Use the Microsoft Graph Security API

To view contributors to this article access rhe link below

https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0&viewFallbackFrom=graph-rest-1.0%3Fwt.mc_id%3D4039827

In this article

The Microsoft Graph Security API provides a unified interface and schema to integrate with security solutions from Microsoft and ecosystem partners. This empowers customers to streamline security operations and better defend against increasing cyber threats. The Microsoft Graph Security API federates queries to all onboarded security providers and aggregates responses. Use the Microsoft Graph Security API to build applications that:

- Consolidate and correlate security alerts from multiple sources

- Unlock contextual data to inform investigations
- Automate security tasks, business processes, workflows, and reporting
- Send threat indicators to Microsoft products for customized detections
- Invoke actions to in response to new threats
- Provide visibility into security data to enable proactive risk management

The Microsoft Graph Security API includes the following key entities.

Alerts

Alerts are potential security issues within a customer's tenant that Microsoft or partner security solutions have identified and flagged for action or notification. With the Microsoft Graph Security alerts entity, you can unify and streamline management of security issues across all integrated solutions. This also enables applications to correlate alerts and context to improve threat protection and response. With the alert update capability, you can sync the status of specific alerts across different security products and services that are integrated with the Microsoft Graph Security API by updating your alerts entity.

Alerts from the following providers are available via the Microsoft Graph Security API. Support for GET alerts, PATCH alerts (updates are available via the Microsoft Graph Security API but might not be exposed in the provider’s management experience), and Subscribe (via webhooks) is indicated in the following table.

Table 1			
Security provider	**GET alert**	**PATCH alert**	**Subscribe to alert**
Azure Security Center	✓	✓	✓
Azure Active Directory Identity Protection	✓	✓	✓
Microsoft Cloud App Security	✓	✓	✓
Microsoft Defender Advanced Threat Protection *	✓	✓	File issue
Azure Advanced Threat Protection **	✓	✓	✓
Office 365 • Default • Cloud App Security	✓	File issue	File issue
Azure Information Protection **(preview)**	✓	✓	✓
Azure Sentinel **(preview)**	✓	✓	✓

Note: New providers are continuously onboarding to the Microsoft Graph Security ecosystem. To request new providers or for extended support from existing providers, file an issue in the Microsoft Graph Security GitHub repo.

* Microsoft Defender Advanced Threat Protection requires additional user roles to those required by the Microsoft Graph Security API. Only the users in both Microsoft Defender Advanced Threat Protection and Microsoft Graph Security API roles can have access to the Microsoft Defender Advanced Threat Protection data. Because application-only authentication is not limited by this, we recommend that you use an application-only authentication token.

** Azure Advanced Threat Protection alerts are available via the Microsoft Cloud App Security integration. This means you will get Azure Advanced Threat Protection alerts only if you have joined the Unified SecOps preview program and connected Azure Advanced Threat Protection into Microsoft Cloud App Security.

Secure Score

Microsoft Secure Score is a security analytics solution that gives you visibility into your security portfolio and how to improve it. With a single score, you can better understand what you have done to reduce your risk in Microsoft solutions. You can also compare your score with other organizations and see how your score has been trending over time. The Microsoft Graph Security secureScore and secureScoreControlProfile entities help you balance your organization's security and productivity needs while enabling the appropriate mix of security features. You can also project what your score would be after you adopt security features.

Common use cases

The following are some of the most popular requests for working with the Microsoft Graph Security API:

Table 2		
Use cases	**REST resources**	**Try it in Graph Explorer**
List alerts	List alerts	https://graph.microsoft.com/v1.0/security/alerts
Update alerts	Update alert	https://graph.microsoft.com/v1.0/security/alerts/{alert-id}
List secure scores	List secureScores	https://graph.microsoft.com/v1.0/security/secureScores
Get secure score	Get secureScore	https://graph.microsoft.com/v1.0/security/secureScores/{id}
List secure score control profiles	List secureScoreControlProfiles	https://graph.microsoft.com/v1.0/security/secureScoreControlProfiles/{id}
Get secure	Get	https://graph.microsoft.com/v1.0/security/secureScoreControlProfiles

Table 2		
Use cases	**REST resources**	**Try it in Graph Explorer**
score control profile	secureScoreControlProfile	
Update secure score control profiles	Update secureScoreControlProfile	https://graph.microsoft.com/v1.0/security/secureScoreControlProfiles/{id}