

# Konfigurieren der Integration der Microsoft Graph API mit Cisco XDR

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Integrationschritte](#)

[Durchführung von Untersuchungen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

---

## Einleitung

In diesem Dokument wird das Verfahren zur Integration der Microsoft Graph-API in Cisco XDR sowie der Typ der abfragbaren Daten beschrieben.

## Voraussetzungen

- Cisco XDR-Administratorkonto
- Microsoft Azure-Systemadministratorkonto
- Zugriff auf Cisco XDR

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Integrationschritte

Schritt 1:

Melden Sie sich als Systemadministrator bei Microsoft Azure an.

# Microsoft Azure



## Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

---

No account? [Create one!](#)

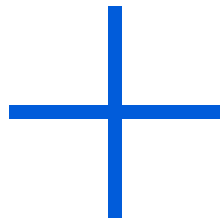
[Can't access your account?](#)

Back

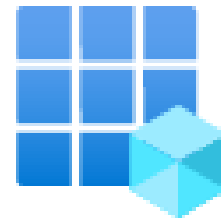
Next

Schritt 2:

Klicken Sie **App Registrations** auf das Azure-Serviceportal.



Create a  
resource



App  
registrations

Schritt 3:

Klicken Sie auf „New registration“

Home >

# App registrations



New registration



Endp

---

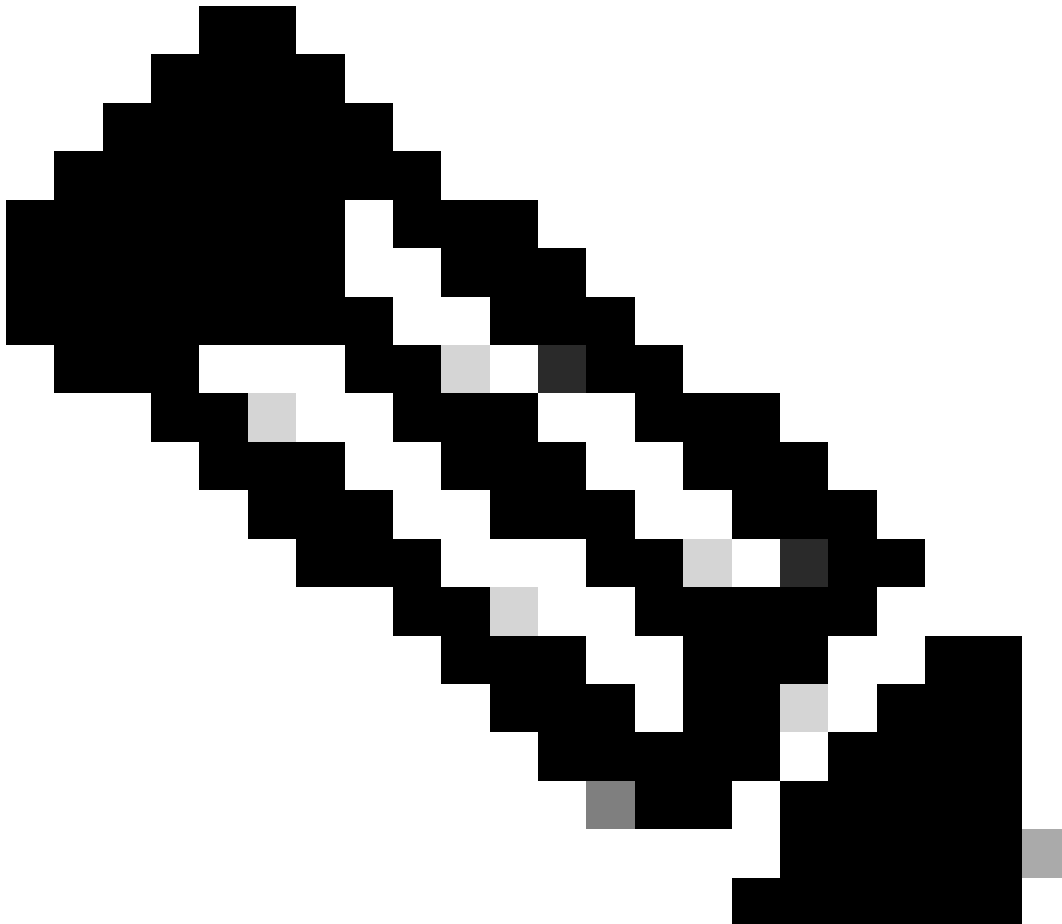
Schritt 4:

Geben Sie einen Namen ein, um Ihre neue App zu identifizieren.

