RiskIQ PassiveTotal Microsoft Setup Guide

Last Edit: October 29th, 2020

Table of Contents

Overview

RiskIQ PassiveTotal integrates with Microsoft Defender and Azure Sentinel in order to bring data from those systems into the RiskIQ PassiveTotal interface. Configuration of each Microsoft product is done through account settings and requires the user to generate a set of API credentials with appropriate permissions. These tokens are saved within RiskIQ PassiveTotal and enable the use of the integration. Once validated, RiskIQ PassiveTotal users will see Microsoft data within search results for domain and IP address indicators.

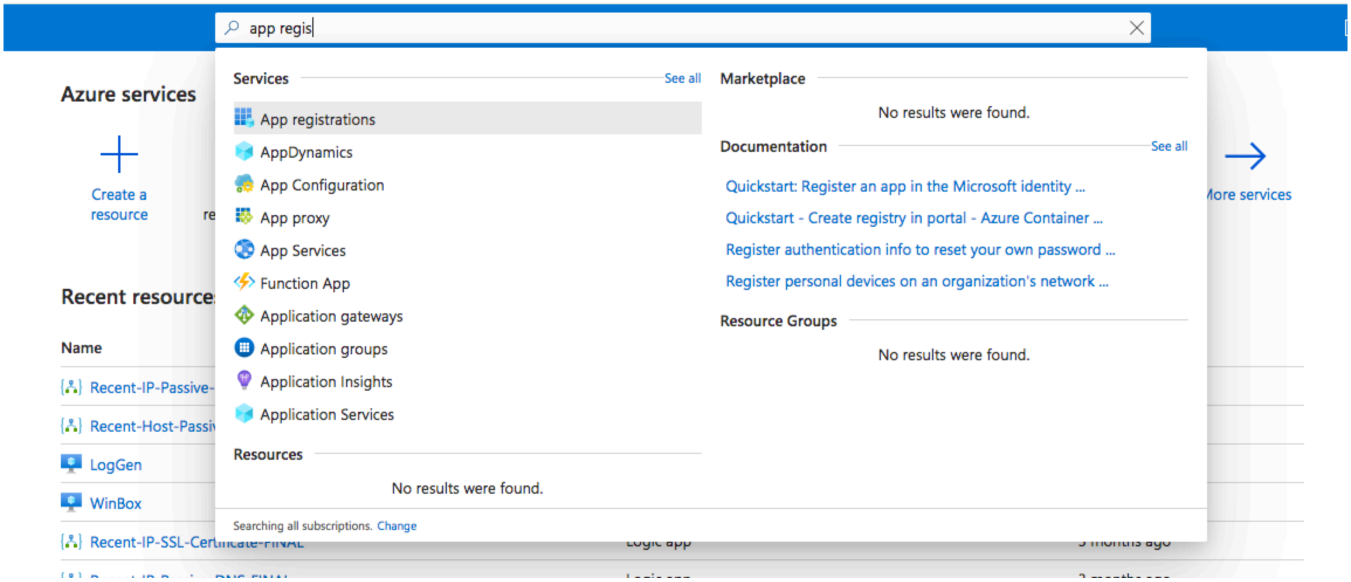
RiskIQ PassiveTotal Settings

This integration between RiskIQ PassiveTotal and Microsoft is one-way with data from Microsoft products being requested and displayed within the RiskIQ PassiveTotal interface. Users can access the integration settings by visiting their account settings.

Within Account Settings, users will need to scroll to the "Microsoft Graph Integration". Under this heading, there are two options for Sentinel Configuration and Advanced Threat Protection (Defender), each displaying a small settings icon next to each. Clicking the icon reveals an input form where the user will need to input their tenant ID, client ID and secret ID. These values are obtained from the Azure portal.

