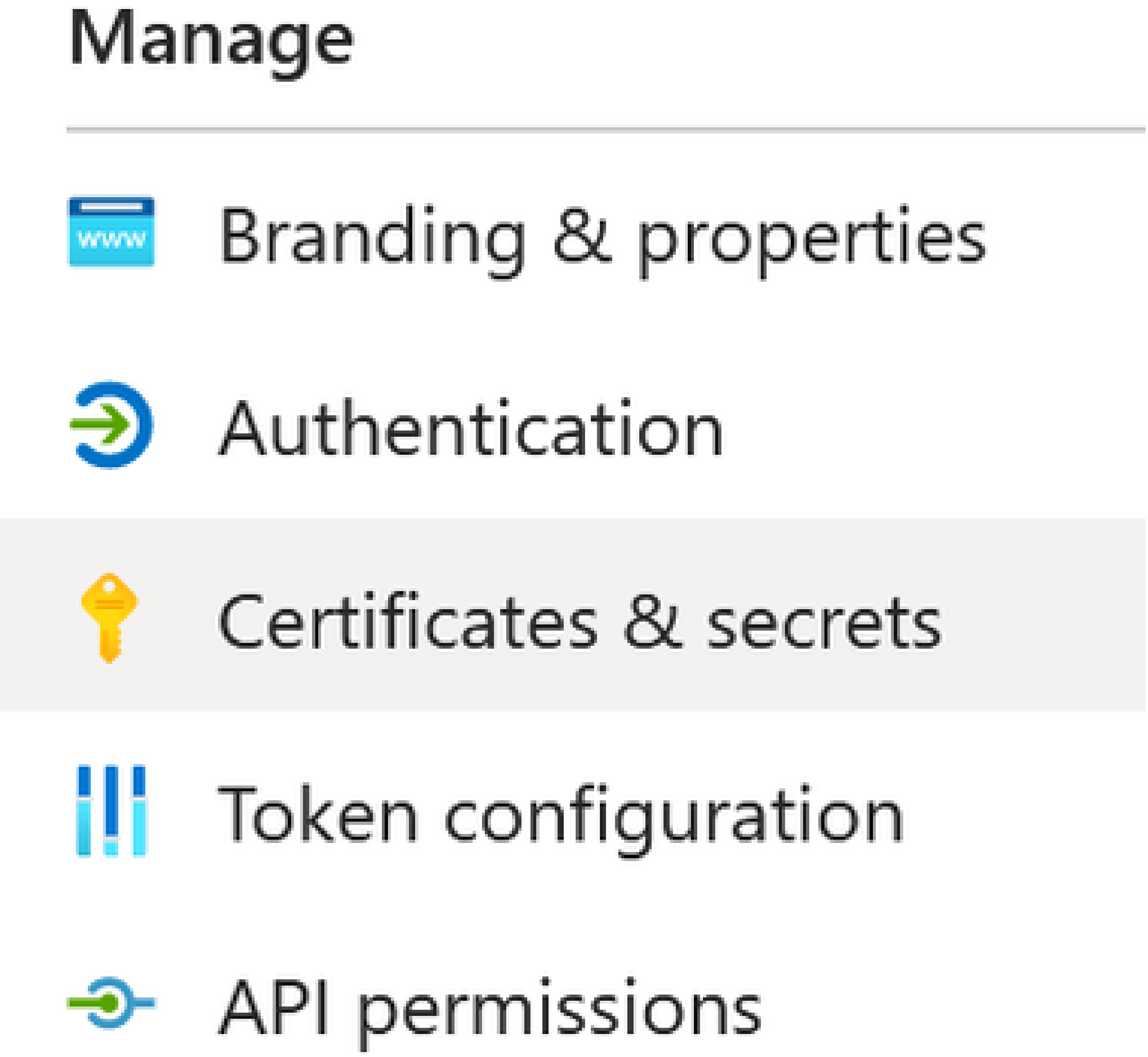
معرف الدليل (المستأجر):



Directory (tenant) ID : f2bf8cd3-[redacted]

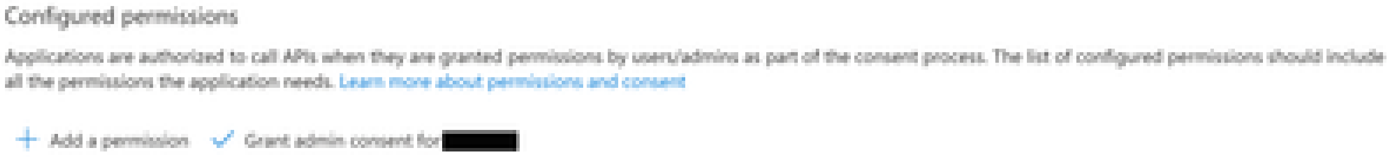
الخطوة 8.

