

Configuración de la integración de la API de Microsoft Graph con Cisco XDR

Contenido

[Introducción](#)

[Prerequisites](#)

[Pasos de integración](#)

[Realizar investigaciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para integrar la API de Microsoft Graph con Cisco XDR y el tipo de datos que se pueden consultar.

Prerequisites

- Cuenta de administrador de Cisco XDR
- Cuenta de administrador del sistema de Microsoft Azure
- Acceso a Cisco XDR

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Pasos de integración

Paso 1.

Inicie sesión en Microsoft Azure como administrador del sistema.

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

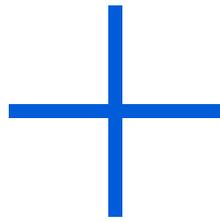
[Can't access your account?](#)

Back

Next

Paso 2.

Haga clic **App Registrations** en Azure Services Portal.



Create a
resource



App
registrations

Paso 3.

Haga clic en New registration.

Home >

App registrations



New registration



Endp

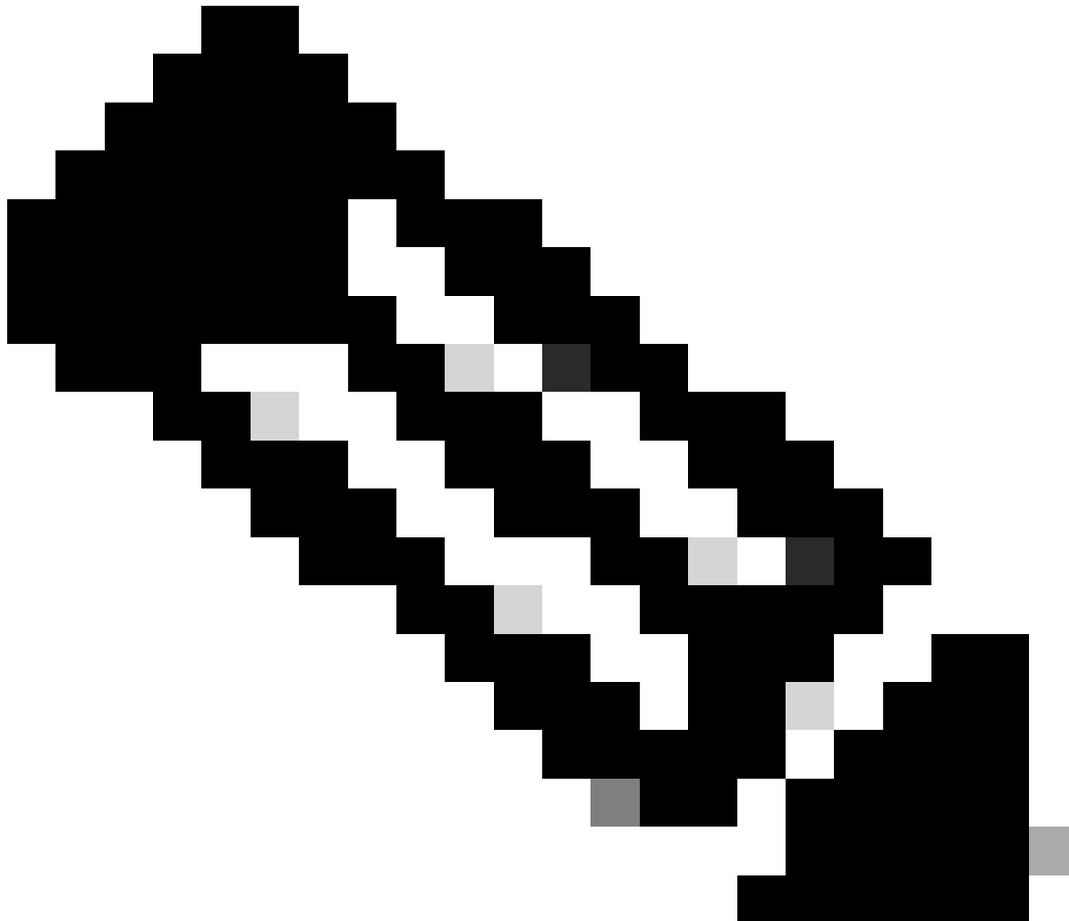
Paso 4.

Escriba un nombre para identificar su nueva aplicación.