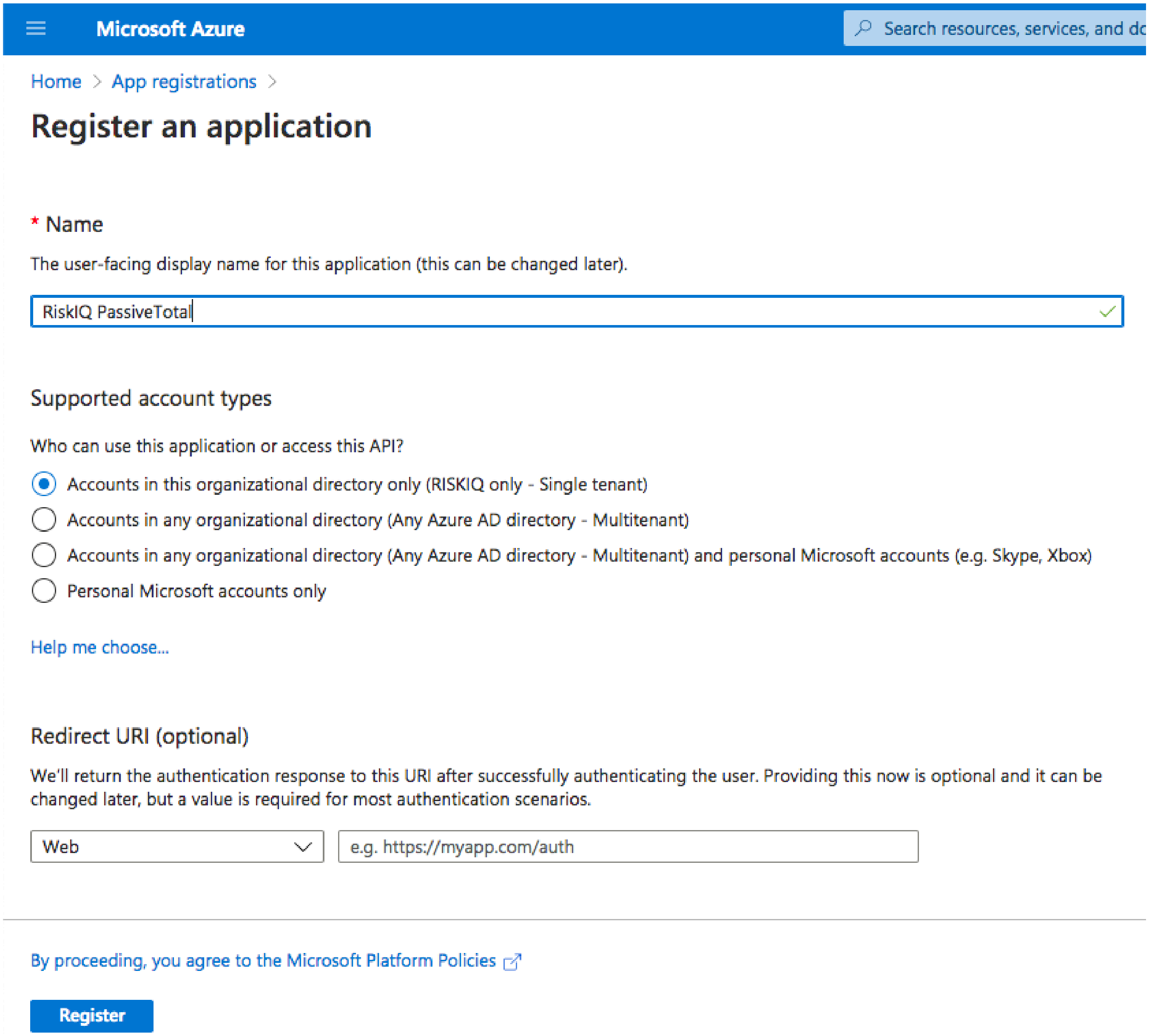
Azure Overview

The Microsoft Azure Portal is the primary location a user will need to access in order to generate the appropriate configuration items for the RiskIQ PassiveTotal integration.



app regis

Once logged into the portal, users will need to visit the “App Registrations” service as shown above.



Microsoft Azure
Search resources, services, and dc
Home > App registrations >

Register an application

* Name

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

RiskIQ PassiveTotal

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (RISKIQ 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

Help me choose...