انتقل إلى Manage Menu > API Permissions.



الخطوة 9.

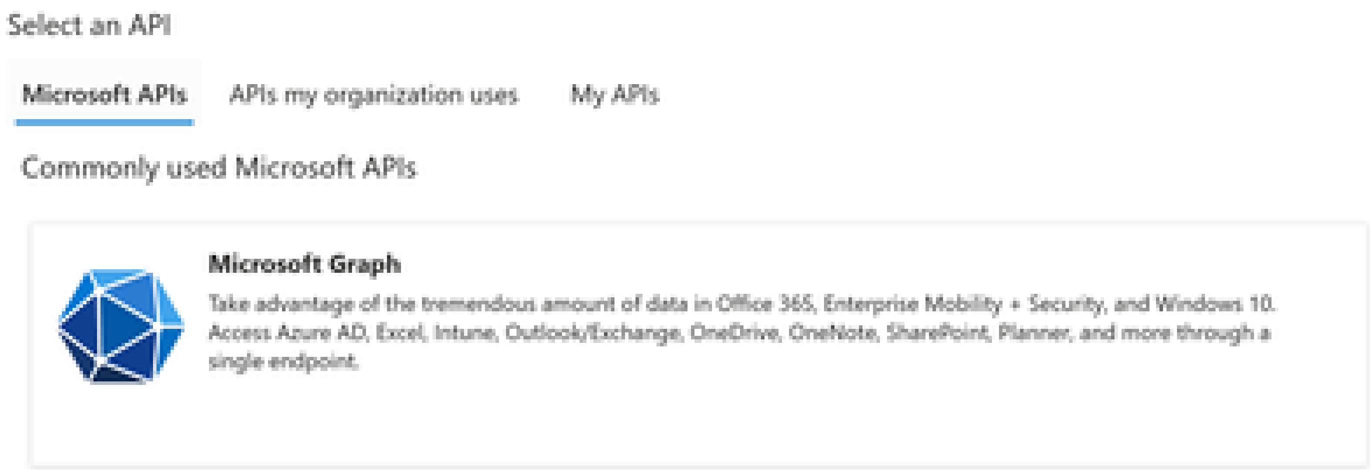
تحت أذونات تم تكوينها، انقر فوق Add a Permission.


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

الخطوة 10.

في القسم طلب أذونات واجهة برمجة التطبيقات (API)، انقر **Microsoft Graph**.



Select an API

Microsoft APIs | APIs my organization uses | My APIs

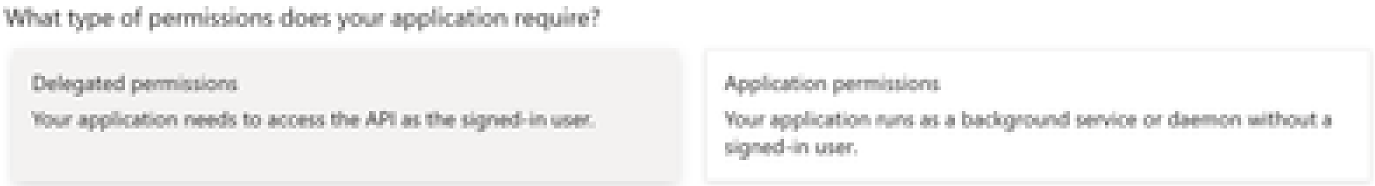
Commonly used Microsoft APIs

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.

الخطوة 11.

تحديد 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.

