

Cisco XDRとのMicrosoft Graph API統合の設定

内容

[はじめに](#)

[前提条件](#)

[統合ステップ](#)

[調査の実行](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Microsoft Graph APIをCisco XDRと統合する手順と、照会できるデータのタイプについて説明します。

前提条件

- Cisco XDR管理者アカウント
- Microsoft Azureシステム管理者アカウント
- Cisco XDRへのアクセス

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。

統合ステップ

ステップ 1:

システム管理者としてMicrosoft Azureにログインします。

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

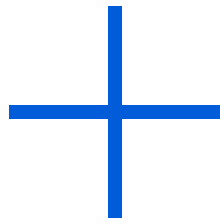
[Can't access your account?](#)

Back

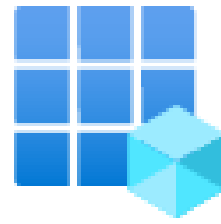
Next

ステップ 2 :

Azure サービスポータル **App Registrations** をクリックします。



Create a
resource



App
registrations

ステップ 3 :

をクリックします。New registration

Home >

App registrations

+ New registration  Endp

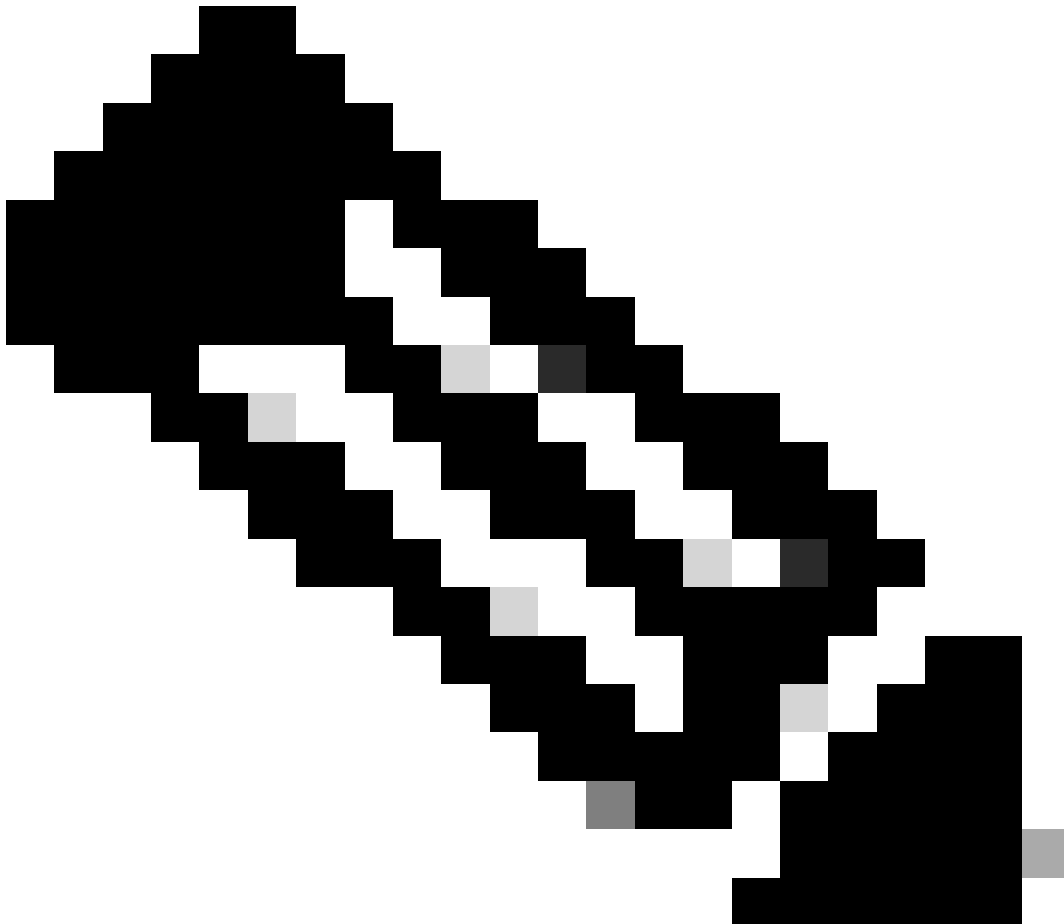
ステップ 4 :

