ThreatQuotient

A Securonix Company

ThreatQuotient App for Splunk

App Version: 3.3.0
Add-On Version: 3.2.0

August 25, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **5**
Support **6**
App Details **7**
Introduction **8**
Getting Started **10**
Prerequisites **11**
Prerequisites 11
Splunk Requirements 11
App Components 12
Deployment Methods 13
Stand-Alone Environment 13
Distributed Environment 13
Option 1 13
Option 2 14
Cloud Environment 15
Supported Matching Modes 17
Determining Which Mode to Use 18
Role-Based Permissions 19
User Capabilities 19
Configuring Account 19
Configuring Input 20
Data Collection Management 21
Use Workflow Actions 22
Use Alert Actions 23
App Configuration 24
Use Raw Matching Saved Searches 25
Use Data Model Saved Searches 26
Use Enterprise Security Searches 27
Installation/Upgrading **28**
Installing/Upgrading 28
Installing the Add-On Component 28
Configuring the Add-On Component 29
Account Tab 29
Authentication via Self-Signed Certificates in ThreatQ 31
Disable Verify SSL Certification for the Add-On 31
Splunk KVStore Rest 32
Proxy 33
Import Timeout 35
Logging 35
Installing the App Component 37
Configuring the App Component 37
Account Tab 38
App Settings 40
Disable Verify SSL Certification for the App 42
Splunk Custom Fields 43
Splunk Forwarder 44
Proxy 46

Import Timeout ... 47
Logging ... 48
Generating ThreatQ OAuth Credentials ... 49
ThreatQ v6 Steps ... 49
ThreatQ v5 Steps ... 49
Upgrading ... 51
Upgrading the App to 3.2.0 ... 51
App Upgrade Steps ... 52
Add-On Upgrade Steps ... 52
Extracting Data from ThreatQ ... 54
Extracting Data from ThreatQ ... 54
Inputs Tab Overview ... 54
Creating a New Input ... 56
Enable/Disable Inputs ... 60
Pagination Support ... 61
Known Limitations ... 63
Sightings and Feedback ... 64
Sightings and Feedback ... 64
About Sightings and Feedback ... 64
Macros ... 66
Saved Searches ... 68
Saved Search Macros ... 70
Separation of Data ... 70
Chunking ... 72
CIM Model Matching ... 73
Enterprise Security Matching ... 78
ThreatQ Indicators to Splunk Enterprise Security Lookup Tables ... 78
Saved Searches for Enterprise Security ... 81
Reporting Sightings in ThreatQ ... 83
Single Event for Each Sighted Indicator ... 83
Multiple Events for Each Sighted Indicator ... 83
Workflow Actions ... 86
Performing Workflow Actions by Non-Admin Users ... 87
Scaling the App ... 89
Performance Testing ... 89
Datamodel Matching Mode ... 89
Raw Matching Mode ... 90
Dashboards ... 93
Threat Dashboards ... 93
Cumulative Counts ... 93
Score Breakdown ... 94
Type Breakdown ... 95
Source Breakdown ... 95
Adversaries Breakdown ... 96
Static View Table ... 96
Top 10 By Sightings ... 97
Sources ... 97
Adversaries ... 98
Indicators Malware Family Distribution ... 98
Indicators with Sightings Malware Family Distribution ... 98
Indicator Dashboards ... 100
Info Tab ... 101
Add Indicator ... 101

Indicator Lookup 101
Application Log Search 102
Edit App Configuration 102
Troubleshooting 103
Change Log 104

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com
Support Web: https://ts.securonix.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

App Details

Current App Version	3.3.0
Current Add-On Version	3.2.0
Compatible with ThreatQ Versions	>=5.11.0
Compatible with Splunk Versions	Enterprise and Cloud 9.4.x, 10.0.x, 10.1.x, 10.2.x, 10.3.x, 10.4.x
Python Version	3
Support Tier	ThreatQ Supported
App Splunkbase Entry	https://splunkbase.splunk.com/app/4418/
Add-On Splunkbase Entry	https://splunkbase.splunk.com/app/4419

ThreatQuotient values our customers and respects that not all 3rd Party products that they choose to integrate with are not fully supported by the 3rd Party Vendor. In these circumstances the ThreatQuotient Support team will apply best efforts to troubleshoot and remediate the issue(s) with that particular Vendor's version of their product. However, a resolution may depend on upgrading to a supported version of the 3rd Party Vendor's software.

Introduction

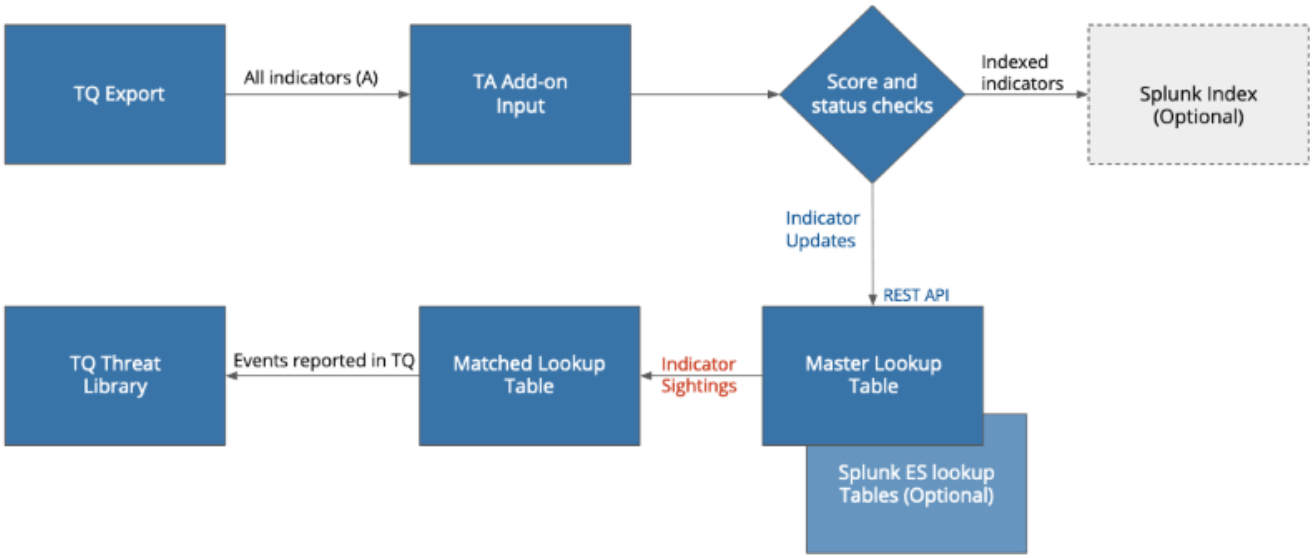
The ThreatQuotient App for Splunk provides users with the ability to pull ThreatQ indicators into their Splunk environment for evaluation. Once the indicators have been imported, they are added to a Splunk index or KVStore to provide further context on possible malicious activity that matches Splunk Events.

The app supports three Splunk Matching models for users to utilize:

- Enterprise Support Matching (ES)
- Common Information Matching (CIM)
- Raw Matching

> See the Supported Matching Modes topic for more details on these matching models.

Users can then review and modify indicators using the Workflow Actions as well as send back the Splunk Sightings, in the form of events, to the ThreatQ platform.



The app itself is composed of two main components:

- **ThreatQuotient Add-On for Splunk** - pulls indicator exports from the ThreatQ platform and submits the data to an index or the KVStore based on user configuration.
- **ThreatQuotient App for Splunk** - uses user-specified matching to identify sightings, updates indicators using app-provided workflow actions, and sends sightings back to the ThreatQ platform in the form of events.

Both of these components are required for the app to operate successfully.

Getting Started

The following is a high-level overview of how to install and configure the app for the first time.

1. Review the Role-Based Permissions topic to determine if you have the required permissions to install and configure the app.
2. Determine your deployment environment. How and where you install the App and Add-On will differ based on your individual environment. See the Deployment Methods topic for more details.
3. Determine which Splunk matching model you intend to use. See the Supported Matching Modes topic for more details.
4. Install and configure the App and Add-On. See the Installing the Add-On Component and Installing the App Component topics for more details.

   > You may see authentication errors as you install and configure the components. These errors will occur until you have completed install and configuration of both components.

5. Set up your Inputs in the App component in order to pull ThreatQ Indicator Exports. See the Creating a New Input topic for more details.

Prerequisites

Prerequisites

The follow section details the require components for the App and Add-On.

Splunk Requirements

The following is required to install the ThreatQuotient App for Splunk:

- A ThreatQ Instance running version 5.11 or greater.
- The ThreatQ Splunk Indicators export. This export is provided by default with the ThreatQ platform.
- Splunk Environment (Enterprise or Cloud): version 9.4.x, 10.0.x., 10.1.x, 10.2.x., 10.3.x, 10.4.x
- A Splunk account with the following role (for installation and configuration):
    - Admin
    - SC_Admin (Splunk Cloud Admin)
    - Splunk_System_Role
    - ess_admin

App Components

The ThreatQuotient App for Splunk is composed of two required components:

- **ThreatQuotient App for Splunk** - uses user-specified matching to identify sightings, updates indicators using app-provided workflow actions, and sends sightings back to the ThreatQ platform in the form of events.
- **ThreatQuotient Add-On for Splunk** - pulls indicator exports from the ThreatQ platform and submits the data to the KVStore based on user configuration. An additional option, based on your setup, you can submit to the Splunk index.

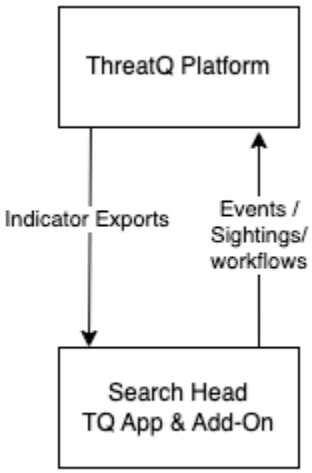
Both components are downloaded and installed via Splunkbase.

Deployment Methods

The following describes and illustrates the most common deployments for the app within a Stand-Alone, Distributed, and Cloud Splunk environment.

Stand-Alone Environment

Deploying in a Stand-Alone environment involves installing both the App and Add-On on the Search head.



Distributed Environment

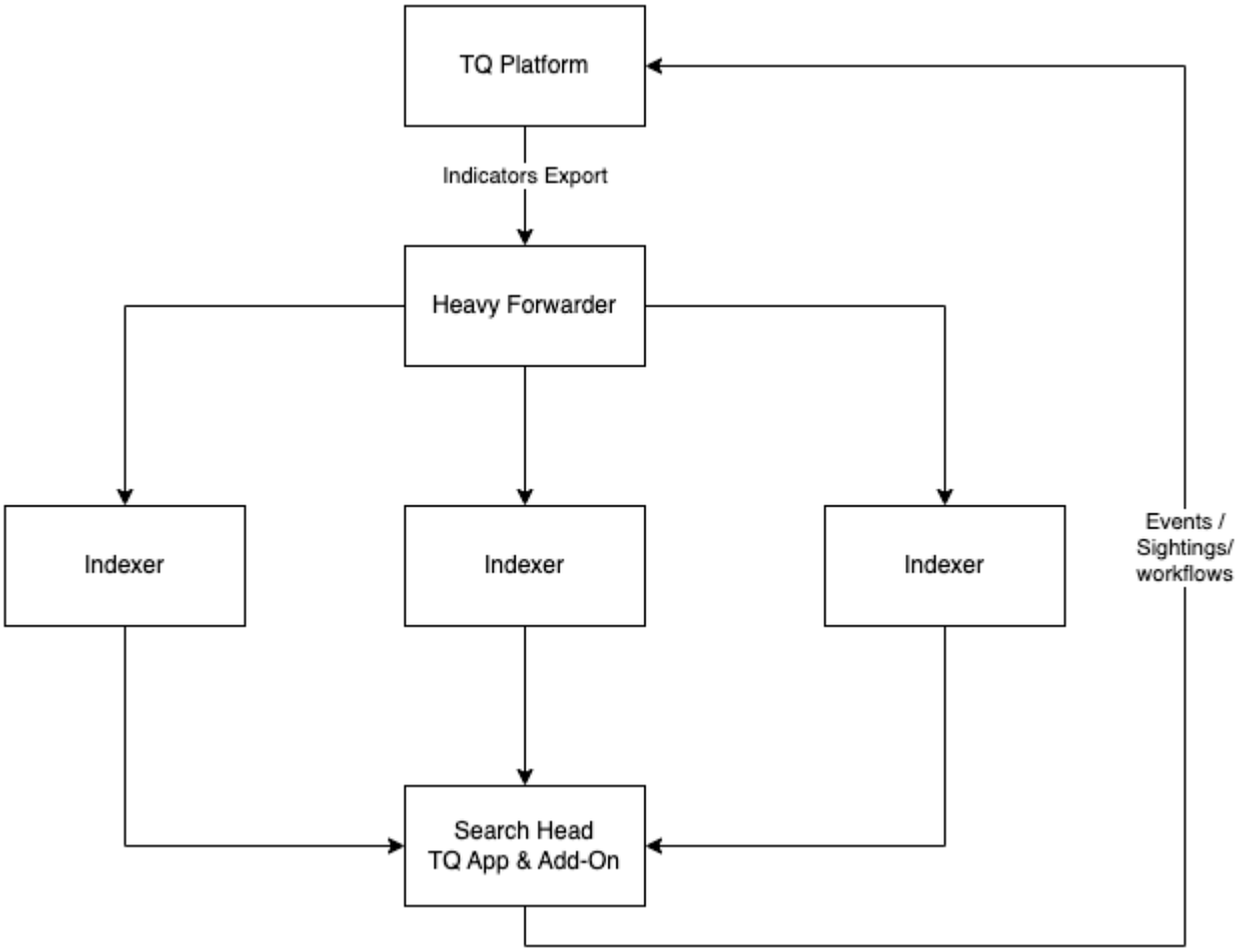
Distributed environments with a cluster of search heads will need to have the Add-On and App both configured on the master node. The Splunk App deployer will then propagate the configuration settings to all nodes.

> For heavy data, it is suggested to install the add-on on the separate Heavy Forwarder and the app on the Search head for optimal performance.

Option 1

This option for a distributed environment is to have both the App and Add-On installed on the Search Head.

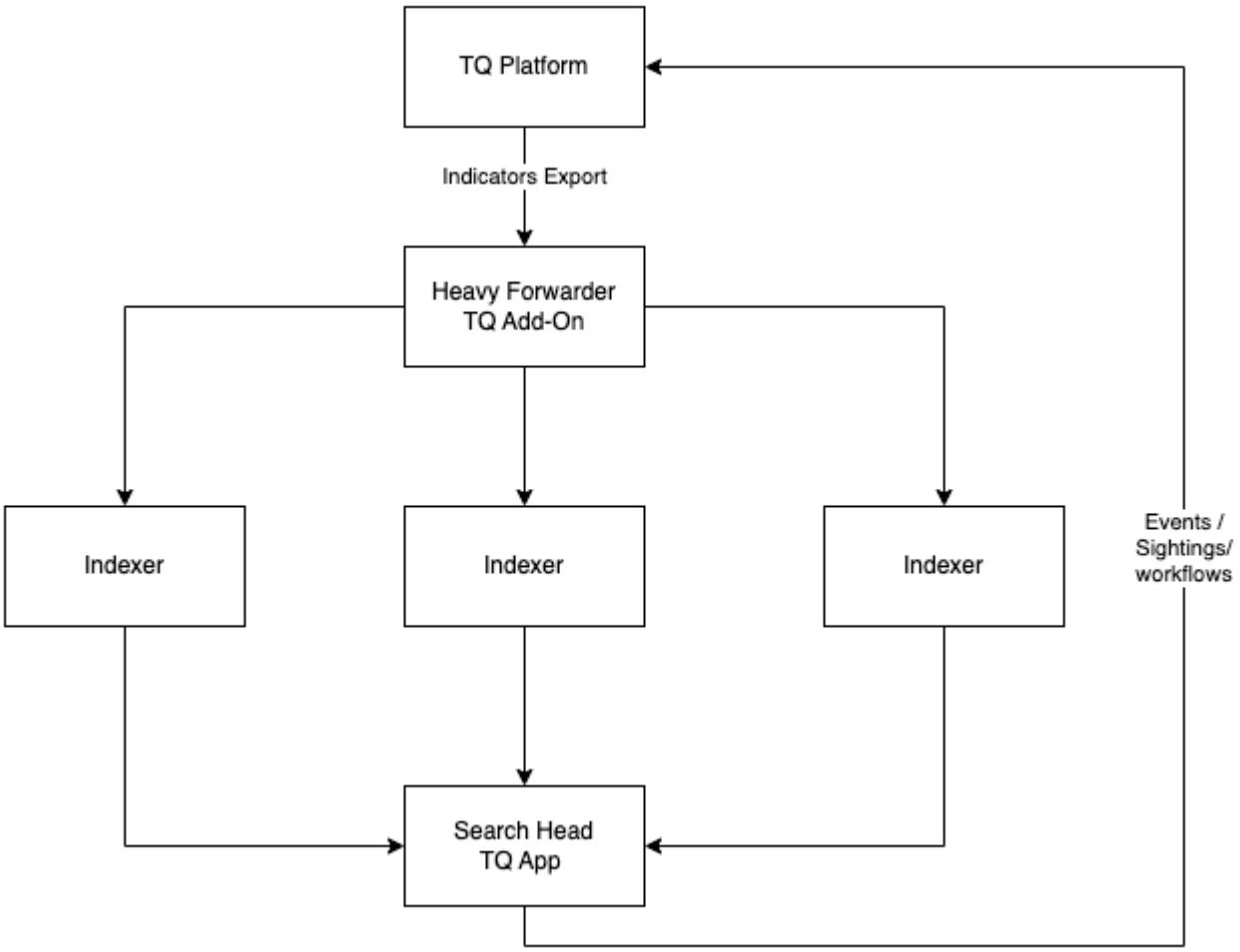
> In this scenario, the KVStore configuration option for the Add-On is not required.