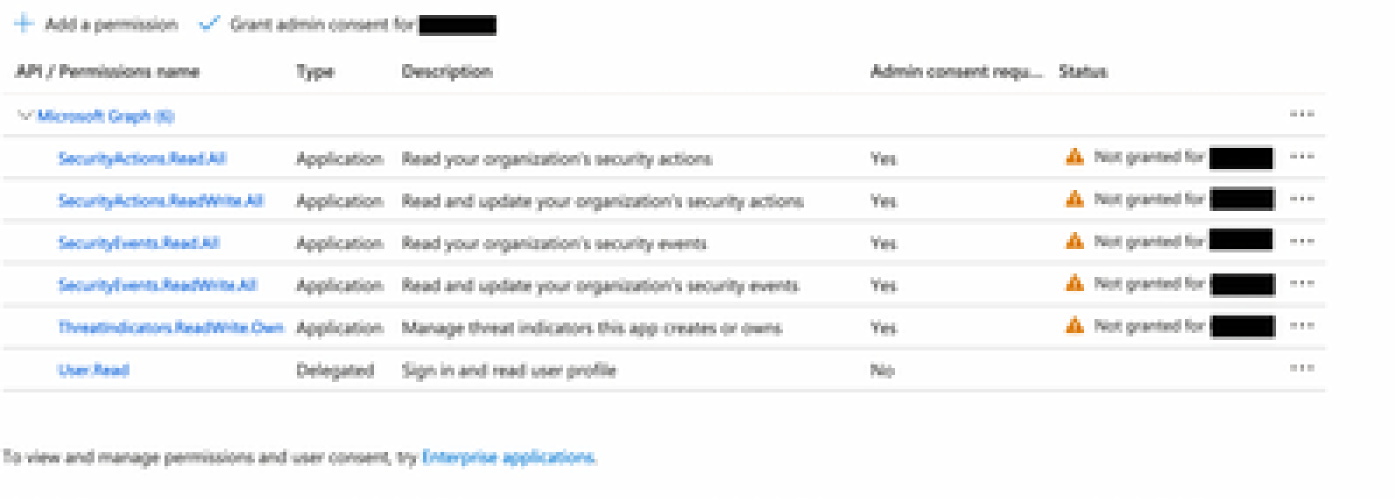
في شريط البحث، ابحث عن Security. توسيع **Security Actions** وتحديد

- **قراءة.الكل**
- **ريدWrite.all**
- **أحداث الأمان وتحديد**
  - **قراءة.الكل**
  - **ريدWrite.all**
- **مؤشرات التهديد واختيار**
  - **ThreatIndicators.ReadWrite.OwnedBy**

انقر.Add permissions

الخطوة 12.

مراجعة الأذونات المحددة.

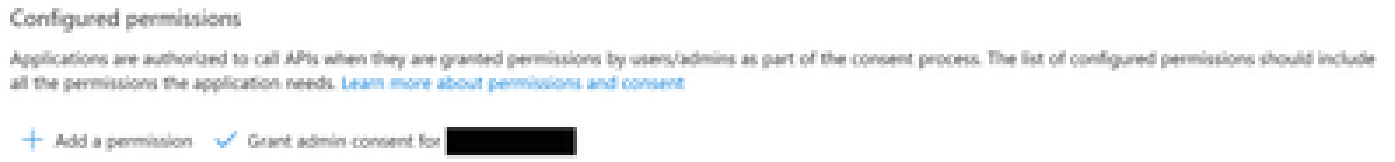


＋ Add a permission ✓ Grant admin consent for [redacted]

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.OwnedBy	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.

انقر **Grant Admin consent** لمؤسستك.



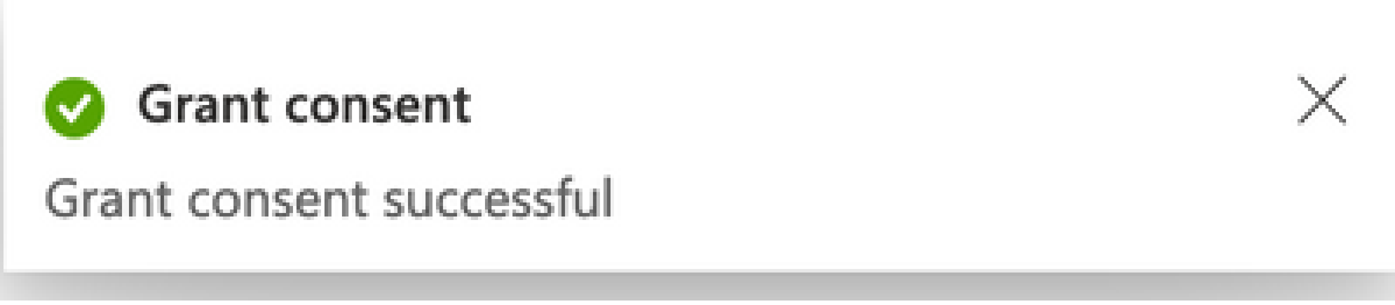
Configured permissions

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]

