Configuring the Microsoft Sentinel Threat Intel Connector

Introduction

Microsoft provides a data connector that allows users of Microsoft Sentinel to import threat intelligence data via the STIX/TAXII protocol. Once you have obtained access to ReversingLab's threat intelligence feed you will need to configure the data connector. The table below outlines the parameters that are needed.

Data Connector Configuration	
Item	Parameter
Friendly name (for server)	**<Name that you will recognize for this data source>**
API root URL	**https://data.reversinglabs.com/api/taxii/ransomware-api-root/**
Collection ID	**f0997a32-b823-562d-9856-c754ac5e1159**
Username	**<enter the username provided during the product activation>**
Password	**<enter the password provided during the product activation>**
Import Indicators	**<up to 30 days of indicators are stored on the server you can leave the default and import all 30 days or select a shorter time frame>**
Polling Frequency	**<we recommend the default of once per hour>**

Note: If you have lost or want to reset your password you can can navigate to the SaaS blade in the Azure portal, find the subscription for ReversingLabs and then click the "Open SaaS Account on publisher's site" link on the subscription details page.

Support can be obtained by contacting support@reversinglabs.com

Data Connector Configuration

1. Navigate to the data connectors section in Sentinel. See Figure 1
2. Type TAXII into the search bar to filter the list of connectors.
3. Click on “Threat intelligence - TAXII” entry to highlight the data connector
4. In the lower left corner of the page click: Open connector page
5. The connector detail page will load. See Figure 2
6. Fill out the following configuration fields from the table above
7. Click the Add button and the configuration will be saved. It may take up to an hour for Sentinel to begin importing indicators.