▪ Name

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

SecureX - Graph API



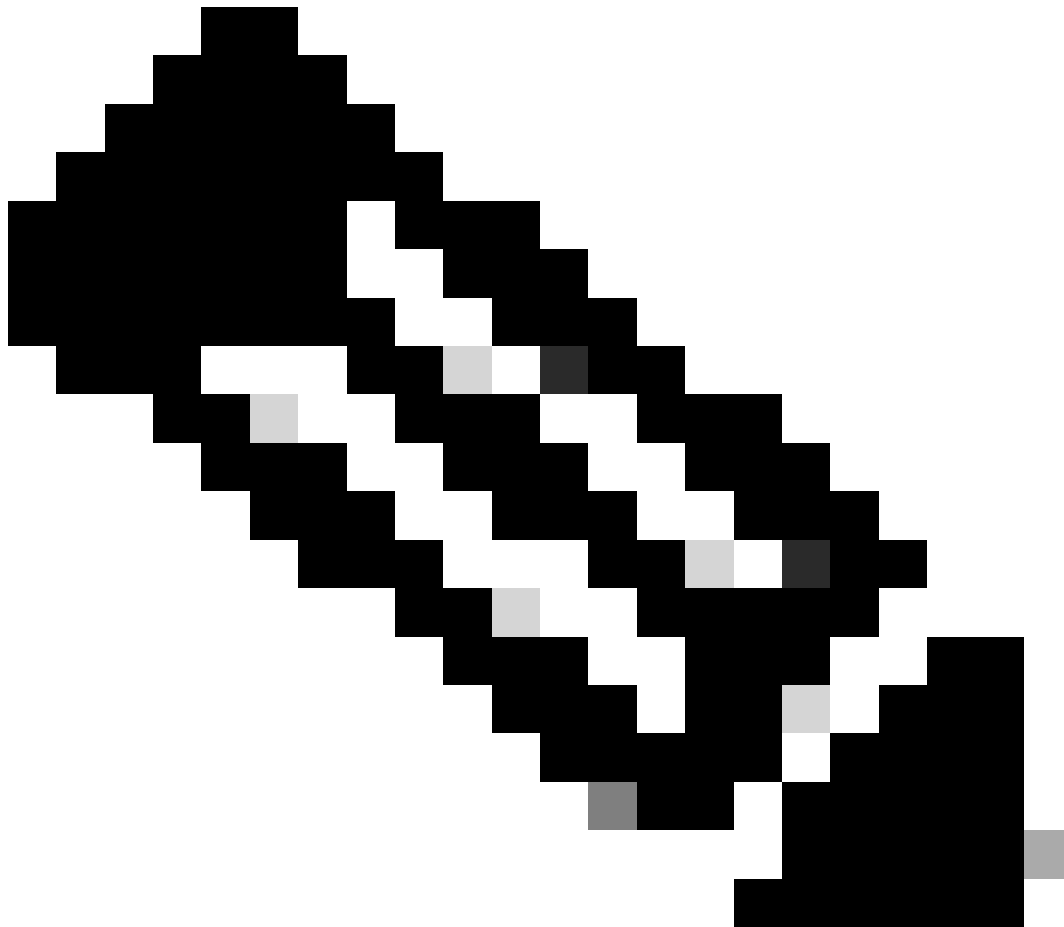
**Hinweis:** Wenn der Name gültig ist, wird ein grünes Häkchen angezeigt.

Wählen Sie für unterstützte Kontotypen die Option **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
- 



**Hinweis:** Sie müssen keinen Umleitungs-URI eingeben.

---

Blättern Sie zum unteren Bildschirmrand, und klicken Sie auf **Register**.