تظهر رسالة حث الاختيار ما إذا كنت تريد منح الموافقة لكافة الأذونات. انقر.Yes

تظهر نسخة منبثقة مماثلة كما هو موضح في هذه الصورة:



Grant consent

Grant consent successful

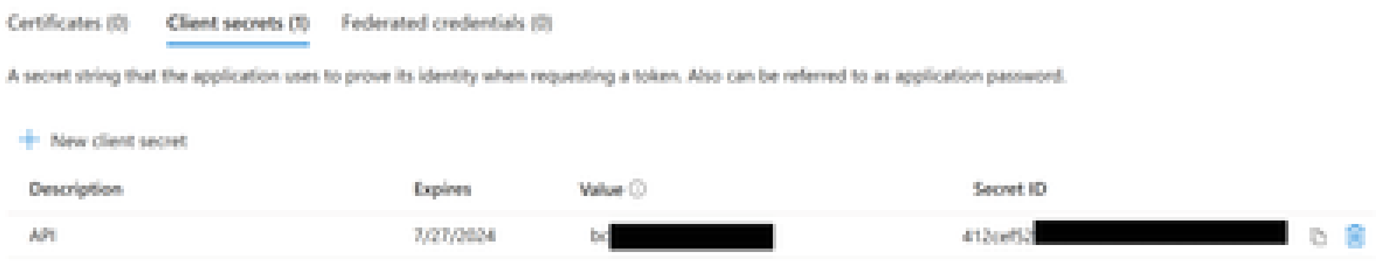
الخطوة 13.

انتقل إلى Manage > Certificates & Secrets.

انقر.Add New Client Secret

اكتب وصفا موجزا وحدد تاريخ صالحExpires. يقترح تحديد تاريخ صلاحية يزيد عن 6 أشهر لمنع انتهاء صلاحية مفاتيح API.

وبمجرد إنشائها، انسخ الجزء الذي يقول **Value**كما هو مستخدم للتكامل واحفظه في مكان آمن.



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

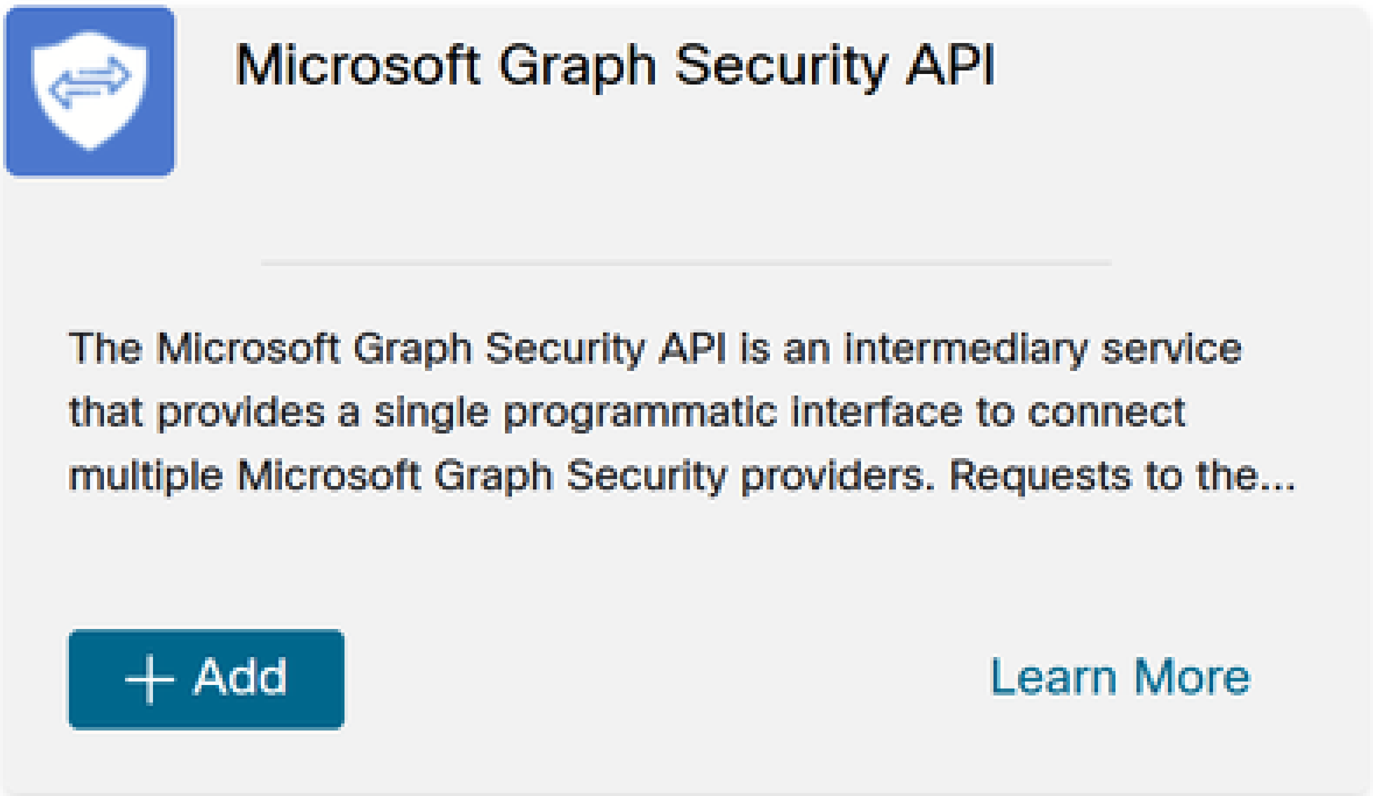
Description	Expires	Value	Secret ID
API	7/27/2024	bc[redacted]	412cef52[redacted]

