

配置Microsoft Graph API与Cisco XDR的集成

目录

[简介](#)

[先决条件](#)

[集成步骤](#)

[执行调查](#)

[验证](#)

[故障排除](#)

简介

本文档介绍将Microsoft Graph API与Cisco XDR集成的过程以及可查询的数据类型。

先决条件

- Cisco XDR管理员帐户
- Microsoft Azure系统管理员帐户
- 访问Cisco XDR

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

集成步骤

步骤1:

以系统管理员身份登录Microsoft Azure。

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

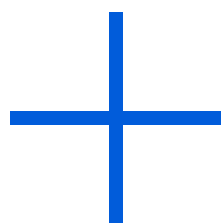
[Can't access your account?](#)

Back

Next

第二步：

点击Azure服务门户App Registrations 上的。



Create a
resource



App
registrations

第三步：

单击。New registration

Home >

App registrations



New registration



Endp

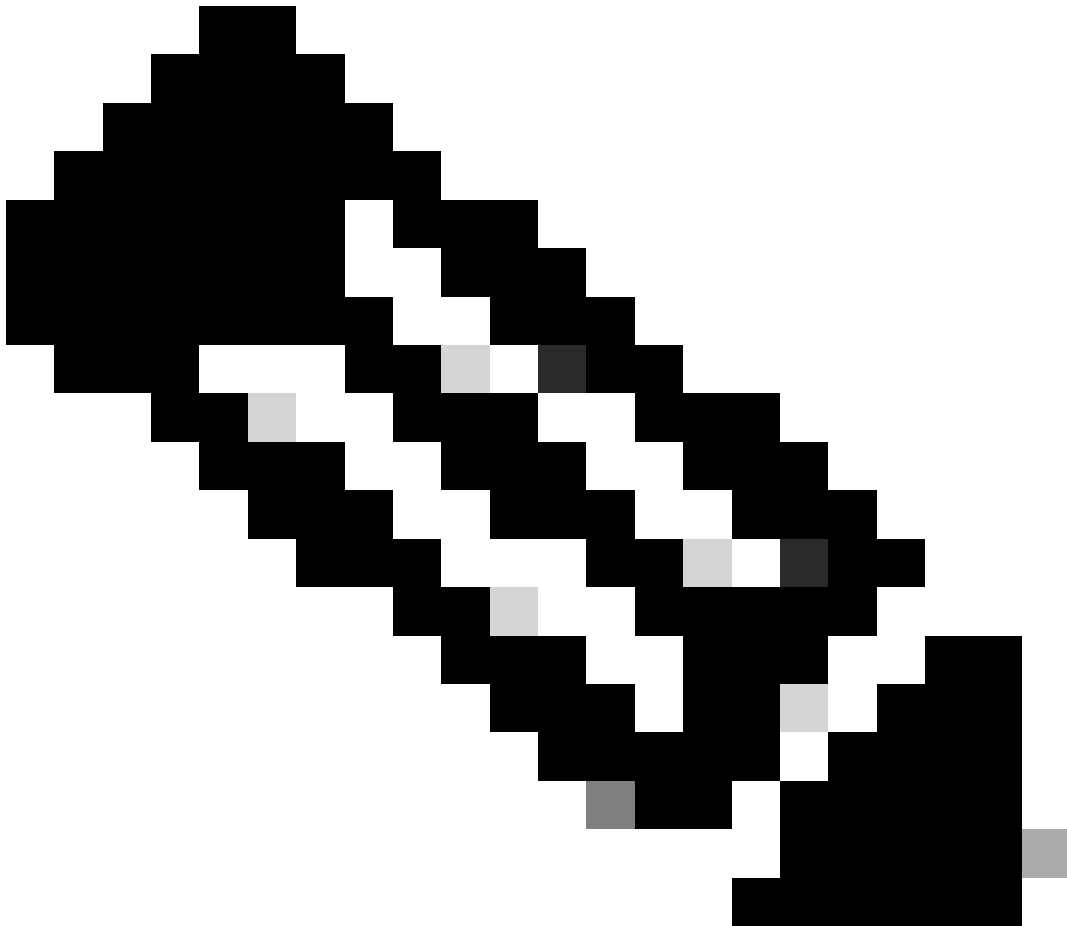
第四步：

