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

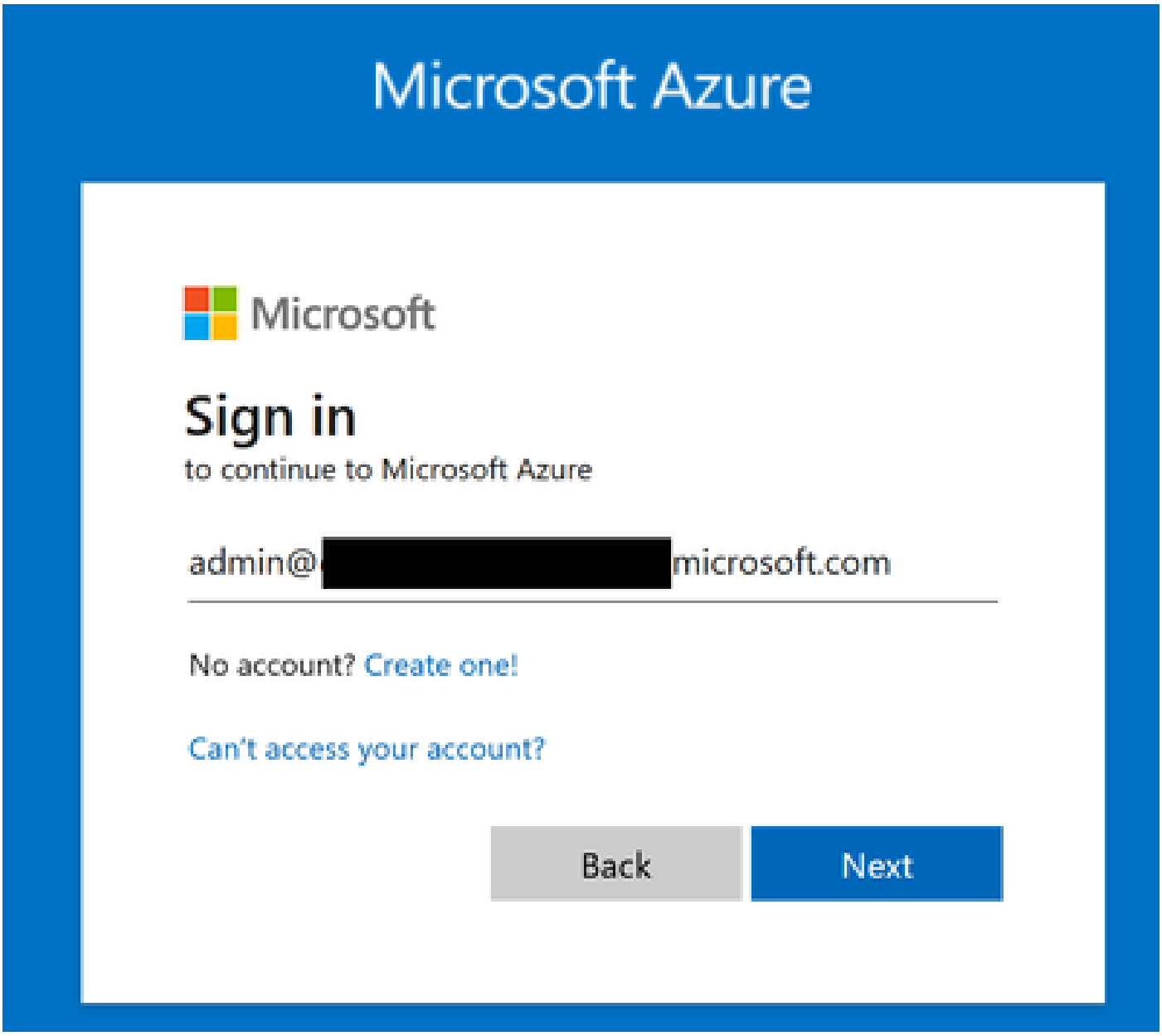
- Cuenta de administrador de Cisco XDR
- Cuenta de administrador del sistema de Microsoft Azure
- Acceso a Cisco XDR

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

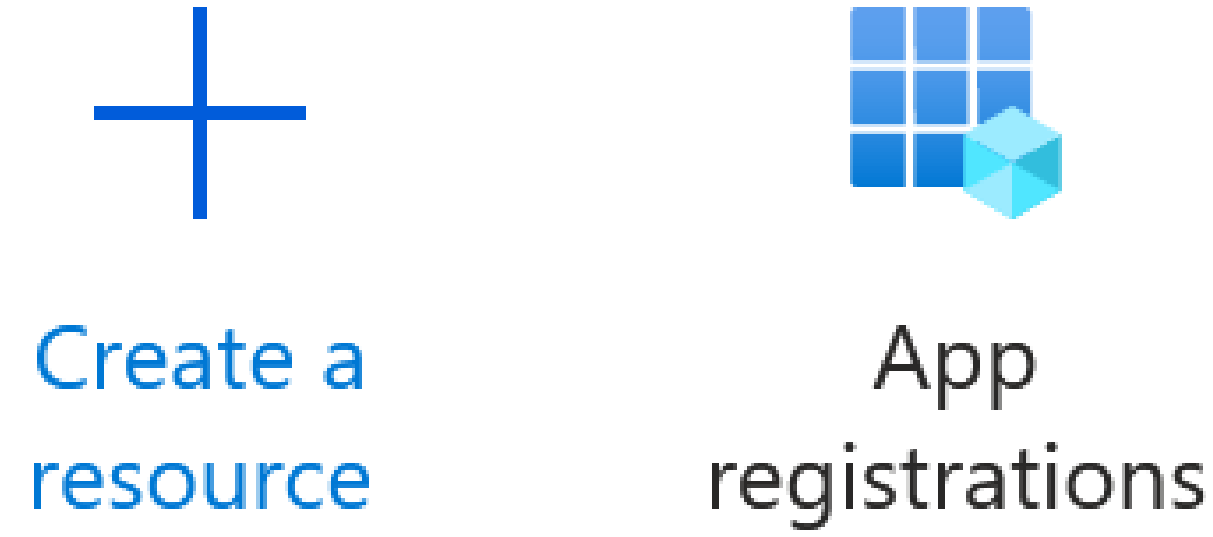
Paso 1.