تحذير: لا يمكن إسترداد هذا الحقل ويجب إنشاء سر جديد.

بمجرد توفر جميع المعلومات لديك، انتقل مرة أخرى إلى قيم تطبيقك **Overview** ونسخها. ثم انتقل إلى SecureX.

الخطوة 14.

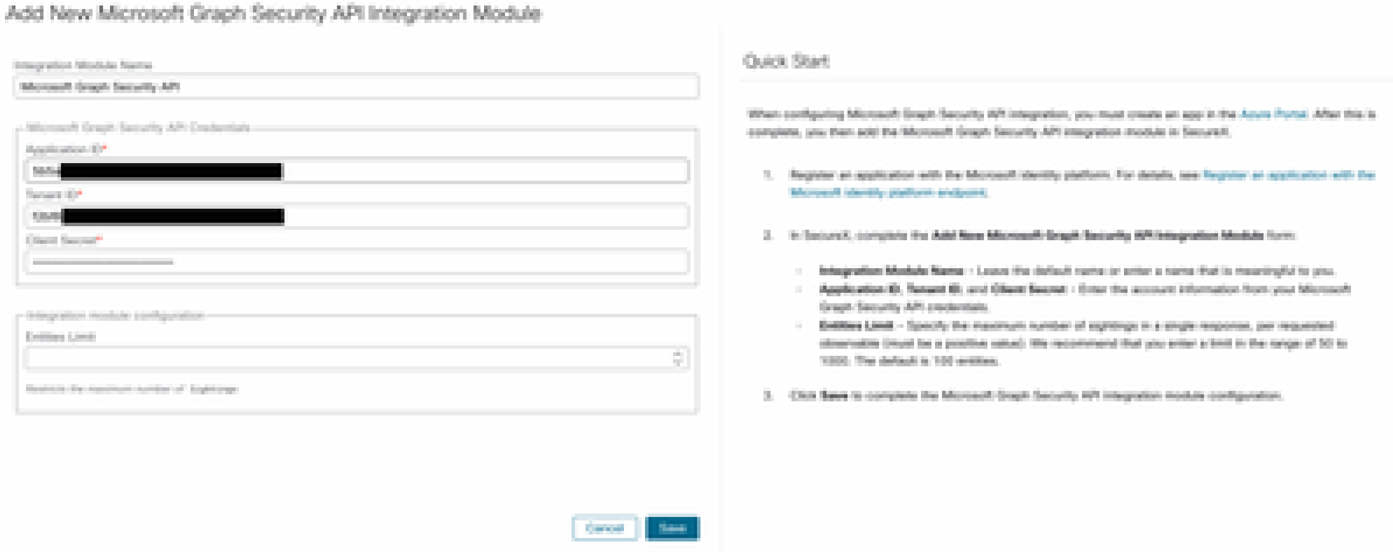
انتقل إلى Integration Modules > Available Integration Modules > تحديد Microsoft Security Graph API، انقر Add.



