

Configurazione dell'integrazione dell'API di Microsoft Graph con Cisco XDR

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Fasi di integrazione](#)

[Esegui indagini](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la procedura per integrare l'API di Microsoft Graph con Cisco XDR e il tipo di dati su cui è possibile eseguire una query.

Prerequisiti

- Account Cisco XDR Admin
- Account amministratore di sistema di Microsoft Azure
- Accesso a Cisco XDR

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Fasi di integrazione

Passaggio 1.

Accedere a Microsoft Azure come amministratore di sistema.

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

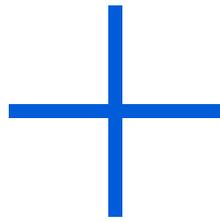
[Can't access your account?](#)

Back

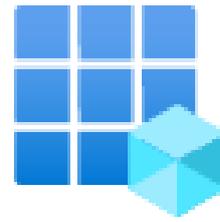
Next

Passaggio 2.

Fare clic **App Registrations** sul portale dei servizi di Azure.



Create a
resource



App
registrations

Passaggio 3.

Fare clic su .New registration

Home >

App registrations

+ New registration  Endp

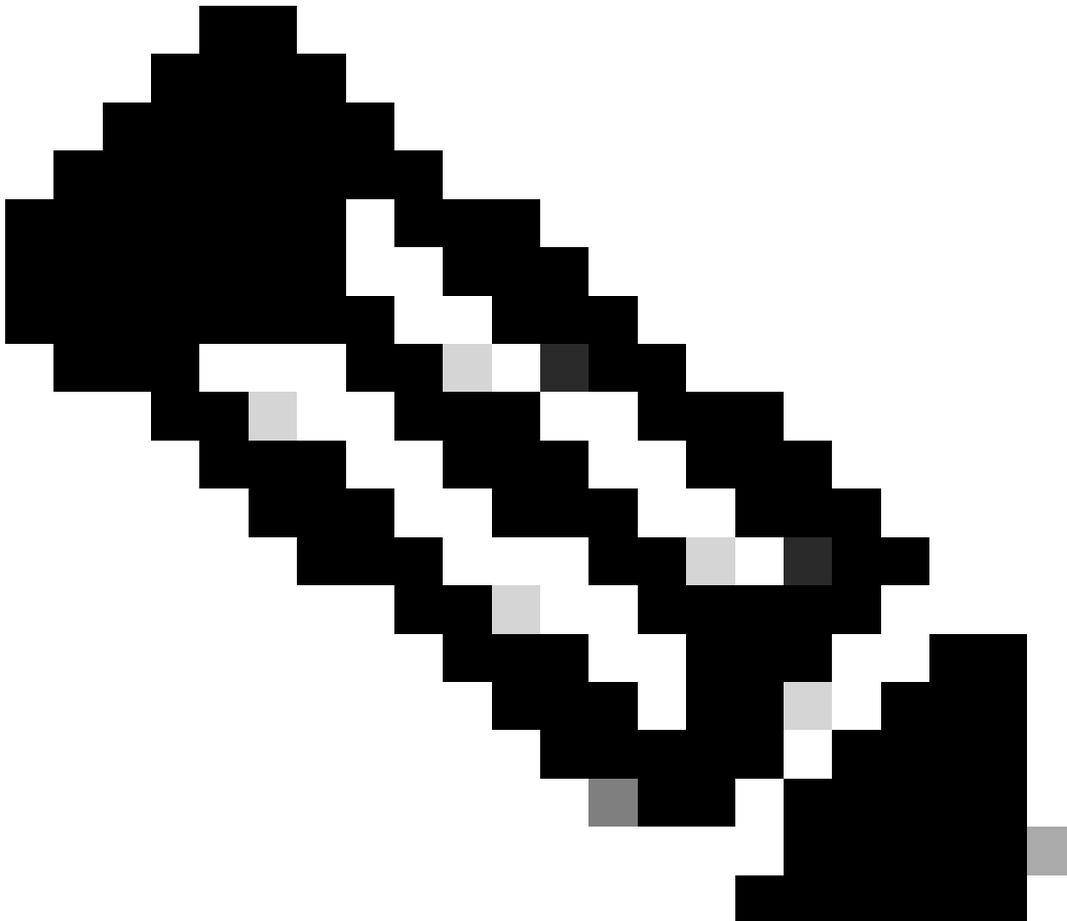
Passaggio 4.

Digitare un nome per identificare la nuova app.

