

Microsoft Graph API-integratie configureren met Cisco XDR

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Integratiestappen](#)

[Onderzoeken uitvoeren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de procedure voor het integreren van Microsoft Graph API met Cisco XDR en het type gegevens dat kan worden opgevraagd.

Voorwaarden

- Cisco XDR Admin-account
- Microsoft Azure-systeembeheerderaccount
- Toegang tot Cisco XDR

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Integratiestappen

Stap 1.

Log in in Microsoft Azure als systeembeheerder.

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

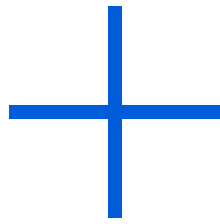
[Can't access your account?](#)

Back

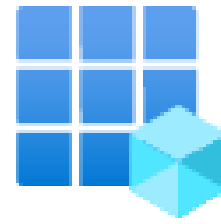
Next

Stap 2.

Klik **App Registrations** op het Azure-serviceportal.



Create a
resource



App
registrations

Stap 3.

Klik op de knop `.New registration`

Home >

App registrations

+ New registration  Endp

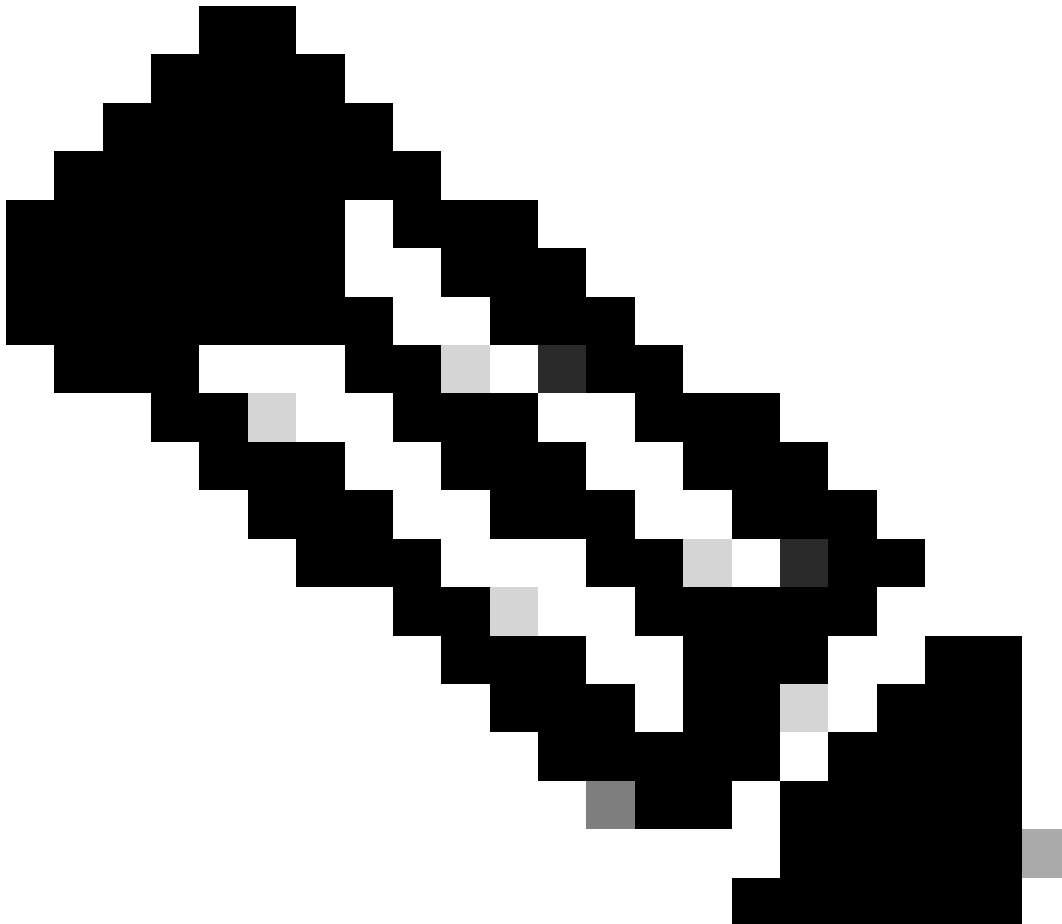
Stap 4.

Typ een naam om uw nieuwe app te identificeren.

