InQuest Threat Intelligence Guide for ThreatConnect™

The InQuest Threat Intelligence Feed Guide provides information to help you quickly get started ingesting Indicators of Compromise (IOCs) into the Threat Connect Platform.

Contents

InQuest Intelligence Guide

Change Log

Version	Date	Changes
1.0.0	April 2021	Initial release.

Requirements

The following conditions must be met before ingesting InQuest feeds into the Threat Connect platform.

- Access to the ThreatConnect instance.
- At least one ThreatConnect API user.
- A valid InQuest provided API key. Separate keys must be used for paid feeds and free feeds.
- InQuest Custom Attributes (noted above) configured in the ThreatConnect instance to be used. This step is not required for customers using the Feed Deployer.

Installation

For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

Introduction

This integration allows the ingestion of InQuest Indicators of Compromise (IOCs) into the Threat Connect Platform. The IOCs are sourced from a variety of aggregate and propriety sources, including InQuest Reputation database, InQuest ingested IOC database, InQuest Deep File Inspection (DFI) IOCs, and InQuest Labs Command and Control (C2) infrastructure research. IOCs from DFI and InQuest Labs require a premium subscription, while the others are provided free of cost. Access to the free and premium feeds are authenticated by an API key, where each subscriber to the InQuest Intelligence feed is given a unique API key, granting access to the subscribed sources.

InQuest Intelligence provides two IOC feeds for ThreatConnect users:

- **Bulk** - InQuest Intelligence IOCs generated by InQuest's advanced, automated research tools. Access to the Bulk feed is free to all ThreatConnect users.
- **Curated** - InQuest Intelligence IOCs that have been vetted by the InQuest research team for the highest fidelity and confidence.

There are three categories of IOCs provided by the InQuest Intelligence feeds:

- **Address** - IP addresses
- **Host** - Domains
- **URL** - URLs with protocol

By default, ThreatConnect will ingest all three IOC categories from the InQuest Intelligence feeds, however, the IOCs can be filtered to the desired IOC in the Feed Deployer Wizard.

There are five categories of data sources that InQuest Intelligence fetches from:

- **IOCDB** - InQuest Labs IOC Database. This includes indicators pulled from Twitter, GitHub, and blogs.

- **REPDB** - InQuest Labs Aggregate Reputation Database. This includes IOCs from InQuest partner reputation feeds.
- **DFIDB** - InQuest Labs Deep File Inspection (Lite). This includes IOCs extracted from malicious files that were processed through the lite version of InQuest's proprietary Deep File Inspection engine.
- **Labs-C2** - InQuest Labs Command and Control. These IOCs have been confirmed by the InQuest research team to be associated with command and control malware and have detailed descriptions.
- **Labs-Reputation** - InQuest Labs Research Reputation. These IOCs have been confirmed by the InQuest research team to be associated with a particular campaign or adversary.

By default, ThreatConnect will ingest all available source categories from the appropriate InQuest Intelligence feeds, however, the sources can be filtered to the desired sources categories in the Feed Deployer Wizard.

***Note**: The **Labs-C2** and **Labs-Reputation** sources are only available on the **Curated** feed.*

All three IOCs have four attributes that are defined by InQuest Intelligence and updated by ThreatConnect for easier filtering within the ThreatConnect platform.:

- **Threat Type** - The IOC category; one of Address, Host, or URL.
- **Threat Rating** - The severity of the IOC on a scale of 1 to 5, with 5 being the highest. This value is mapped from the InQuest score which is on a scale of 1 to 10 with 10 being the highest.
- **Added** - The date the IOC was added to the ThreatConnect platform.
- **Modified** - The date the IOC was last updated on the ThreatConnect platform.

Data Mapping

The labels below document the data mapping between the InQuest Reputation Database and the ThreatConnect Platform.