Inicie sesión en Microsoft Azure como administrador del sistema.



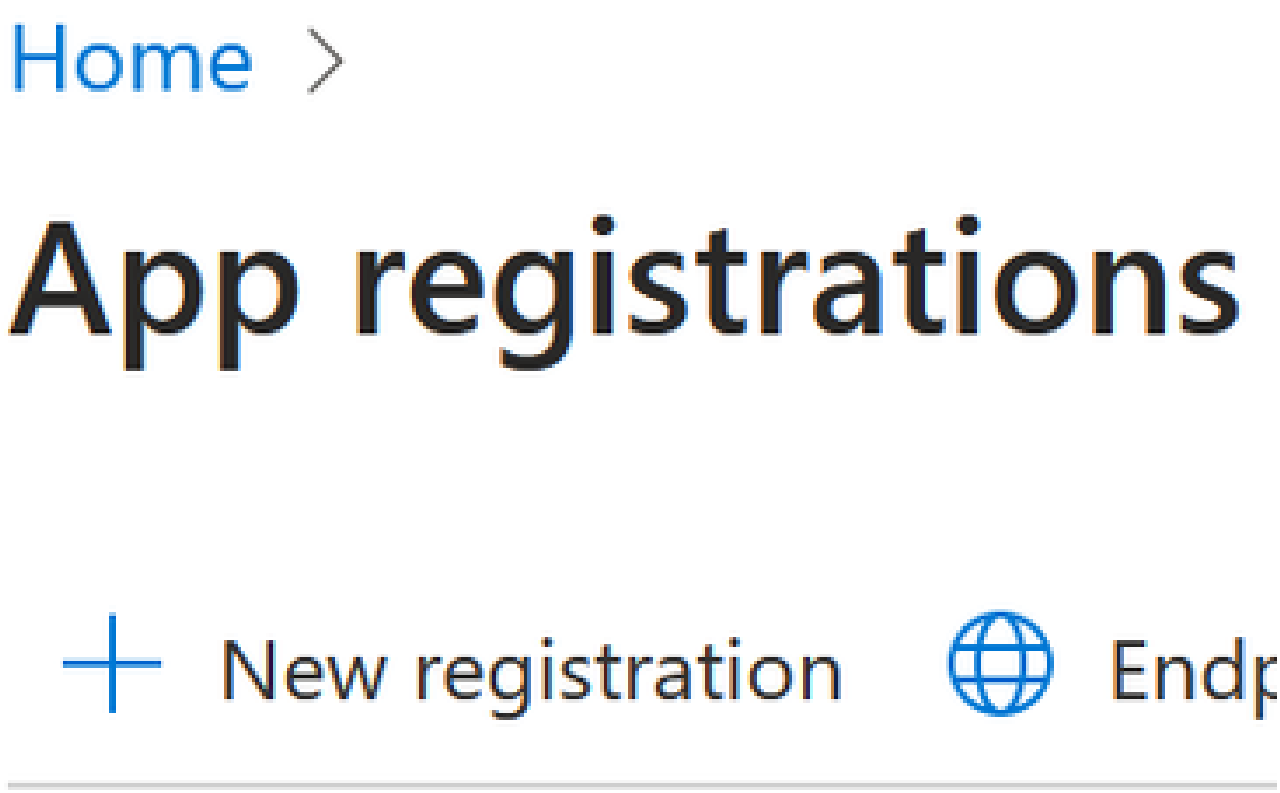
Paso 2.

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



Paso 3.

Haga clic en New registration.



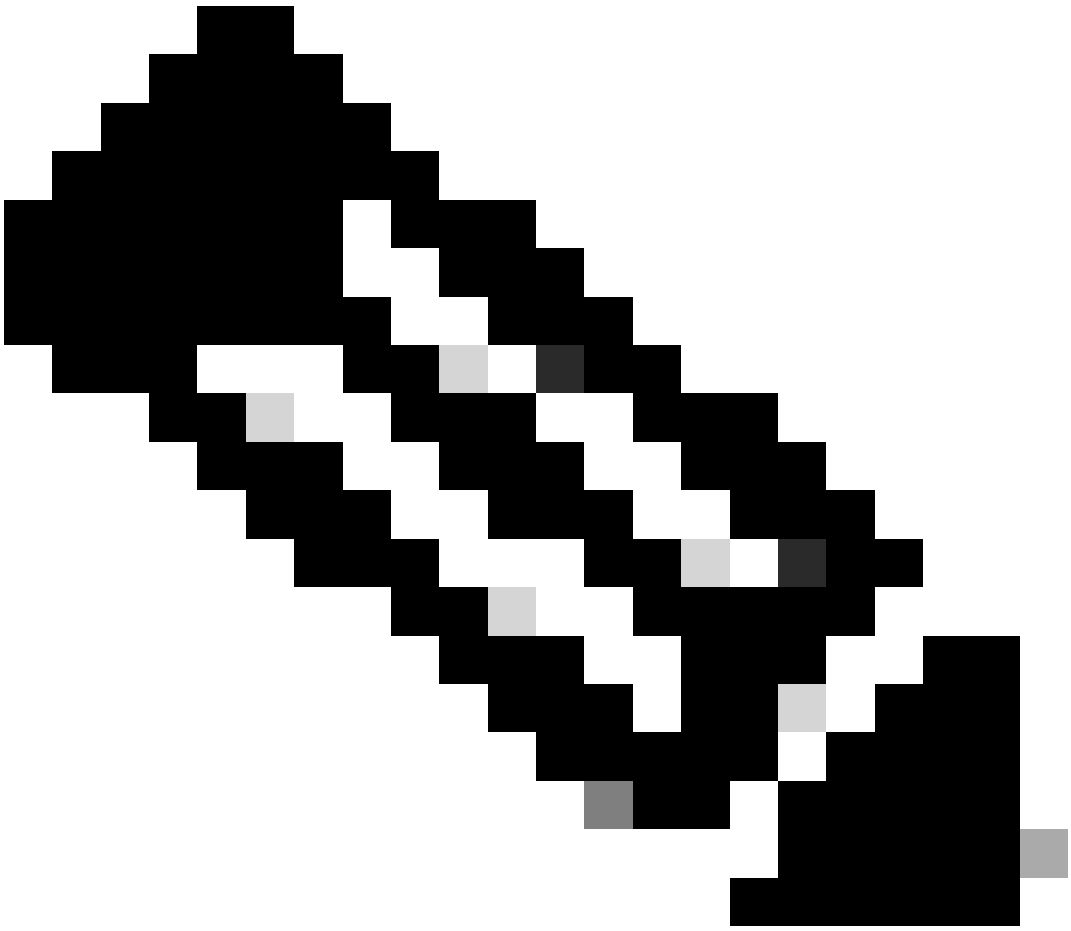
Paso 4.