▪ Name

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

SecureX - Graph API



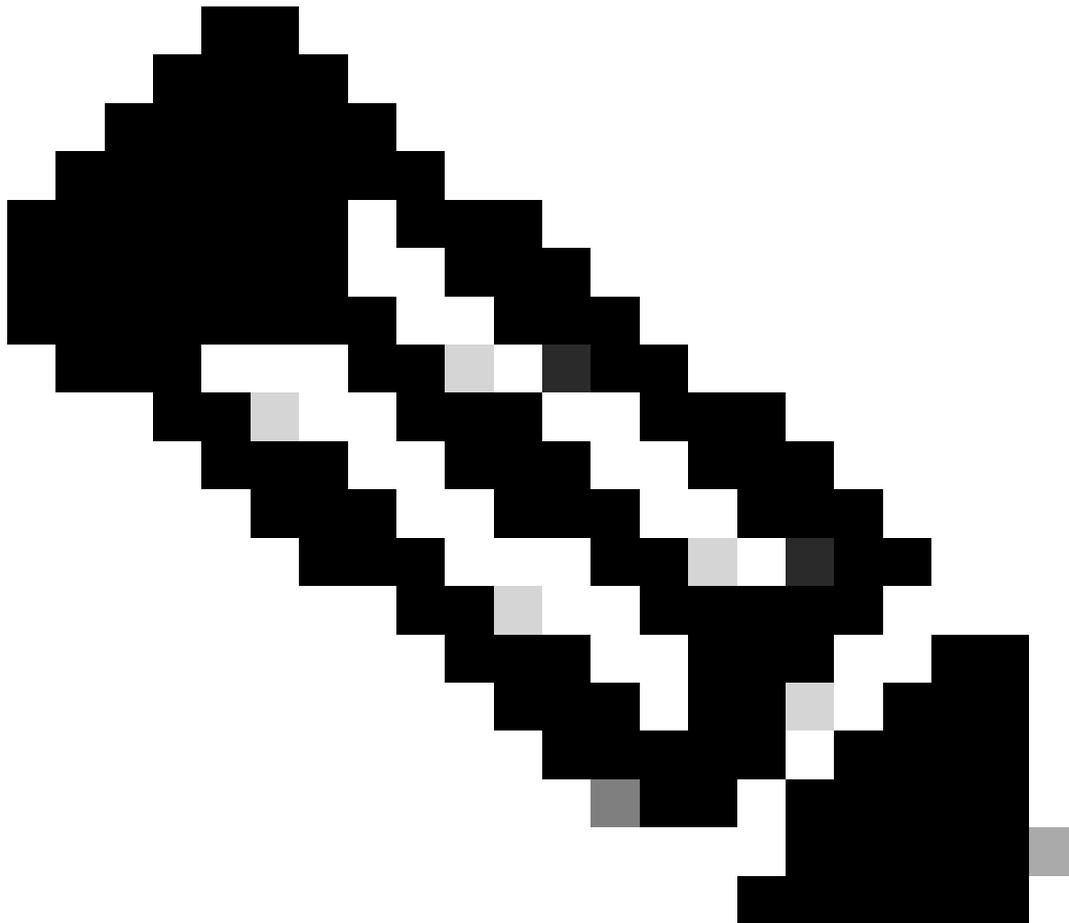
Nota: se il nome è valido, viene visualizzato un segno di spunta verde.

In Tipi di conto supportati, scegliere l'opzione **Accounts in this organizational directory only**.

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
-



Nota: non è necessario digitare un URI di reindirizzamento.

Scorrere fino alla parte inferiore dello schermo e fare clic su **Register**.

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

Register

Passaggio 6.

Tornare alla pagina dei servizi di Azure e fare clic su App Registrations > Owned Applications.

Identificare l'app e fare clic sul nome. Nell'esempio, questo valore è SecureX.

All applications Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [REDACTED]	049831 [REDACTED]
 [REDACTED]	9c669c [REDACTED]
 [REDACTED] Portal	6c3db8c [REDACTED]
 SecureX	16e2bd33-8378-419e-86d7-64e1479efc0

Passaggio 7.

Verrà visualizzato un riepilogo dell'app. Indicare le informazioni pertinenti:

ID applicazione (client):

Display name : [SecureX](#)

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

ID directory (tenant):

Directory (tenant) ID : f2bf8cd3-[REDACTED]

Passaggio 8.

Passare a Manage Menu > API Permissions.

Manage



Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Passaggio 9.

In Autorizzazioni configurate fare clic su 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](#)

+ Add a permission ✓ Grant admin consent for ██████████

Passaggio 10.

Nella sezione Richiedi autorizzazioni API, fare clic su **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.

Passaggio 11.

Selezionare 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.

Nella barra di ricerca, cercare Security. Espandi **Security Actions** e seleziona

- **Leggi.Tutto**
- **ReadWrite.All**

- **Eventi di protezione** e selezionare
 - **Leggi.Tutto**
 - **ReadWrite.All**

- **Indicatori di minaccia** e selezione
 - **IndicatoriMinacce.ReadWrite.OwnedBy**

Fare clic su .Add permissions

Passaggio 12.