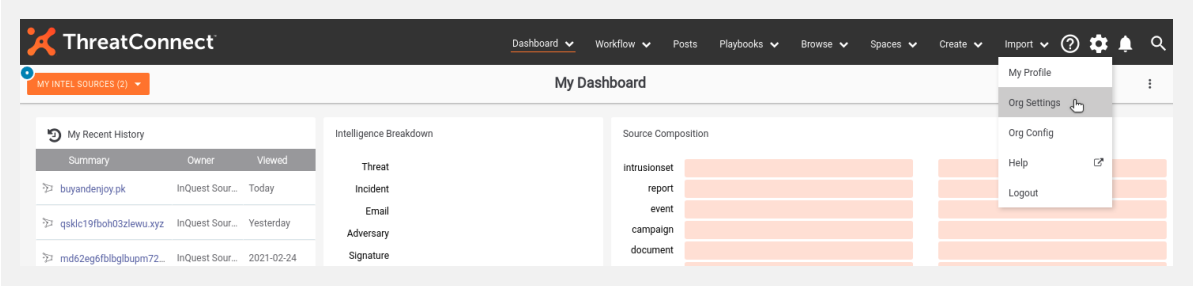
InQuest Field	ThreatConnect Field	Possible Value	Notes
Address	Address	A valid IP address	A valid IP address
Host	Host	A valid domain	The host value may be derived from a URL or provided as first seen.
URL	URL	A valid URL	A valid URL
Score	Threat Rating (1 - 5)	0 - 5	Provided for DFI IOCs. Default scores that are configurable for other indicators.
Confidence	Confidence	0 - 100	IOCDB - 50 REBDB - 70 DFI IOC - 85 C2 - 90
Source	Custom Attribute - InQuest Tool -The name of the InQuest tool providing the IOC. Provided for all IOCs.	One of REPDB, IOCDB, DFI,InQuest Labs	The InQuest tool reporting the IOC and will be provided for all Indicators.

Reference	Attribute - Source	A URL that refers to the IOC details.	This might be a link to the IOC on labs.inquest.net, Twitter, or Virus Total.
Description	Attribute - Description	Any valid string value	Generic field with additional information if available.
Created	Attribute - First Seen	ISO8601 formatted timestamp.	This will be either the creation time of the IOC or the First Seen time in the case of DFI IOCs.
Last Seen	Attribute -Last Seen	ISO8601 formatted timestamp.	This field is available for all Indicators.

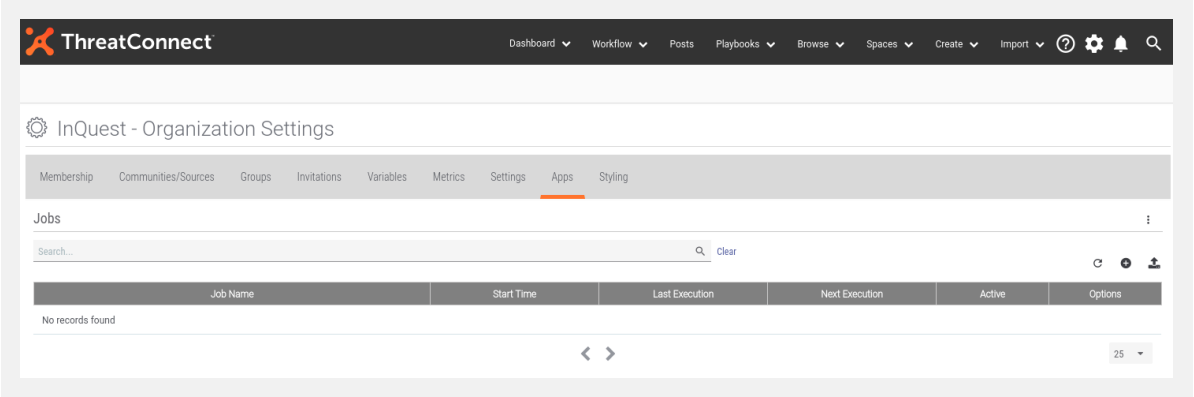
Configuration

The ThreatConnect Platform provides the ability for customers to schedule applications as jobs, specifically known as Job apps, that can be run at configured intervals. InQuest has developed a Job app for ThreatConnect customers by the name of InQuest Intelligence that handles the complete process of downloading and ingesting the threat feed into the ThreatConnect Platform. In order to configure the InQuest job, follow the steps mentioned below:

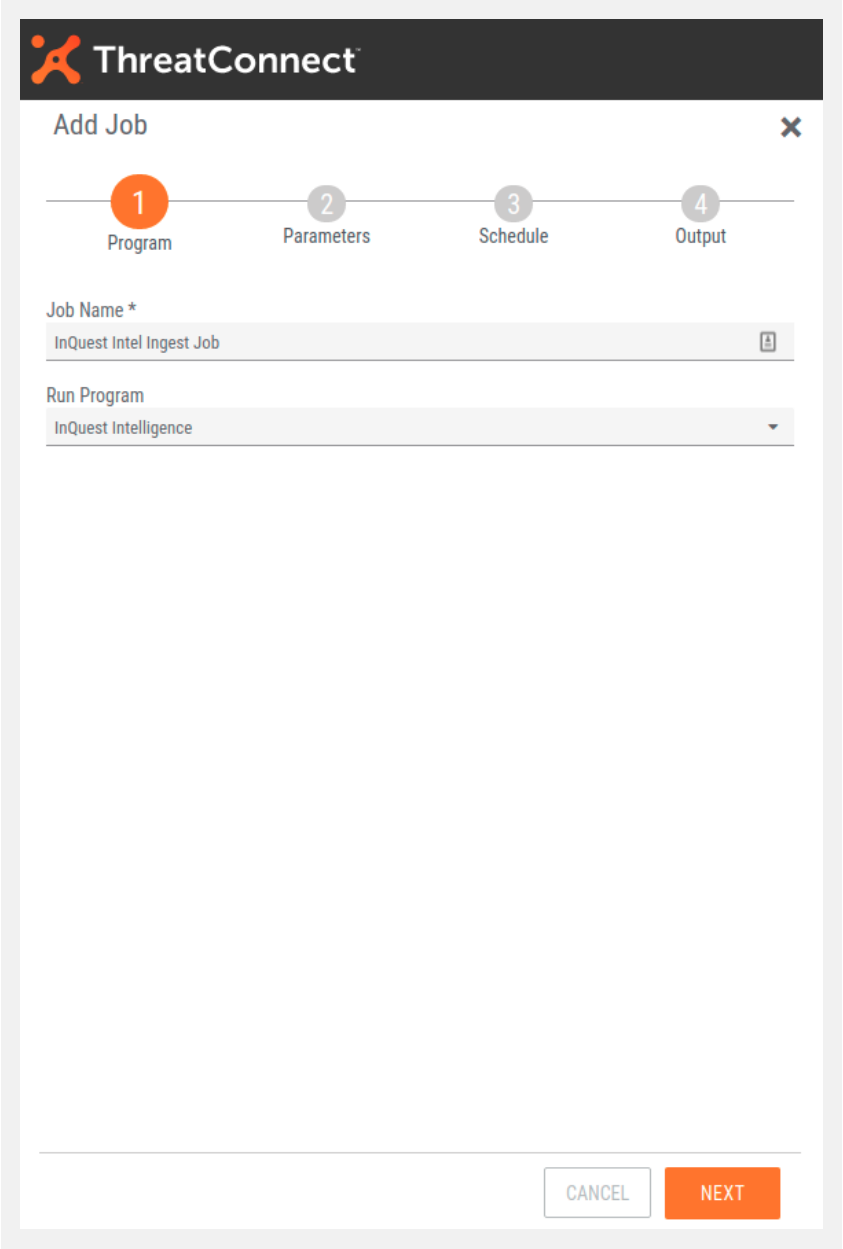
1. In the ThreatConnect console, navigate to the gear-icon on the top menu bar. From the drop-down menu, click on Org Settings.



