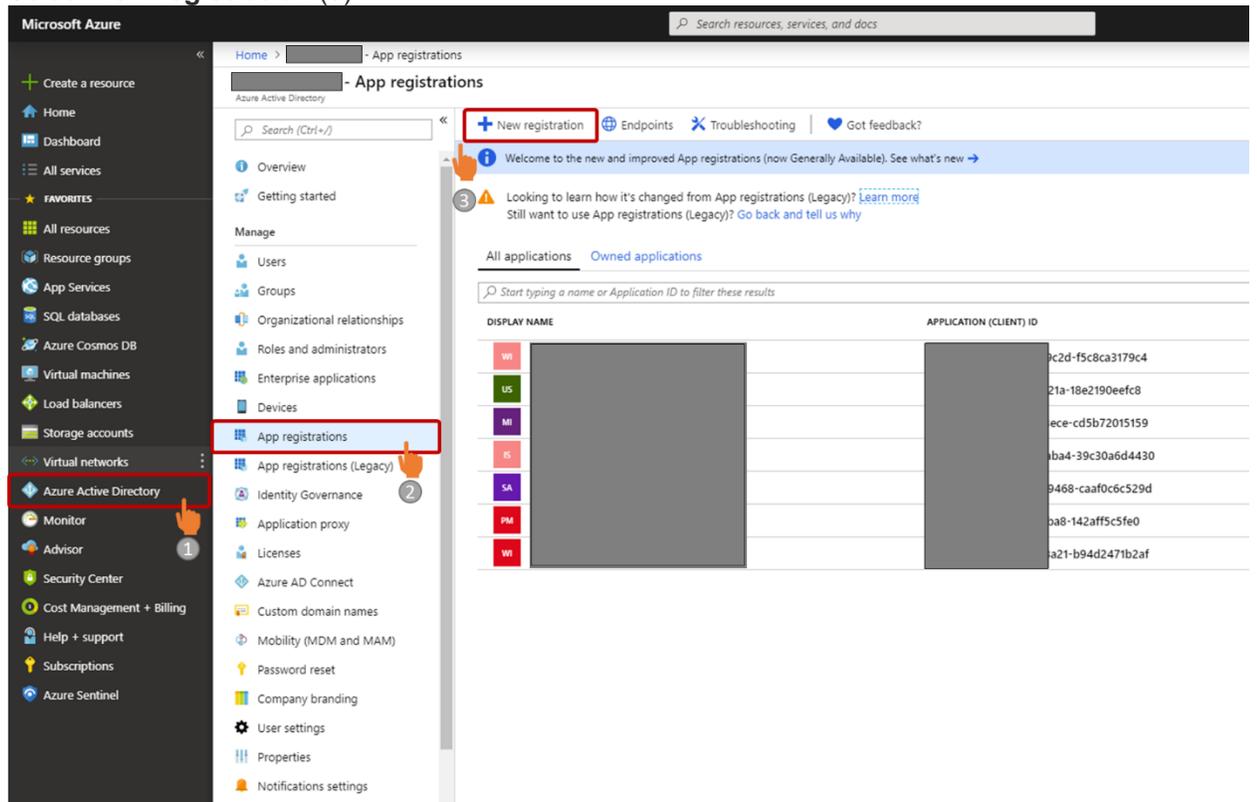


Register a new application for the Splunk Add-On

These steps are needed to authenticate with the Microsoft Graph Security API.