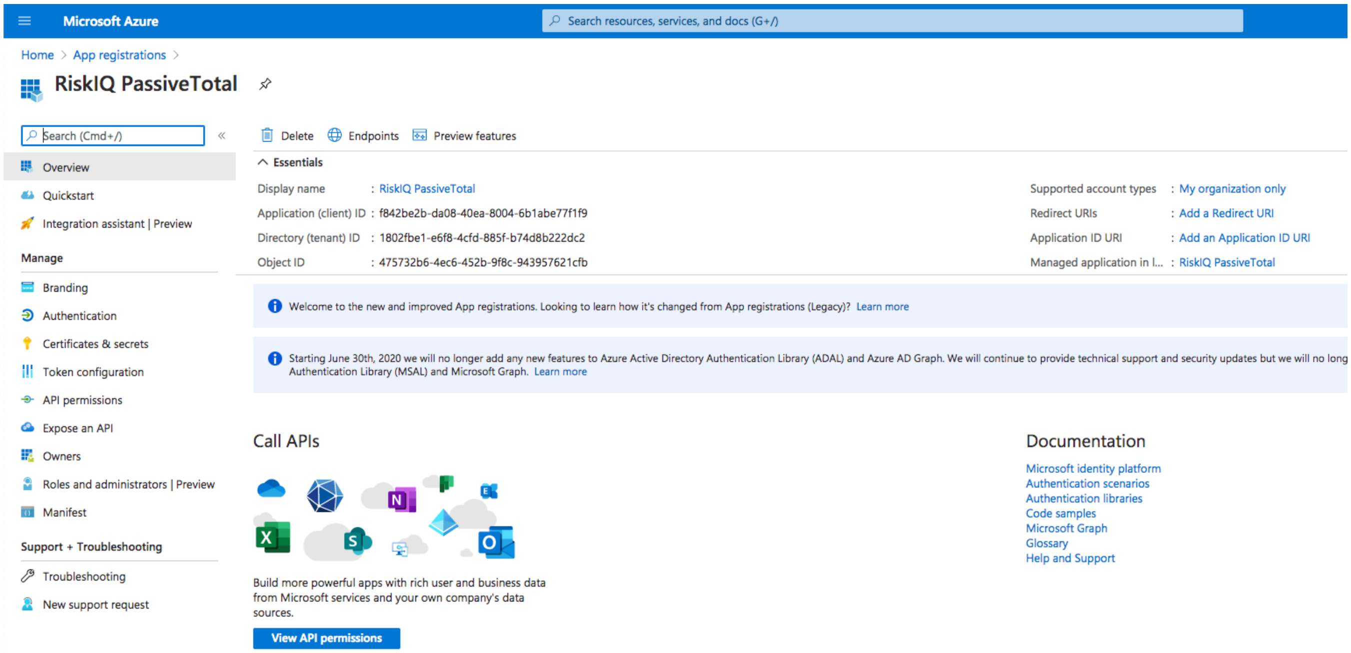
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Click on new app registration and you will be prompted with a form. Give your app a unique name and keep the default account type selection checked. There is no need to provide a redirection URL at this time. Click register.



RiskIQ PassiveTotal

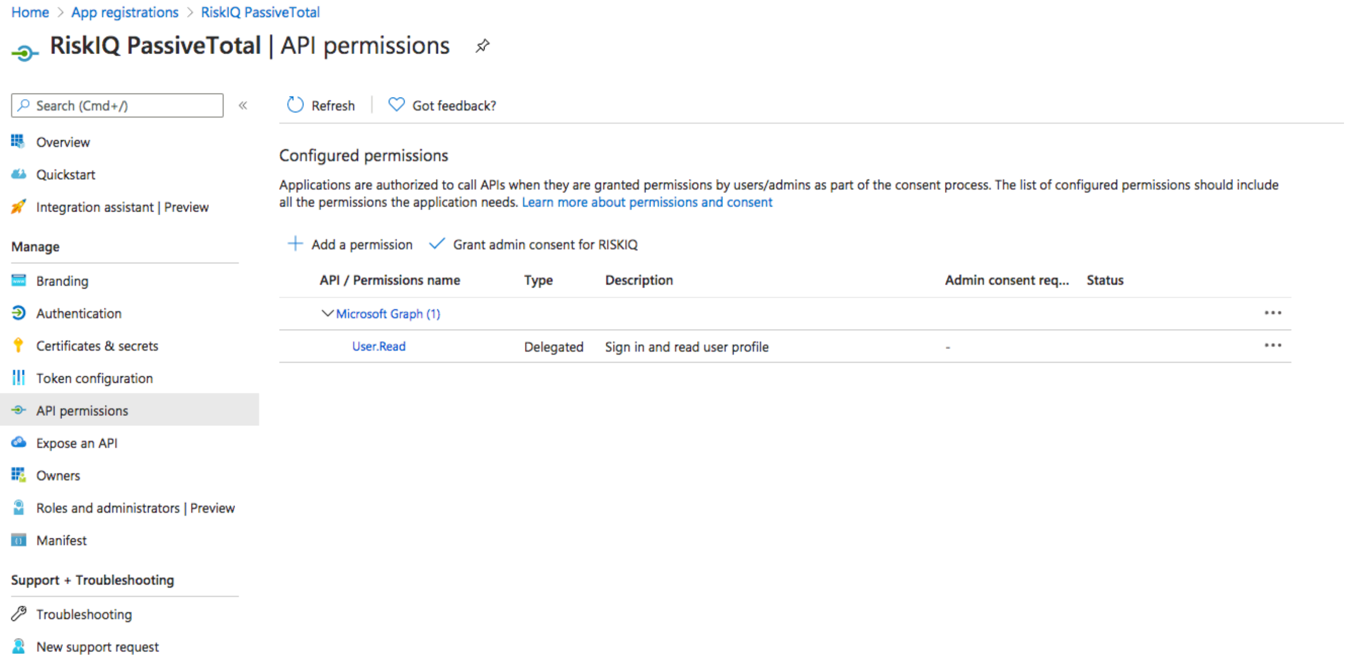
Display name : RiskIQ PassiveTotal
Application (client) ID : f842be2b-da08-40ea-8004-6b1abe77f1f9
Directory (tenant) ID : 1802fbe1-e6f8-4cfd-885f-b74d8b222dc2
Object ID : 475732b6-4ec6-452b-9f8c-943957621cfb
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : RiskIQ PassiveTotal

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no long Authentication Library (MSAL) and Microsoft Graph. Learn more

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Upon successful creation, you will be directed to your app. Note, your Application (client) ID and Directory (tenant) ID are located at the top of this screen. Both of these are required for the integration.