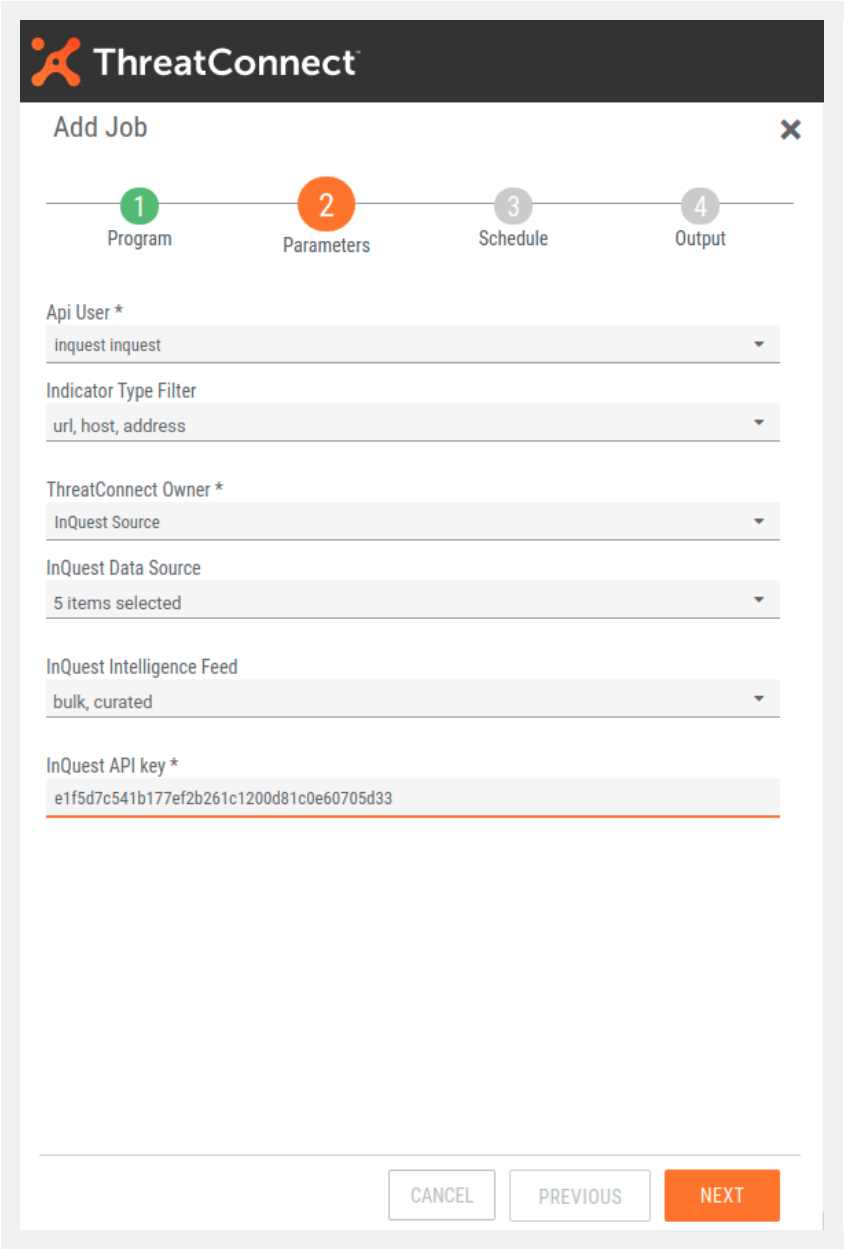
2. Select the Apps tab , then click on the small + icon to add a new job.



3. In the Add Job panel, choose a suitable name for your Job in the Job Name option. Select InQuest Intelligence from the Run Program drop-down list.