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



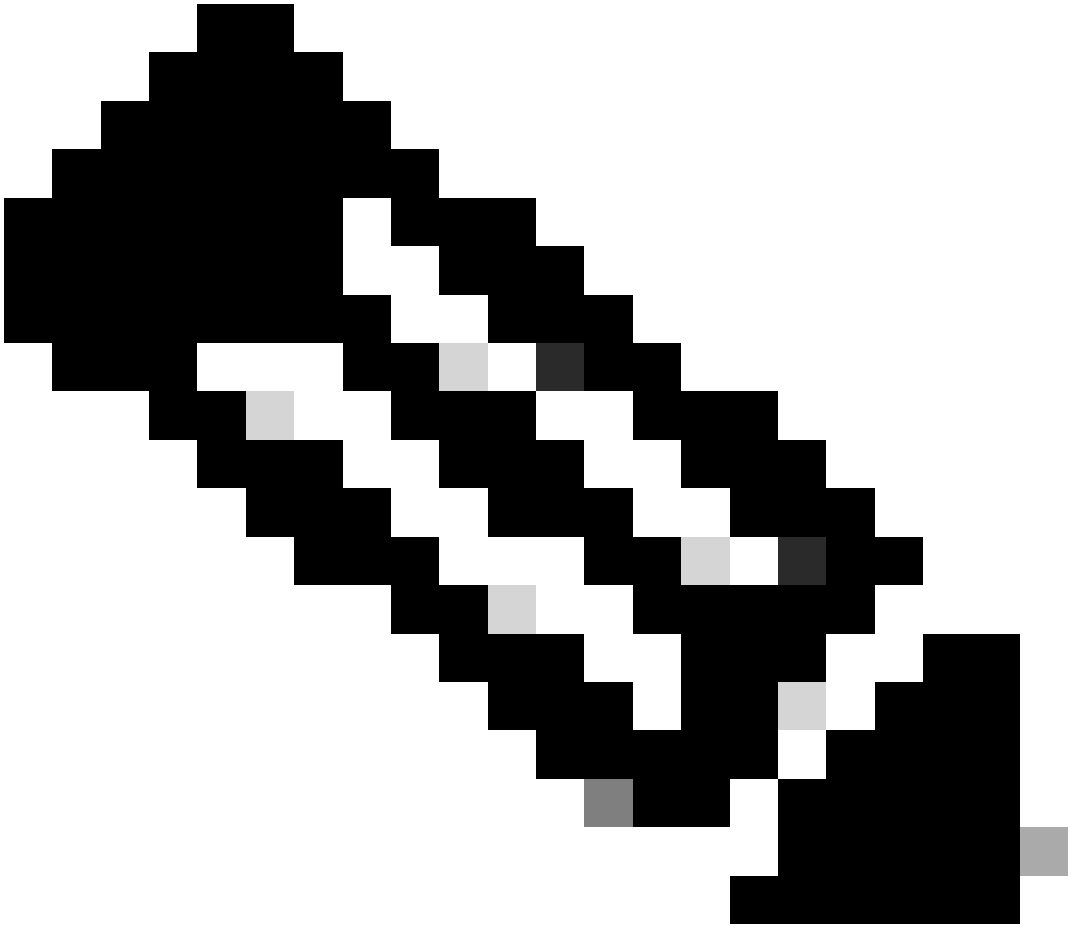
Nota: Si el nombre es válido, aparecerá una marca de verificación verde.

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 ([redacted]: 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.

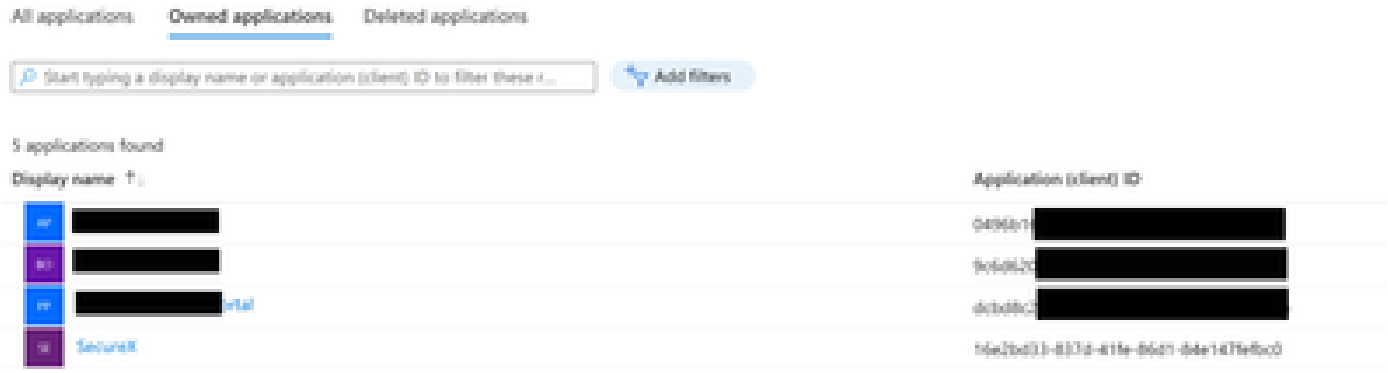
Paso 5.

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



Paso 7.