▪ Name

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

SecureX - Graph API



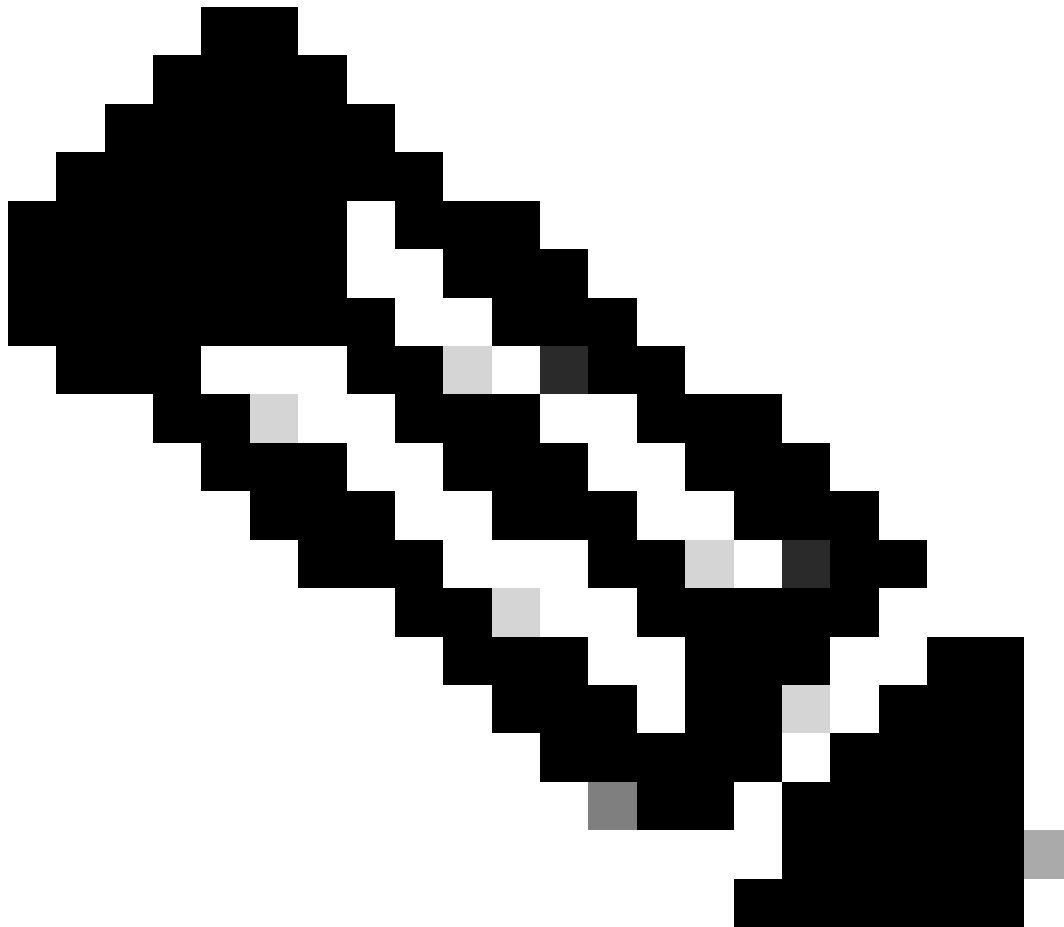
Opmerking: als de naam geldig is, wordt een groen vinkje weergegeven.

Kies de optie voor ondersteunde accounttypen **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
-



Opmerking: u hoeft geen Redirect URI te typen.

Blader naar de onderkant van het scherm en klik op **Register**.

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

Register

Stap 6.





Ga terug naar de Azure-servicepagina, klik op App Registrations > Owned Applications.

Identificeer uw app en klik op de naam. In dit voorbeeld is het dat wel SecureX.

All applications Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [Redacted]	049831 [Redacted]
 [Redacted]	9c660c [Redacted]
 [Redacted] Portal	6c3d8c [Redacted]
 SecureX	16e2bd33-8378-419e-86d1-64e1479fbc0

Stap 7.

Er wordt een samenvatting van uw app weergegeven. Gelieve deze relevante gegevens te vermelden:

Applicatie (client)-ID:

Display name : [SecureX](#)

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

Directory (tenant) ID:

Directory (tenant) ID : f2bf8cd3-[Redacted]

Stap 8.

Navigeer naar Manage Menu > API Permissions.

Manage



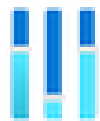
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Stap 9.

Klik onder Configurerde toegangsrechten op 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 ██████████

Stap 10.

Klik in de sectie API-toegangsrechten aanvragen op **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.

Stap 11.

Selecteer 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.

In de zoekbalk, zoek naar Security. Uitvouwen **Security Actions** en selecteren

- **Read.All**
- **ReadWrite.All**

- **Security Events** en selecteer
 - **Read.All**
 - **ReadWrite.All**

- **Bedreigingsindicatoren** en selecteer
 - **ThreatIndicators.readWrite.OwnedBy**

Klik op de knop .Add permissions

Stap 12.