Option 2

This option for a distributed environment has the App installed on the Search Head while the Add-On is installed on the Heavy Forwarder. From this location, the Add-On extracts indicators from your ThreatQ appliance and forwards them to the configured Splunk index.

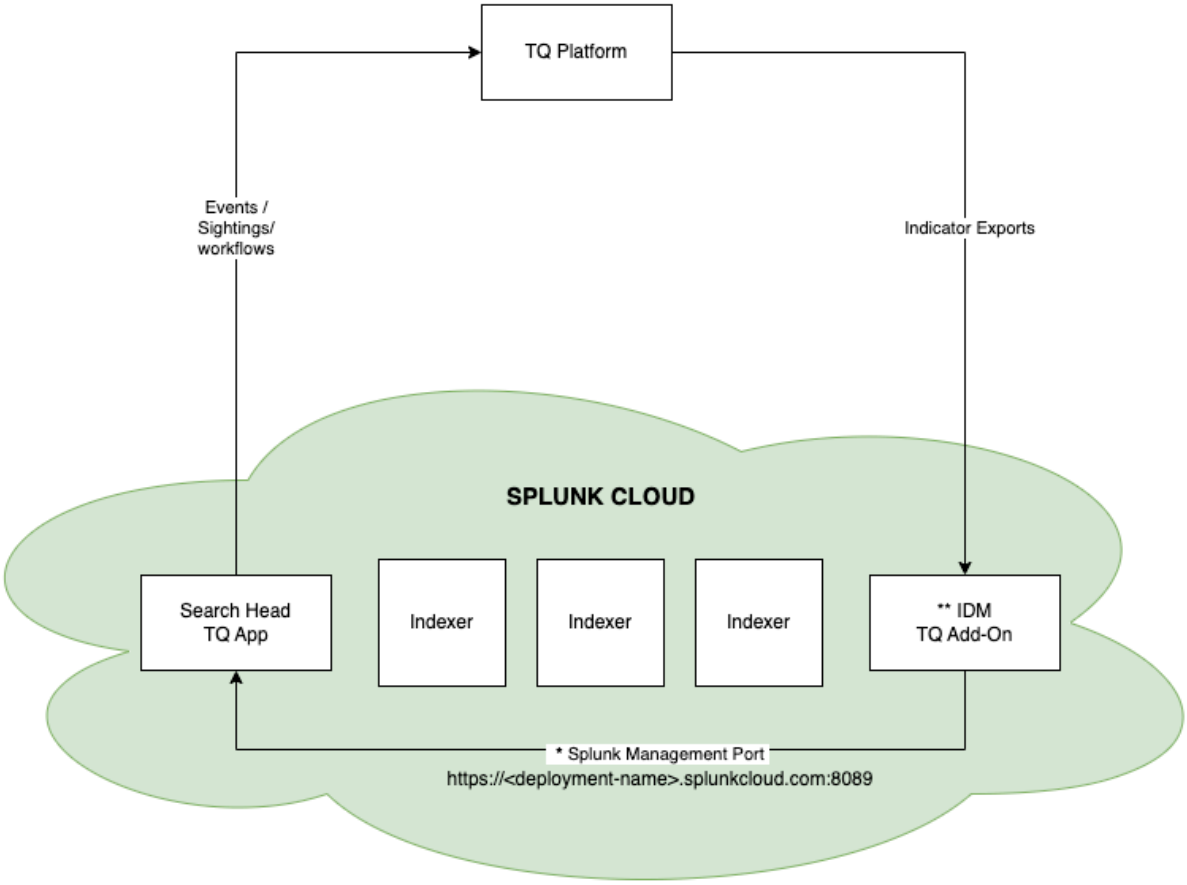
> In this scenario, the KVStore configuration option for the Add-On is required and must point to the Search Head.



Cloud Environment

Deploying in a cloud environment requires that the App be installed on the Search Head. The Add-On must be installed on the IDM or Heavy Forwarder.

> ⚠ It is important to note that a support ticket must be created with Splunk to access the Splunk REST API, which will allow communication between the Search Head and IDM/Heavy Forwarder.



* A support ticket with Splunk is required to enable REST API access to Splunk Cloud.

** A heavy forwarder can be used in place of a IDM.

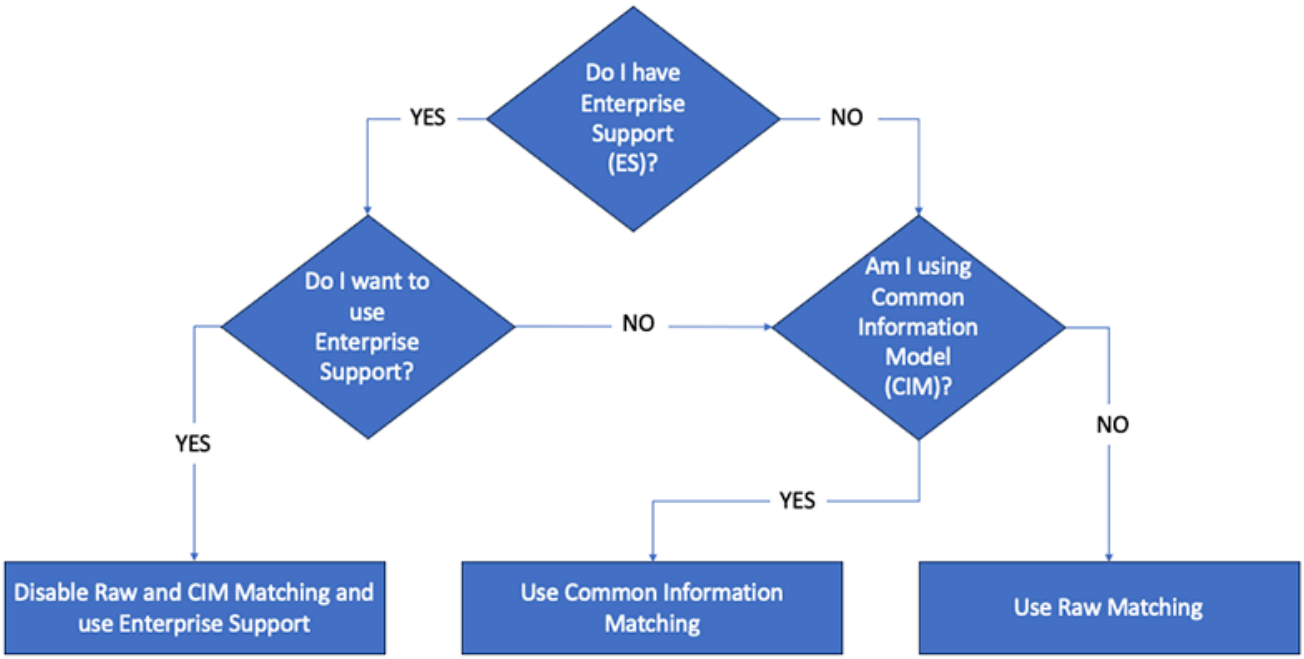
Supported Matching Modes

The ThreatQuotient App for Splunk can be used in one of three possible modes.

MODE	DESCRIPTION	HOW USED
Enterprise Support (ES)	Splunk Enterprise Security is a specialized product offering from Splunk designed specifically for security operations and threat detection. It provides a comprehensive security information and event management (SIEM) solution that allows organizations to collect, analyze, and act upon security data from various sources in real-time.	Indicator data exported from ThreatQ is mapped to lookup tables native to Splunk ES. Threat Intelligence support for Enterprise Security is provided using its REST APIs.
Common Information Matching (CIM)	Splunk CIM (Common Information Model) is a standard for organizing and normalizing data in a consistent format to facilitate interoperability and integration between different security tools and technologies within an organization's security infrastructure. Splunk CIM Support refers to Splunk's built-in capabilities and tools for implementing and leveraging the CIM standard within the Splunk platform.	For users who map third party data (firewall events, logs for example) to Splunk's data models in CIM. The App provides optimized performance by leveraging those data models.
Raw Matching	Raw Matching Mode is applicable if you do not have Splunk Enterprise Security (ES) and do not map your traffic to Splunk's CIM.	In this mode, the App treats all events as raw binary data and looks for evidence of sightings inside said data using optimized regexes. See the tables in the Performance chapter for the expected performance data.

Determining Which Mode to Use

The workflow below can be used to determine which Splunk mode to utilize with the ThreatQ App and Add-On.



Role-Based Permissions

The following sections and tables outline how Splunk roles are mapped with the App and Add-On's permissions.

User Capabilities

If a custom role for a service account is used, the following two capabilities are required for our app to run:

- **list_storage_passwords** - the `list_storage_passwords` capability is required for the `GET` operation.
- **admin_all_objects** - the `admin_all_objects` capability is required for the `POST` operation.

Configuring Account

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	No	No	No	No	No
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	No	No	No	No	No
can_delete	No	No	No	No	No
ess_user	No	No	No	No	No
ess_analyst	No	No	No	No	No
ess_admin	Yes	Yes	Yes	Yes	Yes

Configuring Input

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	No	No	No	No	No
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	No	No	Yes	No	No
can_delete	No	No	No	No	No
ess_user	No	No	Yes	No	No
ess_analyst	No	No	Yes	No	No
ess_admin	Yes	Yes	Yes	Yes	Yes

Data Collection Management

SPLUNK ROLE	ENABLE	DISABLE
Admin	Yes	Yes
Power	Yes	Yes
Splunk_System_Role	Yes	Yes
User	Yes	Yes
can_delete	No	No
ess_user	Yes	Yes
ess_analyst	Yes	Yes
ess_admin	Yes	Yes

Use Workflow Actions

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	No	No	No	No	No
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	No	No	No	No	No
can_delete	No	No	No	No	No
ess_user	No	No	No	No	No
ess_analyst	No	No	No	No	No
ess_admin	Yes	Yes	Yes	Yes	Yes

Use Alert Actions

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	No	No	No	No	No
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	No	No	No	No	No
can_delete	No	No	No	No	No
ess_user	No	No	No	No	No
ess_analyst	No	No	No	No	No
ess_admin	Yes	Yes	Yes	Yes	Yes

App Configuration

SPLUNK ROLE	EDIT	VIEW
Admin	Yes	Yes
Power	No	Yes
Splunk_System_Role	Yes	Yes
User	No	Yes
can_delete	No	No
ess_user	No	Yes
ess_analyst	No	Yes
ess_admin	Yes	Yes

Use Raw Matching Saved Searches

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	Yes	Yes	Yes	Yes	Yes
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	Yes	Yes	Yes	Yes	Yes
can_delete	Yes	Yes	Yes	Yes	Yes
ess_user	Yes	Yes	Yes	Yes	Yes
ess_analyst	Yes	Yes	Yes	Yes	Yes
ess_admin	Yes	Yes	Yes	Yes	Yes

Use Data Model Saved Searches

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	Yes	Yes	Yes	Yes	Yes
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	Yes	Yes	Yes	Yes	Yes
can_delete	Yes	Yes	Yes	Yes	Yes
ess_user	Yes	Yes	Yes	Yes	Yes
ess_analyst	Yes	Yes	Yes	Yes	Yes
ess_admin	Yes	Yes	Yes	Yes	Yes

Use Enterprise Security Searches

SPLUNK ROLE	CREATE	EDIT	VIEW	CLONE	DELETE
Admin	Yes	Yes	Yes	Yes	Yes
Power	Yes	Yes	Yes	Yes	Yes
Splunk_System_Role	Yes	Yes	Yes	Yes	Yes
User	Yes	Yes	Yes	Yes	Yes
can_delete	Yes	Yes	Yes	Yes	Yes
ess_user	Yes	Yes	Yes	Yes	Yes
ess_analyst	Yes	Yes	Yes	Yes	Yes
ess_admin	Yes	Yes	Yes	Yes	Yes

Installation/Upgrading

Installing/Upgrading

The following steps detail how to install and configure both the App and Add-On.

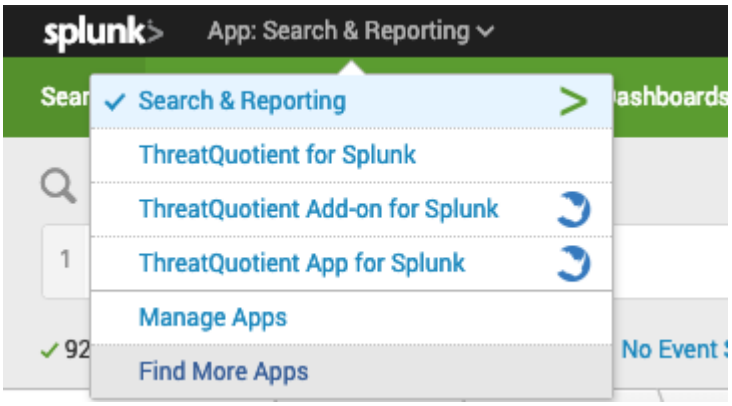
Installing the Add-On Component

Roles Required: Admin, Splunk_System_Role, ess_admin.

You can install and configure the App-On and App in any order. It is important to note that you will receive errors while configuring either until both Add-On and App configuration has been completed.

The installation location for the ThreatQuotient Add-On component depends on the type of environment you are using. See the Deployment Methods chapter for further details.

1. Log into your Splunk instance.
2. Click on the **Down** arrow on the Apps menu located in the main navigation bar.
3. Select the **Find More Apps** option.



4. Search for "**ThreatQuotient**" in the search bar.
5. Select the **ThreatQuotient Add-on for Splunk** option and follow the instructions to install the app.

Configuring the Add-On Component

Roles Required: Admin, Splunk_System_Role, ess_admin.

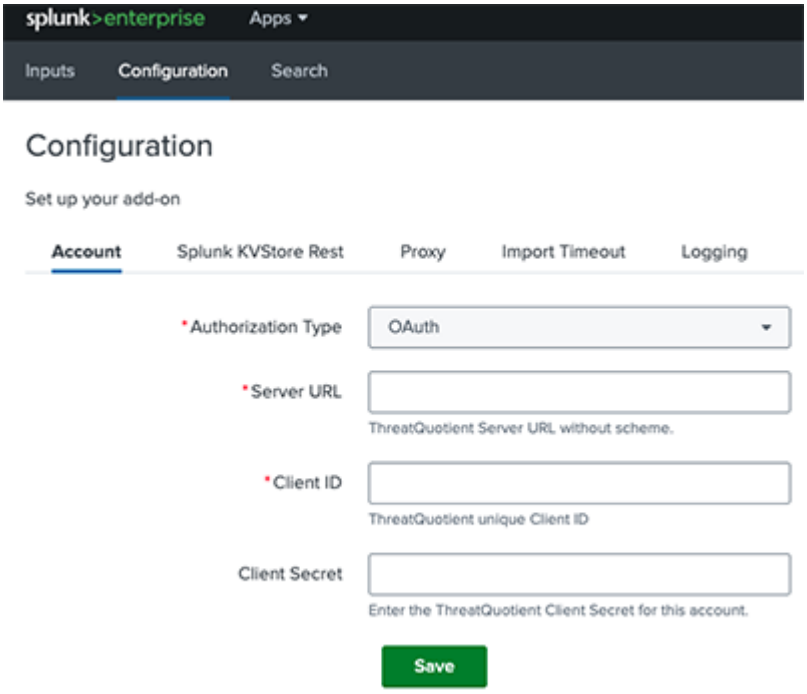
The following instructions detail the configuration tabs that must be completed in order to finish configuring the Add-On.

