

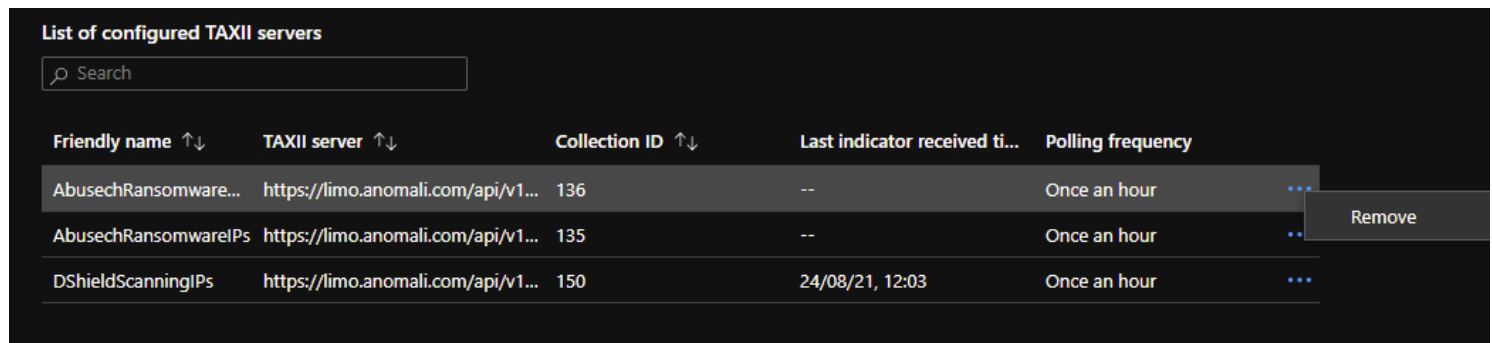
Disconnecting TAXII Data Connector

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

Disconnecting TAXII Data Connector

Removing a TAXII collection ID

Removing a TAXII collection ID is as easy as right-clicking on the ellipsis next to the configured collection and selecting Remove.



Friendly name ↑↓	TAXII server ↑↓	Collection ID ↑↓	Last indicator received ti...	Polling frequency
AbusechRansomware...	https://limo.anomali.com/api/v1...	136	--	Once an hour
AbusechRansomwareIPs	https://limo.anomali.com/api/v1...	135	--	Once an hour
DShieldScanningIPs	https://limo.anomali.com/api/v1...	150	24/08/21, 12:03	Once an hour

Be aware that removing the TAXII collection ID only prevents the ingestion of new Threat Indicators. The Threat Indicators already ingested for that collection ID will remain in the customers Log Analytics workspace. At this time, the only way to remove the actual Threat Indicators is to manually delete them via the Threat Intelligence blade in Azure Sentinel. The Sentinel product group are working on a solution to allow mass update or deletion of Threat Indicators, which is planned to be available by the end of 2021.

Removed TAXII Collection ID appears to continue ingesting new data

When a customer removes a collection from their TAXII data connector configuration, the threat indicators that have already been ingested for that collection will remain in the *ThreatIntelligenceIndicator* table in their Log Analytics workspace. The existing threat indicators will also have their *TimeGenerated* field updated every 12 days as part of the Threat Indicator republishing mechanism. It may therefore appear that a collection that has been removed is still ingesting new data, but it is actually just existing data being republished.

Re-publishing Threat Indicators

Threat Intelligence in Sentinel needs to periodically republish data to Log Analytics in order to keep it available for use by the other areas of Sentinel. 1/12th of a customers Threat Indicators are republished every day, resulting in all Threat Intelligence data being republish every 12 days.

The republishing of Threat Indicators carries an ingestion cost. The product group has indicated that about a million ingested events (monthly) cost around \$2.50.

Reference

[ICM 255322885 - Deleted TAXII data connector still has data being ingested into Sentinel workspace](#) 