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

**Register**

Schritt 6:





Navigieren Sie zurück zur Azure-Dienstseite, und klicken Sie auf App Registrations > Owned Applications.

Identifizieren Sie Ihre App, und klicken Sie auf den Namen. In diesem Beispiel ist dies der FallSecureX.

All applications Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [Redacted]	049831 [Redacted]
 [Redacted]	9c66d0c [Redacted]
 [Redacted] Portal	6c3db8c [Redacted]
 SecureX	16e2bd33-8378-419e-86d7-64e1479efc0

Schritt 7.

Eine Zusammenfassung Ihrer App wird angezeigt. Bitte geben Sie die folgenden relevanten Details an:

**Anwendungs-ID (Client):**

Display name : [SecureX](#)

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

**Verzeichnis-ID (Tenant):**

Directory (tenant) ID : f2bf8cd3-[Redacted]

Schritt 8:

Navigieren Sie zu Manage Menu > API Permissions.

# Manage

---



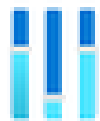
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Schritt 9.

Klicken Sie unter Konfigurierte Berechtigungen auf 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 ██████████

Schritt 10.

Klicken Sie im Abschnitt Anfordern von API-Berechtigungen auf **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.

Schritt 11.

Auswählen 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.

Suchen Sie in der Suchleiste nach Security. Erweitern **Security Actions** und auswählen

- **Lesen.Alle**
  
- **LesenSchreiben.Alle**
  
  
- **Sicherheitsereignisse** auswählen und
  - **Lesen.Alle**
  
  - **LesenSchreiben.Alle**
  
  
- **Bedrohungsindikatoren anzeigen** und auswählen
  - **ThreatIndicators.ReadWrite.OwnedBy**



Klicken Sie auf .Add permissions

Schritt 12:

Überprüfen Sie die ausgewählten Berechtigungen.

+ 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](#).

Klicken Sie hier **Grant Admin consent** für Ihre Organisation.

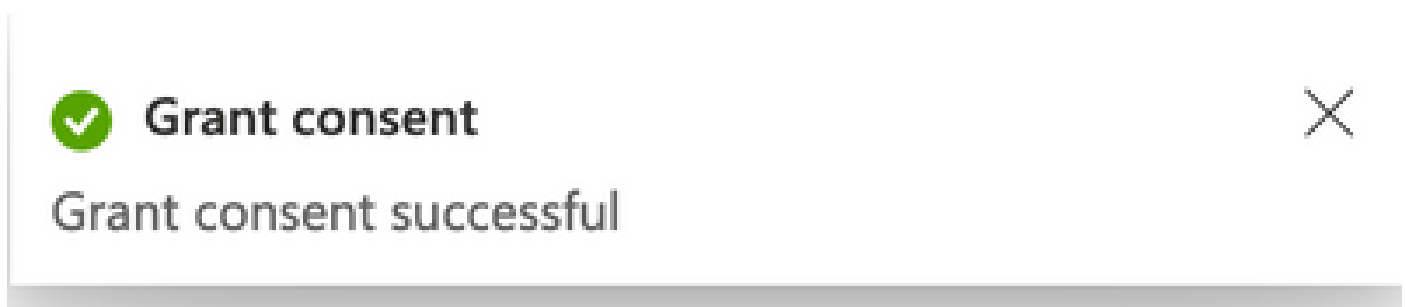
#### Configured permissions

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]

Sie werden aufgefordert, auszuwählen, ob Sie die Zustimmung für alle Berechtigungen erteilen möchten. Klicken Sie auf .Yes

Ein ähnliches Pop-up-Fenster wird angezeigt, wie in dieser Abbildung dargestellt:



Schritt 13:

Navigieren Sie zu Manage > Certificates & Secrets.

Klicken Sie auf .Add New Client Secret

Schreiben Sie eine kurze Beschreibung, und wählen Sie ein gültiges Expires Datum aus. Es wird empfohlen, ein Gültigkeitsdatum von mehr als 6 Monaten zu wählen, um zu verhindern, dass die API-Schlüssel ablaufen.