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...

قم بتعيين اسم ولصق القيم التي حصلت عليها من مدخل Azure.



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

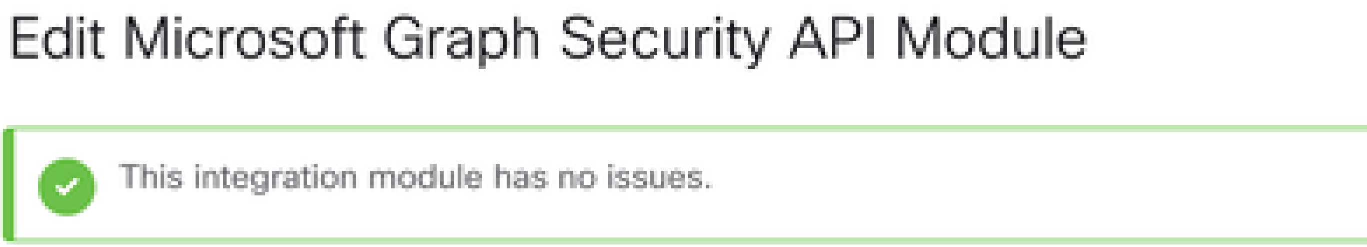
Restricts the maximum number of Sightings

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.

انقر Save وانتظر نجاح HealthCheck.



Edit Microsoft Graph Security API Module

This integration module has no issues.