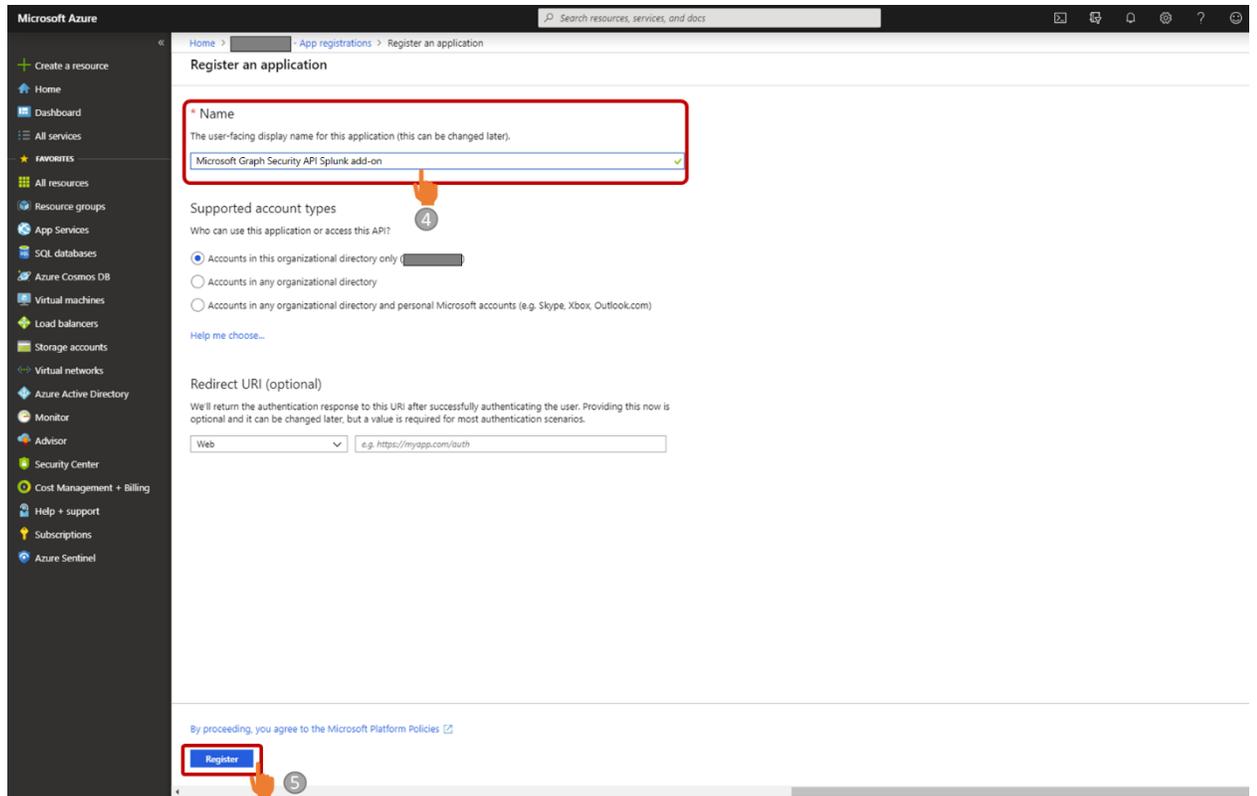
Follow these steps to register a new application:

1. Sign in to the [Azure Portal](#) . *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).

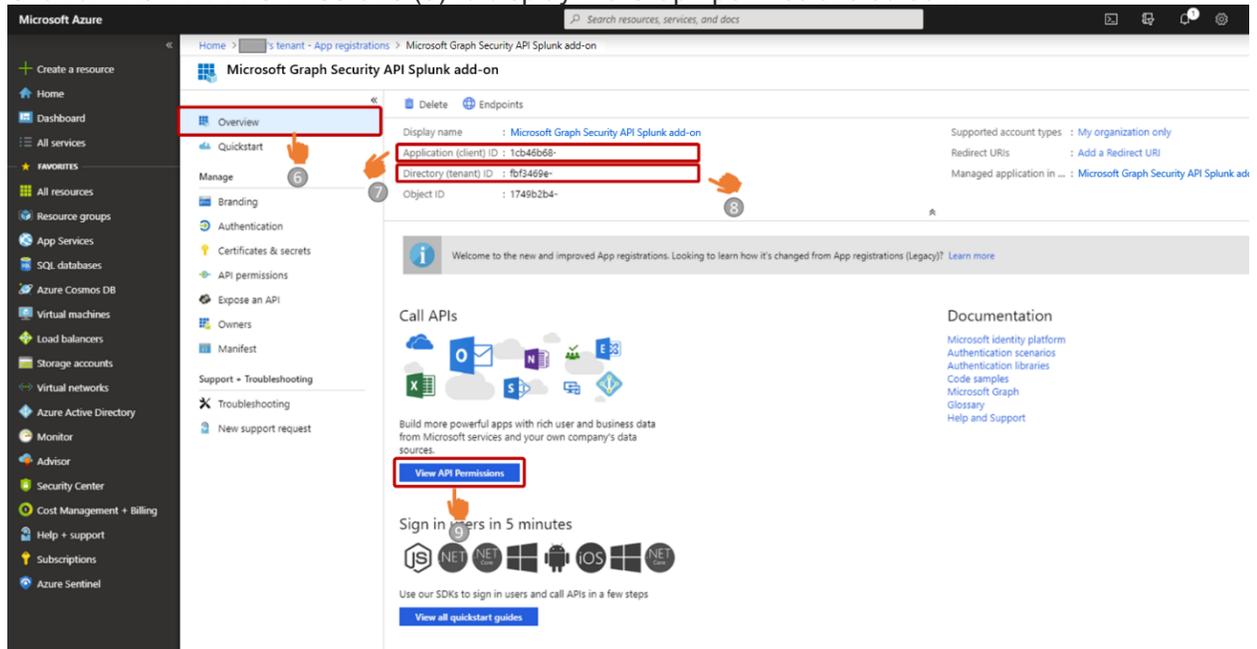


The screenshot shows the Microsoft Azure portal interface. The left-hand navigation pane is visible, with 'Azure Active Directory' highlighted in red and a hand icon labeled '1' pointing to it. Below it, 'App registrations' is also highlighted in red with a hand icon labeled '2'. In the main content area, the 'New registration' button is highlighted in red with a hand icon labeled '3'. The page displays a list of applications under the heading 'App registrations'. The table has two columns: 'DISPLAY NAME' and 'APPLICATION (CLIENT) ID'. The table contains several rows of data, with the first row showing a red 'WI' icon and the application ID 'c2d-f5c8ca3179c4'. The second row shows a green 'US' icon and the application ID '21a-18e2190eefc8'. The third row shows a purple 'MI' icon and the application ID 'ece-cd5b72015159'. The fourth row shows a red 'IS' icon and the application ID 'ba4-39c30a6d4430'. The fifth row shows a purple 'SA' icon and the application ID '9468-caaf0c6c529d'. The sixth row shows a red 'PM' icon and the application ID 'ba8-142aff5c5fe0'. The seventh row shows a red 'WI' icon and the application ID 'a21-b94d2471b2af'.

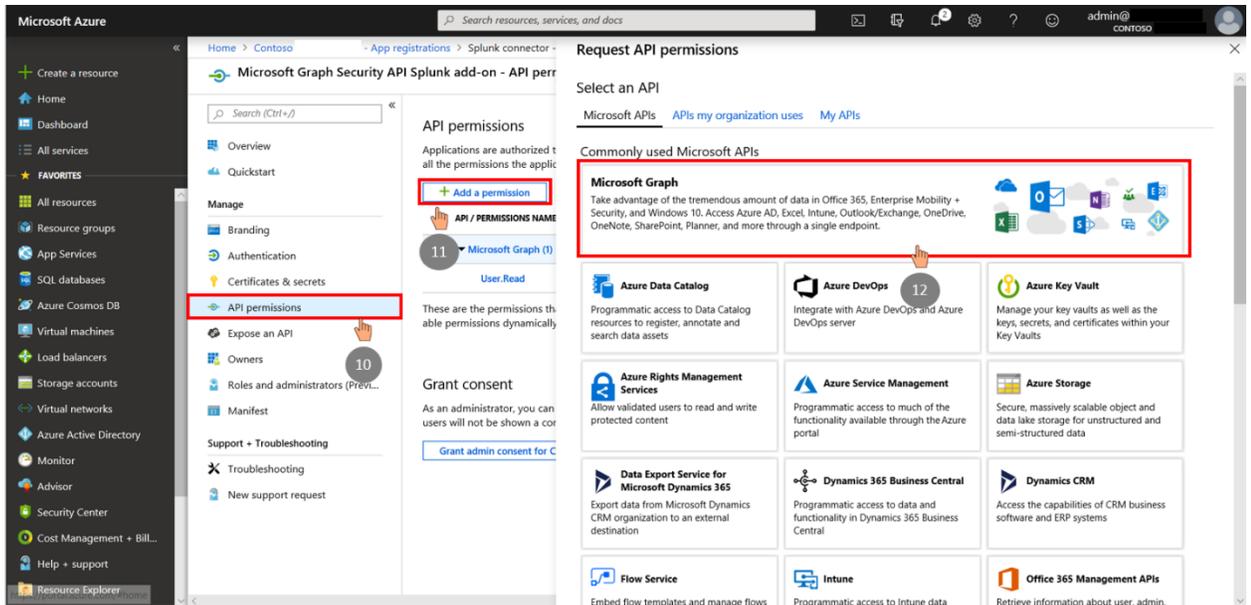
5. In the new registration form that opens, enter an application name (4).
6. Select **Register** (5).



