

# THREATCONNECT

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the [Integrations Overview \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).

## API Calls

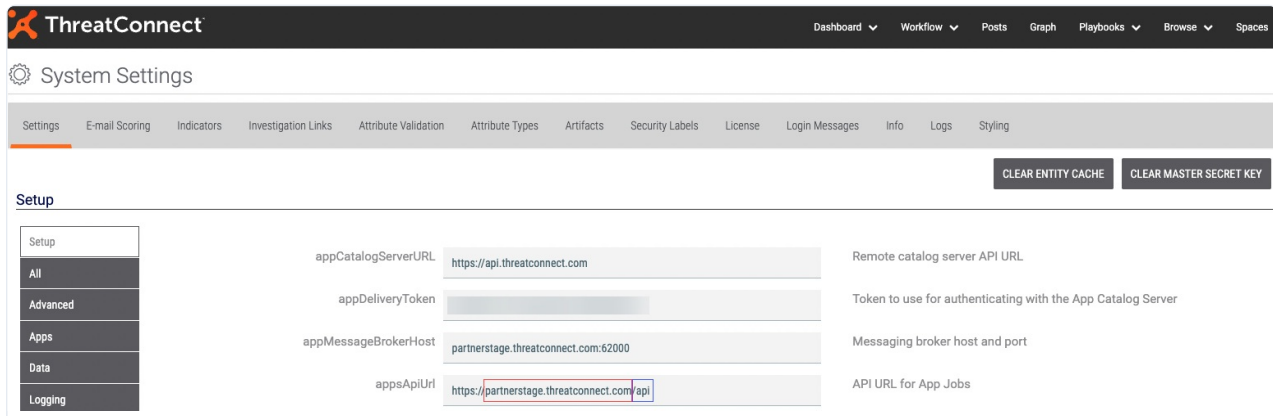
The following API calls are used by the Validation Platform.

Purpose	Call
Retrieve a List of Owners	/v2/owners
Retrieve a List of Threat Actor and details	/v2/groups/adversaries
Retrieve threat actor MITRE ATT&CK tags	/v2/groups/adversaries/<adversary_id>/groups/threats

## Prerequisites

Gather the following information from your ThreatConnect environment before you start.

- Identify the host (red highlighted FQDN of the **appsApiUrl** in the following screenshot), port, and protocol. Note that your appsApiUrl may differ from the one shown in the screenshot.
- Identify the username, API root (blue highlighted value in the following screenshot), Access ID, and API key. Any account that has API access can be used.



The screenshot shows the ThreatConnect System Settings page. The 'Setup' section is active, displaying the following configuration fields:

- appCatalogServerURL:** https://api.threatconnect.com (Remote catalog server API URL)
- appDeliveryToken:** [Redacted] (Token to use for authenticating with the App Catalog Server)
- appMessageBrokerHost:** partnerstage.threatconnect.com:62000 (Messaging broker host and port)
- appsApiUrl:** https://partnerstage.threatconnect.com/api (API URL for App Jobs)

In the **appsApiUrl** field, the host `partnerstage.threatconnect.com` is highlighted in red, and the API root `/api` is highlighted in blue.

appsApiURL value (Host highlighted in red, API Root highlighted in blue) on the ThreatConnect system settings page