键入名称以标识新应用。

▪ Name

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

SecureX - Graph API



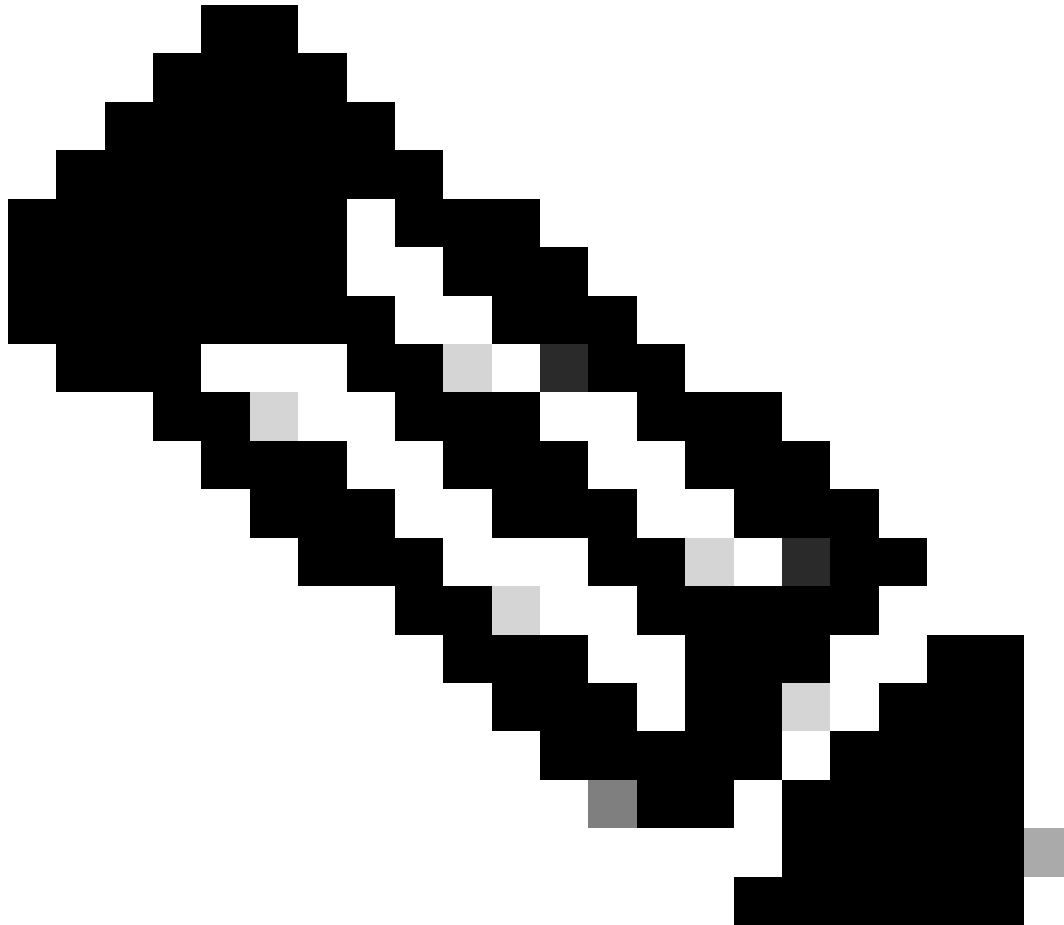
注意：如果名称有效，则会显示绿色的复选标记。

在支持的帐户类型上，选择选项 **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
-



注意：您不需要键入重定向URI。

第五步：

滚动到屏幕底部并单击 **Register**。

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

Register

第六步：





导航回Azure服务页面，点击App Registrations > Owned Applications。

识别您的应用并点击名称。在本例中为SecureX。

All applications Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [Redacted]	049831 [Redacted]
 [Redacted]	9c6692c [Redacted]
 [Redacted] <small>portal</small>	4c32d8c [Redacted]
 SecureX	16e2bd33-8378-413e-86d7-04e1477efbc0

步骤 7.