Controleer de geselecteerde rechten.

+ 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](#).

Klik **Grant Admin consent** voor uw organisatie.

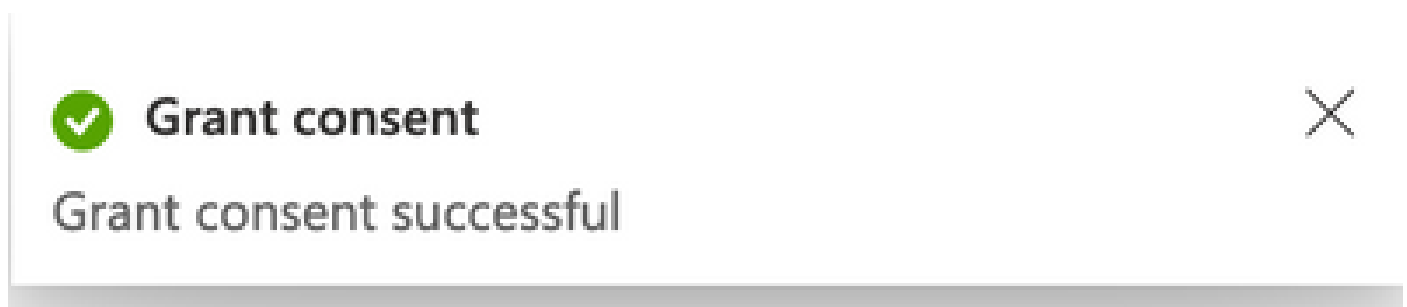
Configured permissions

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]

Er verschijnt een prompt om te kiezen of u toestemming wilt verlenen voor alle machtigingen. Klik op de knop .Yes

Er verschijnt een soortgelijk popup zoals in deze afbeelding:



Stap 13.

Navigeer naar Manage > Certificates & Secrets.

Klik op de knop .Add New Client Secret

Schrijf een korte beschrijving en selecteer een geldige Expires datum. Er wordt voorgesteld om een geldigheidsdatum van meer dan 6 maanden te selecteren om te voorkomen dat de API-sleutels verlopen.

Zodra gemaakt, kopieer en bewaar op een veilige plaats het deel dat zegt **Value**, zoals het wordt gebruikt voor de integratie.

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]



Waarschuwing: dit veld kan niet worden hersteld en u moet een nieuw geheim maken.

Stap 14.

Navigeer om te Integration Modules > Available Integration Modules > selecteren Microsoft Security Graph API, klik 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...

+ Add

[Learn More](#)

Wijs een naam toe en plak de waarden die u uit de Azure-portal hebt gekregen.

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

Entities Limit
[Dropdown menu]

Specifies the maximum number of responses

Quick Start

When configuring Microsoft Graph Security API integration, you must create an app in the [Azure Portal](#). After this is complete, use 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 responses in a single response, per requested identifiability (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.

Klik op Save en wacht tot de gezondheidscontrole is geslaagd.

Edit Microsoft Graph Security API Module



This integration module has no issues.

Onderzoeken uitvoeren

Op dit moment wordt het Cisco XDR Dashboard niet bevolkt door een timer met Microsoft Security Graph API. In plaats daarvan kan de informatie van uw Azure-portal worden opgevraagd bij het gebruik van Onderzoeken.

Houd in gedachten, de Grafiek API kan alleen worden opgevraagd voor:

- ip
- domein
- hostnaam
- url
- bestand_naam
- bestand_pad
- sha256

In dit voorbeeld werd bij het onderzoek gebruik gemaakt van deze SHA
c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148.

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

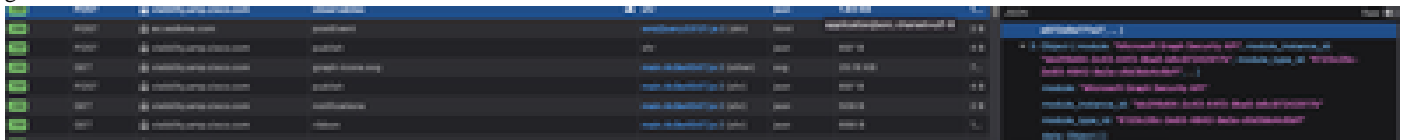
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Zoals u kunt zien, heeft het 0 Sightings in de Lab Environment, dus hoe te testen als Grafiek API werkt?