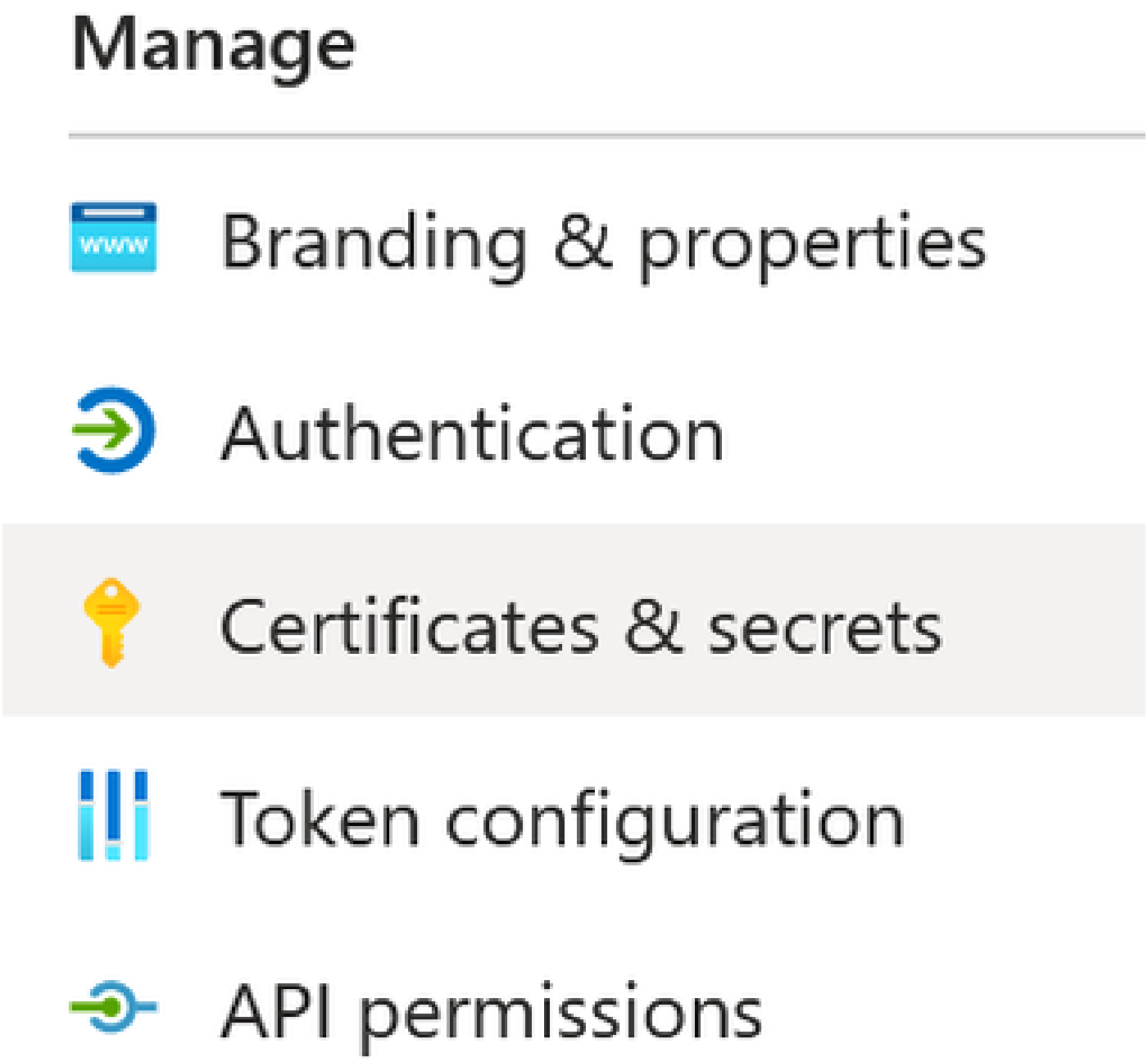
Aparecerá un resumen de su aplicación. Identifique estos datos relevantes:

ID de aplicación (cliente):

ID de directorio (arrendatario):

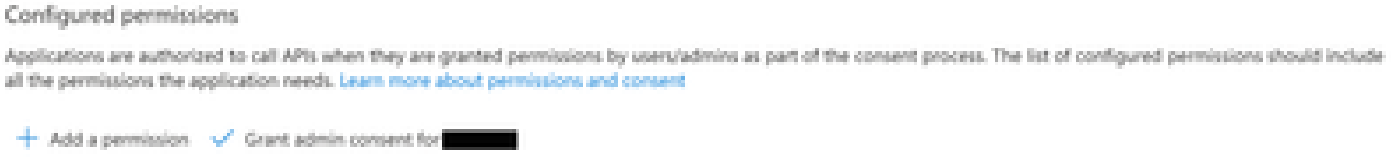
Paso 8.

Desplácese hasta Manage Menu > API Permissions.



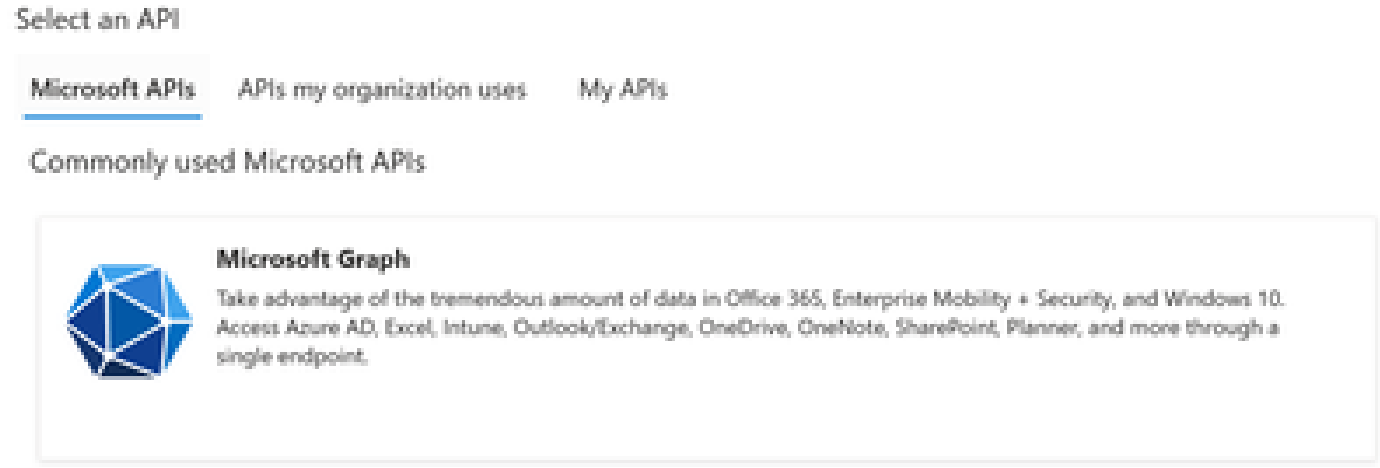
Paso 9.