新しいアプリを識別する名前を入力します。

▪ Name

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

SecureX - Graph API



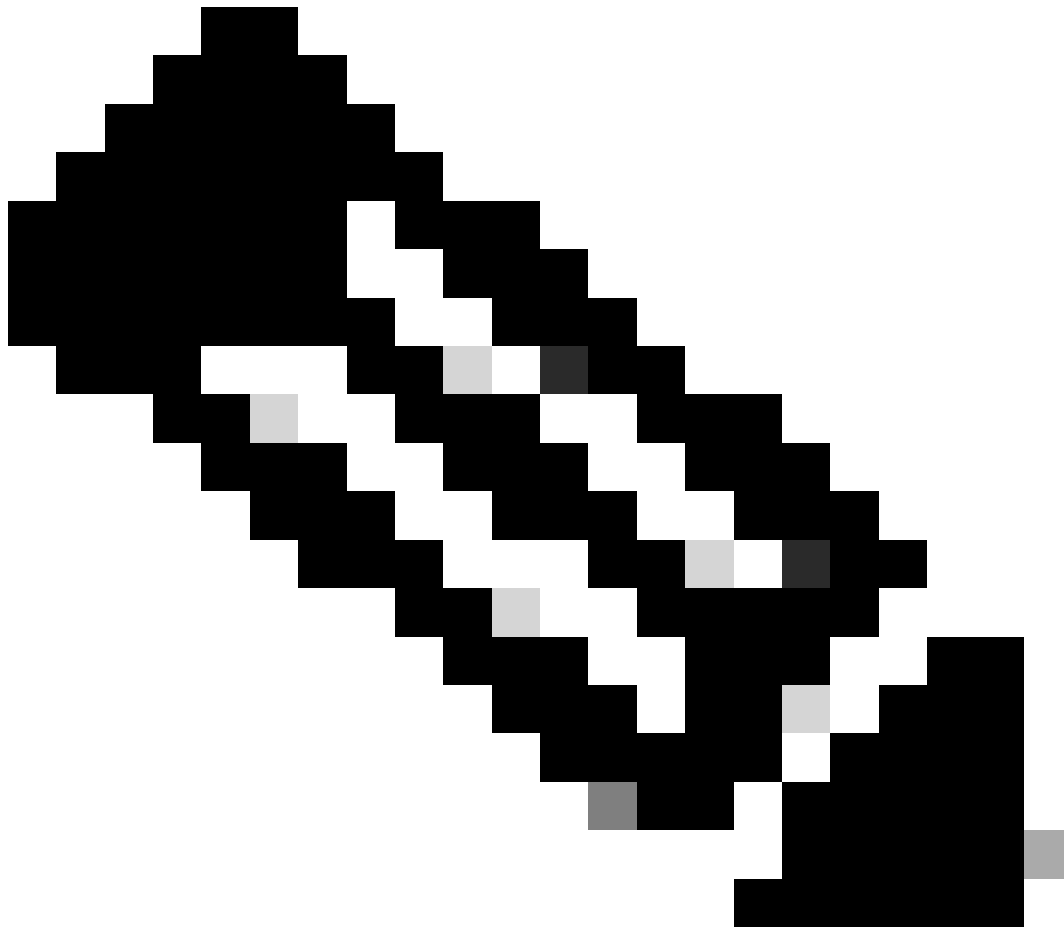
注：名前が有効な場合は、緑色のチェックマークが表示されます。

サポートされているアカウントタイプで、Accounts in this organizational directory only オプションを選択します。

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (██████████ 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：リダイレクトURIを入力する必要はありません。

ステップ 5 :

画面の一番下までスクロールし、**Register**をクリックします。

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

Register

手順 6 :





Azureサービスのページに戻り、App Registrations > Owned Applicationsをクリックします。

アプリを特定し、名前をクリックします。この例では、SecureXです。

All applications Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [Redacted]	049821 [Redacted]
 [Redacted]	9c049c [Redacted]
 [Redacted] Portal	6c0d8c [Redacted]
 SecureX	16e2bd33-8378-419e-86d7-04e1479efc0

手順 7 :

アプリの概要が表示されます。次の関連情報を特定してください。

アプリケーション (クライアント) ID:

Display name : [SecureX](#)

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

ディレクトリ (テナント) ID:

Directory (tenant) ID : f2bf8cd3-[Redacted]

ステップ 8 :

Manage Menu > API Permissionsに移動します。

Manage



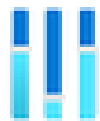
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

ステップ 9 :

Configured PermissionsでAdd a Permissionをクリックします。

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 ██████████

ステップ 10 :

[APIアクセス許可を要求する]セクションで、[Microsoft Graph]をクリックします。

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.

ステップ 11

Application permissionsを選択します。

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.