▪ Name

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

SecureX - Graph API



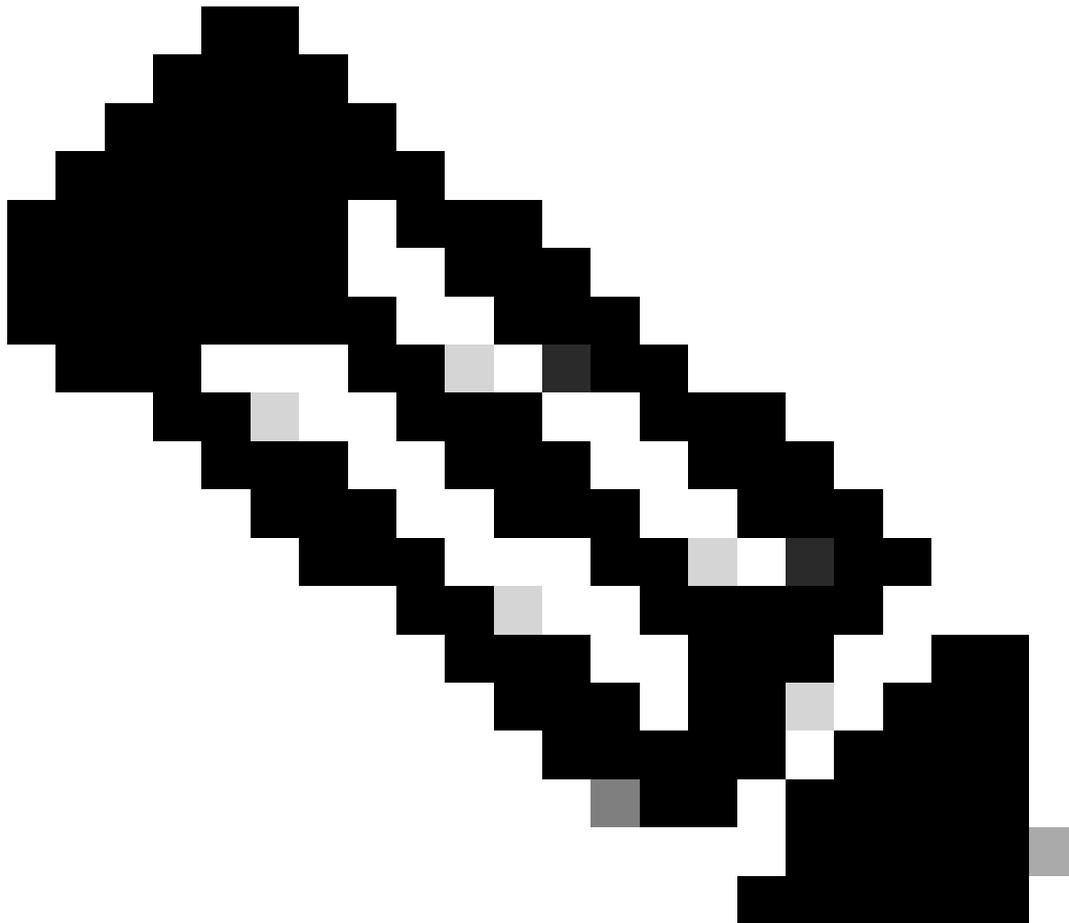
Nota: Si el nombre es válido, aparecerá una marca de verificación verde.

En Tipos de cuenta admitidos, elija la opción **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: No es necesario que escriba un URI de redirección.

Desplácese hasta la parte inferior de la pantalla y haga clic en **Register**.

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

Register

Paso 6.

Vuelva a la página de servicios de Azure y haga clic en App Registrations > Owned Applications.

Identifique su aplicación y haga clic en el nombre. En este ejemplo, es 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	6c3d8b [Redacted]
 SecureX	16e2bd33-8378-413e-86d1-64e1479efc0

Paso 7.

Aparecerá un resumen de su aplicación. Identifique estos datos relevantes:

ID de aplicación (cliente):

Display name : [SecureX](#)

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

ID de directorio (arrendatario):

Directory (tenant) ID : f2bf8cd3-[Redacted]

Paso 8.

Desplácese hasta Manage Menu > API Permissions.

Manage



Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Paso 9.

En Permisos configurados, haga clic en 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 ██████████

Paso 10.

En la sección Solicitar permisos de API, haga clic en **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.

Paso 11.

Seleccione 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.