En Permisos configurados, haga clic en Add a Permission.



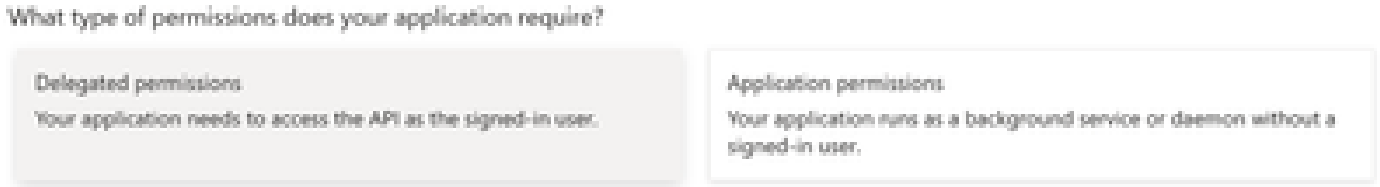
Paso 10.

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



Paso 11.

Seleccione Application permissions.



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

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

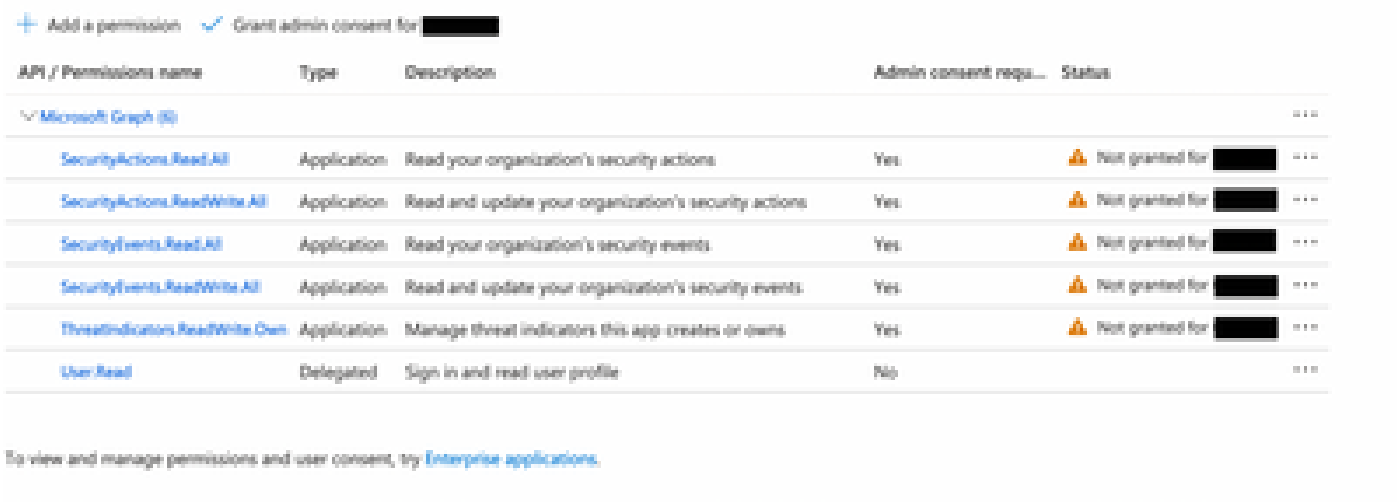
- **Eventos de seguridad** y seleccione
  - **Leer.Todo**
  - **ReadWrite.All**

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

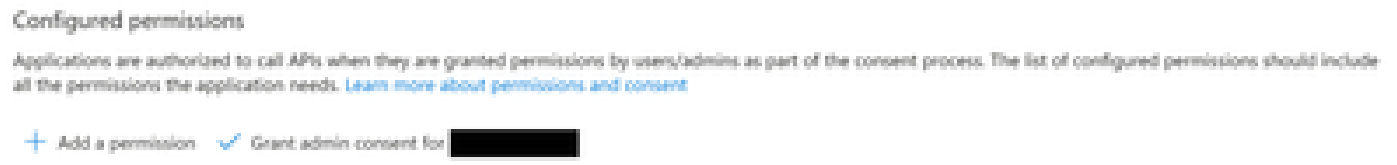
Haga clic en Add permissions.

Paso 12.

Revise los permisos seleccionados.

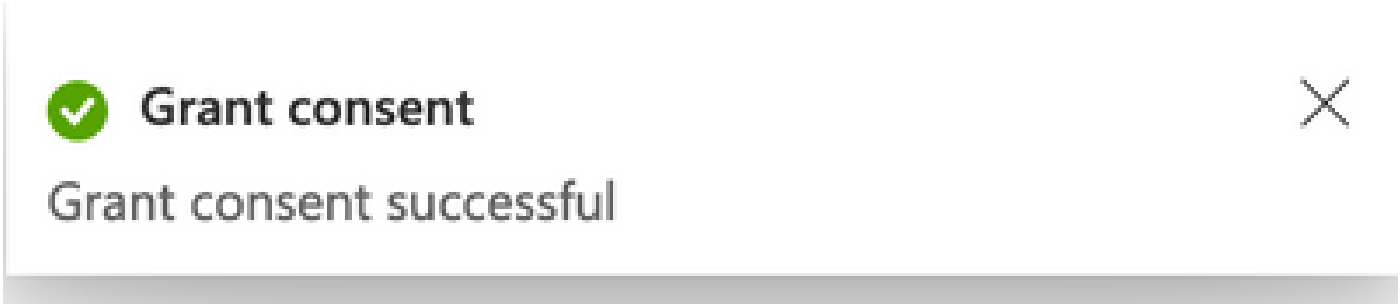


Haga clic **Grant Admin consent** en para su organización.