検索バーでSecurityを探します。展開 **Security Actions** して選択

- 読み取り。すべて
- 読み取り/書き込み.All
- **Security Events**とselect
 - 読み取り。すべて
 - 読み取り/書き込み.All
- 脅威の指標と選択
 - 脅威インジケータ ◦ 読み取り書き込み。所有者

をクリックします。Add permissions

ステップ 12

選択したアクセス許可を確認します。

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

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
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](#).

組織の Grant Admin consent 場合は、をクリックします。

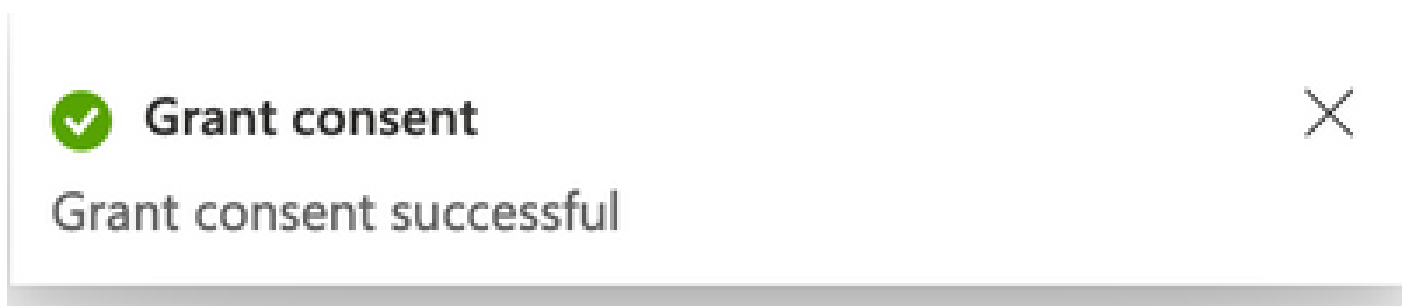
Configured permissions

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]

すべての権限に同意を与えるかどうかを選択するプロンプトが表示されます。をクリックします。Yes

次の図に示すようなポップアップが表示されます。



ステップ 13

Manage > Certificates & Secretsに移動します。

をクリックします。Add New Client Secret

簡単な説明を入力し、有効なExpires日を選択します。APIキーの有効期限が切れないように、有効期間を6か月以上選択することをお勧めします。

作成後、Valueという部分は統合で使用するため、コピーして安全な場所に保存してください。

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]	412ref53 [REDACTED]		



警告：このフィールドは回復できないため、新しいシークレットを作成する必要があります。

すべての情報を取得したら、**Overview**に戻り、アプリの値をコピーします。次に、SecureXに移動します。

ステップ 14 :

Integration Modules > Available Integration Modules > selectに移動し、Microsoft Security Graph APIAdd をクリックします。



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...

+ Add

[Learn More](#)

名前を割り当て、Azureポータルから取得した値を貼り付けます。

Add New Microsoft Graph Security API Integration Module

Integration Module Name
Microsoft Graph Security API

Microsoft Graph Security API Credentials

Application ID
Name

Tenant ID
Name

Client Secret
Name

Integration Module configuration

Entities Limit
1000

Resolves the maximum number of entities

Cancel Save

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 Secured.

1. Register an application with the Microsoft identity platform. For details, see [Register an application with the Microsoft identity platform endpoints](#).
2. In Secured, 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 entities 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.

Saveをクリックし、ヘルスチェックが成功するまで待ちます。

Edit Microsoft Graph Security API Module



This integration module has no issues.

調査の実行

現時点では、Microsoft Security Graph APIはCisco XDRダッシュボードにタイルを入力しません。Azureポータル情報は、調査を使用して照会できます。

Graph APIは次の目的でのみ照会できることに注意してください。

- ip
- domain
- ホスト名
- URL
- ファイル名
- ファイルのパス
- sha256

この例では、調査でこのSHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148`を使用しています。

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

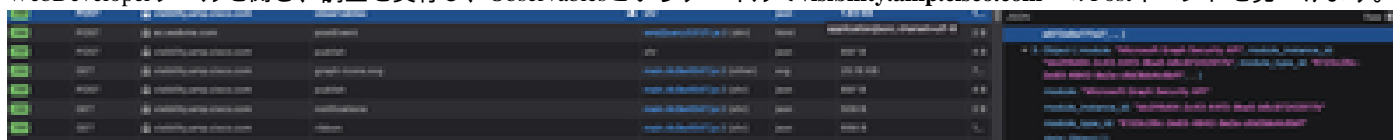
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