En la barra de búsqueda, busque Security. Expandir **Security Actions** y seleccionar

- **Leer.Todo**
- **ReadWrite.All**

- **Eventos de seguridad** y seleccione
 - **Leer.Todo**
 - **ReadWrite.All**

- **Indicadores de amenazas** y seleccione
 - **ThreatIndicators.ReadWrite.OwnedBy**

Haga clic en Add permissions.

Paso 12.

Revise los permisos seleccionados.

+ 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](#).

Haga clic **Grant Admin consent** en para su organización.

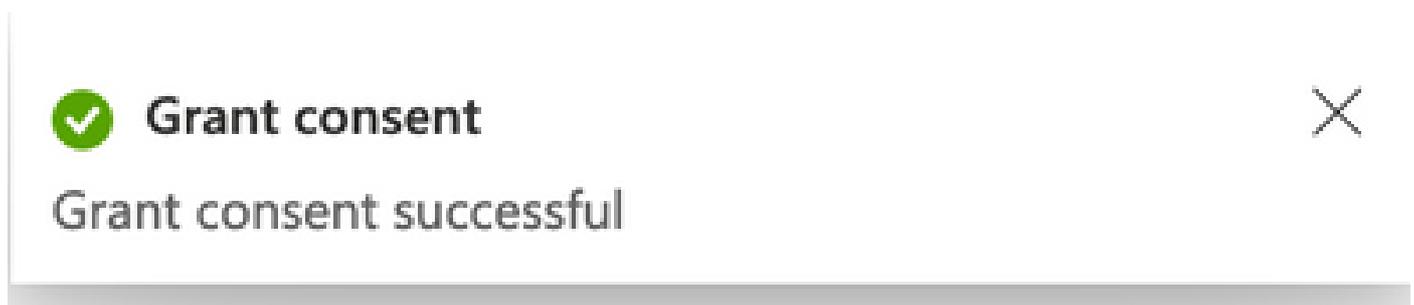
Configured permissions

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]

Aparecerá un mensaje que le preguntará si desea conceder el consentimiento para todos los permisos. Haga clic en Yes.

Aparece una ventana emergente similar a la mostrada en esta imagen:



Paso 13.

Desplácese hasta Manage > Certificates & Secrets.

Haga clic en Add New Client Secret.

Escriba una breve descripción y seleccione una fecha válida. Expire. Se recomienda seleccionar una fecha de validez de más de 6 meses para evitar la caducidad de las claves API.

Una vez creada, copie y guarde en un lugar seguro la parte que dice **Value**, ya que se utiliza para la integración.

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]



Advertencia: este campo no se puede recuperar y debe crear un nuevo secreto.

Una vez que tengas toda la información, navega de nuevo a **Overview** y copia los valores de tu App. A continuación, vaya a SecureX.

Paso 14.

Desplácese hasta Integration Modules > Available Integration Modules > seleccionar Microsoft Security Graph API y haga clic en 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 API as an intermediary service for connecting multiple 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".

Asigne un nombre y pegue los valores obtenidos en el portal de Azure.

Add New Microsoft Graph Security API Integration Module

Integration Module Name

Microsoft Graph Security API Credentials

Application ID*

Tenant ID*

Client Secret*

Integration Module configuration

Entities Limit

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, 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.
 - **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.

Haga clic Save y espere a que la comprobación de estado se realice correctamente.

Edit Microsoft Graph Security API Module



This integration module has no issues.

Realizar investigaciones

A partir de ahora, la API de Microsoft Security Graph no rellena el panel de Cisco XDR con un mosaico. Más bien, la información de su portal de Azure se puede consultar con el uso de Investigaciones.

Tenga en cuenta que la API de Graph sólo se puede consultar para:

- ip
- domain
- nombre del host
- url
- file_name
- file_path
- sha256

En este ejemplo, la investigación utilizó este SHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148`.

Results

Details Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Como puede ver, tiene 0 avistamientos en el entorno de laboratorio, así que ¿cómo probar si Graph API funciona?