Account Tab

1. Click on **Info** dropdown and select **Edit App Configuration**.
2. Click on the **Account** tab.
3. Enter the following parameters:

PARAMETER	DESCRIPTION
Authorization Type	Select your authentication method. Options include: ◦ Basic Authentication ◦ OAuth ◦ CAC (Common Access Card)
Server URL	Enter your ThreatQ server URL without the scheme.
Username	Enter your ThreatQ username. This parameter is only accessible if you have selected the `Basic Authentication` option for the **Authorization Type** parameter.
Password	Enter your ThreatQ password. This parameter is only accessible if you have selected the `Basic Authentication` option for the **Authorization Type** parameter.
Client ID	Enter your ThreatQ user Client ID.

PARAMETER	DESCRIPTION
Client Secret	Enter your ThreatQ Client Secret. See the Generating ThreatQ OAuth Credentials section for steps on creating a ThreatQ Client Secret. This parameter is only accessible if you have selected the `OAuth` option for the **Authorization Type** parameter.
Certificate PEM File	Attach your Certificate PEM file. This can be obtained by running the following command to extract the cert file from the PFX file: `openssl pkcs12 -in your_pfx_file.pfx -clcerts -nokeys -out client_cert.pem` This parameter is only accessible if you have selected the CAC option for the Authorization Type parameter.
Key PEM File	Attach your Key PEM file. his can be obtained by running the following command to extract the key file from the PFX file: `openssl pkcs12 -in your_pfx_file.pfx -nocerts -nodes -out client_key.pem` This parameter is only accessible if you have selected the CAC option for the Authorization Type parameter.



4. Click on **Save**.

Authentication via Self-Signed Certificates in ThreatQ

It is common for many ThreatQ users to leverage self-signed certificates. If this is the case, you must perform the following additional configuration steps in the Splunk Add-On App:

1. Navigate and open the following file:

   `${SPLUNK_HOME}/etc/apps/TA-threatquotient-add-on/default/ta_threatquotient_add_ on_settings.conf`

2. Make the following change to the Splunk Search for Listing TQ Indicators section:

```
[additional_parameters]
verify_cert = False
```

Disable Verify SSL Certification for the Add-On

One important change that was made with the release of 2.6.0 versions of the App and Add-On was the removal of the Verify SSL Certification configuration fields in the UI. This change was made to meet Splunk Cloud Validation requirements. The steps below detail how to manually disable Verify SSL Certification, if needed.

1. Open the following file:

```
$SPLUNK_HOME/etc/apps/TA-threatquotient-add-on/bin/
threatq_const.py
```

2. Update the `VERIFY_SSL` line to **False**.

Splunk KVStore Rest

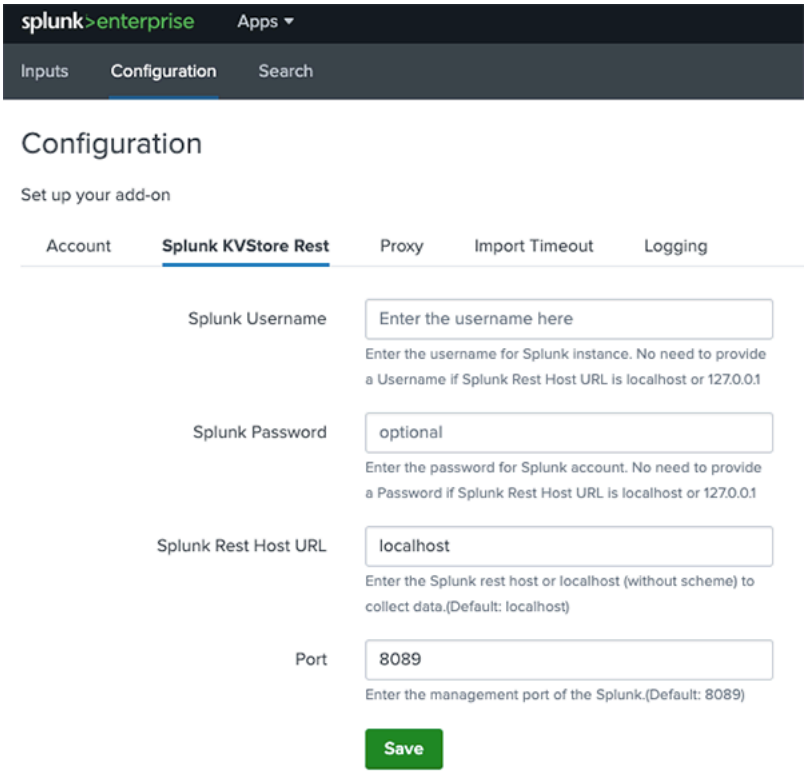
The App Key Value Store, commonly referred to as the **Splunk KVStore**, is a Splunk Enterprise feature that allows you to save/retrieve data within Splunk apps. The Splunk KVStore is requirequed if the Add-On is not installed on the Search Head.

> You can read more about the KVStore Splunk feature in Splunk's Developer documentation: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/.

The Splunk KVStore Rest configuration should be updated for distributed setups to ensure data is saved into the KVStore.

1. Click on the **Splunk KV Store Rest** tab and complete the following fields:

FIELD	DESCRIPTION
Splunk Username	Your username for your Splunk instance.
Splunk Password	The password for your Splunk user account.
Splunk Rest Host URL	The Splunk rest host or localhost (without scheme) to collect data. > This is the Splunk Management Host, commonly the Search Head or Cluster member.
Port	The Management port for Splunk.



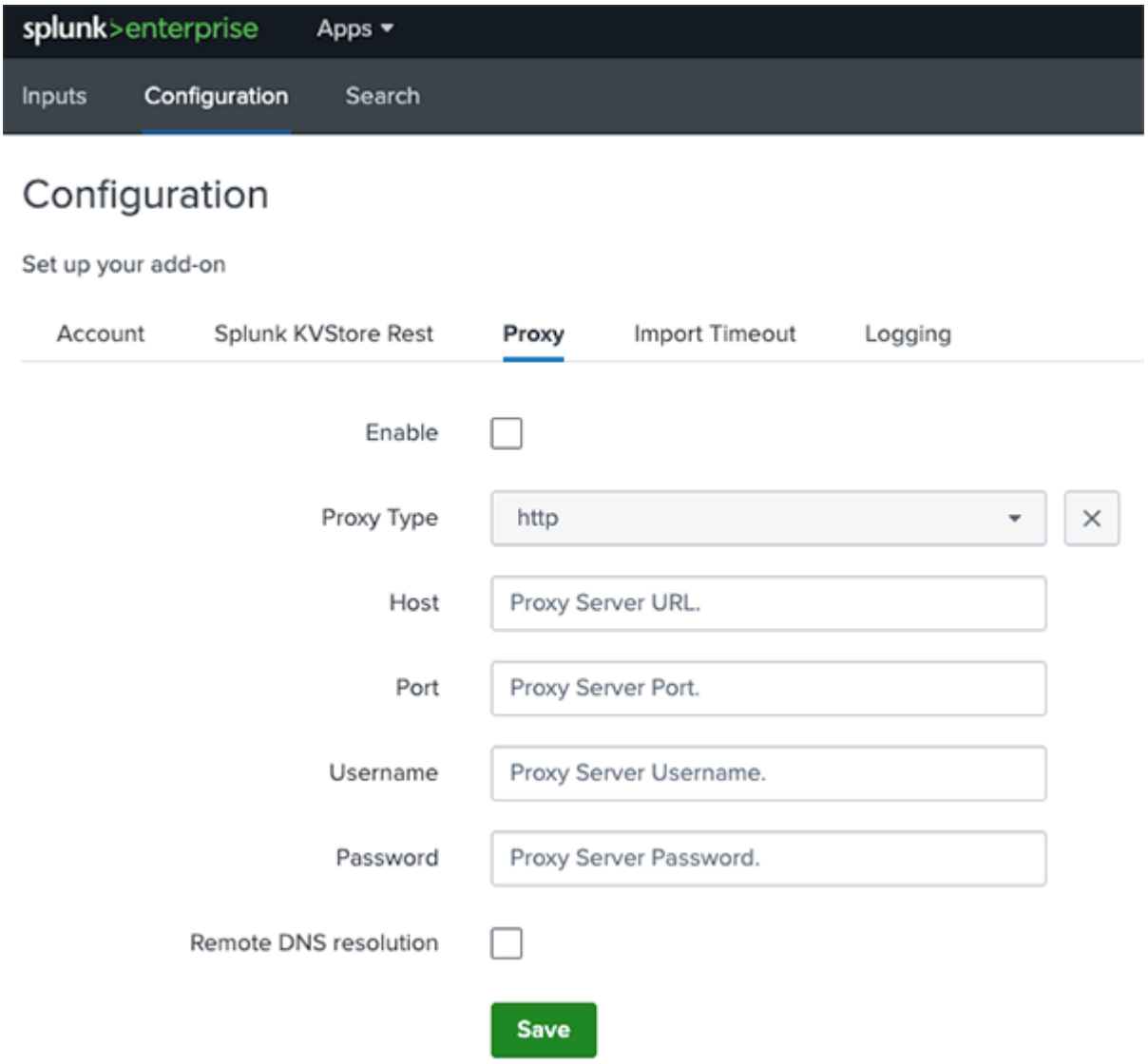
2. Click on **Save**.

Proxy

1. Click on the **Proxy** tab to set proxy settings if required.
2. Complete following parameters fields:

PARAMETER	DESCRIPTION
Enable	Use the checkbox to enable or disable the proxy.
Proxy Type	Select the type of proxy. Options include: ◦ http ◦ socks4 ◦ socks5
Host	Enter the proxy server URL.
Port	Enter the proxy server port.

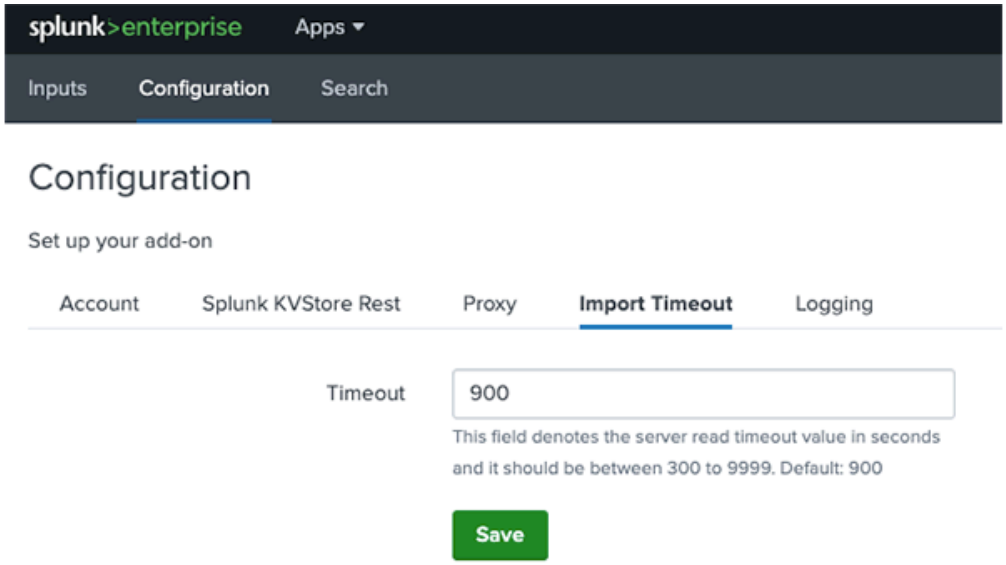
PARAMETER	DESCRIPTION
Username	Enter the proxy server username.
Password	Enter the password associated with the username above.
Remote DNS Resolution	Use this check box to enable remote DNS resolution.



3. Click on **Save**.

Import Timeout

1. Click on the Import Timeout tab
2. Use the Timeout field to set server read timeout value (in seconds).

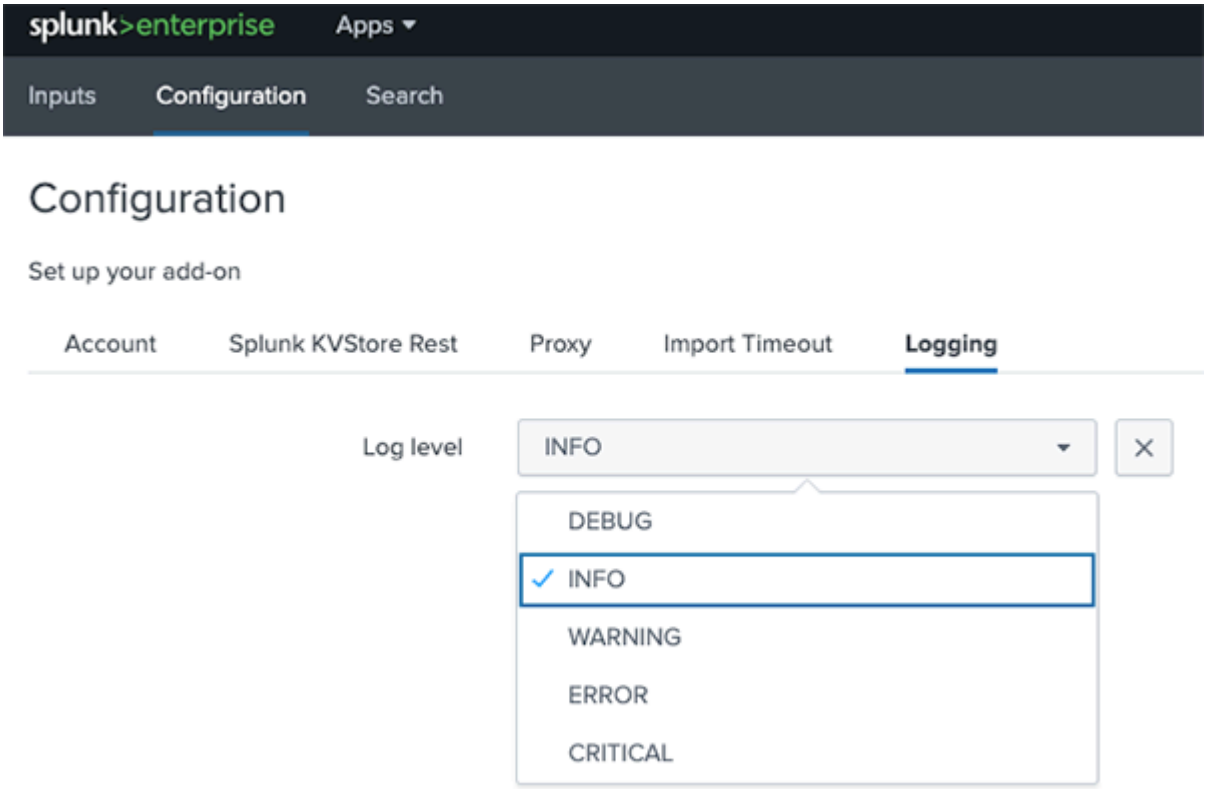


> The default value is 900 seconds. The minimum value allowed is 300 seconds.

3. Click on **Save** after you make your updates.

Logging

1. Click on the Logging tab.
2. Select your Log level. Options include:
    - Debug
    - Info
    - Warning
    - Error
    - Critical



3. Click on **Save**.

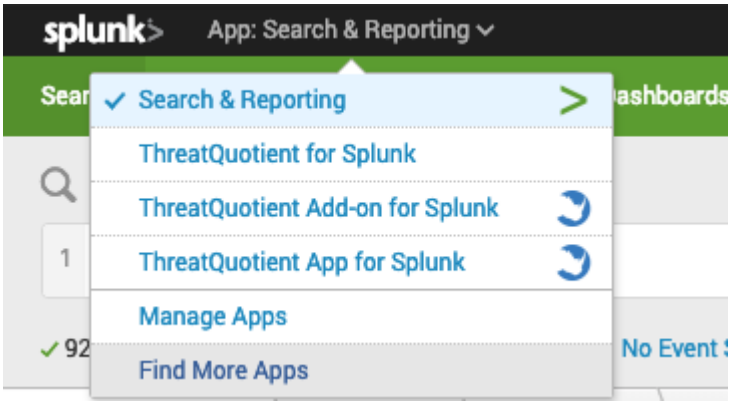
Installing the App Component

Roles Required: Admin, Splunk_System_Role, ess_admin.

You can install and configure the App and Add-On in any order. It is important to note that you will receive errors while configuring either until both App and Add-On configuration has been completed.

The installation location for the ThreatQuotient App component depends on the type of environment you are using. See the Deployment Methods chapter for further details.