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:



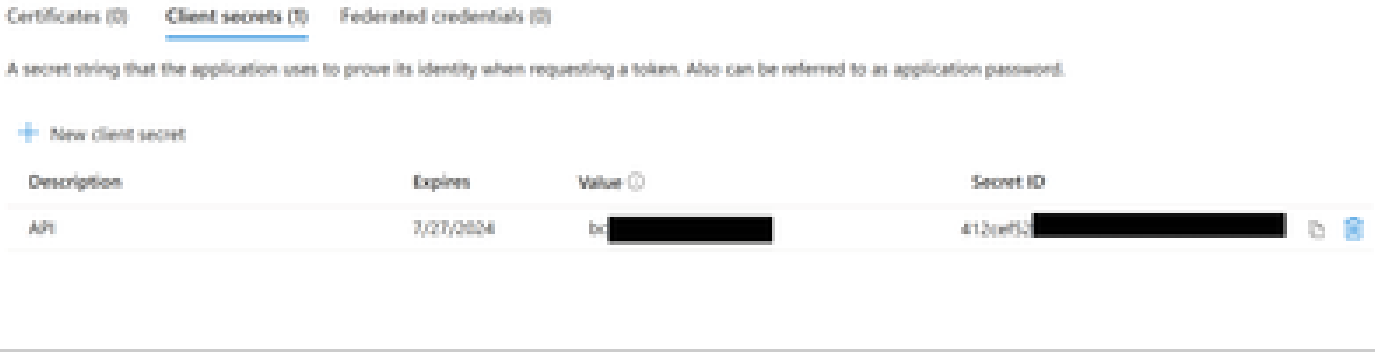
Paso 13.

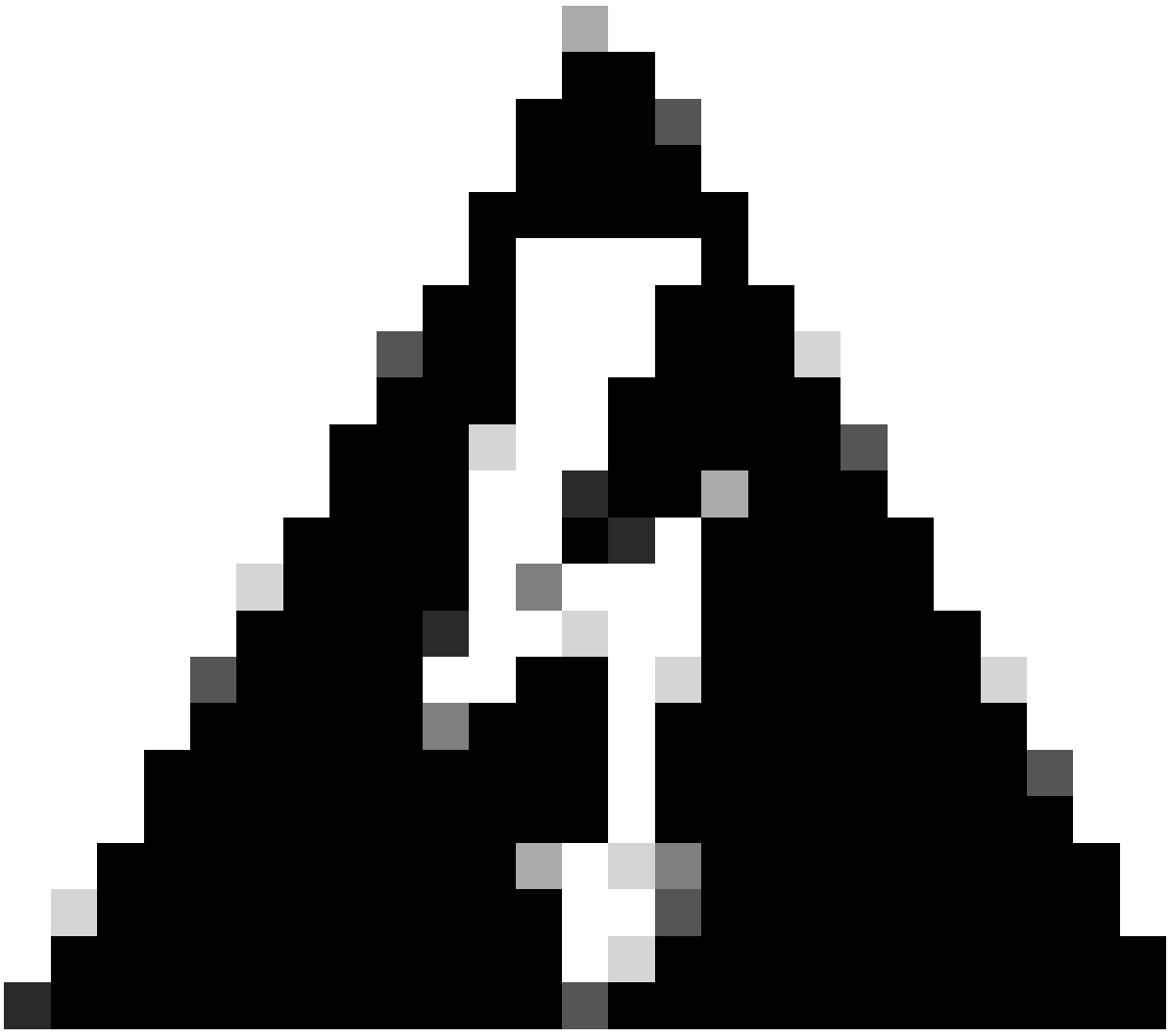
Desplácese hasta Manage > Certificates & Secrets.

Haga clic en Add New Client Secret.

Escriba una breve descripción y seleccione una fecha válidaExpires. 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.