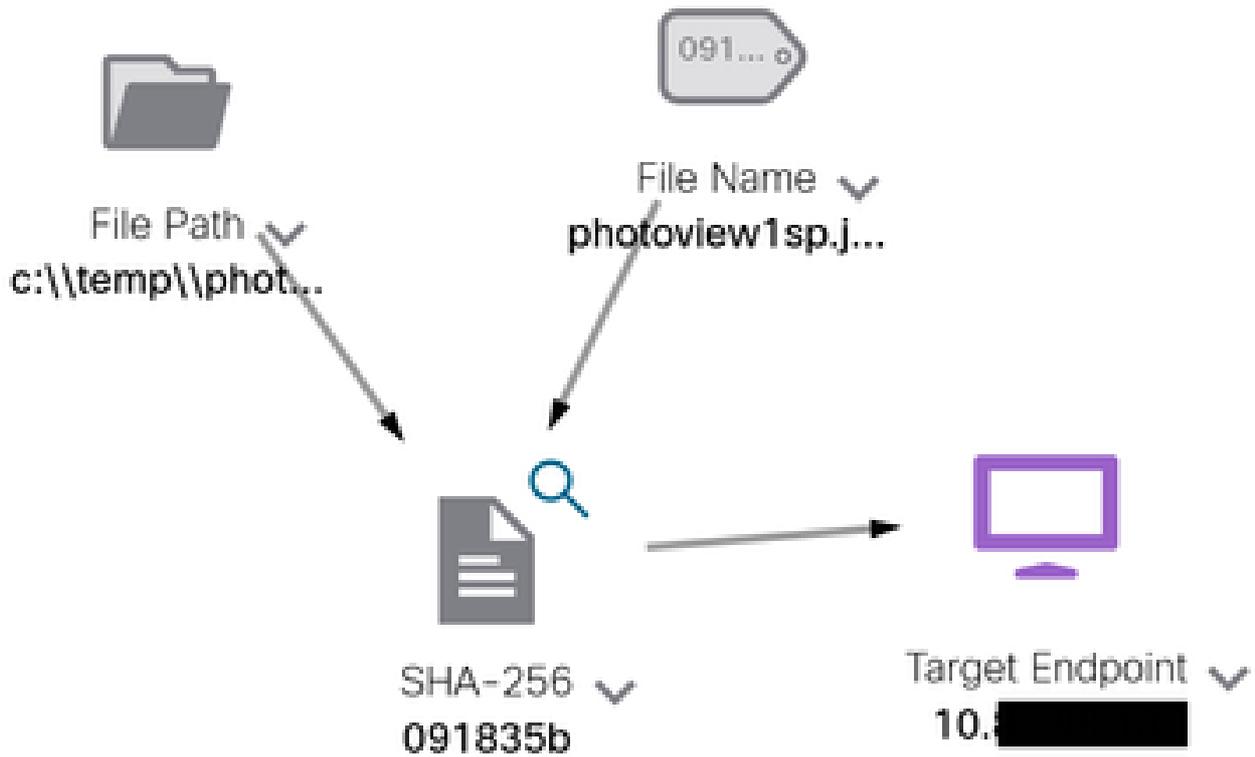
Abra WebDeveloper Tools, ejecute la investigación, busque un evento Post en **visibility.amp.cisco.com** en el archivo llamado Observables.



Verificación

Puede utilizar este enlace: [Instantáneas de seguridad gráfica de Microsoft](#) para obtener una lista de Instantáneas que le ayudarán a entender la respuesta que puede obtener de cada tipo de observable.

Puede ver un ejemplo como se muestra en esta imagen:



Expanda la ventana, puede ver la información proporcionada por la integración:

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 `photoviewggjps1` disguises itself as `photoview1sp.jpg`

OBSERVABLES RELATED TO SIGHTING (1)

SHA-256 Hash: `091835b16193e53fee1b1a04d0fce7534544cad306673066f3ad6973a4b18b19`

Tenga en cuenta que los datos deben existir en el portal de Azure y que la API de Graph funciona mejor cuando se utiliza con otras soluciones de Microsoft. Sin embargo, debe ser validado por el Soporte técnico de Microsoft.

Troubleshoot

- Mensaje de error de autorización:
 - Asegúrese de que los valores de **Tenant ID** y Client ID son correctos y de que siguen siendo válidos.

- No se muestran datos en la investigación:
 - Asegúrese de copiar y pegar los valores adecuados para **Tenant ID** y **Client ID**.
 - Asegúrese de utilizar la información del campo **Value** de la Certificates & Secrets sección.
 - Utilice las herramientas de WebDeveloper para determinar si se consulta la API de Graph cuando se produce una investigación.
 - A medida que la API de Graph combina datos de varios proveedores de alertas de Microsoft, asegúrese de que OData es compatible con los filtros de consulta. (Por ejemplo, Seguridad y cumplimiento de Office 365 y ATP de Microsoft Defender).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).