1. Log into your Splunk instance.
2. Click on the **Down** arrow on the Apps menu located in the main navigation bar.
3. Select the **Find More Apps** option.



4. Search for "**ThreatQuotient**" in the search bar.
5. Select the **ThreatQuotient App for Splunk** option and follow the instructions to install the app.

Configuring the App Component

Roles Required: Admin, Splunk_System_Role, ess_admin.

The following instructions detail the configuration tabs that must be completed in order to finish configuring the app.

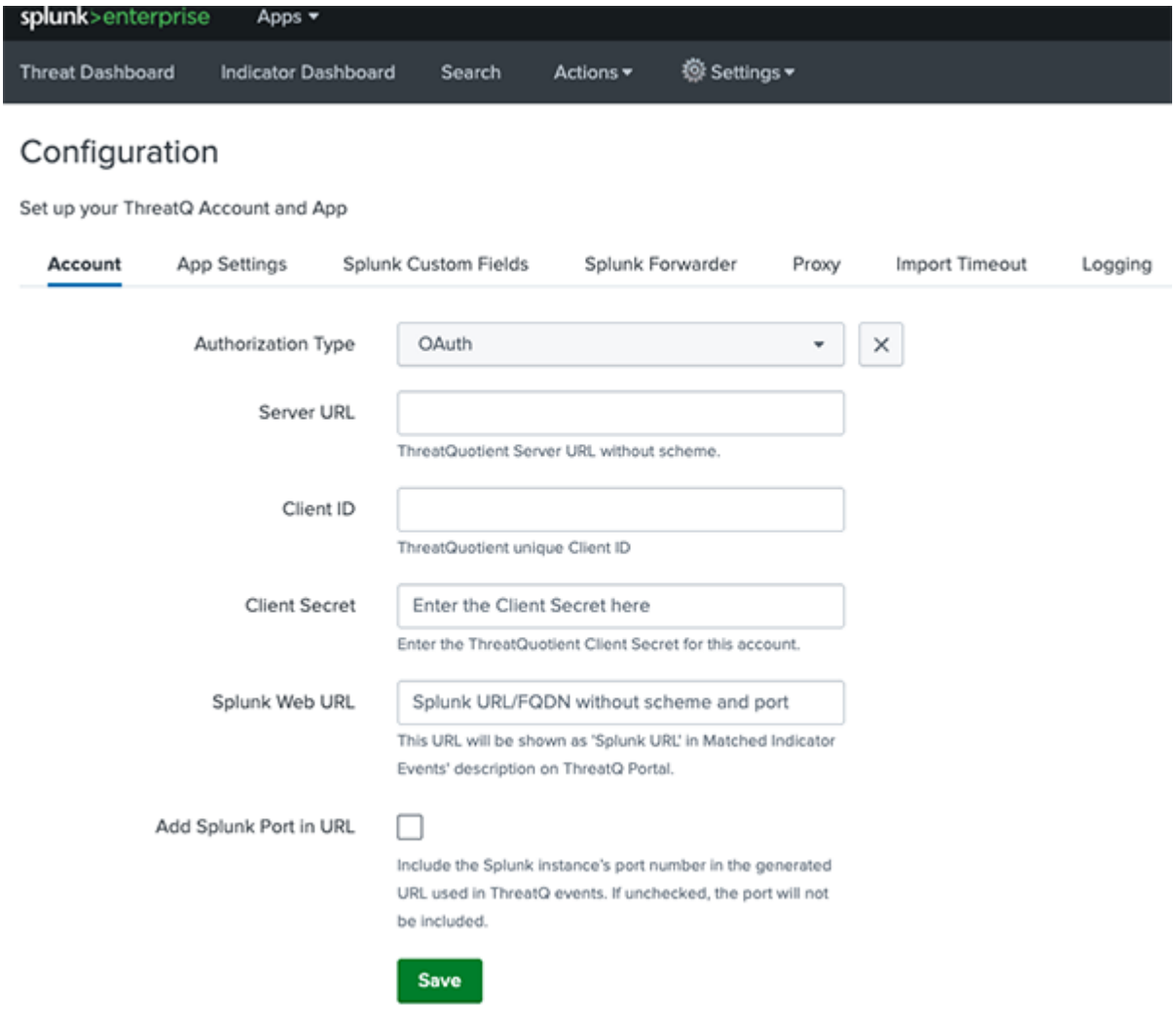
Account Tab

> The Verify SSL Certificate checkbox option was removed to meet Splunk Cloud Validation requirements with version 2.6.0. See the Disabling Verify SSL Certification topic for details on disabling the Verify SSL Certificate option.

1. Click on **Info** dropdown and select **Edit App Configuration**.
2. Click on the **Account** tab.
3. Enter the following parameters:

PARAMETER	DESCRIPTION
Authorization Type	Select your authentication method. Options include: ◦ Basic Authentication ◦ OAuth ◦ CAC (Common Access Card)
Server URL	Enter your ThreatQ server URL without the scheme.
Username	Enter your ThreatQ username. This parameter is only accessible if you have selected the `Basic Authentication` option for the **Authorization Type** parameter.
Password	Enter your ThreatQ password. This parameter is only accessible if you have selected the `Basic Authentication` option for the **Authorization Type** parameter.
Client ID	Enter your ThreatQ user Client ID.
Client Secret	Enter your ThreatQ Client Secret. See the Generating ThreatQ OAuth Credentials section for steps on creating a ThreatQ Client Secret.

PARAMETER	DESCRIPTION
	This parameter is only accessible if you have selected the `OAuth` option for the **Authorization Type** parameter.
Certificate PEM File	Attach your Certificate PEM file. This can be obtained by running the following command to extract the cert file from the PFX file: `openssl pkcs12 -in your_pfx_file.pfx -clcerts -nokeys -out client_cert.pem` This parameter is only accessible if you have selected the CAC option for the Authorization Type parameter.
Key PEM File	Attach your Key PEM file. his can be obtained by running the following command to extract the key file from the PFX file: `openssl pkcs12 -in your_pfx_file.pfx -nocerts -nodes -out client_key.pem` This parameter is only accessible if you have selected the CAC option for the Authorization Type parameter.
Splunk Web URL	Enter the Splunk URL that will be provided in the Matched Indicators Events description in ThreatQ. The hypertext for the link will read as **Splunk URL**.
Add Splunk Port to URL	Enable this parameter to include the Splunk instance's port number in the generated URL used in ThreatQ events.



4. Click on **Save**.

App Settings

The App Settings tab allows you to select datamodels, search matching algorithm, macro configurations.

1. Click on **Info** dropdown and select **Edit App Configuration**.
2. Click on the **App Settings** tab.
3. Enter the following parameters:

PARAMETER	DESCRIPTION
Hostname Configuration	The Hostname will be used as a Source Name when Splunk updates attributes on the ThreatQ platform.

Macro Configuration	ThreatQ indicators will be matched against the events from the selected indexes.
Sighting Event	Configuration option for event creation in ThreatQ for sighted indicators.
Enable Splunk ES savedsearches	Enable this option to upload ThreatQ indicators in Splunk ES Threat Intelligence Lookup. This option can be used with either **Raw Search** or **Datamodel Search**.
Splunk ES Threat Group Field	Select the indicator field used to group related indicators when uploading them to Splunk Enterprise Security.
Splunk ES Threat Category Field	Select the indicator field used to categorize indicators when uploading them to Splunk Enterprise Security. The default value is `Type`.
Search Matching Algorithm	You can select from the following: ◦ **Raw Search** ◦ **Datamodel Search** ◦ **Datamodel tstats Search** At the initial setup, you do not have to select any of the modes listed above. This disables the matching algorithm completely and gives you the opportunity to determine the right scale of data your installation can handle. See the Scaling the App chapter for more details. Attempting to search too much data may result in some saved searches being skipped based on your Splunk deployment type and hardware specification.

Select Datamodels	Select the datamodels to be used.
Custom Datamodel	Select this option when working with a custom data model for matching.
Select Custom Datamodel	Select the appropriate custom data model from the list of available options. This parameter is for custom data model matching only.
Enable Regex Matching	(For Raw matching only) Enable regex-based matching against raw events. Use this option with caution, as complex or high-volume regex patterns may significantly impact search performance.
Enable Partial Matching	(For Raw Matching only) Enable partial matching against raw events for IOC entries of type `String` only. Use this option with caution, as it may increase processing overhead and negatively impact search performance on large datasets.
Send Raw Event to ThreatQ	Enable this option to send the latest raw event for the matched indicator to the ThreatQ platform.

4. Click on **Save**.

Disable Verify SSL Certification for the App

One important change that was made with the release of 2.6.0 versions of the App and Add-On was the removal of the Verify SSL Certification configuration fields in the UI. This change was made to meet Splunk Cloud Validation requirements. The steps below detail how to manually disable Verify SSL Certification, if needed.

1. Open the following file:

```
$SPLUNK_HOME/etc/apps/ThreatQAppforSplunk/bin/threatq_const.py
```

2. Update the `VERIFY_SSL` line to **False**.

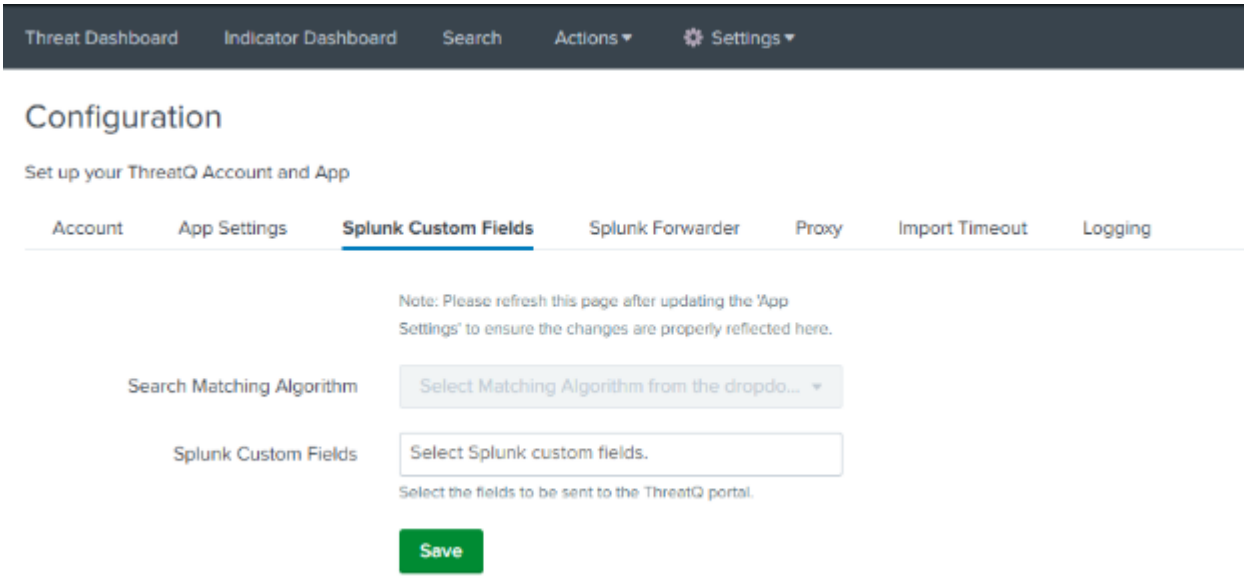
Splunk Custom Fields

The Splunk Custom fields tab provides you with a way to configure app to export custom attributes and fields to ThreatQ.

1. Click on the **Splunk Custom Fields** tab to set proxy settings if required.

   The following parameters are available:

PARAMETER	DESCRIPTION
ThreatQ Custom Attributes	Include custom attributes that will be exported from ThreatQ using a comma-separated list. **Values entered here will be treated as case-sensitive.** This configuration option requires that you create a custom export. This can be achieved by making a copy of the default Splunk export and adding the required fields. Contact ThreatQ Support for further guidance on this process.
ThreatQ Custom Fields	Include custom fields that will be exported from ThreatQ using a comma-separated list. **Values entered here will be treated as case-sensitive except for the ID field. The ID field should be lower-case only.** This configuration option requires that you create a custom export. This can be achieved by making a copy of the default Splunk export and adding the required fields. Contact ThreatQ Support for further guidance on this process.

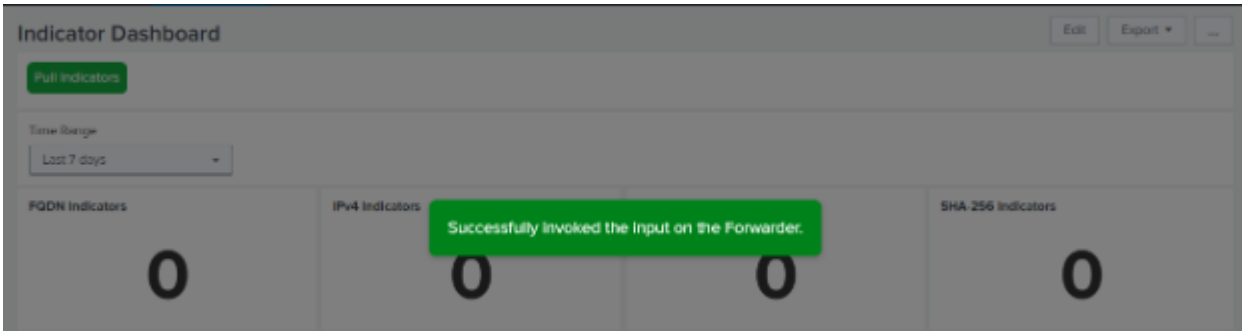


2. Click on **Save**.

Splunk Forwarder

The Splunk Forwarder tab allows you to enter the details of the Forwarder instance if the Add-On is configured on the forwarder machine. This is required if you plan to use the **Pull Indicators** button on the Indicator and Threat dashboards from the App itself instead of navigating to the Forwarder machine.

Example:

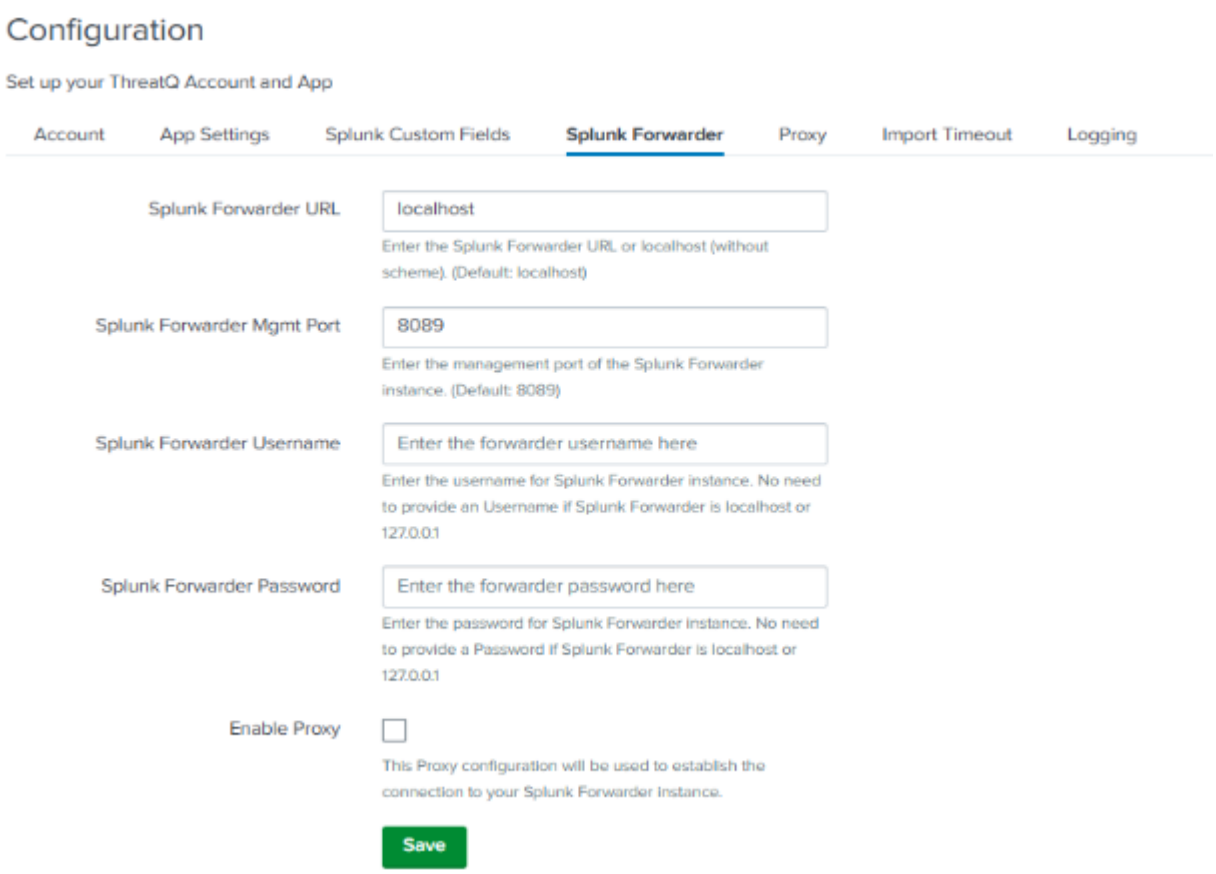


1. Click on the **Splunk Forwarder** tab.

   The following parameters are available:

PARAMETER	DESCRIPTION
Splunk Forwarder URL	Use the checkbox to enable or disable the proxy.