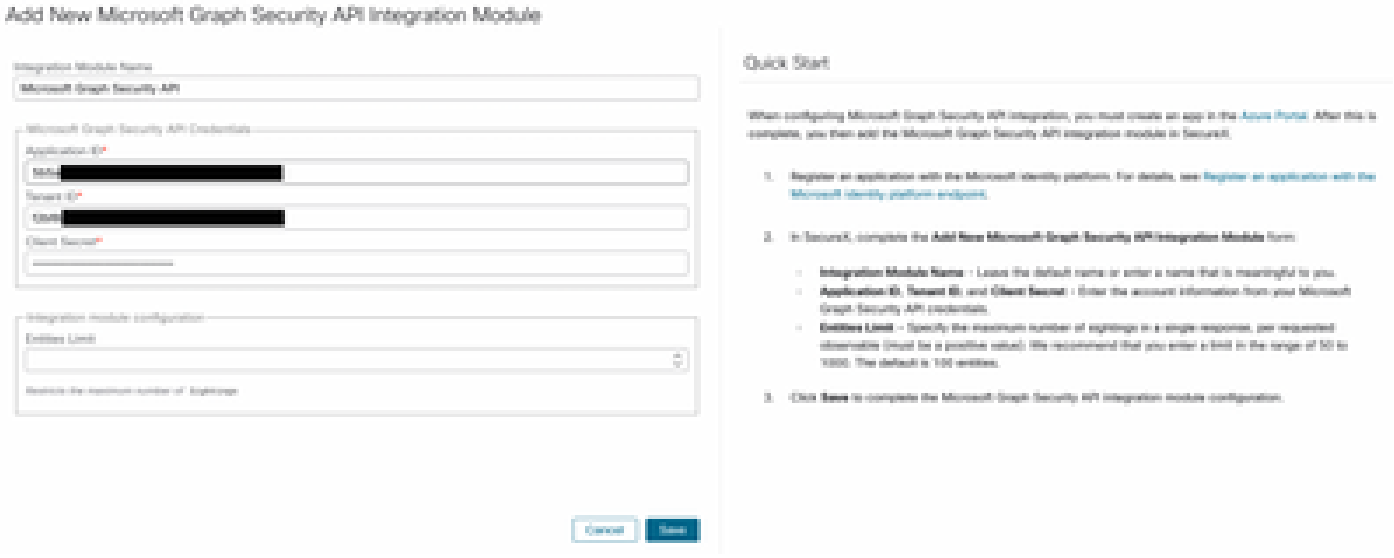
Advertencia: este campo no se puede recuperar y debe crear un nuevo secreto.

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

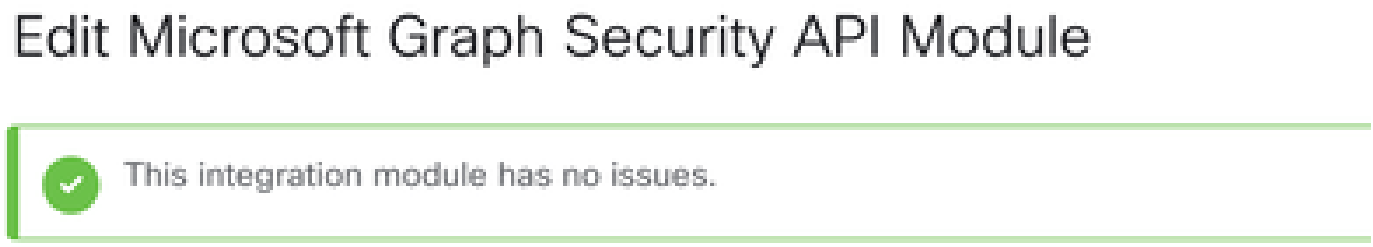
Paso 14.

Desplácese hasta Integration Modules > Available Integration Modules > seleccionarMicrosoft Security Graph API y haga clic en Add.