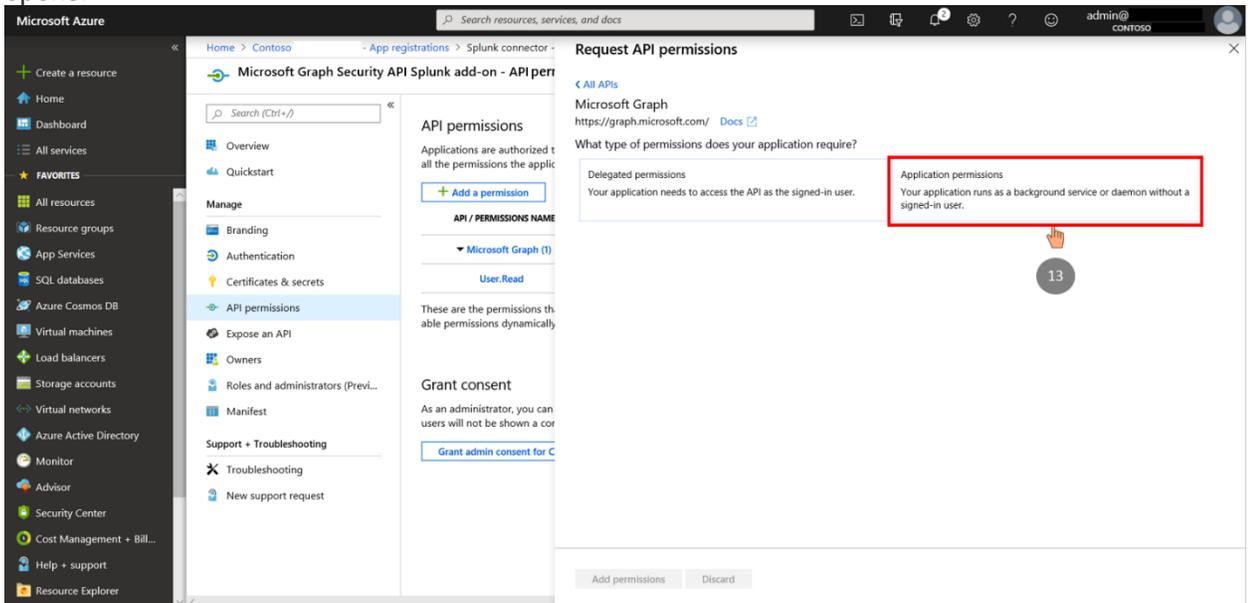
- Next, you'll see the **overview page** and your app ID (7), and Directory (tenant) ID (8). Copy and save these fields. You will need them later to complete the configuration process.
- Click on **View API Permissions** (9) to display the Graph permissions screen.



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



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



- Under **Request API permissions**, select **SecurityEvents.Read.All** (14). Then click **Add permissions** (15).
- [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

Home > Contoso > App registrations > Microsoft Graph Security API Splunk add-on - API permissions

Microsoft Graph Security API Splunk add-on - API permissions

Search (Ctrl+/)

API permissions

Applications are authorized to call APIs when they are granted permissions that all the permissions the application needs.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile information in Microsoft Graph.

These are the permissions that this application requests statically. You can also request permissions dynamically through code. [See best practices for requesting permissions.](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this organization. This consent will not be shown a consent screen when using the application.

[Grant admin consent for Contoso](#) (16)

Request API permissions

All APIs

- OnlineMeetings
- OnPremisesPublishingProfiles
- Organization
- People
- Place
- Policy
- ProgramControl
- Reports
- RoleManagement
- SecurityActions
- SecurityEvents (1)
 - SecurityEvents.Read.All
Read your organization's security events.
 - SecurityEvents.ReadWrite.All
Read and update your organization's security events.
- Sites
- ThreatIndicators
- TrustFrameworkKeySet
- UserNotification
- User

[Add permissions](#) (15) [Discard](#)

13. 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.

Microsoft Azure

Home > Contoso > App registrations > Microsoft Graph Security API Splunk add-on - Certificates & secrets

Microsoft Graph Security API Splunk add-on - Certificates & secrets

Search (Ctrl+/)

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES
------------	------------	---------

Client secrets

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](#) (18)

DESCRIPTION	EXPIRES	VALUE
-------------	---------	-------

No client secrets have been created for this application.