PARAMETER	DESCRIPTION
Splunk Forwarder Mgmt Port	Select the type of proxy. Options include: ◦ http ◦ socks4 ◦ socks5
Splunk Forwarder Username	Enter the proxy server URL.
Splunk Forwarder Password	Enter the proxy server port.
Enable Proxy	Enter the proxy server username.



2. Click on **Save**.

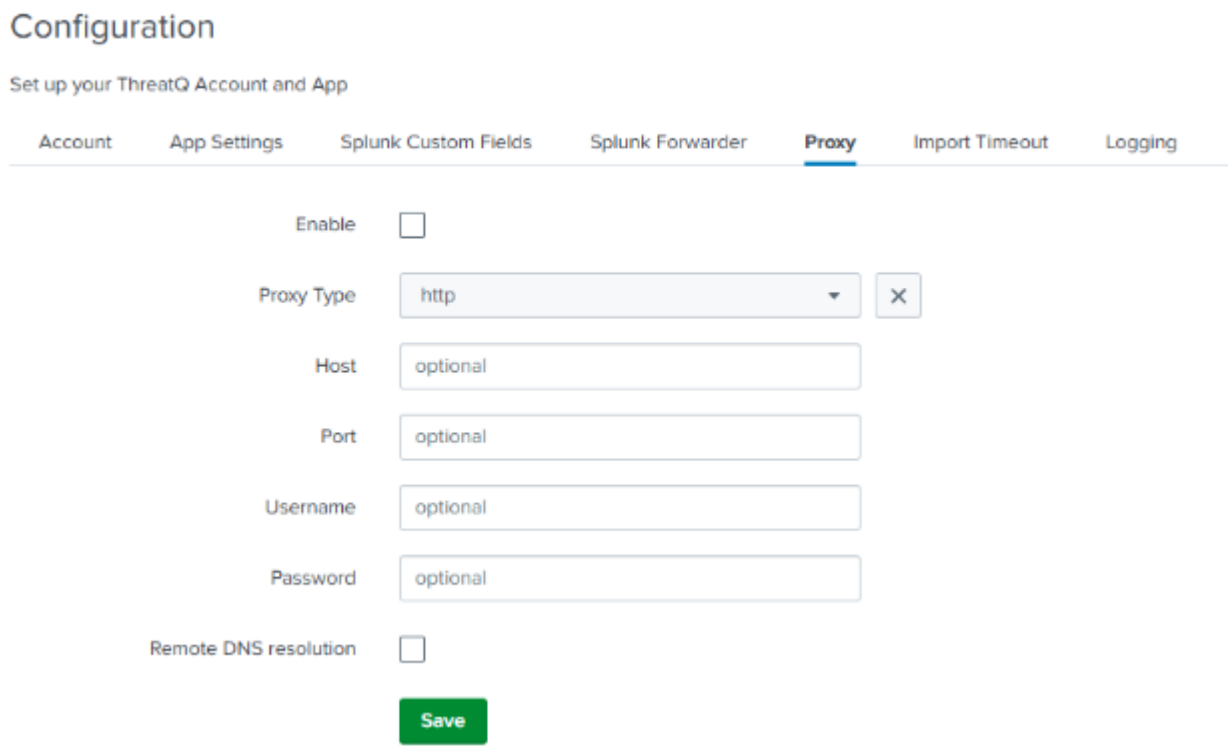
Proxy

The Proxy tab provides you with a way to configure proxy settings, if required, for the app.

1. Click on the **Proxy** tab to set proxy settings if required.

   The following parameters are available:

PARAMETER	DESCRIPTION
Enable	Use the checkbox to enable or disable the proxy.
Proxy Type	Select the type of proxy. Options include: ◦ http ◦ socks4 ◦ socks5
Host	Enter the proxy server URL.
Port	Enter the proxy server port.
Username	Enter the proxy server username.
Password	Enter the password associated with the username above.
Remote DNS Resolution	Use this check box to enable remote DNS resolution.



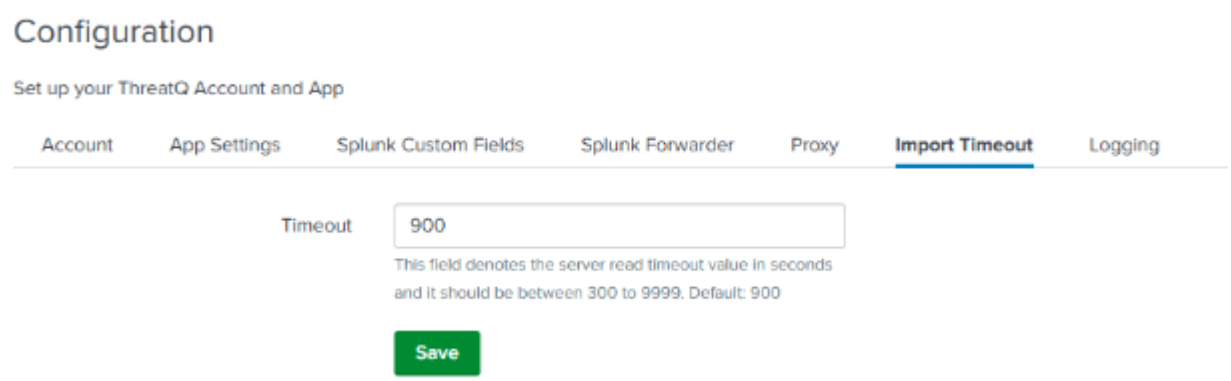
2. Click on **Save**.

Import Timeout

The Import Timeout tab provides you with a way to set the server read timeout setting in seconds.

1. Click on the **Import Timeout** tab.
2. Enter a value, in seconds, in the Timeout field provided.

> The default value is 900 seconds. The minimum value allowed is 300 seconds. The max value allowed is 9999.

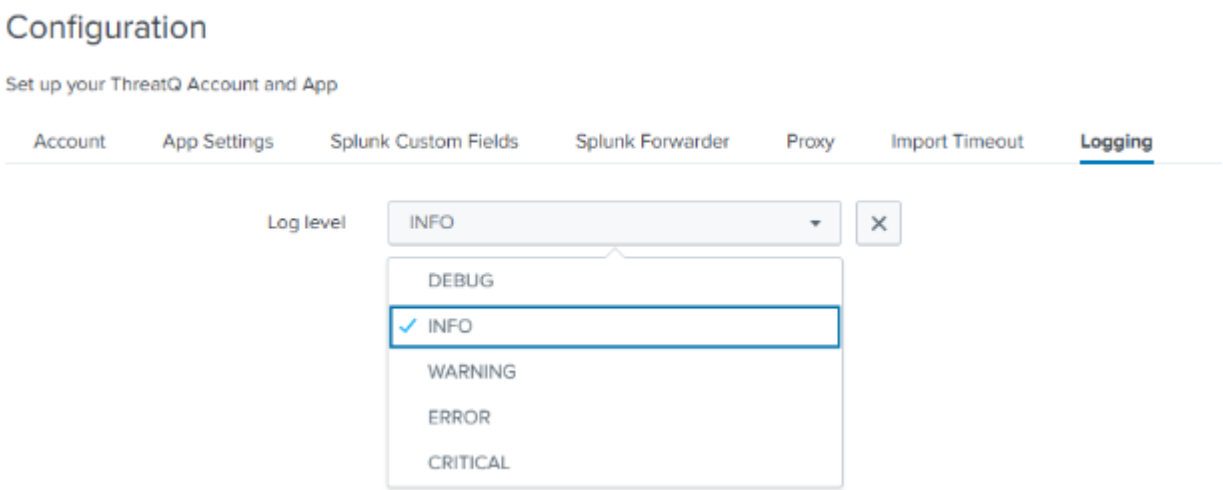


3. Click on **Save**.

Logging

The Logging tab allows you to select the

1. Click on the Logging tab.
2. Use the Log Level dropdown to select the log level. Options include:
    - Debug
    - Info
    - Warning
    - Error
    - Critical



3. Click on **Save**.

Generating ThreatQ OAuth Credentials

You will need to generate oauth2 client credentials in order to successfully have the app authenticate with ThreatQ if you have selected the OAuth authentication method. This is performed using the command line of the ThreatQ appliance.

ThreatQ v6 Steps

1. SSH to your ThreatQ installation.
2. Create a new client id and client secret password using the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/
api-schedule-run -- ./artisan threatq:oauth2-client --
name="Splunk"
```

3. Copy the client_id and client_secret from the output for use in the configuration of the Splunk application.
   Example Output:

```
session_timeout_minutes: 1440
name: Splunk
type: private
client_id: ntdjzwe3mduyyjqxyjdiyza5mzyxmtkx
client_secret:
YThlOTBlZjM0YTYxNWM1YjVkODdmMTdjNGY5MzZkYTg4M2RmYmRiZGJmNjk1O
TRm
updated_at: 2020-01-14 14:03:27
created_at: 2020-01-14 14:03:27
```

ThreatQ v5 Steps

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Create a new client id and client secret password using the following command:

```
php artisan threatq:oauth2-client --name="Splunk"
```

4. Copy the client_id and client_secret from the output for use in the configuration of the ThreatQ Splunk application.
   Example Output:

```
session_timeout_minutes: 1440
name: Splunk
type: private
client_id: ntdjzwe3mduyyjqxyjdiyza5mzyxmtkx
client_secret:
YThlOTBlZjM0YTYxNWM1YjVkODdmMTdjNGY5MzZkYTg4M2RmYmRiZGJmNjk1O
TRm
updated_at: 2020-01-14 14:03:27
created_at: 2020-01-14 14:03:27
```

Upgrading

The following steps are the standard way to upgrade the App and Add-On.

Upgrading the App to 3.2.0

Version 3.2.0 for the App introduces support for unique sightings per data model, which requires an update to the `threatq_matched_indicators` lookup format. If Matching is enabled under **App Settings**, follow the steps below to migrate your existing data to the new format. If Matching is not enabled, no action is required.

1. Open **ThreatQuotient App For Splunk > Search** and run the following query to create composite keys. Wait for the query to complete.

```
| inputlookup threatq_matched_indicators
| eval key_datamodel_name=if(isnotnull(raw_event) AND
(isnull(datamodel_name) OR datamodel_name=""), "Raw",
coalesce(datamodel_name, "Unknown"))
| eval key_dm_safe=replace(key_datamodel_name, "[^A-Za-
z0-9_-]", "_")
| eval _key=ioc_value . "_" . key_dm_safe
| table ioc_id, ioc_value, _key, match_time, first_seen,
last_seen, match_count, score, status, type, updated_at,
sources, adversaries, sid, last_run_first_seen,
last_run_last_seen, last_run_match_count, malware_family,
datamodel_name, raw_event
| outputlookup threatq_matched_indicators key_field=_key
```

2. Run the next query:

```
| inputlookup threatq_matched_indicators
| eval key_datamodel_name=if( isnotnull(raw_event) AND
(isnull(datamodel_name) OR datamodel_name=""), "Raw",
coalesce(datamodel_name, "Unknown") )
| eval key_dm_safe=replace(key_datamodel_name, "[^A-Za-
z0-9_-]", "_")
| eval composite_key = ioc_value . "_" . key_dm_safe
| eval key = _key
| where key = composite_key
| outputlookup threatq_matched_indicators append=F
```

> After this step, only composite-key rows remain in `threatq_matched_indicators` and old-key rows are removed.

3. Run the following verification query to confirm that all entries have been successfully updated with composite keys:

```
| inputlookup threatq_matched_indicators
| eval has_composite_key=if(match(_key, "^.+_.+$"), "Yes",
"No")
| stats count by has_composite_key
```

> All entries should now show `has_composite_key=Yes`.

4. Proceed with the standard App Upgrade steps listed below.

App Upgrade Steps

> Review the Upgrading the App to 3.2.0 section above if you upgrading from a version `<3.2.0` before proceeding.

1. Follow the standard Splunkbase upgrade steps to upgrade the app.

> Wait for the upgrade process to complete before proceeding with the next step.

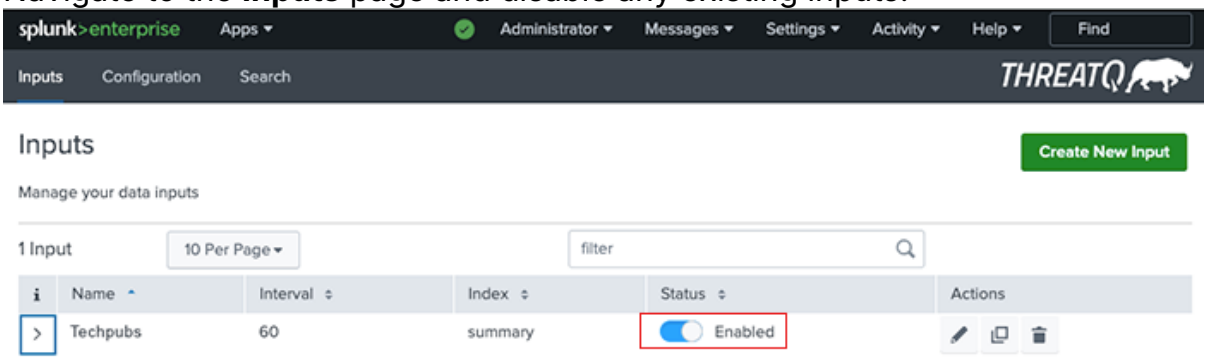
2. Navigate to **Info > Edit App Configuration > Account**.
3. Configure the account for the app to perform workflow actions and AR actions.
4. Review and configure the Proxy and a Logging settings if needed.

> If you are upgrading to a newer version of the App component and are currently using Enterprise Support matching, you will need to run the **threatq_cleanup_es_lookups** saved search once to remove the old data prior to upgrading. All the threat intelligence data will be automatically added upon upgrade using the Enterprise Security's REST APIs.

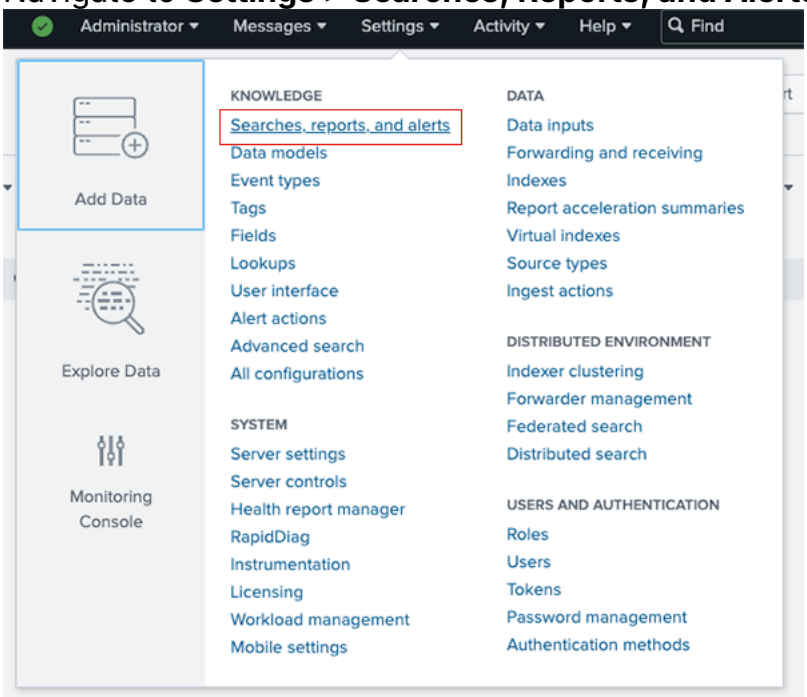
Add-On Upgrade Steps

1. Navigate to the **ThreatQuotient Add-on for Splunk**.

2. Navigate to the **Inputs** page and disable any existing inputs.



3. Navigate to **Settings > Searches, Reports, and Alerts**.



4. Delete any existing alerts.
5. Follow the standard Splunkbase upgrade steps to upgrade the Add-on.

> Wait for the upgrade process to complete before proceeding with the next step.

6. Navigate back to the **ThreatQuotient Add-on for Splunk**.
7. Navigate to the Inputs page and enable any existing input or create a new input in the fields supplied.

Extracting Data from ThreatQ

Extracting Data from ThreatQ

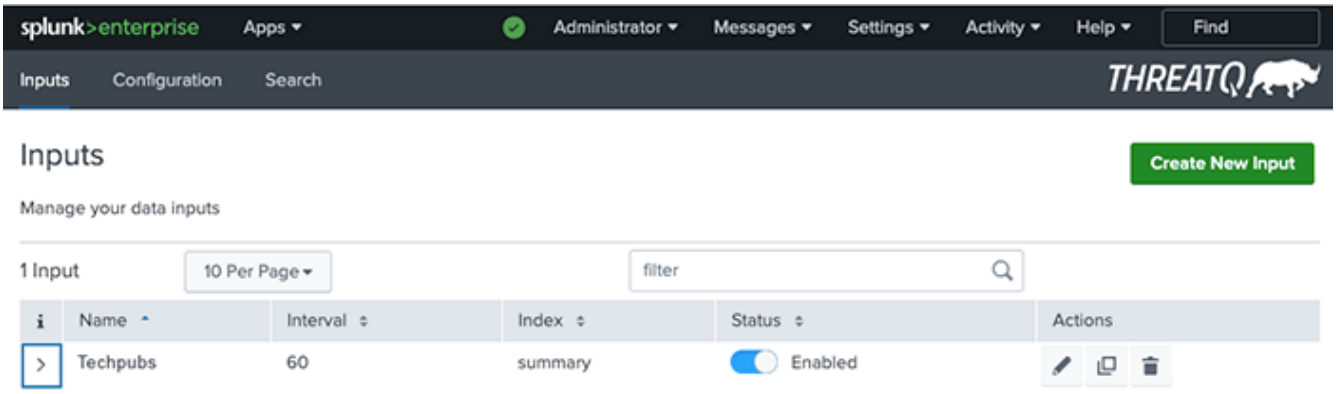
The following section details configuration steps for what data is transfered from ThreatQ exports.

Inputs Tab Overview

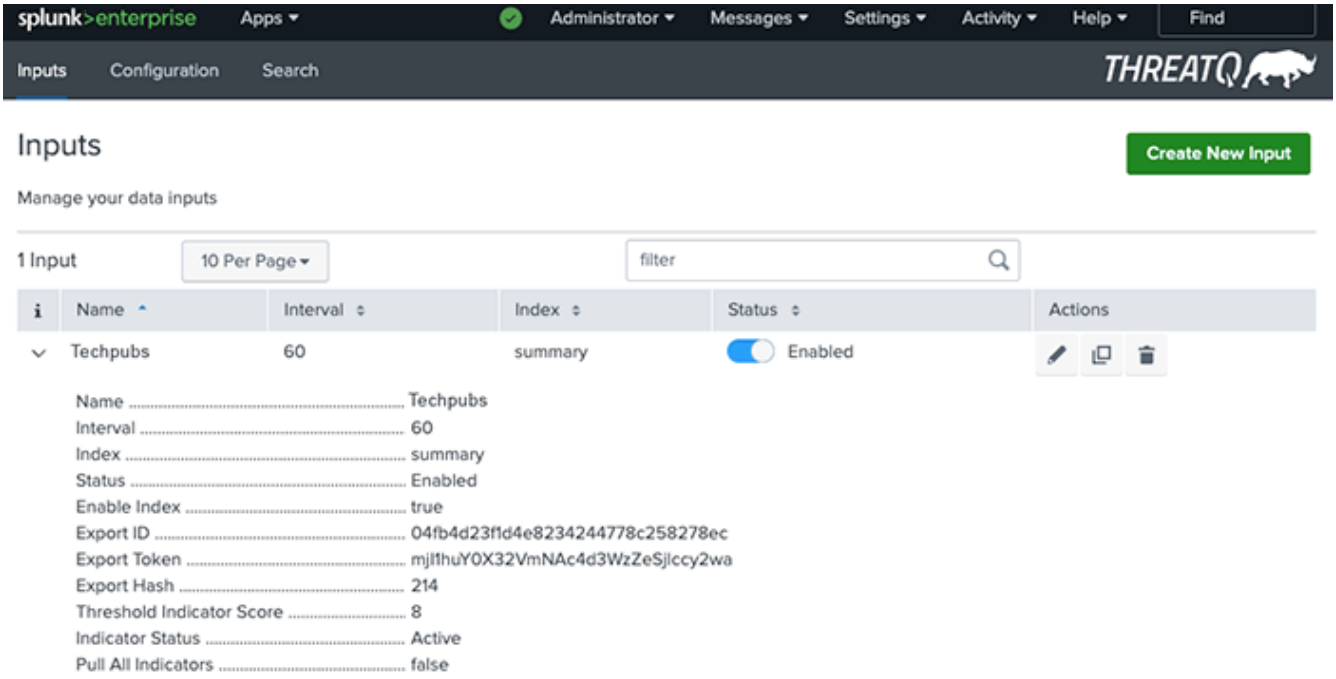
Roles Required to View: Admin, Splunk_System_Role, User, ess_user, ess_analyst, ess_admin.
Roles Required To Create/Modify: Admin, Splunk_System_Role, ess_admin.

The Inputs tab on ThreatQ Add-On for Splunk allows you to configure what data is being received from ThreatQ exports in the form of Inputs.

You can access this page by clicking on the Inputs option in the top navigation menu. From this page, you can create, view, edit, clone, and delete inputs for the application.



You can click on the arrow next to an existing input to view its summary.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Inputs
Configuration
Search
THREATQ
Inputs
Create New Input
Manage your data inputs
1 Input
10 Per Page
filter
Name
Interval
Index
Status
Actions
Techpubs
60
summary
Enabled
Name ..... Techpubs
Interval 60
Index ..... summary
Status ..... Enabled
Enable Index ..... true
Export ID 04fb4d23f1d4e8234244778c258278ec
Export Token mjl1huY0X32VmNAc4d3WzZeSjlccy2wa
Export Hash 214
Threshold Indicator Score 8
Indicator Status ..... Active
Pull All Indicators ..... false

Creating a New Input

Roles Required: Admin, Splunk_System_Role, ess_admin.

ThreatQ instances, starting with version 4.16.0, are shipped with a default export that this App uses: **Splunk Indicators Export**. You can find this export in ThreatQ by clicking on the **Settings gear icon** and selecting **Exports**.

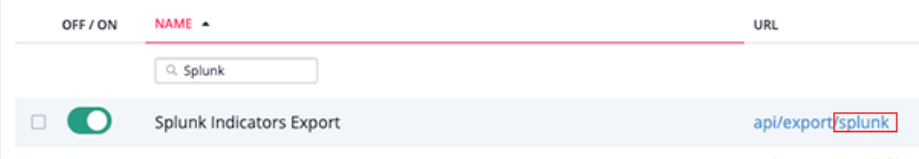
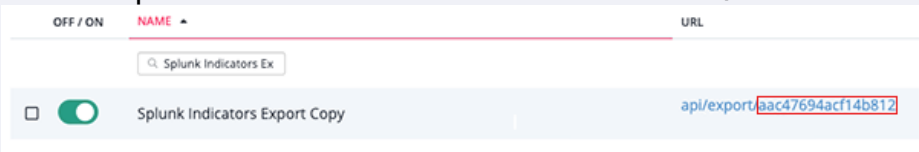
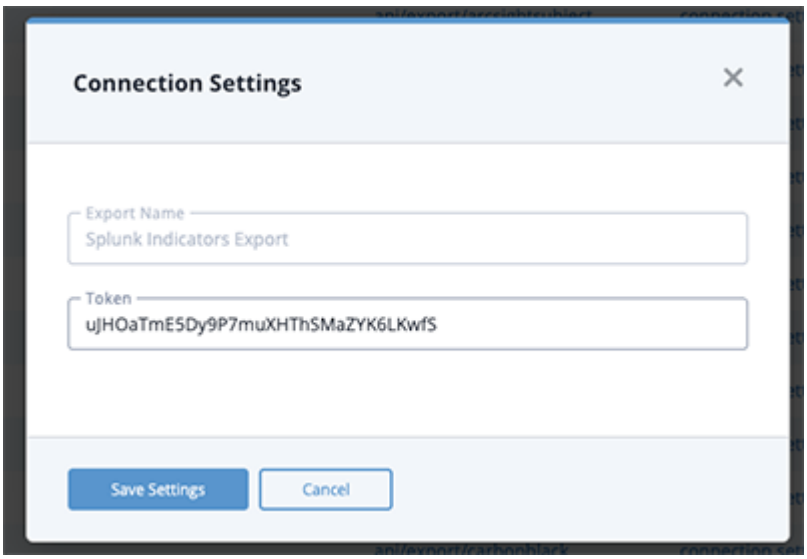
The ThreatQuotient App for Splunk only supports one input.

First execution of this export results in the export of all indicators. Every subsequent run of this export will result in receiving new indicators as well as previously exported indicators that have since changed.

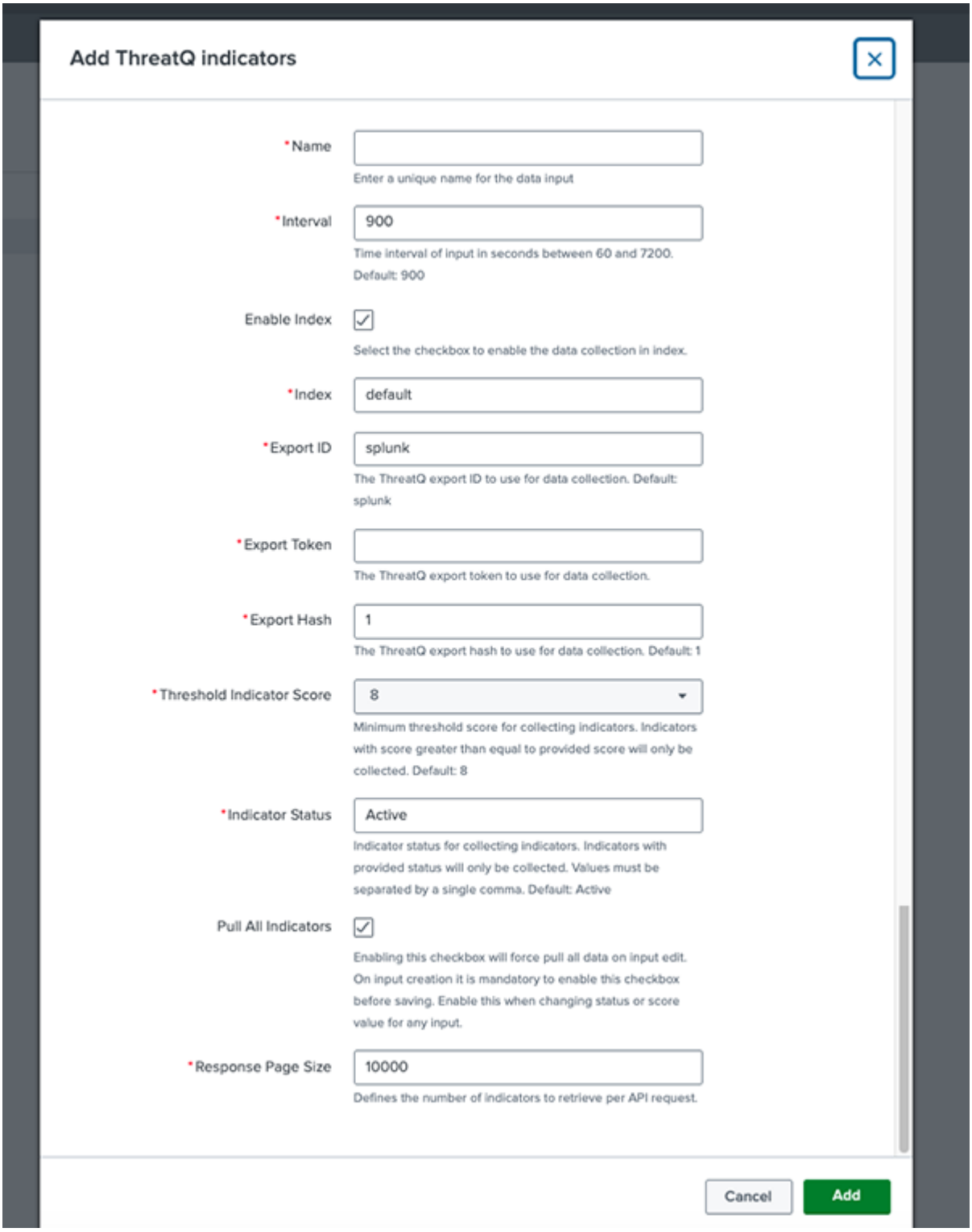
While in the ThreatQ Add-On for Splunk interface:

1. Click on the **Inputs** menu heading.
2. Click on **Create New Input**.
3. Complete the following fields:

PARAMETER	DESCRIPTION
Interval	The frequency of this job. This value can be reduced for faster detection and response. Minimum allowed is 60 seconds.
Enable Index	Enabling this option will result in data being saved to the designated index. Unchecking this option will result in data being saved directly to the KVStore. You must first complete the Splunk KVStore Rest configuration tab before disabling index storage. See the Configuring the KVStore section in the Installing the Add-On Component topic for more details. The Index parameter allows you to map the data extracted from a job in a predetermined Splunk index. You can create multiple jobs and map them to different Splunk indexes as needed.

PARAMETER	DESCRIPTION
Index	Select from available indexes in the system. This is the Splunk index that you can optionally store data to.
Export ID	The Export ID is the final segment of the export's URL. The default ID in the Splunk Indicators Export seeded with the ThreatQ platform is **splunk**. As such, the default value in the Inputs form is **splunk.**  If you make a copy of the export, you must configure the ID of the export in this field as seen on the ThreatQ instance. 
Export Token	Enter the ThreatQ Splunk Indicator Export's Token in this field. The Export Token is located under the export's **Connection Settings** modal in ThreatQ. 
Export Hash	Defaults to 1. In the event you want to re-export all indicators from ThreatQ for any reason (such as installing a new Splunk instance), use this configuration. You can

PARAMETER	DESCRIPTION
	configure a different alphanumeric value of length up to 32 and cause exporting all indicators from ThreatQuotient again. If you need to re-pull all data after initial configuration, select the Pull All Indicators checkbox and then click Update.
Threshold Indicator Score	Any indicator below this score is not indexed in Splunk. This threshold is very useful to reduce the data being indexed in the ThreatQuotient App. The default value is 8.
Indicator Status	Similar to the score threshold, any indicator not matching the status configured here is not indexed in Splunk. This technique is useful for reducing indexed data. The default values are **Active**.
Pull All Indicators	Enabling this checkbox will force pull all data on input edit. Initial import of ThreatQ data will now be performed using the pagination feature which imports a maximum of 10,000 records at once - see the Pagination Support topic for more details. The checkbox must be selected, upon input creation, before saving. This option should be utilized when changing the status or score of any input.
Response Page Size	Define the number of indicators to retrieve per API request. The default value is `10000`. Increasing this limit may cause memory exhaustion and result in the exports failing.



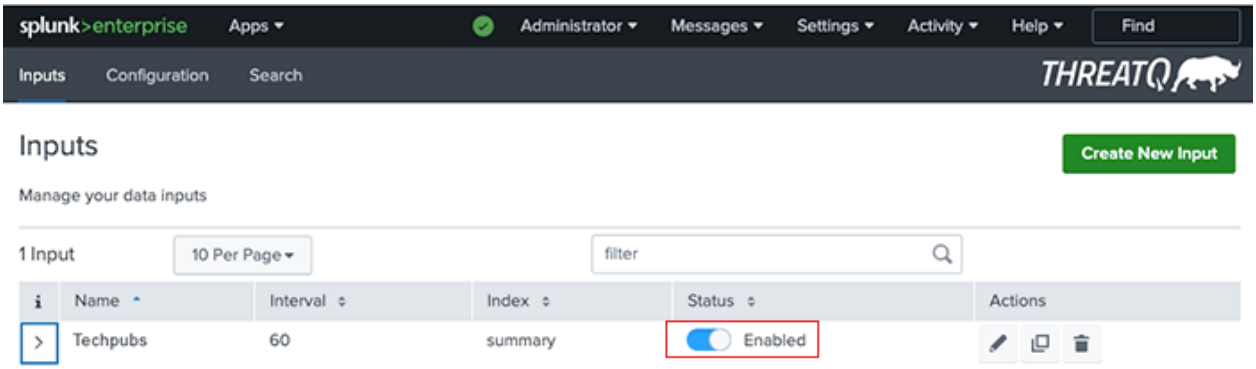
4. Click on **Add**.

Enable/Disable Inputs

Roles Required: Admin, Splunk_System_Role, ess_admin.

You can enable or disable an existing input from the Inputs page.

1. Click on the **Inputs** heading to load the *Inputs* page.
2. Locate the input to enable or disable and click on the toggle switch under the Status column.



Pagination Support

When you create and enable a new input, the initial import of ThreatQ data will be performed using the pagination feature, which imports a maximum of 10,000 records at once.

This is the default behavior whenever a new input is created.

After the initial import is complete, the import will revert to the differential method of pulling data.

The commands below are CLI alternatives to the **Pull All Indicators Input** configuration option when creating a new Input.

ACTION	COMMAND
View the pagination setting for each input	`curl -k -u username:password https://localhost:8089/servicesNS/n obody/TA-threatquotient-add- on/storage/collections/data/TA_ threatquotient_add_on_checkpointer`
Update the pagination setting for an input	`curl -k -u username:password https://localhost:8089/servicesNS/n obody/TA-threatquotient-add- on/storage/collections/data/TA_ threatquotient_add_on_checkpointer/{input_name} -H 'Content-Type: application/json' -d '{"state" : " {\"pull_all_iocs\": true|false}"}'`
Add a pagination setting for an input	`curl -k -u user:password https://localhost:8089/servicesNS/n obody/TA-threatquotient-add- on/storage/collections/data/TA_ threatquotient_add_on_checkpointer -H 'Content-Type: application/json' -d '{"_key":`

ACTION	COMMAND
	`"<input_name>", "state" : "{\"pull_all_iocs\": <true|false>}"}'`
Delete the pagination setting for an input	`curl -k -u username:password -X DELETE https://localhost:8089/servicesNS/n obody/TA-threatquotient-add- on/storage/collections/data/TA_ threatquotient_add_on_checkpointer/{input_name}`

Whenever a new input is created, the pagination setting (`pull_ all_iocs`) will default to true and will be automatically set to false after the initial import is completed.

Known Limitations

- **Score and Status Changes** - reducing the set of indicators in Splunk comes at the expense of inability to detect change of scores and/or statuses in indicators. ThreatQuotient recommends that users use the "Whitelisted" status in ThreatQ to mark indicators as false positives rather than reducing the indicator score or using custom statuses.
- **Advanced Filters** - if you want to use advanced filters (such as adversaries, attributes or sources) to export only a subset of indicators from ThreatQuotient to Splunk, there are two ways to do it:
  1. Duplicate the default export and configure advanced filters. On the Splunk Add-On App, configuring the scoring filter in such a way that all indicators are accepted (i.e. value of 0).
  2. Configure a scoring policy to influence indicator scores on certain adversaries, sources or attributes only. On the Splunk Add-On App, configure the scoring filter to accept only certain scores (i.e. value >= 8 for example).
- **Exporting Large Number of Indicators** - it is not recommended that you export an exceptionally large number of indicators from ThreatQ to Splunk. ThreatQuotient recommends that at any one time, users export no more than 500K indicators. If this limit is not observed, you may encounter problems including loading the data to Splunk, and assuming the data was loaded correctly anyway, with the performance of your Splunk deployment itself.