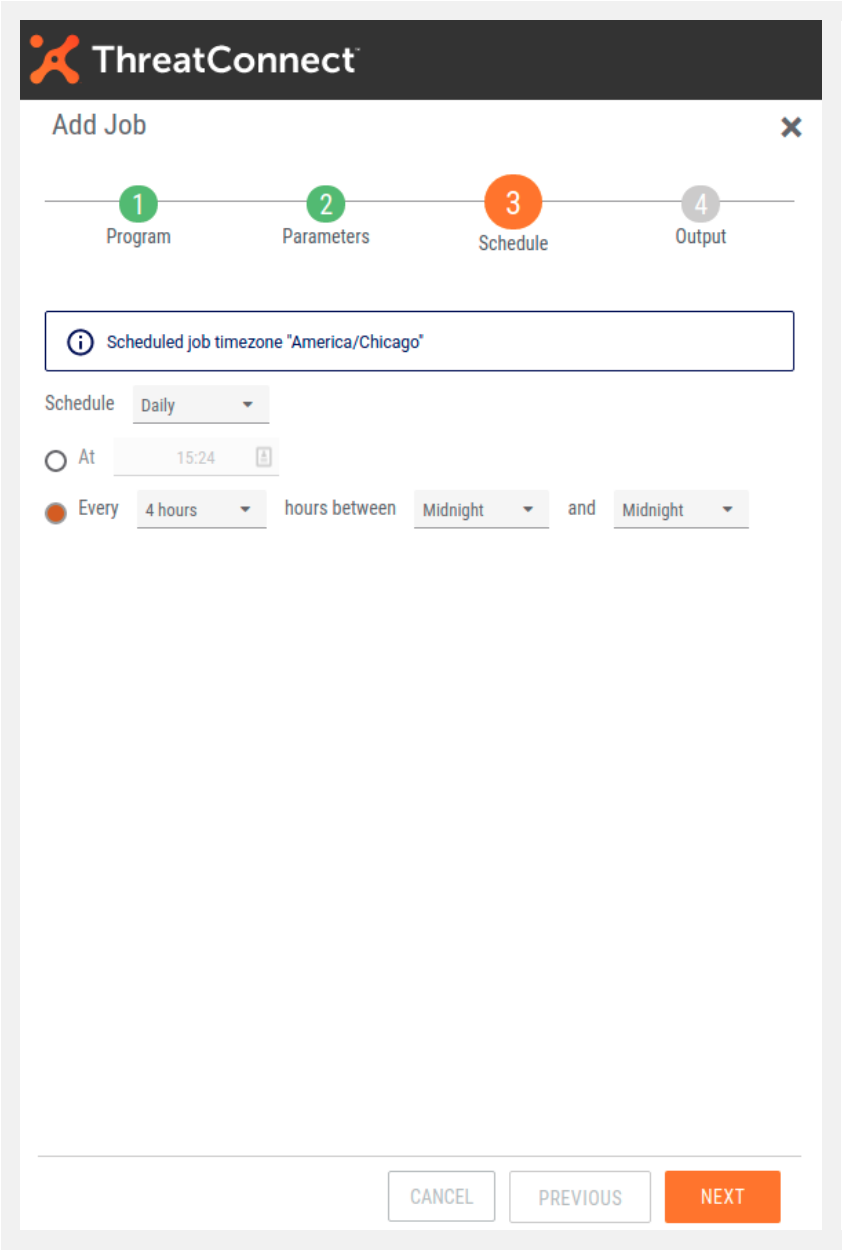


4. In the next screen configure the Job parameters as follows:

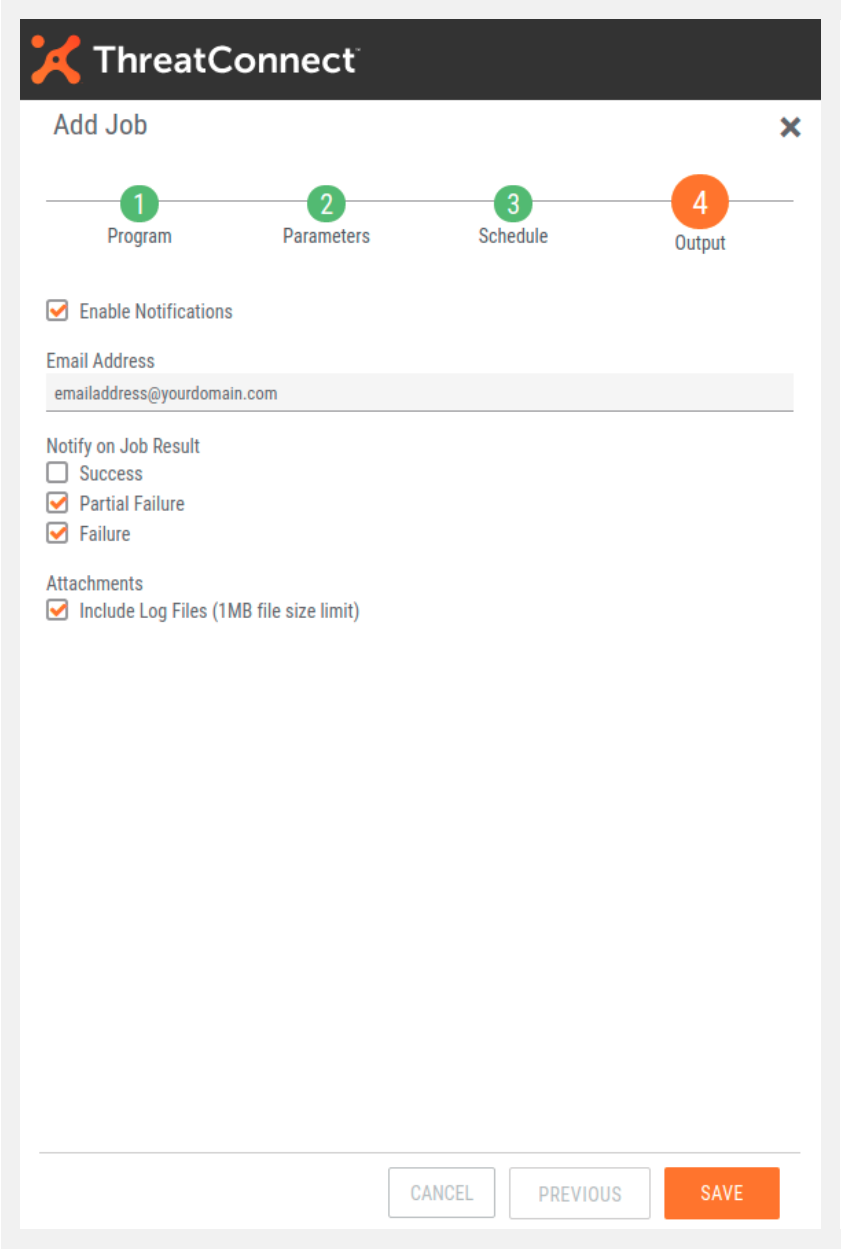


Configurable Field	Possible Value	Notes
Indicator Type filter	URL, Host, Address	The optional indicator type to filter updates by.
ThreatConnect Owner	Feed owner name	The owner from which indicators (and maybe groups) will be counted.
InQuest Data Source	REPDB, IOCDB, DFIDB, InQuest Labs C2 and InQuest Labs Reputation	The InQuest indicator data source to include updates from. Note: DFIDB, InQuest Labs C2, and InQuest Labs Reputation require a premium subscription.
InQuest Intelligence Feed	Bulk or Curated	Bulk collected indicators are available included in the base integration offering to all ThreatConnect users. Ingesting InQuest curated indicators requires contacting support@inquet.net about upgrading to a premium API key.
InQuest API Key	40 character string	A valid InQuest provided API key. Ingesting a premium feed requires contacting support@inquest.net about upgrading to a premium API key.

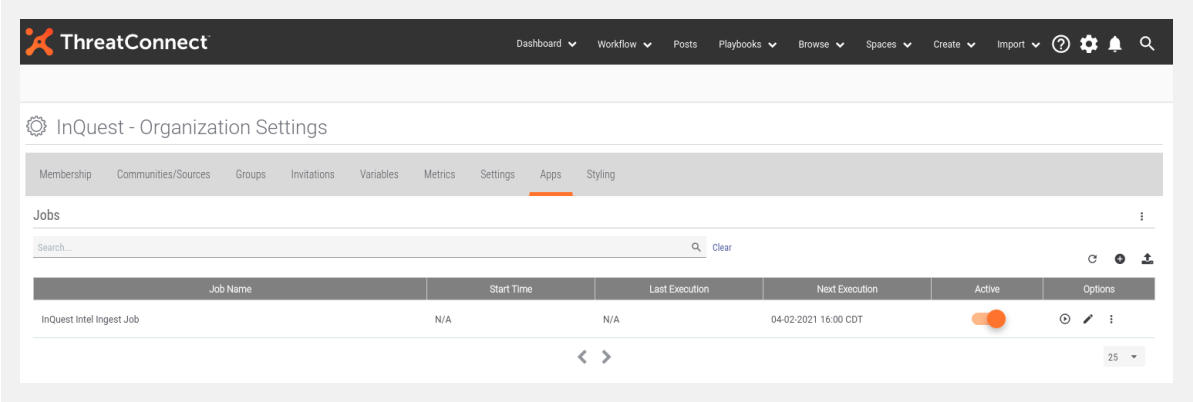
5. Click Next button to configure the schedule of running the job app, at which the feed will be ingested in your instance. Select the suitable period from the Schedule drop-down menu. InQuest recommends updating every 4 hours for free indicator sources and feeds, and updating daily for premium feeds.



6. Finally, click Next to setup the Output of the job app. Optionally, you can check the Enable Notifications checkbox to enable email notifications upon completion of the Job and provide the receiving Email Address. Under the Notify on Job Result option, check all the required scenarios at which email notifications are desired to be received. Also, click on Include Log Files checkbox under the Attachments option to receive job execution logs as attachments in the email notifications.



7. Click on Save button to save the job configuration. At this point, the job app is configured but is currently not active for execution. Click on the toggle button under Active as shown below to activate the job for running. The job configuration step is now complete.



Contacting Support

Please contact InQuest support (support@inquest.net) for assistance with the InQuest intelligence feed integration.