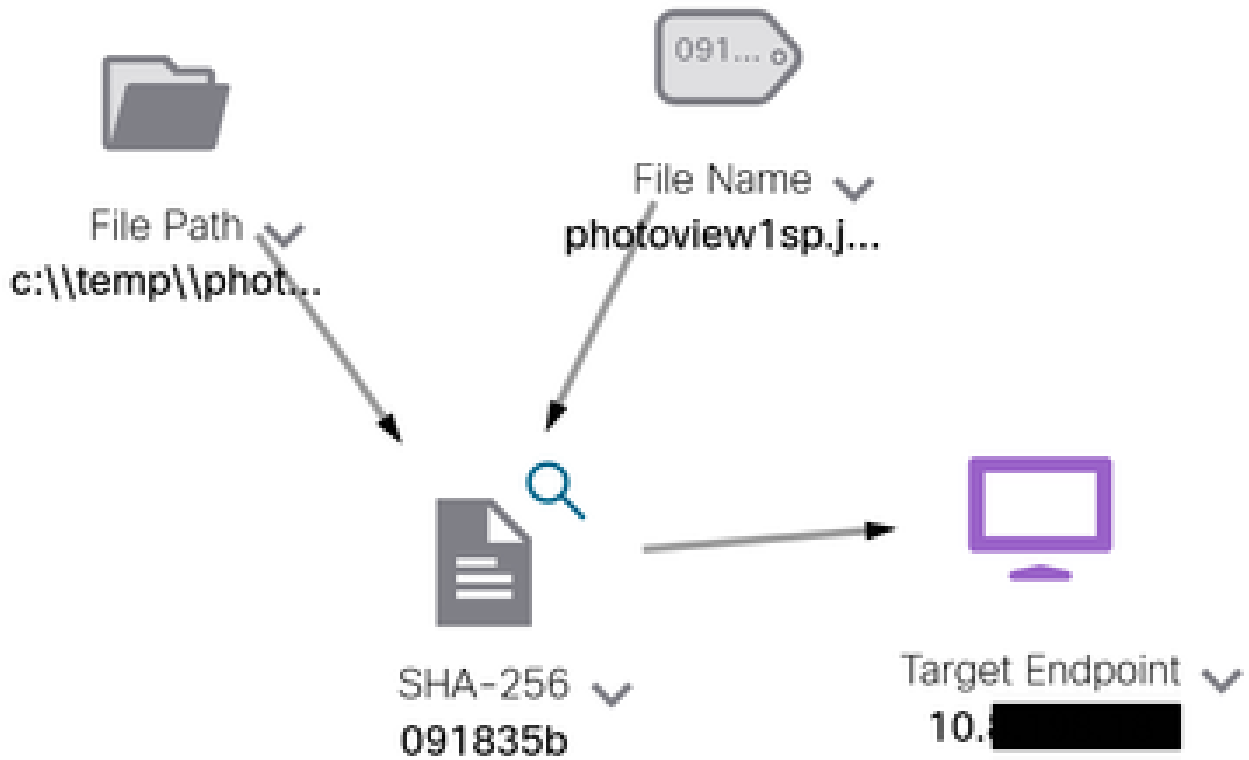
Open de WebDeveloper Tools, voer het onderzoek uit, vind een Post Event naar **zichtbaarheid.amp.cisco.com** het bestand Observables genaamd.



Verifiëren

U kunt deze link gebruiken: [Microsoft grafiek security Snapshots](#) voor een lijst van snapshots die u helpen om de respons te begrijpen die u kunt krijgen van elk type waarneembaar.

U kunt een voorbeeld zien zoals in deze afbeelding:



Breid het venster uit, kunt u de informatie zien die door de integratie wordt verstrekt:

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 SIGHTING (1)

SHA-256 Hash: 091835b16193e53f6e1b1a04d0cef534544cad306673066f3ad6973a4b18b19

Houd in gedachten dat gegevens moeten bestaan in uw Azure-portal, en Graph API werkt beter bij gebruik met andere Microsoft-oplossingen. Dit moet echter worden gevalideerd door Microsoft Support.

Problemen oplossen

- Bericht autorisatie is mislukt:
 - Zorg ervoor dat de waarden voor **Tenant ID** en **Client ID** correct zijn en nog steeds geldig zijn.

- Geen gegevens tijdens onderzoek:
 - Zorg ervoor dat u de juiste waarden voor **Tenant ID** en **Client ID** hebt gekopieerd en geplakt.
 - Zorg ervoor dat u de informatie uit het veld **Value** uit de Certificates & Secrets sectie hebt gebruikt.
 - Gebruik WebDeveloper tools om te bepalen of de Graph API wordt gevraagd wanneer er een onderzoek plaatsvindt.
 - Aangezien de Graph API gegevens van diverse Microsoft waakzame leveranciers samenvoegt, zorg ervoor dat OData voor de vraagfilters wordt gesteund. (Bijvoorbeeld Office 365 Security and Compliance en Microsoft Defender ATP).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.