RiskIQ PassiveTotal | API permissions

Configured permissions

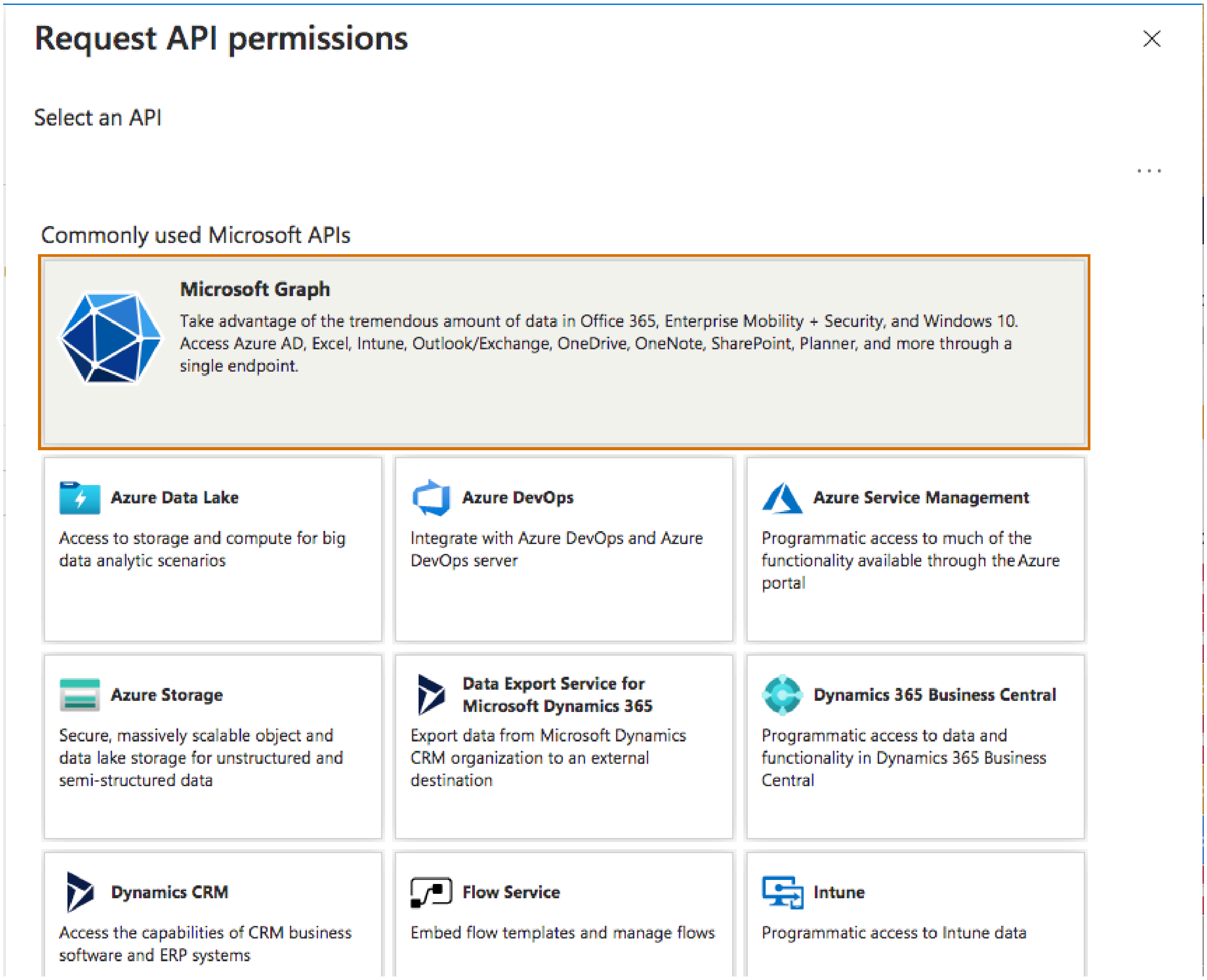
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

Select "API Permissions" to see the current configured services. From here, you will need to add a permission depending on the product you wish to integrate.

Azure Sentinel Setup

Azure Sentinel does not have a direct set of APIs or permissions and instead uses the Microsoft Security Graph as its primary interface.



Request API permissions

Select an API

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.