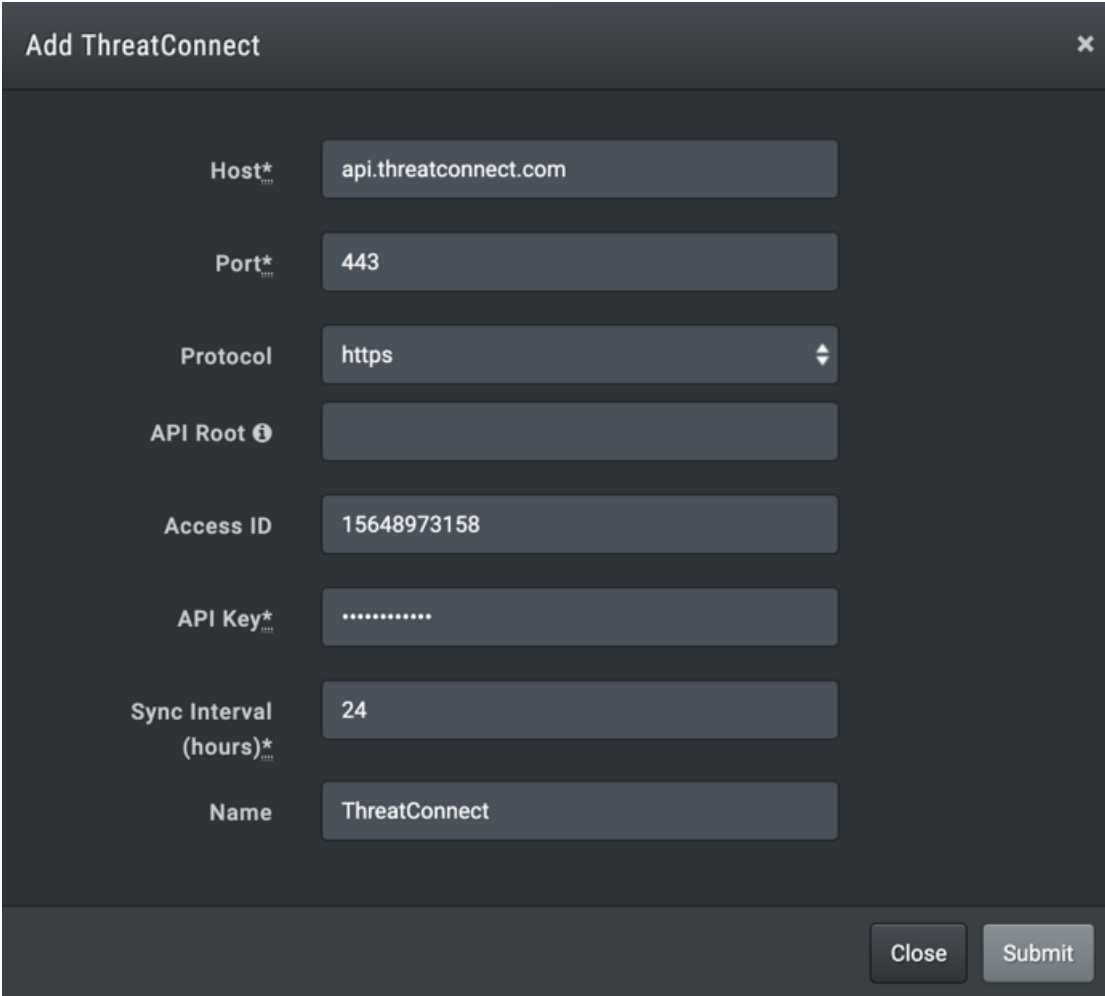
## Configuration

### TO ADD THE THREATCONNECT INTEGRATION

1. Go to **Settings > Integrations**.
2. In the Threat Intelligence Platform Integrations table, click **Add Integration > ThreatConnect**.
3. For **Host**, enter the FQDN value (this comes from the **appsApiUrl** field that you noted in the ThreatConnect

environment).

4. Enter the **Port**.
5. Select the **Protocol**.
6. Enter the **API Root**, if one is available from the ThreatConnect environment.  
This is an optional prefix to add to API calls. If unsure, check to see if there is an API value after the **appsApiUrl** FQDN in the ThreatConnect environment.
7. Enter the **Access ID**.
8. Enter the **API Key**.
9. Enter the **Sync Interval** in hours (default: 24 hours).
10. (Optional) Assign a **Name**.
11. Click **Submit**. The integration automatically starts to sync after it is added.



**Add ThreatConnect**

Host\*

Port\*

Protocol

API Root ⓘ

Access ID

API Key\*

Sync Interval (hours)\*

Name

Close Submit

Add ThreatConnect Integration

### Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see [Proxy Rules \(https://docs.mandiant.com/home/msv-proxy-rules\)](https://docs.mandiant.com/home/msv-proxy-rules).