Nach der Erstellung können Sie den Abschnitt, der Ihnen sagt, **Value** wie er für die Integration verwendet wird, kopieren und an einem sicheren

Ort speichern.

Certificates (0) Client secrets (3) Federated credentials (0)

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]	4120ef52 [REDACTED]		



**Warnung:** Dieses Feld kann nicht wiederhergestellt werden, und Sie müssen einen neuen Schlüssel erstellen.

Sobald Sie alle Informationen haben, navigieren Sie zurück zu **Overview** und kopieren Sie die Werte Ihrer App. Navigieren Sie anschließend zu SecureX.

Schritt 14:

Navigieren Sie zur Integration Modules > Available Integration Modules > Option Microsoft Security Graph API, und klicken Sie auf Add.



The card features a blue shield icon with a white double-headed arrow on the left. The main title is "Microsoft Graph Security API". Below the title is a descriptive paragraph: "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...". At the bottom left is a blue button with a white plus sign and the text "+ Add". At the bottom right is a blue link that says "Learn More".

Weisen Sie einen Namen zu, und fügen Sie die Werte ein, die Sie aus dem Azure-Portal erhalten haben.

#### 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  
[Dropdown menu]

Defines the maximum number of endpoints

#### 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 SecureX.

1. Register an application with the Microsoft identity platform. For details, see [Register an application with the Microsoft identity platform endpoints](#).
2. In SecureX, 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.

Klicken Sie Save, und warten Sie, bis der Statuscheck erfolgreich ist.

# Edit Microsoft Graph Security API Module



This integration module has no issues.

## Durchführung von Untersuchungen

Bislang wird im Cisco XDR Dashboard mit der Microsoft Security Graph API keine Kachel angezeigt. Stattdessen können die Informationen aus Ihrem Azure-Portal mithilfe von Investigations abgefragt werden.

Beachten Sie, dass die Graph-API nur abgefragt werden kann für:

- ip
- Domäne
- hostname
- url
- Dateiname
- Dateipfad
- SHA256

In diesem Beispiel wurde diese SHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148` verwendet.

# Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

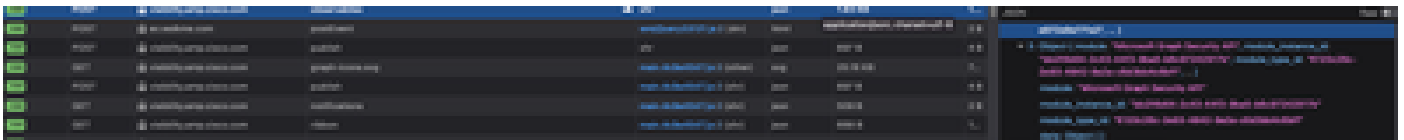
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Wie Sie sehen können, hat es 0 Sichtungen in der Lab-Umgebung, wie also zu testen, ob Graph API funktioniert?