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

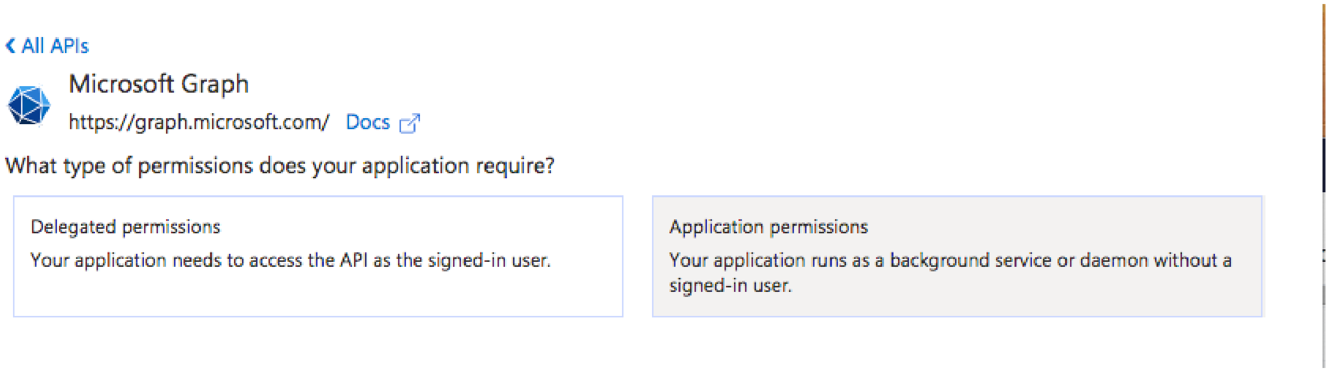
Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Select the Microsoft Graph API after adding a new permission.



< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

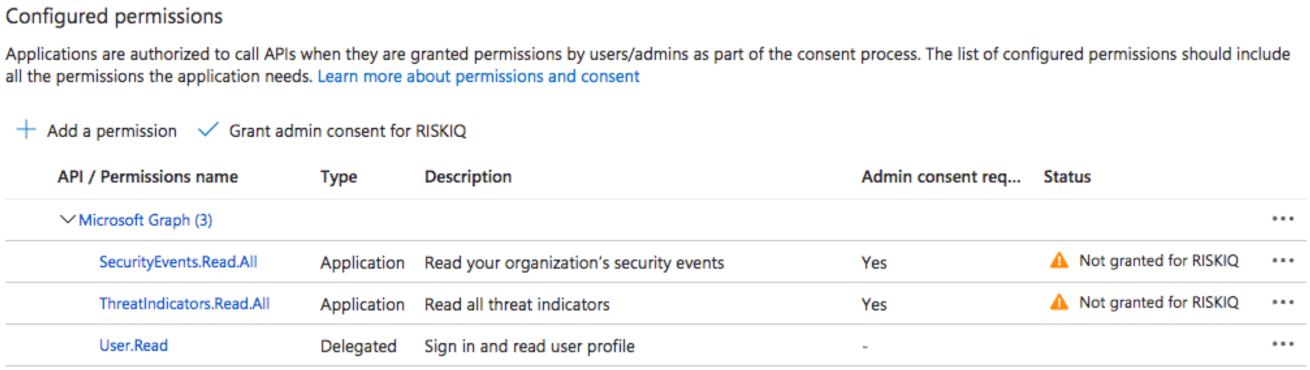
What type of permissions does your application require?

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.

Upon clicking, you will be asked if these permissions are for delegated purposes or for an application. Select application.

Using the filter bar, search for "SecurityEvents.Read.All" and "ThreatIndicators.Read.All", then click add permissions. If successful, these permissions should now show up under the API Permissions screen for your application.



