Register a new application for the Splunk Add-On

These steps are needed to authenticate with the Microsoft Graph Security API. Follow these steps to register a new application:

- 1. Sign in to the <u>Azure Portal</u>. Note: this stage does not require an AAD tenant admin.
- 2. Select Azure Active Directory (1).
- 3. Select App registrations (2).
- 4. Select New registration (3).



- 5. In the new registration form that opens, enter an application name (4).
- 6. Select Register (5).

Microsoft Azure	P Search resources, services, and docs D □ □ □ □ □ □ □ □ □ □						
«	Home > App registrations > Register an application						
+ Create a resource	Register an application						
🛖 Home							
🔲 Dashboard	* Name						
∃ All services	The user-facing display name for this application (this can be changed later).						
- 🛨 FAVORITES	Microsoft Graph Security API Splunk add-on						
All resources							
📦 Resource groups	Supported account types						
🔇 App Services	Who can use this application or access this API?						
🥫 SQL databases	Accounts in this organizational directory only						
🬌 Azure Cosmos DB	Accounts in any organizational directory						
Virtual machines	Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)						
💠 Load balancers	Help me choose						
Storage accounts							
Virtual networks	Redirect UPI (antional)						
Azure Active Directory	Redirect Uni (optional) Well return the submittation areasons to this LBL after successfully authentication the user. Browkillon this new is						
Monitor	optional and it can be changed later, but a value is required for most authentication scenarios.						
Advisor	Web e.g. https://myapp.com/auth						
Security Center							
O Cost Management + Billing							
Help + support							
Y Subscriptions							
Azure Sentinel							
	By proceeding, you agree to the Microsoft Platform Policies 🖸						
	Register						
	 6						
	By proceeding, you agree to the Microsoft Platform Policies 🔀						

- 7. Next, you'll see the **overview page** and your app ID (7), and Directory (tenant) ID (8). Copy and save these fields. You will need them later to complete the configuration process.
- 8. Click on View API Permissions (9) to display the Graph permissions screen.



9. In the **API Permission screen**, click on the **Add a permission** button (11) and select **Microsoft Graph** (12).

Microsoft Azure		, ○ Search resources, servi	ices, and docs	D 🕼 ¢² 🕸	з? 😳 admin@ сомтоso	
«	Home > Contoso - App regi	strations > Splunk connector -	Request API permissions			>
+ Create a resource			Select an API			
A Home		ADI permissions	Microsoft APIs APIs my organization	uses My APIs		
	😽 Overview	Applications are authorized t	Commonly used Microsoft APIs			
- 🛨 FAVORITES	📣 Quickstart	all the permissions the applic	Microsoft Graph			
All resources	Manage	+ Add a permission	Take advantage of the tremendous amount Security, and Windows 10. Access Azure AD	of data in Office 365, Enterprise Mobility + , Excel, Intune, Outlook/Exchange, OneDrive,	🚬 💽 🔊 👋 👯 🛛	
😭 Resource groups	Branding	API / PERMISSIONS NAME	OneNote, SharePoint, Planner, and more the	rough a single endpoint.	🎽 💿 🔹 😪	
🔇 App Services	Authentication	11 Microsoft Graph (1)				
🐱 SQL databases	📍 Certificates & secrets	User.Read	Azure Data Catalog	Azure DevOps	(?) Azure Key Vault	
🦉 Azure Cosmos DB	API permissions	These are the permissions the	Programmatic access to Data Catalog	Integrate with Azure DevOps and Azure	Manage your key vaults as well as the	
Virtual machines	🐼 Expose an API	able permissions dynamically	resources to register, annotate and search data assets	DevOps server	keys, secrets, and certificates within your Key Vaults	
💠 Load balancers	Owners 10					
🧮 Storage accounts	Roles and administrators (Previ	Grant consent	Azure Rights Management Services	Azure Service Management	Azure Storage	
Virtual networks	10 Manifest	As an administrator, you can	Allow validated users to read and write protected content	Programmatic access to much of the functionality available through the Azure	Secure, massively scalable object and data lake storage for unstructured and	
Azure Active Directory	Support + Troubleshooting			portal	semi-structured data	
Monitor	X Troubleshooting	Grant admin consent for C	Data Evanat Samisa for	•		
🔷 Advisor	New support request		Microsoft Dynamics 365	ංලිං Dynamics 365 Business Central	Dynamics CRM	
Security Center			Export data from Microsoft Dynamics CRM organization to an external	Programmatic access to data and functionality in Dynamics 365 Business	Access the capabilities of CRM business software and ERP systems	
Ost Management + Bill			destination	Central		
Help + support			Tlaur Samira		Collice 265 Management ADIa	
Resource Explorer			Flow Service			