ご覧のように、ラボ環境では目撃が0件あります。グラフAPIが機能するかどうかをテストする方法は？

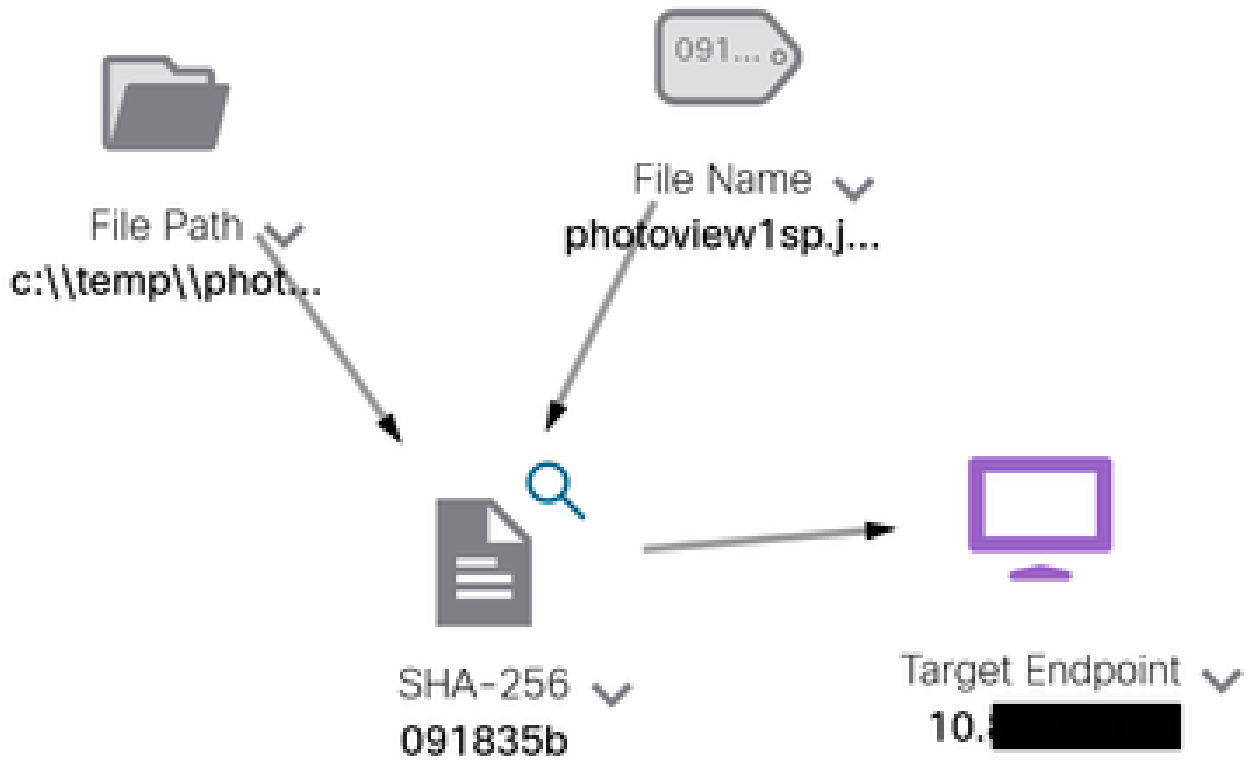
WebDeveloperツールを開き、調査を実行し、Observablesというファイルでvisibility.amp.cisco.comへのPostイベントを見つけます。



確認

「[Microsoft graph security Snapshots](#)」を参照すると、監視対象の各タイプから取得できる応答を理解するのに役立つスナップショットのリストを確認できます。

次の図に示す例を参照してください。



ウィンドウを展開すると、統合によって提供された情報が表示されます。

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 photoview[gg]ps1 disguises itself as photoview1sp.jpg

OBSERVABLES RELATED TO SIGNING (1)

SHA-256 Hash: 091835b16192e506ee1bba04d0fce7534544cad3066730603ad6973a4b18b19

データはAzureポータルに存在する必要があり、Graph APIは他のMicrosoftソリューションと使用すると効果的です。ただし、これはMicrosoftサポートによって検証される必要があります。

トラブルシューティング

- Authorization Failedメッセージ :

Tenant ID

- とClient IDの値が正しく、有効であることを確認します。

- Investigationにデータが表示されない :

Tenant ID

- と **Client ID**に適切な値をコピーして貼り付けたことを確認します。
Certificates & Secrets
- のセクション **Value** のフィールドの情報を使用していることを確認します。
- WebDeveloperツールを使用して、調査の発生時にGraph APIが照会されるかどうかを確認します。
- Graph APIは、さまざまなMicrosoftアラートプロバイダーからのデータをマージするため、ODataがクエリーフィルタでサポートされていることを確認します。(たとえば、Office 365 Security and Compliance、Microsoft Defender ATPなど)。

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。