系统将显示您的应用的摘要。请确定以下相关详细信息：

应用程序（客户端）ID：

Display name : [SecureX](#)

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

目录（租户）ID：

Directory (tenant) ID : f2bf8cd3-[Redacted]

步骤 8

导航到Manage Menu > API Permissions。

Manage



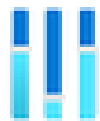
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

步骤 9

在“配置的权限”下，单击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 ██████████

步骤 10

在“请求API权限”部分，单击 **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.

步骤 11

选择.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.

在搜索栏中，查找Security。展开 **Security Actions** 并选择

- **Read.All**
- 全部读

- 安全事件并选择
 - **Read.All**
 - 全部读

- 威胁指示器并选择
 - **ThreatIndicators.ReadWrite.OwnedBy**

单击。Add permissions

步骤 12

检查您选择的权限。

+ 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](#).

为您的组织单击 **Grant Admin consent** 。

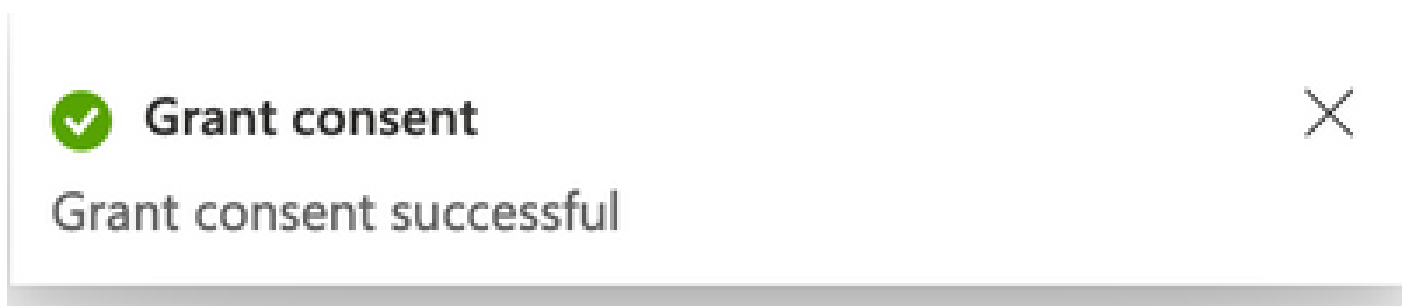
Configured permissions

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]

系统将显示一个提示，提示您选择是否要同意所有权限。单击。Yes

此时将显示类似弹出窗口，如下图所示：



步骤 13

导航到Manage > Certificates & Secrets。

单击。Add New Client Secret

写下简要描述并选择有效的日期Expires。建议选择6个月以上的有效日期，以防止API密钥过期。

创建后，在用于集成的情况下，将 **Value**部分复制并存储在安全位置。

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]




警告：此字段无法恢复，您必须创建新密钥。

获取所有信息后，导航回 **Overview** 并复制应用的值。然后导航到SecureX。

步骤 14

导航至Integration Modules > Available Integration Modules > 选择Microsoft Security Graph API，点击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](#)

分配名称并粘贴从Azure门户获得的值。

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

Entries Limit
Default

Resolves the maximum number of endpoints

[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.
 - **Entries Limit** - Specify the maximum number of endpoints 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 entries.
3. [Click Save](#) to complete the Microsoft Graph Security API integration module configuration.

单击Save，然后等待运行状况检查成功。

Edit Microsoft Graph Security API Module



This integration module has no issues.