Configured permissions

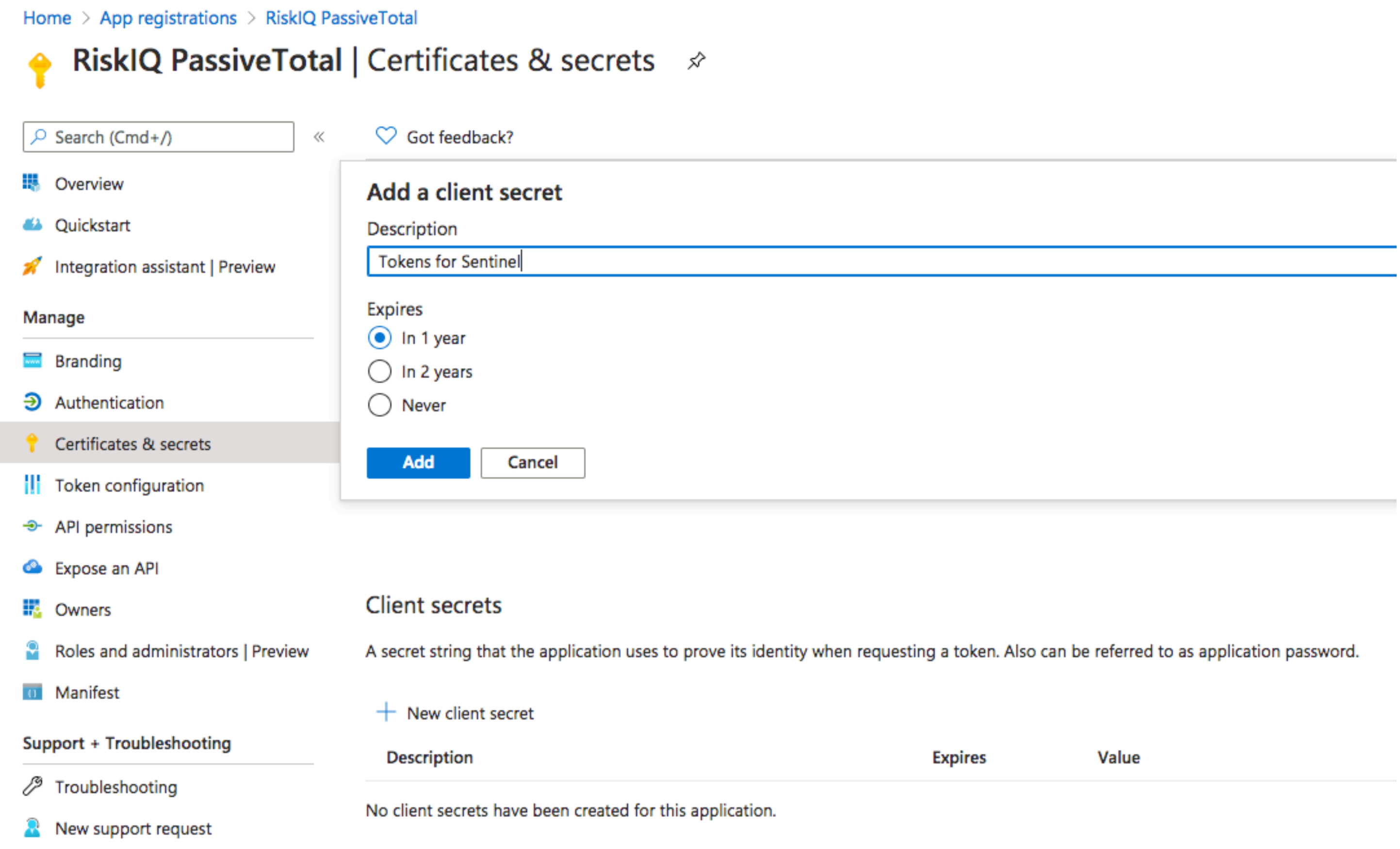
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	⚠ Not granted for RISKIQ
ThreatIndicators.Read.All	Application	Read all threat indicators	Yes	⚠ Not granted for RISKIQ
User.Read	Delegated	Sign in and read user profile	-	

Depending on your role within the Azure Portal, you may need to have an administrator consent to these permissions. This will be evident via an alert icon and message letting you know consent is required.

Further Support

If you have questions or run into issues, please reach out to the RiskIQ team via support@riskiq.com or through your account representative.



RiskIQ PassiveTotal | Certificates & secrets

Add a client secret

Description: Tokens for Sentinel

Expires

● In 1 year
○ In 2 years
○ Never

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.

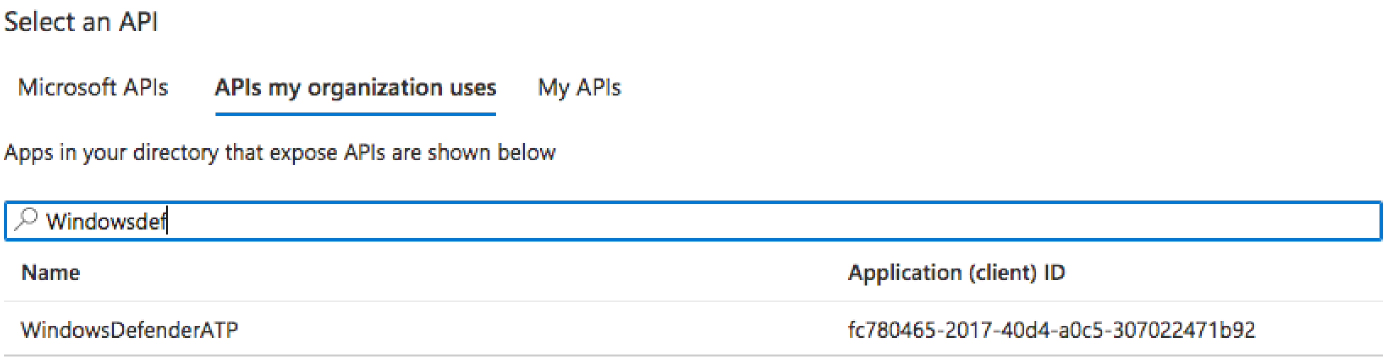
Description	Expires	Value

No client secrets have been created for this application.

