RiskIQ PassiveTotal Microsoft Setup Guide

Last Edit: October 29th, 2020
Table of Contents

Overview ...........................................................................................................................................3
RiskIQ PassiveTotal Settings........................................................................................................3
Azure Overview .......................................................................................................................... 4
Azure Sentinel Setup................................................................................................................... 8
Further Support............................................................................................................................ 9
Microsoft Defender Setup.........................................................................................................10
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.

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

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.

Select the Microsoft Graph API after adding a new permission.
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.

<table>
<thead>
<tr>
<th>API / Permissions name</th>
<th>Type</th>
<th>Description</th>
<th>Admin consent req.</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurityEvents.Read.All</td>
<td>Application</td>
<td>Read your organization’s security events</td>
<td>Yes</td>
<td><img src="status.png" alt="Icon" /> Not granted for RiskIQ</td>
</tr>
<tr>
<td>ThreatIndicators.Read.All</td>
<td>Application</td>
<td>Read all threat indicators</td>
<td>Yes</td>
<td><img src="status.png" alt="Icon" /> Not granted for RiskIQ</td>
</tr>
<tr>
<td>User.Read</td>
<td>Delegated</td>
<td>Sign in and read user profile</td>
<td>-</td>
<td><img src="status.png" alt="Icon" /></td>
</tr>
</tbody>
</table>

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.
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.

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

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.
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.