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



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



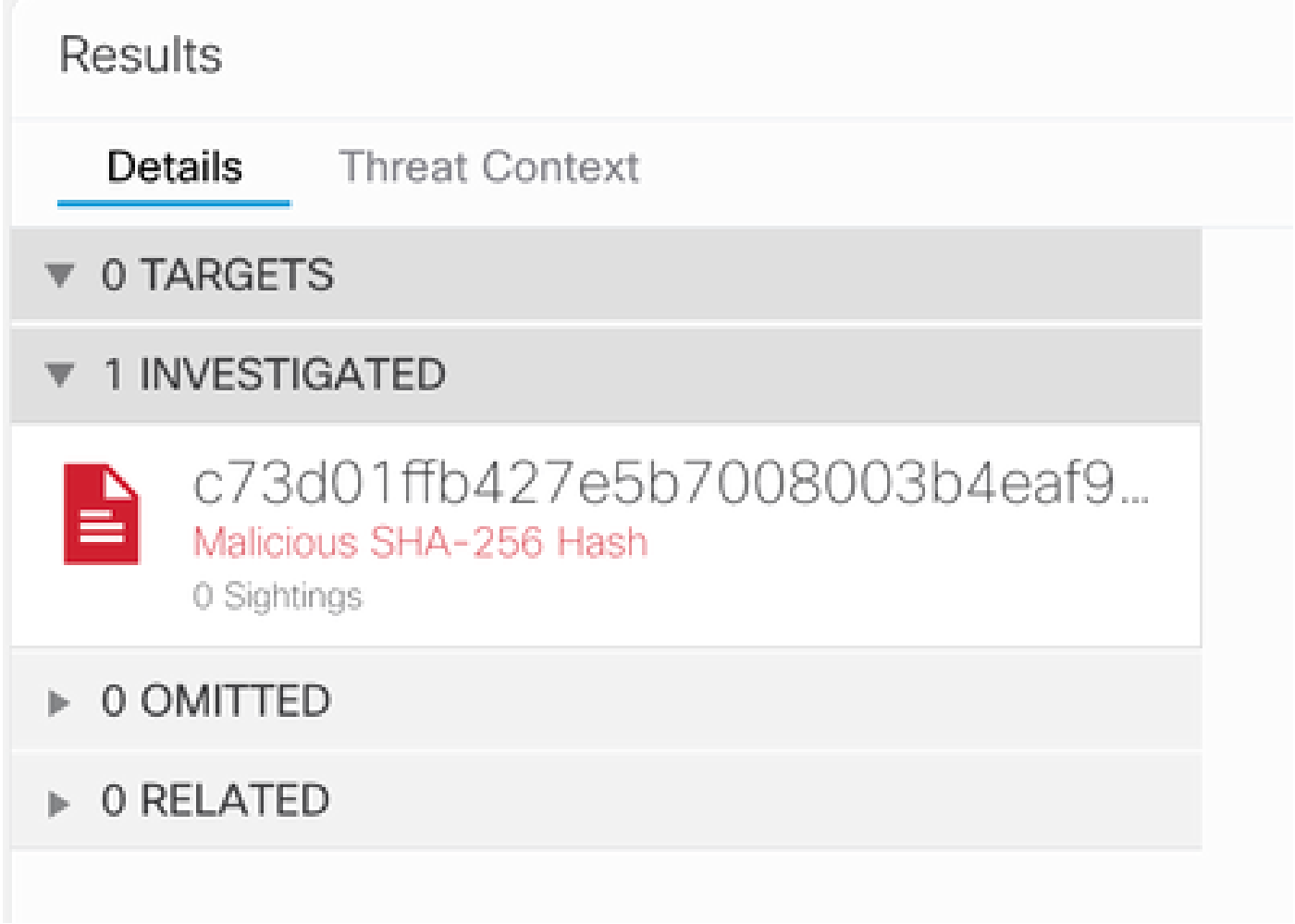
Realizar investigaciones

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.



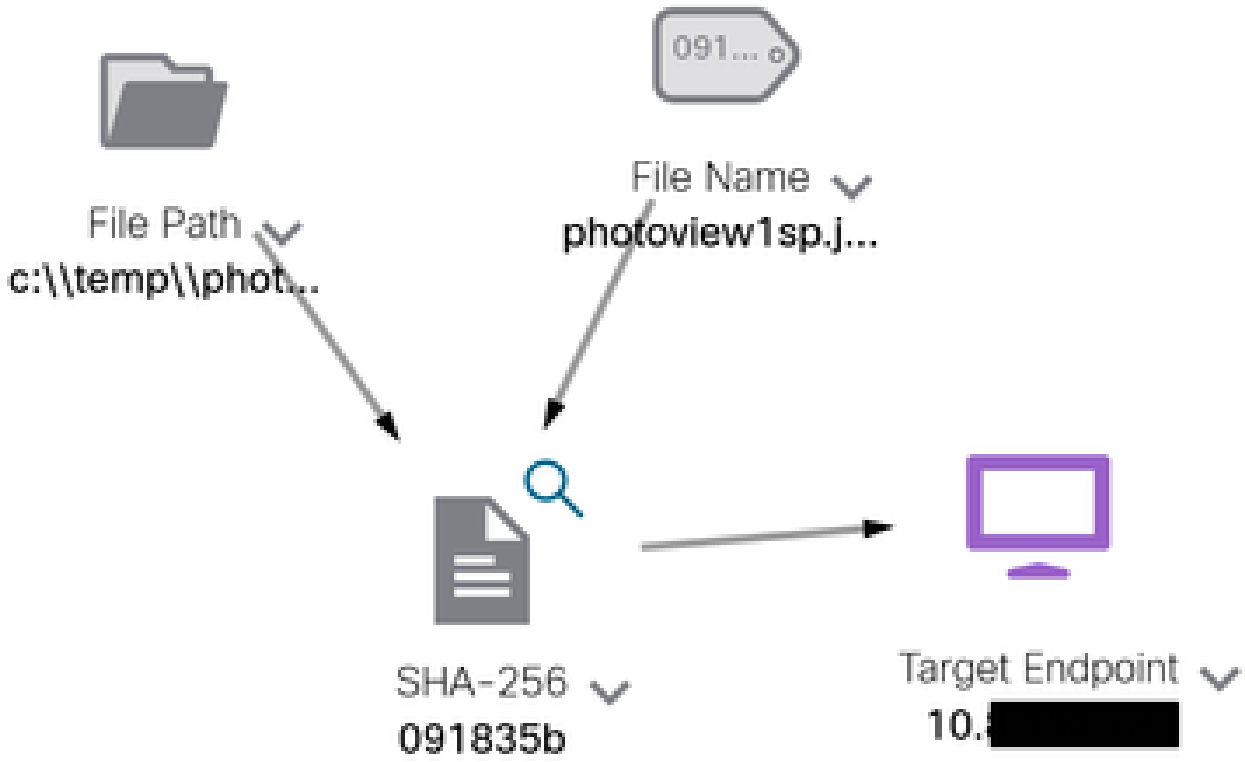
Como puede ver, tiene 0 avistamientos en el entorno de laboratorio, así que ¿cómo probar si Graph API funciona?

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

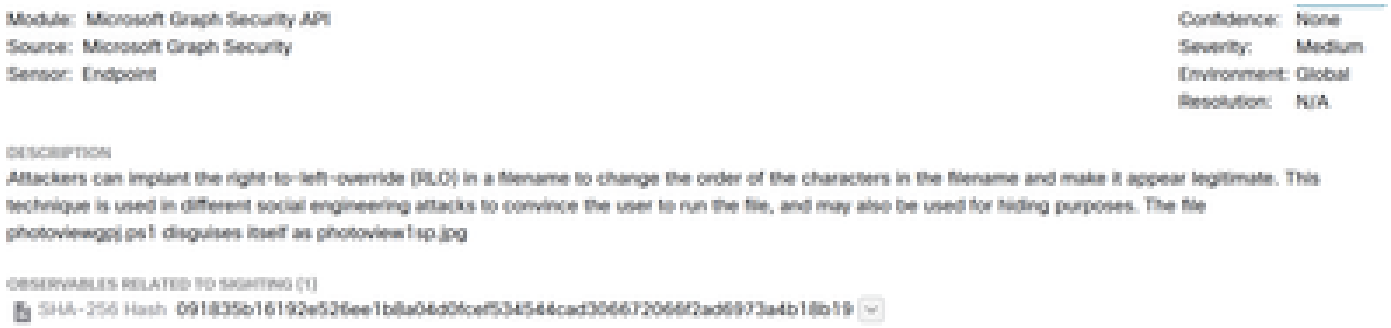
Verificación

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:



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).