  > If there is a need to re-import the data from ThreatQ, revert the pagination setting for the input to True. This will ensure that the data is imported in batches of 10,000 records at a time.

  The default export shipped with the ThreatQ appliance does not apply any filters on the indicators to restrict the set of data being exported. However, you may make a copy of this export and specify any additional filters under Special Parameters. An example is shown in the picture below in which a user has configured a filter with score > 5.

Sightings and Feedback

Sightings and Feedback

The following section details how the application identifies and reports sightings to ThreatQ.

About Sightings and Feedback

One of the primary features of this application is to identify sightings and report them back to ThreatQ.

Sighting in this context is defined as evidence that a ThreatQ Indicator was discovered in one or more of the events in Splunk collected via other sources. Recording these sightings and reporting them back to ThreatQ provides analysts with important context around indicators included in their threat intelligence holdings.

The following steps summarize how indicators are stored in Splunk and how sightings are reported back to ThreatQ.

1. The Input job configured on **ThreatQuotient Add-on** pulls indicators from ThreatQ.
2. The Add-On sends the indicators to the indexer which indexes the indicators to the **default** index (user can override) or KVStore.

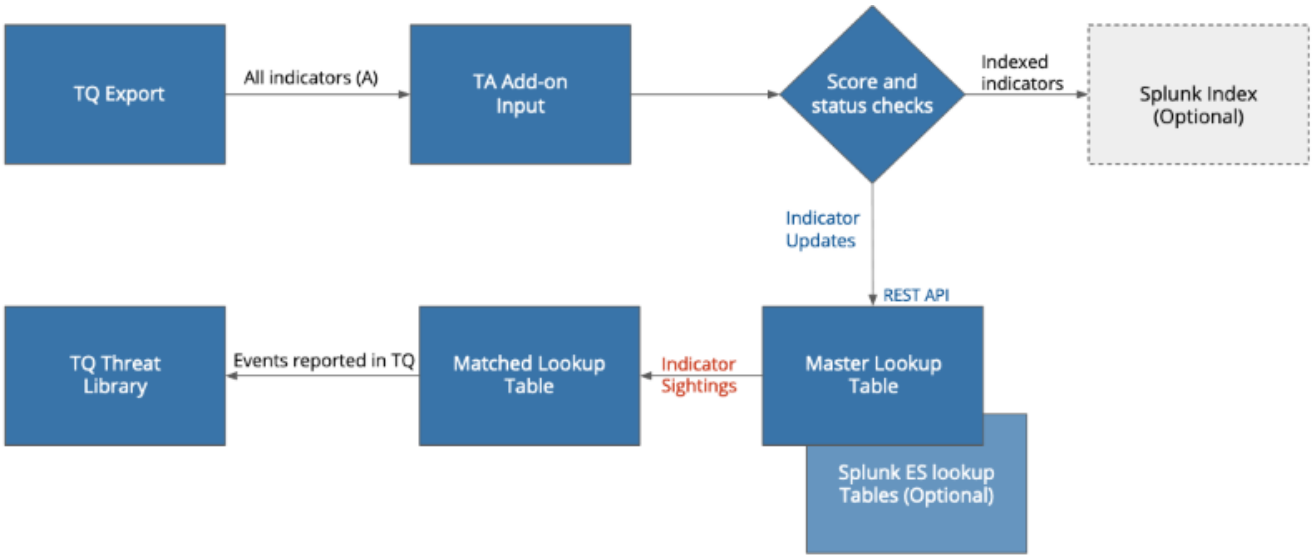
   > You can configure how data is saved, to the designed index or KVStore, via the Enable Index checkbox on the Add ThreatQ Indicators form. See the Creating a New Input section of this guide for more details.

3. The periodic saved search job `threatq_match_indicators` finds evidence of sightings of all indicators in the **master lookup table** against all events in Splunk (as filtered via various configurable macros described above in this section).

   > If evidence of sightings is found for a specific indicator, it is moved to the **match lookup table**.

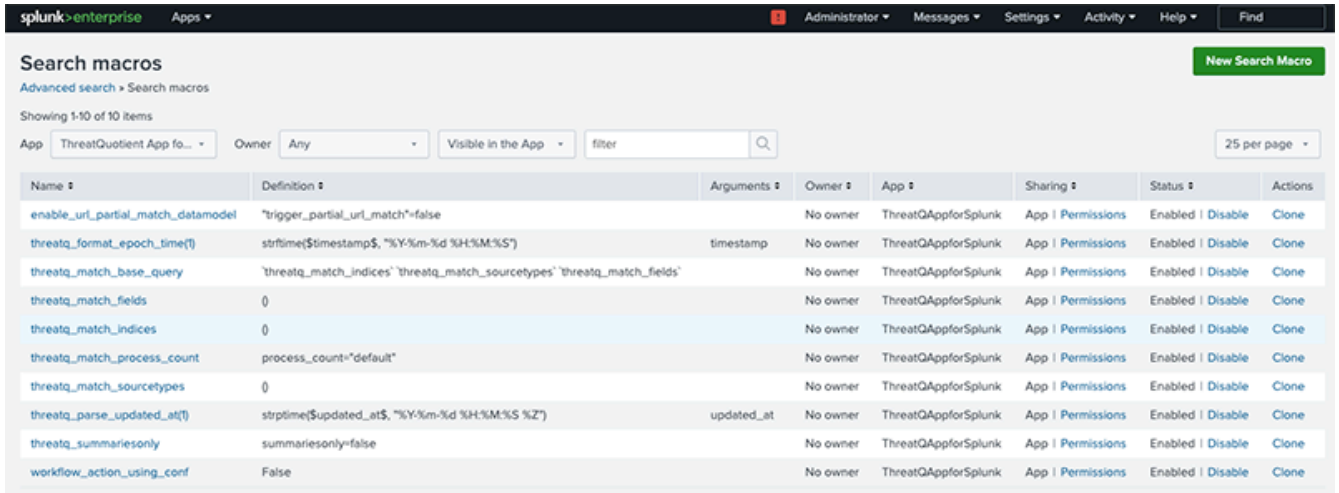
4. Simultaneously, another periodic saved search job `threatq_update_matched_indicators` finds more sightings for all indicators from the match lookup table against all events in Splunk (as filtered by the same configurable macros).
5. A periodic saved search `threatq_consume_indicators` will create events in ThreatQ to represent evidence of sightings in Splunk.

6. The periodic saved search job `threatq_update_retired_indicators` takes all indicators that are not updated in the past 90 days out of both the master lookup table and matched lookup table.



Macros

The following macros are used in most of the saved searches this App is configured with (available under Settings > Advanced Search > Search Macros).



Name	Definition	Arguments	Owner	App	Sharing	Status	Actions
enable_url_partial_match_datamodel	"trigger_partial_url_match"=false		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_format_epoch_time(1)	strftime($timestamp$, "%Y-%m-%d %H:%M:%S")	timestamp	No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_match_base_query	`threatq_match_indices` `threatq_match_sourcetypes` `threatq_match_fields`		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_match_fields	()		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_match_indices	()		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_match_process_count	process_count="default"		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_match_sourcetypes	()		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_parse_updated_at(1)	strptime($updated_at$, "%Y-%m-%d %H:%M:%S %Z")	updated_at	No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
threatq_summariesonly	summariesonly=false		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone
workflow_action_using_conf	False		No owner	ThreatQAppforSplunk	App | Permissions	Enabled | Disable	Clone

The description of some of these search macros is provided below.

SAVED SEARCH MACRO	DESCRIPTION
threatq_index	Configures the name of the Splunk index that all ThreatQ indicators are mapped to.
threatq_match_indices	Configures which Splunk indices are considered for matching. The users can apply more specific filters here.
threatq_match_sourcetypes	Configures which sourcetypes should be **excluded** from matching (the sourcetype **threatq:indicators** is automatically excluded).
threatq_match_process_count	Determines the number of cpu cores utilized for processing the saved searches that are responsible for finding evidence of sightings.
enable_url_partial_match_ datamodel	Configures partial URL indicator matching for the **Datamodel**. The default setting is **False**. This macro should be set to **True** if URL indicators are sent to Splunk with a scheme. EX http://, https://
threatq_match_base_query	Allows you to alter the base query used for matching. Sub macros included are: • threatq_match_indices • threatq_match_sourcetypes • threatq_match_fields
threatq_match_fields	Allows you to match based on specific fields.

Saved Searches

The Splunk App uses saved searches for discovering sightings and reporting them back to ThreatQ. The App is preconfigured with saved searches, which are periodic processes (registered to the crontab) designed to map indicators to specific Splunk indices and match these indicators to events. Saved search processes also move older indicators out of the main lookup tables and for ES customers, move indicators to specific ES lookup tables according to the mapping described in this document.

The table below describes some of the saved searches with which this App is preconfigured. This table displays two searches applicable only for Raw Matching Mode. Equivalent searches are available for each data model in the Datamodel Matching Mode.

> ThreatQuotient does not recommend setting the frequency to less than 30 minutes, the application default for `threatq_match_ indicator` saved searches, if using the configuration option for creating multiple events for each sighted indicator.

SAVED SEARCH	DESCRIPTION	DEFAULT PERIOD
`threatq_consume_ indicators_new`	Post matched indicators to the consume endpoint of ThreatQ and create atomic events. This search will only be enabled if using the "Create multiple events for each sighted indicator" configuration.	30 minutes
`threatq_match_ indicators (Raw Matching Mode only)`	Finds evidence of sightings for all indicators in the master lookup table. If sightings are detected, indicators are moved to the match lookup table.	30 minutes
`threatq_match indicators`	Finds evidence of sightings for all indicators in the match lookup table.	30 minutes
`threatq_update_ matched_indicators`	Finds evidence of sightings for all indicators in the match lookup table.	30 minutes

SAVED SEARCH	DESCRIPTION	DEFAULT PERIOD
`threatq_consume_ indicators`	Creates events in ThreatQ for all newly detected sightings.	15 minutes
`threatq_update_ retired_indicators`	Clean up indicators that haven't been updated in the last 90 days from both master lookup table and match lookup table.	1,440 minutes

Edibility Rules: Because of the way sightings are found in Splunk using two saved searches (threatq_match_indicators and threatq_update_ matched_indicators), their frequency must be the same if edited. The default frequency for both saved searches is 30 minutes.

Saved Search Macros

The following table documents the macros for saved searches as configured by default on the ThreatQuotient App.

SAVED SEARCH	DEFAULT MACRO
threatq_consume_indicators_new		inputlookup threatq_matched_indicators	eval start_time=relative_time(now(), "-35m")	where match_time > start_time	sort 10000 -num(score), -num(match_count)	threatqconsumeindicatorsnew
threatq_cleanup_indicators_ on_indicators_ change		inputlookup master_lookup	search NOT [search `threatq_index` sourcetype="threatq:indicators"	dedup value	search [	inputlookup master_lookup	table ioc_value	rename ioc_value as value	format] NOT (`threatq_score_filter` `threatq_status_filter`)	table value	rename value as ioc_value	format]	outputlookup master_lookup	join ioc_value [	inputlookup threatq_matched_indicators	table ioc_value, match_time, first_seen, last_seen, match_count, sid]	outputlookup threatq_matched_indicators
threatq_match_indicators (only Raw Matching Mode)	`threatq_match_indices` `threatq_match_sourcetypes` sourcetype!="threatq:indicators"	threatqmatchiocs
threatq_update_matched_ indicators (only Raw Matching Mode)	`threatq_match_indices` `threatq_match_sourcetypes` sourcetype!="threatq:indicators"	threatqmatchiocs is_update=true
threatq_consume_indicators		inputlookup threatq_matched_indicators	eval start_time=relative_time(now(), "-16m")	where last_seen > start_time	threatqconsumeindicators
threatq_update_retired_ indicators		inputlookup master_lookup	search NOT [| inputlookup master_lookup	search NOT [| inputlookup threatq_matched_indicators	search NOT [| inputlookup threatq_matched_indicators	eval threshold_time=now()-7776000, value=ioc_value	where last_seen < threshold_time	outputlookup key_field=value threatq_retired_matched_indicators	table ioc_value	format]	outputlookup threatq_matched_indicators	table ioc_value	format]	eval threshold_time=now()-7776000, updated_at_epoch=`threatq_parse_updated_at(updated_at)`, value=ioc_value	where updated_at_epoch < threshold_time	outputlookup key_field=value threatq_retired_indicators	table ioc_value	format]	outputlookup master_lookup

As described above, two of the saved searches are applicable only for the Raw Matching Mode. If you select **Datamodel Matching Mode** from the configuration as described in the Configuration section in the Installing the App Component topic, the above two saved searches for **Raw Matching Mode** will disable automatically, and the equivalent saved searches for the **Datamodel Matching Mode** will be enabled.

Separation of Data

ThreatQ indicator data is separated from the rest of the data in this App using a specific sourcetype. You can use the following Splunk search query to discover all indicators exported from ThreatQuotient.

Splunk Search for Listing TQ Indicators

`sourcetype="threatq:indicators"`

The same indicator can be exported multiple times if it experienced a change of status and/or score.

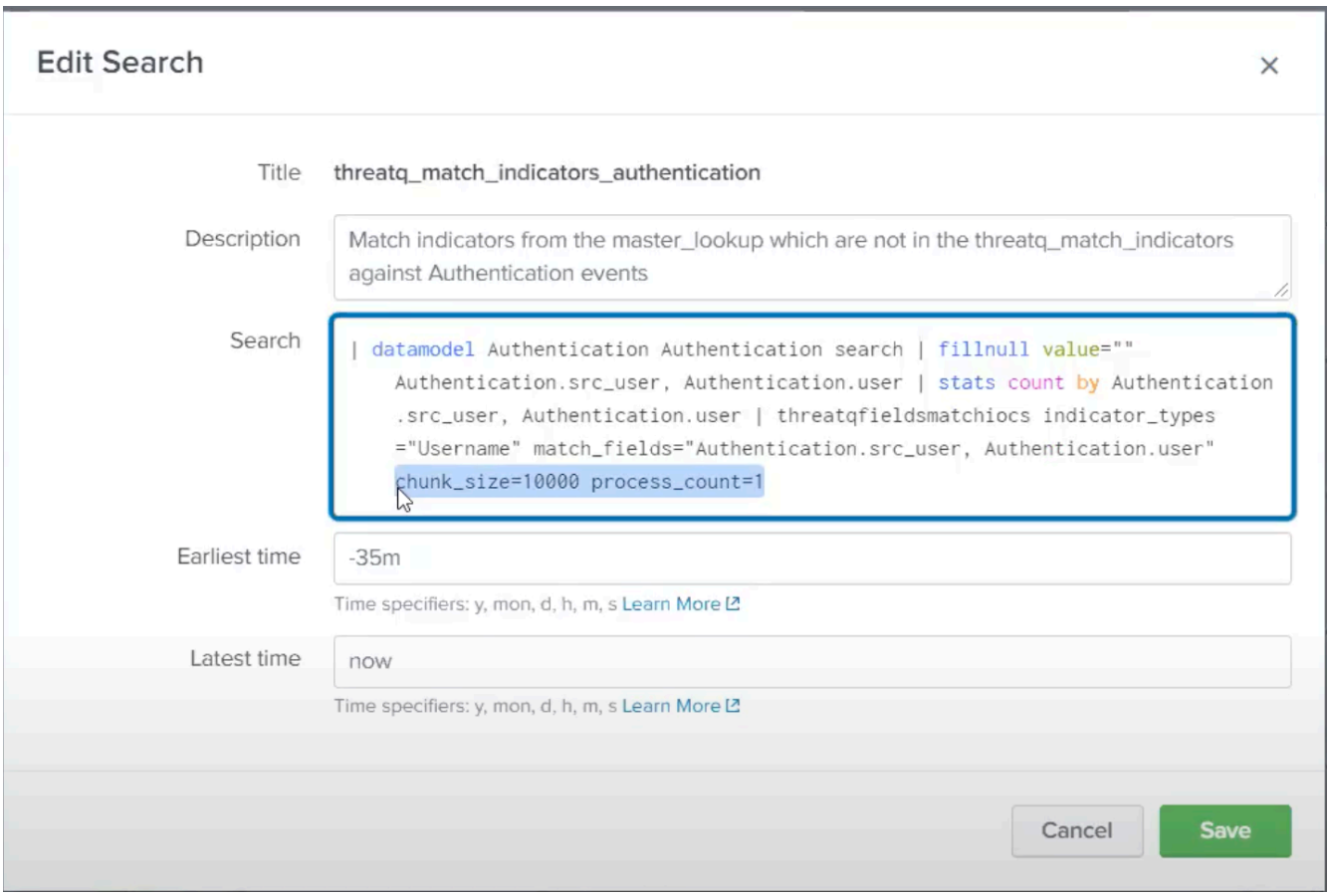
Chunking

You can apply chunking to your datamodel searches using the following option:

`chunk_size=<value>`