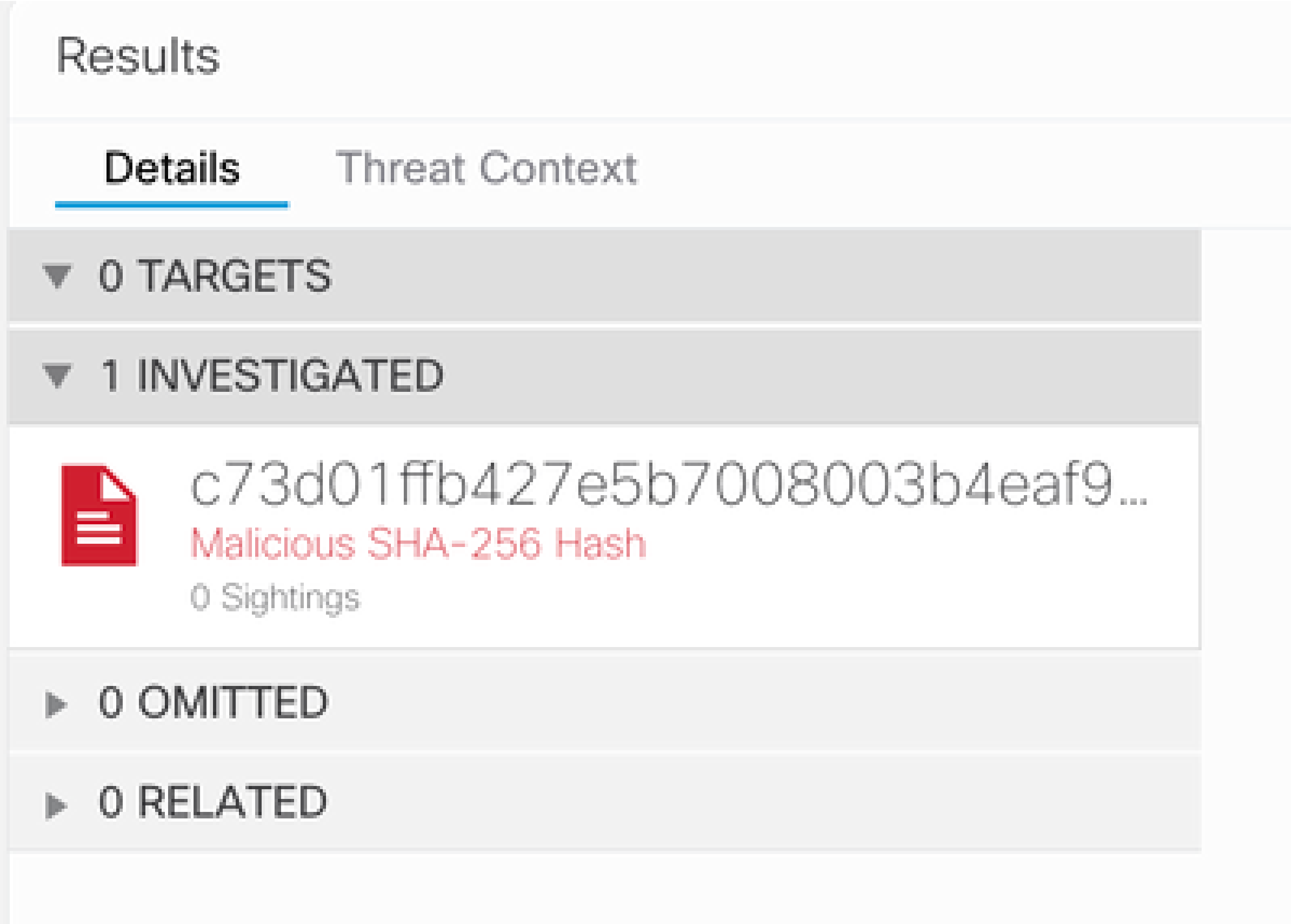
إجراء التحقيقات

حتى الآن، لا يقوم Microsoft Security Graph API بملء لوحة معلومات Cisco XDR باستخدام تجانب. بدلا من ذلك، يمكن الاستعلام عن المعلومات من بوابة Azure الخاصة بك باستخدام Investigations.

تذكر دائما، لا يمكن الاستعلام عن واجهة برمجة التطبيقات (API) الخاصة بالرسم البياني إلا عن:

- ip
- مجال
- اسم المضيف
- url
- file_name
- file_path
- شا 256

في هذا المثال، أستخدم التحقيق شاc73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148 هذا.



Results

Details | Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED

c73d01ffb427e5b7008003b4eaf9...
Malicious SHA-256 Hash
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

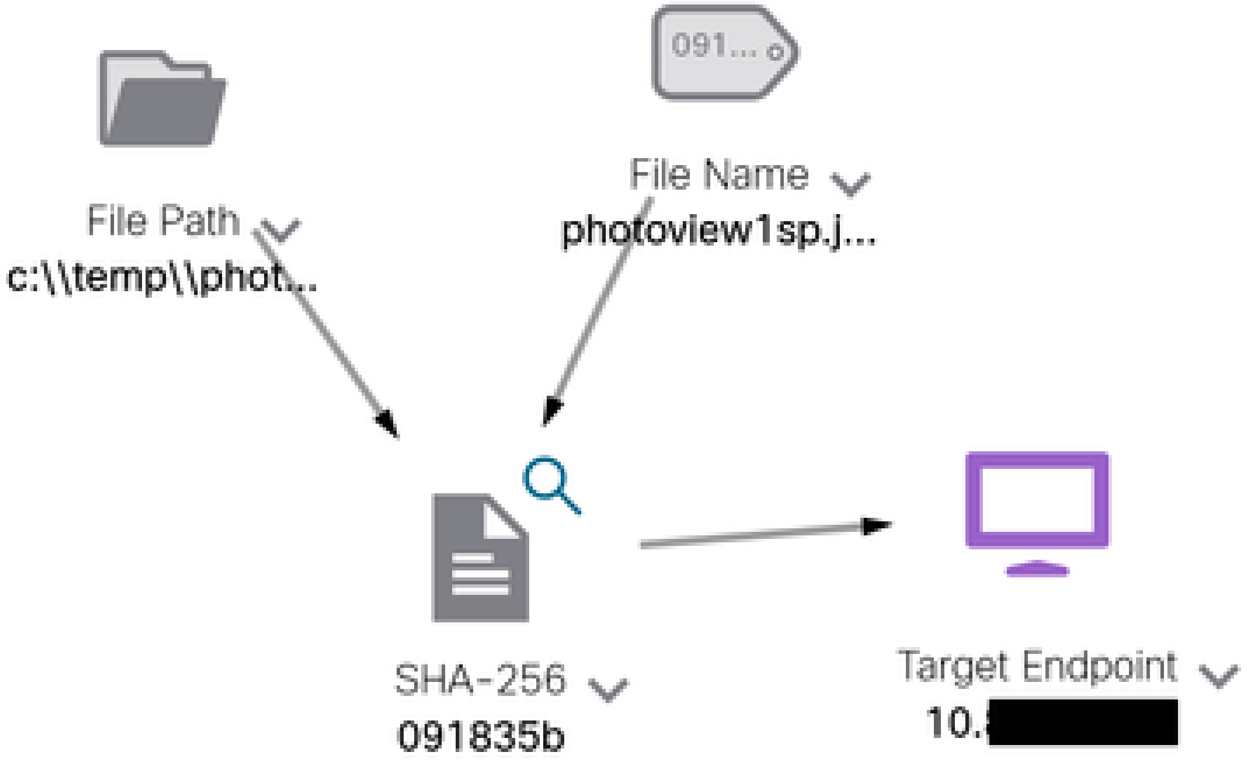
كما ترون، لديه 0 مشاهد في بيئة المختبر، فكيف نختبر إذا كان Graph API يعمل؟