Rivedere le autorizzazioni selezionate.

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

API / Permissions name	Type	Description	Admin consent reqa...	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](#).

Fare clic su **Grant Admin consent** per l'organizzazione.

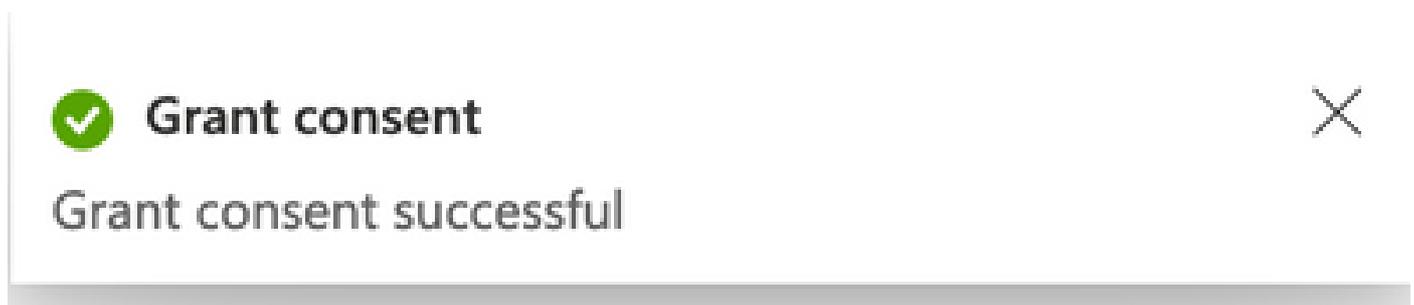
Configured permissions

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]

Viene visualizzato un prompt che richiede se si desidera concedere il consenso per tutte le autorizzazioni. Fare clic su .Yes

Viene visualizzato un popup simile a quello mostrato nell'immagine:



Passaggio 13.

Passare a Manage > Certificates & Secrets.

Fare clic su .Add New Client Secret

Scrivere una breve descrizione e selezionare una data validaExpires. Si consiglia di selezionare una data di validità superiore a 6 mesi per evitare la scadenza delle chiavi API.

Una volta creata, copiare e conservare in un luogo sicuro la parte che dice **Value**, così come viene utilizzata per l'integrazione.

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]	412ref5 [REDACTED]



Avviso: questo campo non può essere recuperato ed è necessario creare un nuovo segreto.

Dopo aver ottenuto tutte le informazioni, tornare ai valori dell'App **Overview** e copiarli. Passare quindi a SecureX.

Passaggio 14.

Passare alla sezione Integration Modules > Available Integration Modules > Seleziona Microsoft Security Graph API, quindi fare clic su Add.



The card features a blue shield icon with a white double-headed arrow. The title "Microsoft Graph Security API" is in a large, bold, black font. Below the title is a horizontal line. The main text describes the service as an intermediary that provides a single programmatic interface to connect multiple Microsoft Graph Security providers. At the bottom left is a dark blue button with a white plus sign and the text "Add". At the bottom right is a blue link that says "Learn More".

Assegnare un nome e incollare i valori ottenuti dal portale di 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
[REDACTED]

Integration Module configuration

Entries Limit
[REDACTED]

Specifies the maximum number of responses.

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 Secured3.

1. Register an application with the Microsoft identity platform. For details, see [Register an application with the Microsoft identity platform endpoints](#).
2. In Secured3, 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.
 - **Entries Limit** - Specify the maximum number of responses in a single response, per requested identifier (must be a positive value). We recommend that you enter a limit in the range of 50 to 1000. The default is 100 entries.
3. Click [Save](#) to complete the Microsoft Graph Security API integration module configuration.

Fare clic su Save e attendere il completamento del controllo di integrità.

Edit Microsoft Graph Security API Module



This integration module has no issues.

Esegui indagini

Al momento, l'API di Microsoft Security Graph non popola Cisco XDR Dashboard con una tessera. Le informazioni del portale di Azure possono invece essere richieste tramite le indagini.

Tenete presente che è possibile eseguire una query sull'API Graph solo per:

- ip
- dominio
- nome host
- url
- file
- percorso
- sha256

In questo esempio, l'indagine ha utilizzato questo Agente integrità sistema
c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148.

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Come potete vedere, ha 0 Avvistamenti nell'ambiente Lab, quindi come verificare se l'API di Graph funziona?