10. Next, select **Application permissions** (13) in the Request API permission pane that opens.

Microsoft Azure			ices, and docs	দ্দি µ ² ঞ্জ ? ্ত admin@ ০০৸గ০১০
Microsoft Azure	Home ≥ Contoso App ree Microsoft Graph Security AP Search (Cut+2) « Cutickstart Manage Branding Authentication Certificates & secrets Alt permissions Expose an API Coverse Overse	Search resources, serve pistrations > Splunk connector = I Splunk add-on - API perr API permissions Applications are authorized t al the permissions the applic API / PENNISSION NAME Microsoft Graph (f) User.Read These are the permissions the able permissions dynamically	Arices, and docs 2 Request API permissions CAILAPIS Microsoft Graph https://graph.microsoft.com/ Docs [2] 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.
 Cost usancers Storage accounts Vritual networks Azure Active Directory Monitor Advisor Security Center Cost Management + Bill Help + support Resource Explorer 	 Owners Roles and administrators (Previ Manifest Support + Troubleshooting Y Troubleshooting New support request 	Add permissions Discard		

- 11. Under **Request API permissions**, select **SecurityEvents.Read.All** (14). Then click **Add permissions** (15).
- 12. [This step needs to be completed by the **Azure Active Directory tenant admin**] Login to the Azure Portal as the Azure Active Directory Tenant Administrator for your organization and navigate to App registration/API permissions screen. Click on **Grant admin consent for 'the AAD tenant'** (16).

Microsoft Azure		\wp Search resources, services, and docs	E 17 0 ⁸ 8 ? 6
«	Home > Contoso - App reg	gistrations > Microsoft Graph Security API Splunk add-on - API permissions	Request API permissions
+ Create a resource	Microsoft Graph Security AP	ו Splunk add-on - API permissions	
🛧 Home	«		A PILIPEID
🔤 Dashboard	, Search (Ctrl+/)	API permissions	OnlineMeetings
i≡ All services	Overview	Applications are authorized to call APIs when they are granted permissi	 OnPremisesPublishingProfiles
* FAVORITES	🕰 Quickstart	all the permissions the application needs.	► Organization
III resources	Manage	+ Add a permission	▶ People
😭 Resource groups	Branding	AFI / PERMISSIONS NAME ITPE DESCRI	▶ Place
🔇 App Services	Authentication	Microsoft Graph (1)	> Policy
🗧 SQL databases	Certificates & secrets	User.Read Delegated Sign in	ProgramControl
🬌 Azure Cosmos DB	 API permissions 	These are the permissions that this application requests statically. You re	> ProgramContact
Virtual machines	Expose an API	able permissions dynamically through code. See best practices for requ	▶ Reports
💠 Load balancers	Owners		► RoleManagement
🧮 Storage accounts	Roles and administrators (Previ	Grant consent	SecurityActions
Virtual networks	10 Manifest	As an administrator, you can grant consent on behalf of all users in this	▼ SecurityEvents (1)
Azure Active Directory	Support + Troubleshooting	users will not be snown a consent screen when using the application.	SecurityEvents.Read.All
😁 Monitor	X Troubleshooting	Grant admin consent for Contoso	Kead your organization's security events
今 Advisor	New support request		Read and update your organization's security events e
Security Center	-	16	▶ Sites
Ost Management + Bill		•	ThreatIndicators
Page Help + support			► TructFrameworkKevSet
Resource Explorer			
💡 Subscriptions			UserNotification
💡 Key vaults			▶ User
(ਨ) Logic Apps		15	
🕹 Logic Apps Custom Con			Adv pernasions Discard

Under Certificates & secrets (17), choose New client secret (18). A new secret will be displayed in the Value column. Copy this password – this is the only time you'll be able to. You will need it later to complete the configuration process.

Create a resource More > Contoso - App registrations > Microsoft Graph Security API Splunk add-on - Certificates & secrets Microsoft Graph Security API Splunk add-on - Certificates & secrets Microsoft Graph Security API Splunk add-on - Certificates & secrets						
Create a resource Oracle a resource						
A Home						
Deshboard Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). Deshboard	Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a					
E All services 🗮 Overview nigher revel of assurance, we recommend using a certaincate (instead of a client secret) as a credemial.						
★ FAVORITIS ▲ Quickstart Certificates						
HI resources All resources Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.					
Resource groups Eranding T Upload certificate						
🗞 App Services 🥥 Authentication No certificates have been added for this application.						
SQL databases Certificates & secrets						
Arure Cosmos DB & API permissions						
Virtual machines & Expose an API 17						
💠 Load balancers 🔣 Owners Client secrets						
🔚 Storage accounts 🔰 Roles and administrators (Previ A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.						
<>> Virtual networks III Manifest + New Client secret 100 -	+ New client secret					
Azure Active Directory Support + Troubleshooting DESCRIPTION I8 EXPIRES VALUE						
Monitor X Troubleshooting						
Advisor Construction and Construction an						
Security Center						
😮 Cost Management + Bili						