Upon successful consent, you will now need to generate a client secret. Click on the “Certificates & Secrets” menu item, then add a new secret. After adding, you will have the ability to copy the secret.

Microsoft Defender Setup

Similar to Azure Sentinel, in order to configure Microsoft Defender, you will need to grant a set of permissions to the application.



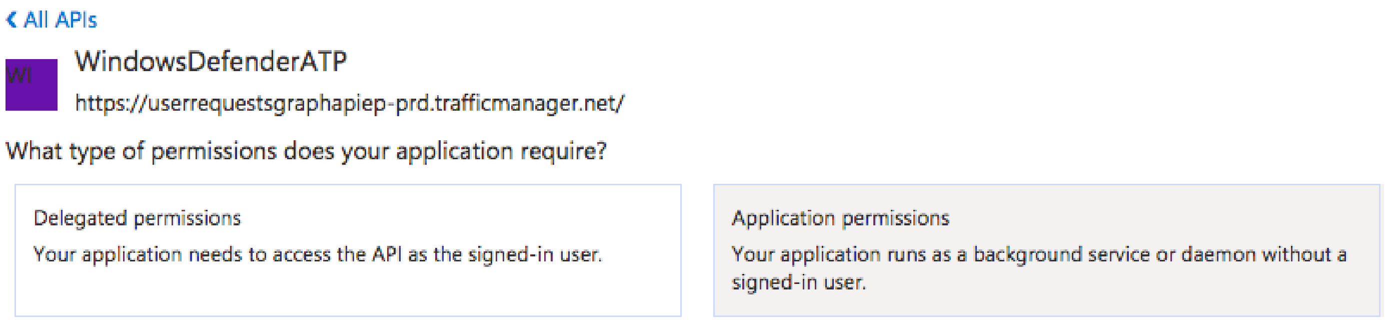
Select an API

Apps in your directory that expose APIs are shown below

Windowsdef

Name	Application (client) ID
WindowsDefenderATP	fc780465-2017-40d4-a0c5-307022471b92

Click on the sub-tab “APIs my organization uses” in order to expose a list of interfaces. Identify “WindowsDefenderATP”.



‹ All APIs

WI WindowsDefenderATP

https://userrequestsgraphapiep-prd.trafficmanager.net/

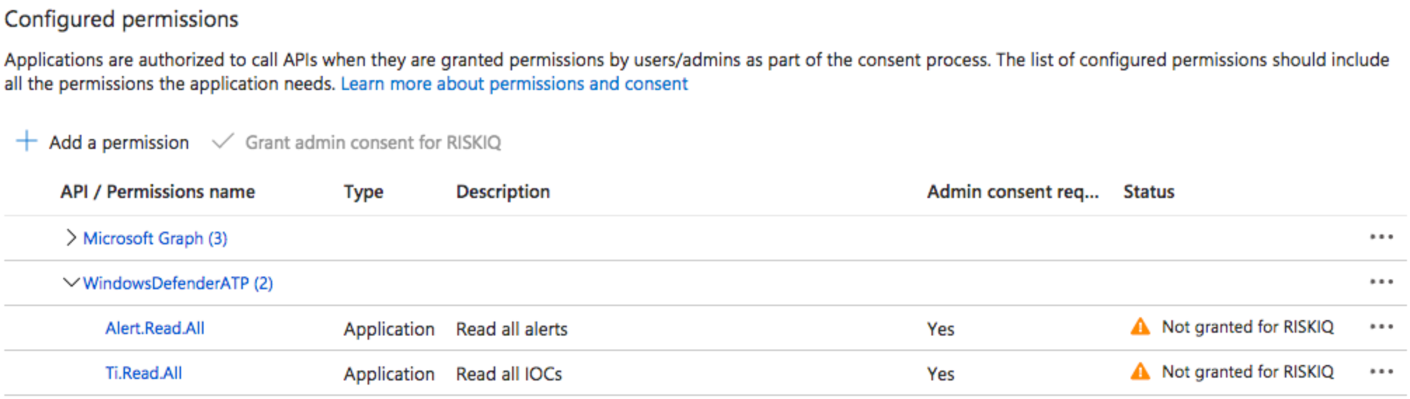
What type of permissions does your application require?

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.

Upon clicking, you will be asked if these permissions are for delegated purposes or for an application. Select application.

Using the filter bar, search for "Alert.Read.All" and "Ti.Read.All", then click add permissions. If successful, these permissions should now show up under the API Permissions screen for your application.