Figure 1

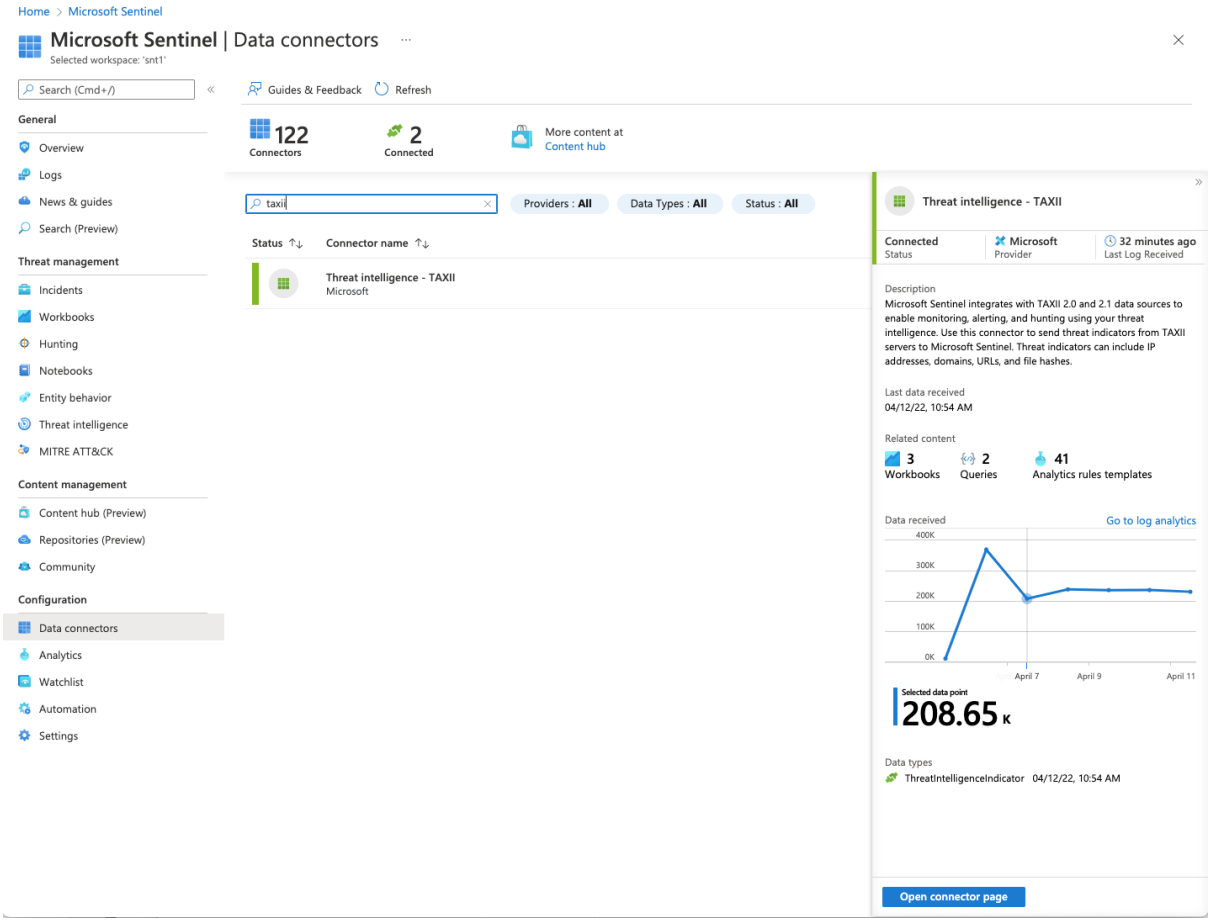
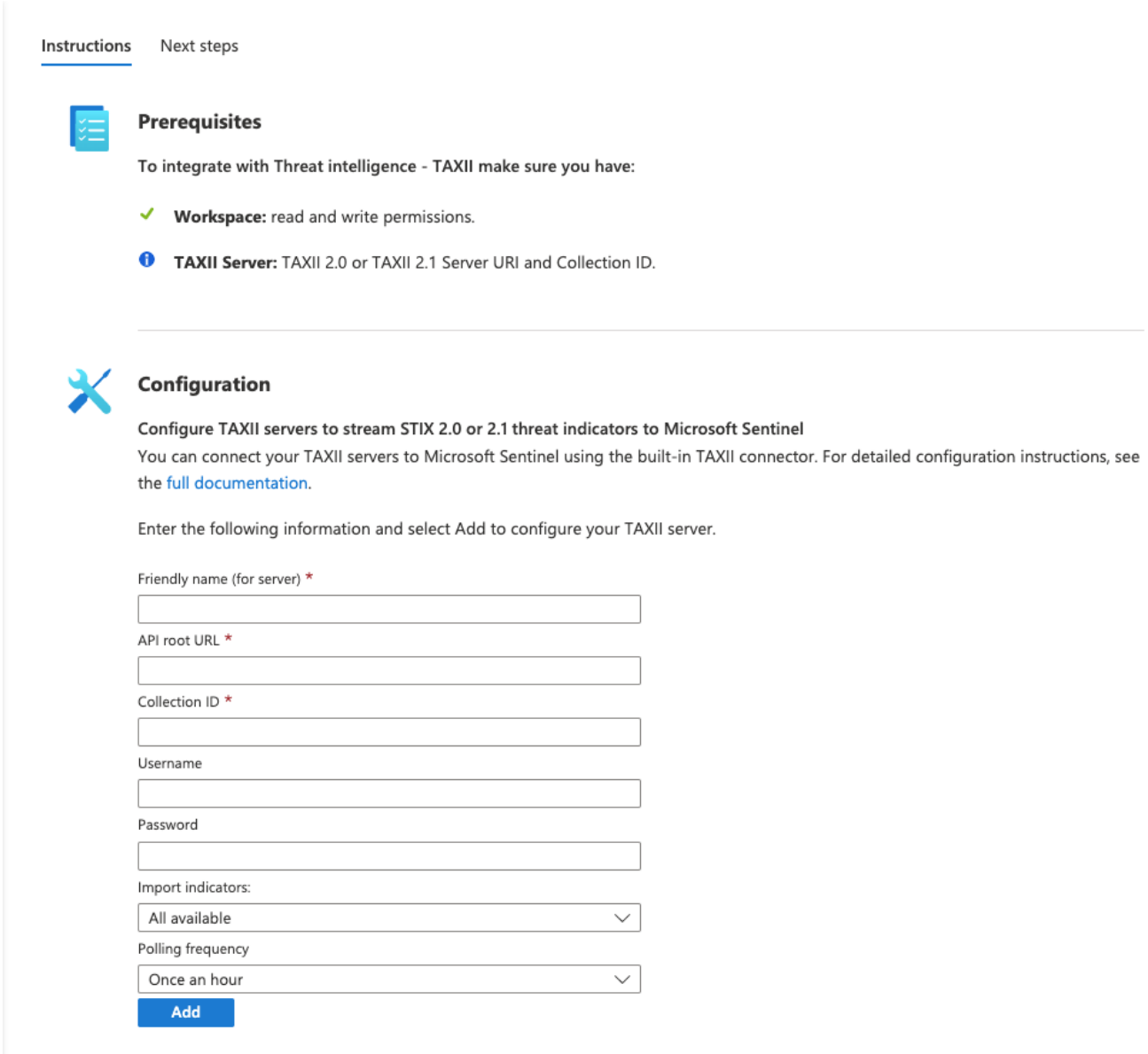


Figure 2


Instructions
Next steps
Prerequisites
To integrate with Threat intelligence - TAXII make sure you have:
Workspace: read and write permissions.
TAXII Server: TAXII 2.0 or TAXII 2.1 Server URI and Collection ID.
Configuration
Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel
You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the full documentation.
Enter the following information and select Add to configure your TAXII server.
Friendly name (for server) *
API root URL *
Collection ID *
Username
Password
Import indicators:
All available
Polling frequency
Once an hour
Add