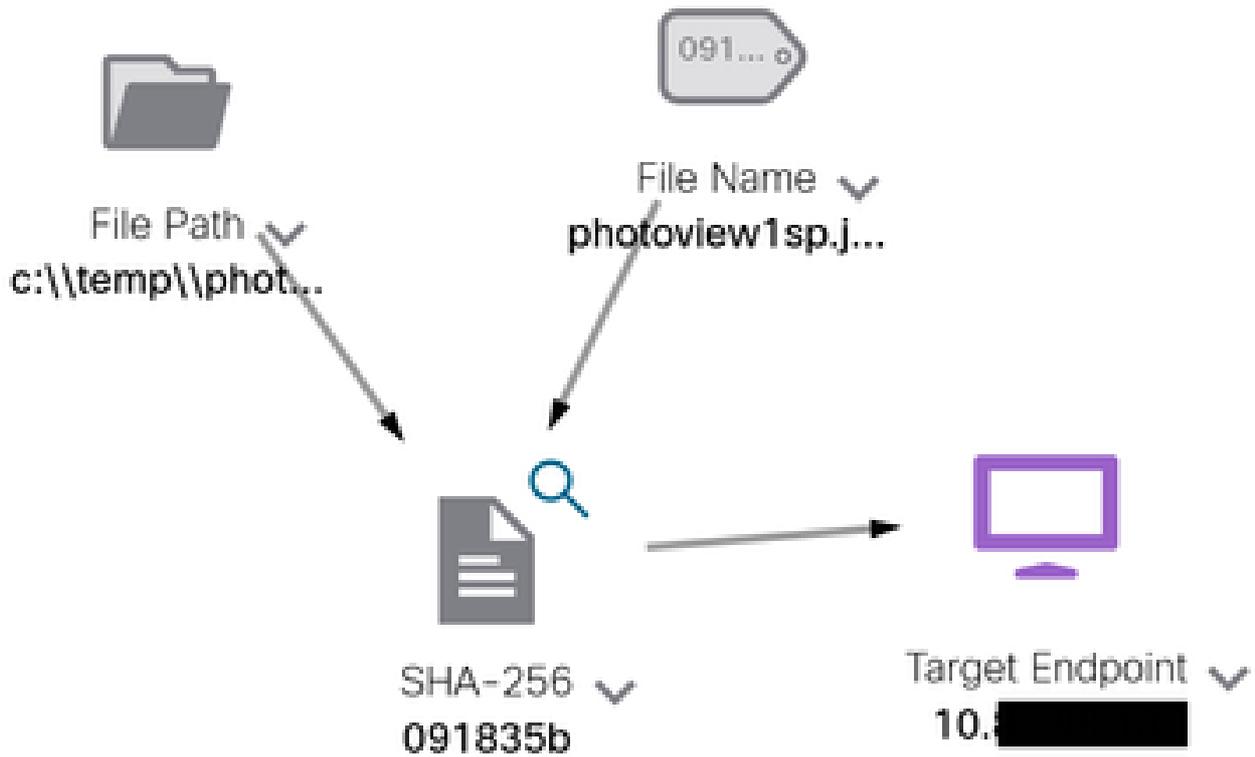
Aprire WebDeveloper Tools, eseguire l'indagine, trovare un evento post per **visibility.amp.cisco.com** il file chiamato Observables.



Verifica

È possibile utilizzare questo collegamento: [Microsoft graph security Snapshots](#) per un elenco di Snapshot che aiutano a comprendere la risposta che si può ottenere da ogni tipo di osservabile.

Di seguito è riportato un esempio:



Espandere la finestra per visualizzare le informazioni fornite dall'integrazione:

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 DIGITING (1)

SHA-256 Hash: 091835b16193e53bee1b1a04d0fce7534544cad306673066f3ad6973a4b18b19

Tenere presente che i dati devono esistere nel portale di Azure e che l'API Graph funziona meglio se utilizzata con altre soluzioni Microsoft. Tuttavia, questa condizione deve essere convalidata dal supporto tecnico Microsoft.

Risoluzione dei problemi

- Messaggio Autorizzazione Non Riuscita:
 - Verificare che i valori di **Tenant ID** e Client ID siano corretti e che siano ancora validi.

- Nessun dato visualizzato nell'investigazione:
 - Assicurarsi di aver copiato e incollato i valori appropriati per **Tenant ID** e **Client ID**.
 - Assicurarsi di aver utilizzato le informazioni del campo **Value** della Certificates & Secrets sezione.
 - Utilizzare gli strumenti di WebDeveloper per determinare se viene eseguita una query sull'API Graph quando viene eseguita un'indagine.
 - Quando l'API Graph unisce i dati provenienti da vari provider di avvisi Microsoft, verificare che OData sia supportato per i filtri query. (ad esempio, Office 365 Security and Compliance e Microsoft Defender ATP).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).