افتح "أدوات مطور الويب"، وقم بتشغيل التحقيق، والبحث عن حدث نشر إلى **visibility.amp.cisco.com** الملف الذي يسمى Observables.

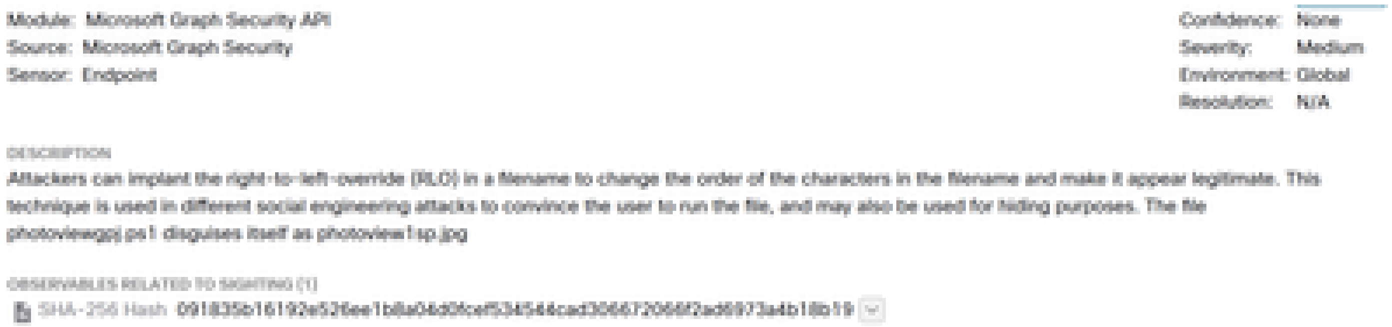
التحقق من الصحة

يمكنك إستخدام هذا الارتباط: [نقاط أمان Microsoft Graph]() للحصول على قائمة بالنقاط التي تساعدك على فهم الاستجابة التي يمكنك الحصول عليها من كل نوع من أنواع إمكانية الملاحظة.

يمكنك رؤية مثال كما هو موضح في هذه الصورة:



قم بتوسيع الإطار، يمكنك رؤية المعلومات المقدمة من التكامل:



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

تذكر أنه يجب أن تكون البيانات موجودة في مدخل Azure، ويعمل API للرسم البياني بشكل أفضل عند إستخدامه مع حلول Microsoft الأخرى. ومع ذلك، يجب التحقق من صحة ذلك بواسطة دعم Microsoft.

استكشاف الأخطاء وإصلاحها

- رسالة فشل التفويض:
  - تأكد من صحة القيم **Tenant ID** Client ID ومن أنها لا تزال صالحة.

- لا تظهر بيانات أثناء التحقيق:

  - تأكد من نسخ ولصق القيم المناسبة ل **Tenant ID** و **Client ID**.

    - تأكد من إستخدام معلومات الحقل **Value** من Certificates & Secrets القسم.

    - أستخدم أدوات WebDeveloper لتحديد ما إذا كان قد تم الاستعلام عن واجهة برمجة تطبيقات Graph عند حدوث تحقيق.

    - بينما تقوم واجهة برمجة تطبيقات Graph بدمج البيانات من موفري تنبيه Microsoft المختلفين، تأكد من دعم OData لمرشحات الاستعلام. (على سبيل المثال، Office 365 Security and Compliance و Microsoft Defender ATP).

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).