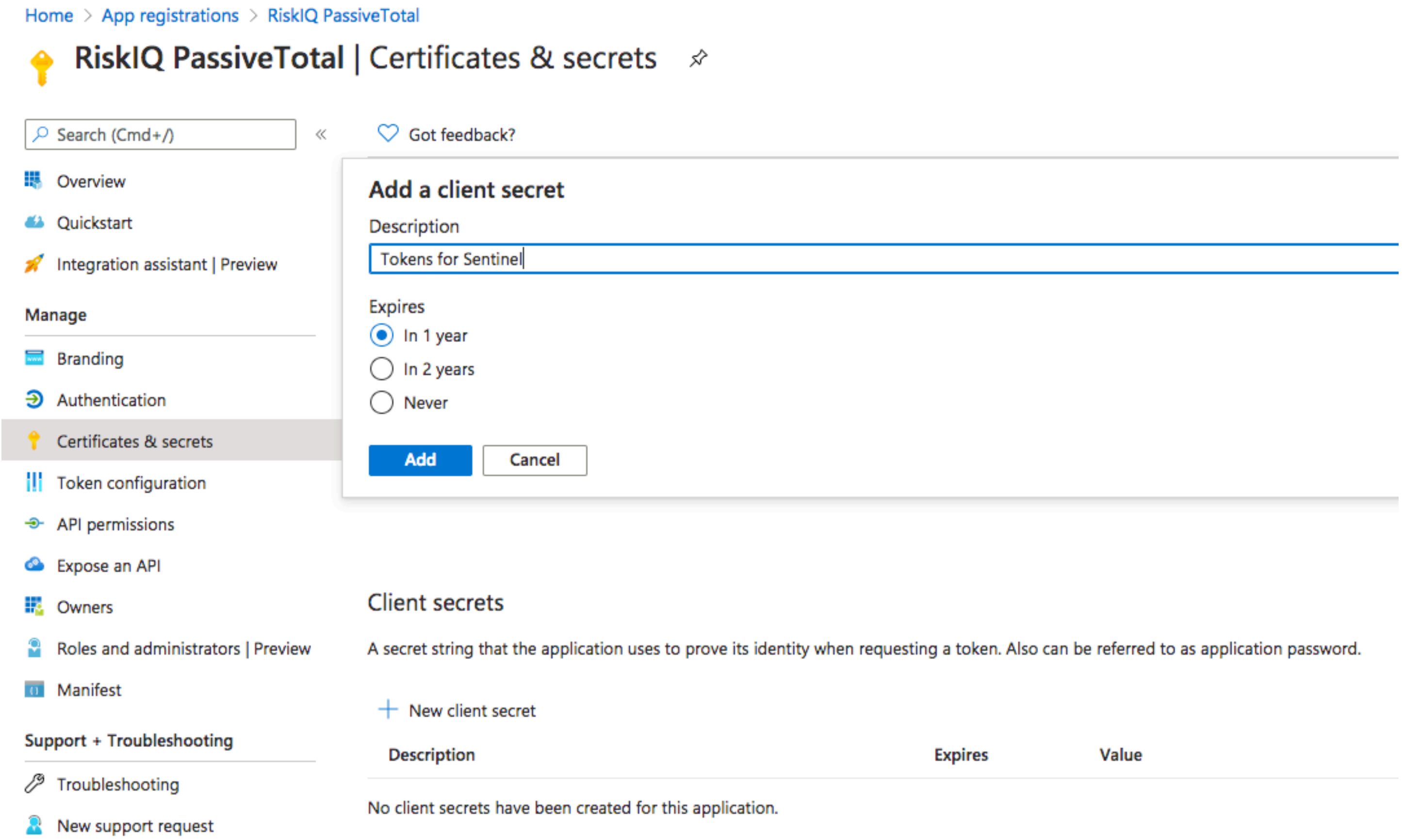


Configured permissions

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

API / Permissions name	Type	Description	Admin consent req...	Status
› Microsoft Graph (3)				
⌄ WindowsDefenderATP (2)				
Alert.Read.All	Application	Read all alerts	Yes	⚠ Not granted for RISKIQ
Ti.Read.All	Application	Read all IOCs	Yes	⚠ Not granted for RISKIQ

Depending on your role within the Azure Portal, you may need to have an administrator consent to these permissions. This will be evident via an alert icon and message letting you know consent is required.



RiskIQ PassiveTotal | Certificates & secrets

Add a client secret

Description

Tokens for Sentinel

Expires

● In 1 year

○ In 2 years

○ Never

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.

Description	Expires	Value
No client secrets have been created for this application.		

Upon successful consent, you will now need to generate a client secret. Click on the “Certificates & Secrets” menu item, then add a new secret. After adding, you will have the ability to copy the secret.