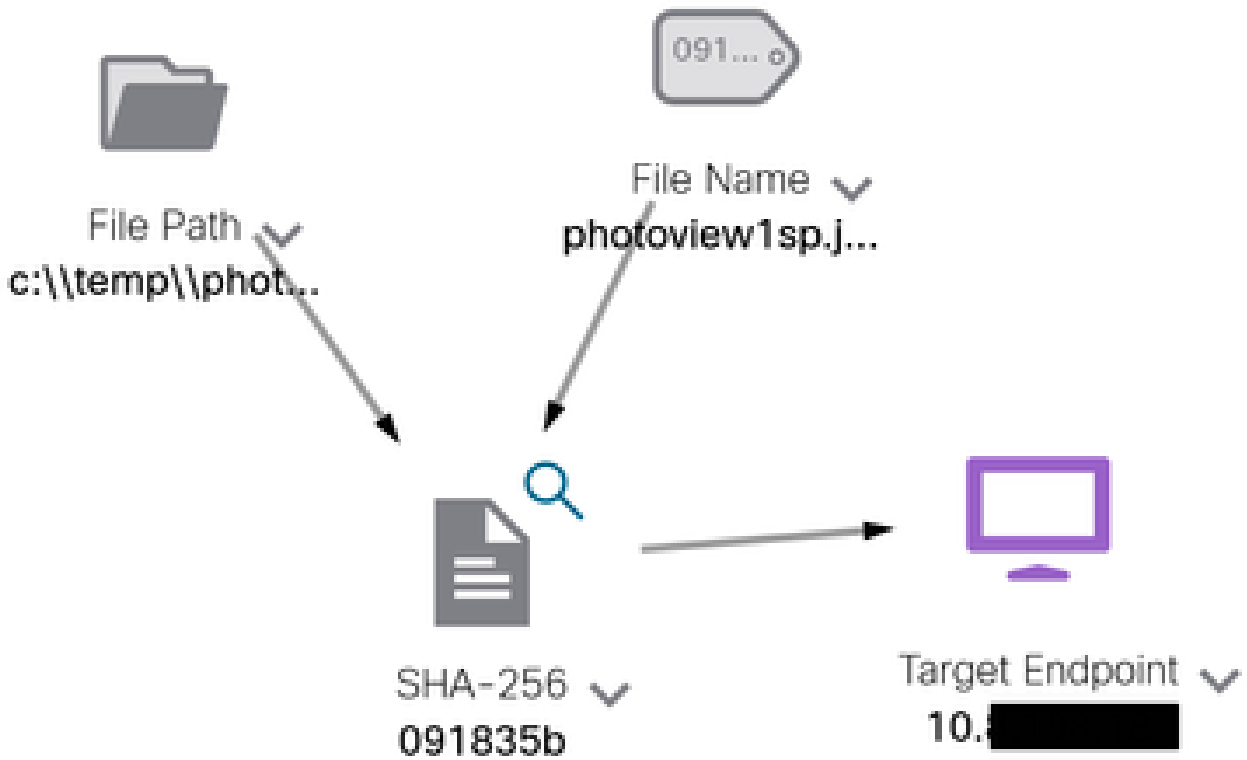
Öffnen Sie die WebDeveloper-Tools, führen Sie die Untersuchung aus, suchen Sie nach einem Post Event, um **visibility.amp.cisco.com** die Datei mit dem Namen Observables.



## Überprüfung

Sie können diesen Link verwenden: [Microsoft Graph Sicherheit Snapshots](#) für eine Liste von Snapshots, die Ihnen helfen zu verstehen, die Antwort, die Sie von jeder Art von beobachtbaren erhalten können.

Sie können ein Beispiel sehen, wie in der folgenden Abbildung dargestellt:



Erweitern Sie das Fenster, können Sie die Informationen sehen, die durch die Integration bereitgestellt werden:

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 091835b16193e536ee1bba04d0fceff534544cad306673066f3ad6973a4b18b19

Beachten Sie, dass Daten in Ihrem Azure-Portal vorhanden sein müssen, und die Graph-API funktioniert besser, wenn sie mit anderen Microsoft-Lösungen verwendet wird. Dies muss jedoch vom Microsoft Support validiert werden.

Fehlerbehebung

- Meldung "Autorisierung fehlgeschlagen":
  - Stellen Sie sicher, dass die Werte für **Tenant ID** und Client ID korrekt sind und dass sie weiterhin gültig sind.

- Keine Daten werden in der Untersuchung angezeigt:
  - Stellen Sie sicher, dass Sie die entsprechenden Werte für **Tenant ID** und **Client ID** kopiert und eingefügt haben.
    - Stellen Sie sicher, dass Sie die Informationen aus dem Feld **Value** aus dem Certificates & Secrets Abschnitt verwendet haben.
    - Verwenden Sie WebDeveloper-Tools, um festzustellen, ob die Graph-API bei einer Untersuchung abgefragt wird.
    - Wenn die Graph-API Daten von verschiedenen Microsoft-Warnungsanbietern zusammenführt, stellen Sie sicher, dass OData für die Abfragefilter unterstützt wird. (z. B. Office 365 Security and Compliance und Microsoft Defender ATP).

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.