执行调查

到目前为止，Microsoft安全图API未使用磁贴填充Cisco XDR控制面板。相反，可以使用调查来查询Azure门户中的信息。

请记住，Graph API只能查询以下内容：

- ip
- 域
- 主机名
- url
- file_name
- file_path
- sha256

在本示例中，调查使用此SHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148`。

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

如您所见，它在实验室环境中有0次发现，那么如何测试Graph API是否有效？

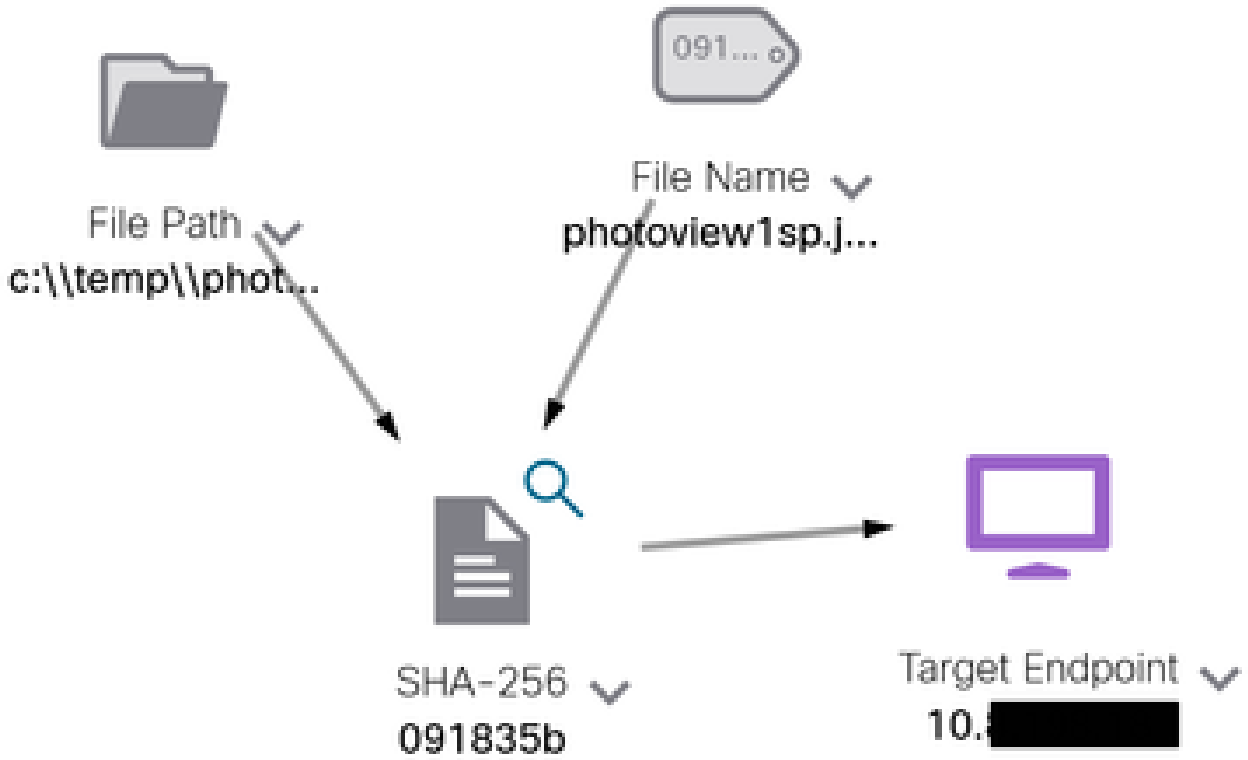
打开WebDeveloper工具，运行调查，然后向visibility.amp.cisco.com查找帖子事件，并找到名为Observables的文件。



验证

您可以使用此链接：[Microsoft图形安全快照](#)获取快照列表，以帮助您了解可从每种可观察类型获得的响应。

您可以看到如下图所示的示例：



展开此窗口，您可以看到集成提供的信息：

Module: Microsoft Graph Security API	Confidence: None
Source: Microsoft Graph Security	Severity: Medium
Sensor: Endpoint	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 SIGNING (1)
 SHA-256 Hash: 091835b16192e506ee1b8a04d0fceff534544cad306673060f3ad6973a4b18b19

请记住，数据必须存在于Azure门户中，Graph API在与其他Microsoft解决方案配合使用时效果更好。但是，这必须由Microsoft支持部门进行验证。

故障排除

- 授权失败消息：
 - 确保 Tenant ID 和Client ID的值正确并且仍然有效。

- 调查中未显示任何数据：

- 确保复制并粘贴了 **Tenant ID** 和 **Client ID**的适当值。

- 确保您使用了Certificates & Secrets部分 **Value** 的字段信息。

- 使用WebDeveloper工具确定调查发生时是否查询图形API。

- 当图形API合并来自各种Microsoft警报提供者的数据时，请确保查询过滤器支持OData。（例如，Office 365安全与合规性和Microsoft Defender ATP）。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。