Default chunk size is 50,000.

Example



CIM Model Matching

The ThreatQuotient App for Splunk runs in the Datamodel Search mode when you are taking advantage of Splunk's CIM and mapping your logs and events to various data models provided by Splunk.

The following table summarizes how the matching algorithm will match specific data model fields to specific indicator types in ThreatQuotient.

ThreatQ indicator type to CIM field map for the matching algorithm

CIM DATA MODELS	DATA MODEL FIELDS	THREA INDICA TYP MATC
Authentication	Authentication.src_user	Userna
	Authentication.user	Userna
Certificates	Certificates.All_Certificates.SSL.ssl_hash	SHA-1, SHA-25 SHA-38 SHA- 5
	Certificates.All_Certificates.SSL.ssl_issuer_email	Email Addres
	Certificates.All_Certificates.SSL.ssl_subject_ email	Email Addres
	Certificates.All_Certificates.SSL.ssl_subject_ common_name	String
	Certificates.All_Certificates.SSL.ssl_issuer_common_name	String
	Certificates.All_Certificates.SSL.ssl_subject_ organization	String
	Certificates.All_Certificates.SSL.ssl_issuer_ organization	String

CIM DATA MODELS	DATA MODEL FIELDS	THREA INDICA TYP MATC
	Certificates.All_Certificates.SSL.ssl_serial	String
	Certificates.All_Certificates.SSL.ssl_subject_ unit	String
	Certificates.All_Certificates.SSL.ssl_issuer_unit	String
Endpoint	Endpoint.Services.service	Service Name
	Endpoint.Processes.process_name	Service Name
	Endpoint.Filesystem.file_name	Filenan
	Endpoint.Filesystem.file_hash	SHA-1, SHA-2 SHA-3 SHA-5
Email	Email.All_Email.file_name	Filenan
	Email.All_Email.file_hash	SHA-1, SHA-2 SHA-3 SHA-5
	Email.All_Email.subject	Email Subjec
	Email.All_Email.src_user	Email Addres

CIM DATA MODELS	DATA MODEL FIELDS	THREA INDICA TYP MATC
Intrusion_Detection	Intrusion_Detection.IDS_Attacks.src	IP Addr IPv6 Addres
	Intrusion_Detection.IDS_Attacks.signature	String
	Intrusion_Detection.IDS_Attacks.user	Userna
Inventory	All_Inventory.User.user	Userna
Malware	Malware.Malware_Attacks.file_name	Filenam
	Malware.Malware_Attacks.file_hash	SHA-1, SHA-25 SHA-38 SHA- 5
	Malware.Malware_Attacks.signature	String
	Malware.Malware_Attacks.sender	Email Addres
	Malware.Malware_Attacks.src	IP Addr IPv6 Addres
	Malware.Malware_Attacks.user	Userna
Network_Traffic	Network_Traffic.All_Traffic.src	IP Addr IPv6 Addres

CIM DATA MODELS	DATA MODEL FIELDS	THREA INDICA TYP MATC
Network Resolution (DNS)	Network_Resolution.DNS.query	FQDN, String
	Network_Resolution.DNS.answer	FQDN, String
Updates	Updates.Updates.file_name	Filenan
	Updates.Updates.file_hash	SHA-1, SHA-25 SHA-38 SHA- 5
Web	Web.Web.user	Userna
	Web.Web.http_referrer	URL
	Web.Web.url	URL
	Web.Web.http_user_agent	User-a
	Web.Web.src	IP Addr IPv6 Addres
	Web.Web.dest	IP Addr IPv6 Addres
Incident_Management	Incident_Management.Notable_Events.src	IP Addr IPv6 Addres

CIM DATA MODELS	DATA MODEL FIELDS	THREA INDICA TYP MATC
	Incident_Management.Suppressed_Notable_ Events.src	IP Addr IPv6 Addres
	Incident_Management.Notable_Event_Suppressions. Suppression_Audit.signature	String
	Incident_Management.Notable_Event_Suppressions. Suppression_Audit_Expired.signature	String
	Incident_Management.Notable_Event_Suppressions. Suppression_Audit.user	Userna

Enterprise Security Matching

Splunk's Enterprise Security App provides the means of using your threat intelligence data to match against events mapped to standard Splunk models. Refer to the Splunk's documentation on **Enterprise Security Workflow for Threat Intelligence** as described here: http://dev.splunk.com/view/enterprise-security/SP-CAAAFBC.

ThreatQuotient provides mapping of the threat intelligence data to the standard lookup tables in Splunk Enterprise Security via the saved searches described above. Using the default Threat Generation Searches in Enterprise Security, the ES app will find matches and report those matches in the `threat_activity` index as described in the link above.

Threat Intelligence data will be added to Enterprise Security using their REST APIs with a threat_key of `threatq_indicator`. The score for ThreatQ Indicators will be mapped to the **Weight** attribute in ES. Any updates to the score will be automatically reflected in ES using the periodic saved searches.

The indicator will be updated in ES and put into a disabled state (will no longer be used in further correlation) if the score or status of a ThreatQ indicator changes to a value that is no longer within the parameters configured in the macro settings for ThreatQ Splunk App.

> When using the Enterprise Security App, you will not have additional context (sources and adversaries), workflow actions ,and reporting sightings back to ThreatQuotient available to you.

ThreatQ Indicators to Splunk Enterprise Security Lookup Tables

The ThreatQuotient App for Splunk provides support to the Splunk Enterprise Security (ES) customers by making ThreatQ data more accessible using Splunk's native ES lookup tables. The following table provides how ThreatQ data is mapped to the Splunk ES lookup tables.

> This data is then available in various ES dashboards.

ThreatQ Indicator Type Mapping to Enterprise Security Lookup Tables

THREATQ TYPE	THREAT INTELLIGENCE TYPE
CIDR Block	local_ip_intel

THREATQ TYPE	THREAT INTELLIGENCE TYPE
Email Address	local_email_intel
Email Subject	local_email_intel
File Name	local_file_intel
FQDN	local_domain_intel
Fuzzy Hash	local_file_intel
GOST Hash	local_file_intel
IP Address	local_ip_intel
MD5	local_file_intel
Registry Key	local_registry_intel
Service Name	local_service_intel
SHA-1	local_file_intel
SHA-256	local_file_intel
SHA-384	local_file_intel
SHA-512	local_file_intel
x509 Serial	local_certificate_intel
x509 Subject	local_certificate_intel
URL	local_http_intel

THREATQ TYPE	THREAT INTELLIGENCE TYPE
URL Path	local_http_intel
Username	local_user_intel

To view the events and indicators, navigate to **Enterprise Security > Security Intelligence > Threat Intelligence**.

- **Threat Activity:** Shows the list of events which are compatible with CIM apps.
- **Threat Artifacts:** Shows the list of indicators fetched from the ThreatQ.

Saved Searches for Enterprise Security

In addition to the core saved searches, the following saved searches apply for Enterprise Security (ES) customers. The saved searches listed run once a day and map ThreatQ indicators by type to Splunk ES lookup tables as described in the ThreatQ Indicators to Splunk Enterprise Security Lookup Tables section in this topic.

By default, the **scheduling** of all saved searches for porting Threat Intelligence data from ThreatQ to lookup tables in the ES are **disabled**. This is because not all users have Enterprise Security App installed. If you have this App installed and want to port the Threat Intelligence data over, you will need to enable the scheduling of these saved searches.

Saved Searches for Mapping ThreatQ Indicator data to Splunk's CIM

ES SAVED SEARCH	DESCRIPTION
threatq_update_threat_intelligence_lookup_email_address	Map ThreatQ **type 4** indicators to **local_email_intel**
threatq_update_threat_intelligence_lookup_email_subject	Map ThreatQ **type 6** indicators to **local_email_intel**
threatq_update_threat_intelligence_lookup_file_name	Map ThreatQ **type 9** indicators to **local_file_intel**
threatq_update_threat_intelligence_lookup_fqdn	Map ThreatQ **type 10** indicators to **local_domain_intel**
threatq_update_threat_intelligence_lookup_hash	Map ThreatQ **type [11,12,15,20,21,22,23]** indicators to **local_file_intel**
threatq_update_threat_intelligence_lookup_ip	Map ThreatQ **type 14** indicators to **local_ip_intel**

ES SAVED SEARCH	DESCRIPTION
threatq_update_threat_intelligence_lookup_registry	Map ThreatQ **type 18** indicators to **local_registry_intel**
threatq_update_threat_intelligence_lookup_service	Map ThreatQ **type 19** indicators to **local_service_intel**
threatq_update_threat_intelligence_lookup_certificate_serial	Map ThreatQ **type 25** indicators to **local_certificate_intel**
threatq_update_threat_intelligence_lookup_certificate_subject	Map ThreatQ **type 26** indicators to **local_certificate_intel**
threatq_update_threat_intelligence_lookup_url	Map ThreatQ **type 27** indicators to **local_http_intel**
threatq_update_threat_intelligence_lookup_user	Map ThreatQ **type 30** indicators to **local_user_intel**

Reporting Sightings in ThreatQ

A sighting in Splunk is evidence that an indicator from ThreatQ was seen in one or more events in Splunk. This is important information for an analyst that can be reported back in the form of an Event.

Single Event for Each Sighted Indicator

ThreatQ captures all sightings for an indicator in a single event. When more sightings are detected for the same indicator, certain attributes for that event are updated. This allows the analyst to gather context on sightings for that indicator.

Multiple Events for Each Sighted Indicator

If multiple sightings for the event are seen during the same time period, all sightings will be captured in a single event. However, if more sightings are seen in the future for the same indicator, a new event will be created in ThreatQ.

See the **Sighting Event Configuration** instructions under the Installing the App Component section (App Configuration tab) for more details.

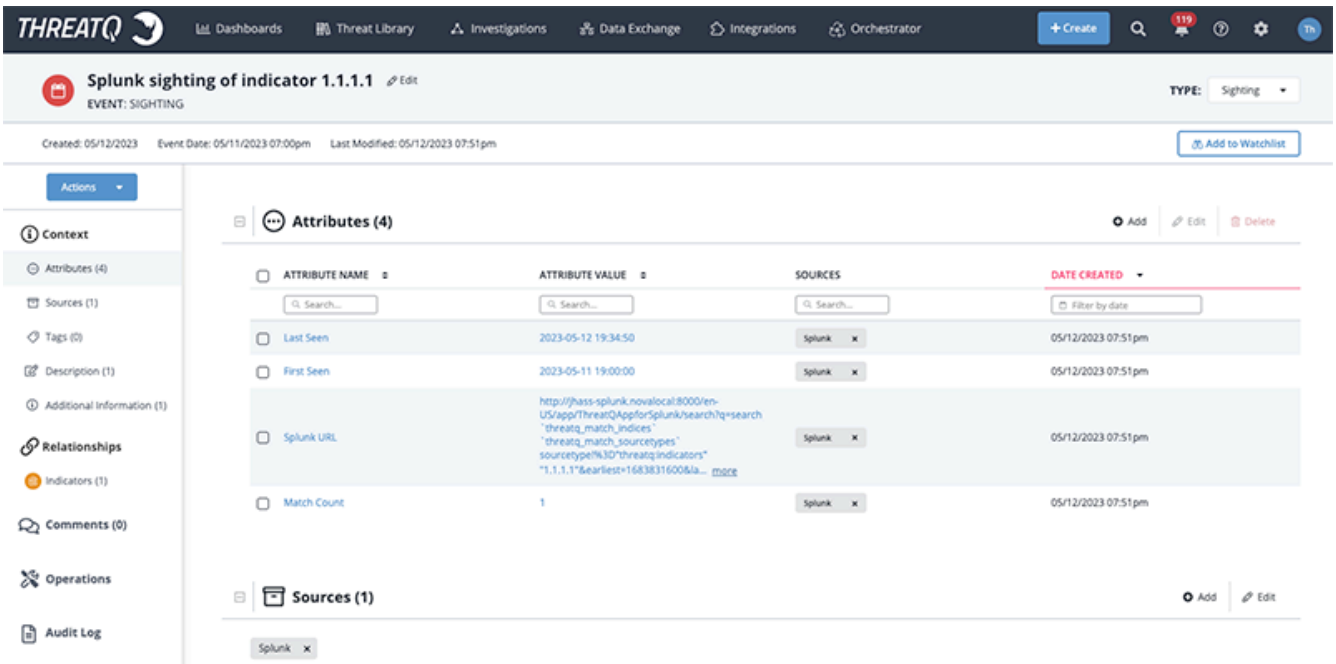
The following attributes are recorded for the event.

ATTRIBUTE	DESCRIPTION
First Seen	Timestamp when the first sighting for this indicator was recorded in Splunk. This attribute does not change.
Last Seen	Timestamp when the latest sighting for this indicator is recorded in Splunk. This attribute updates as newer sightings are detected.
Count	The total count of all sightings recorded for this indicator starting from the time First Seen until Last Seen.
Splunk URL	The URL that allows the analyst to view all sightings for this indicator in Splunk starting from First Seen until Last Seen.
Datamodel Name	The Datamodel name will be included if the matching was performed using a datamodel.

ATTRIBUTE	DESCRIPTION
Splunk Custom Fields	The custom fields matching what is in the Splunk Custom Fields configuration setting will be included.

> The latest matched raw event from Splunk will also be added as the description if the raw matching is enabled and the app is configured to send the latest event to ThreatQ.

The screen capture below shows an example event recorded in ThreatQuotient by the Splunk App.



The following contextual data is added to the indicator:

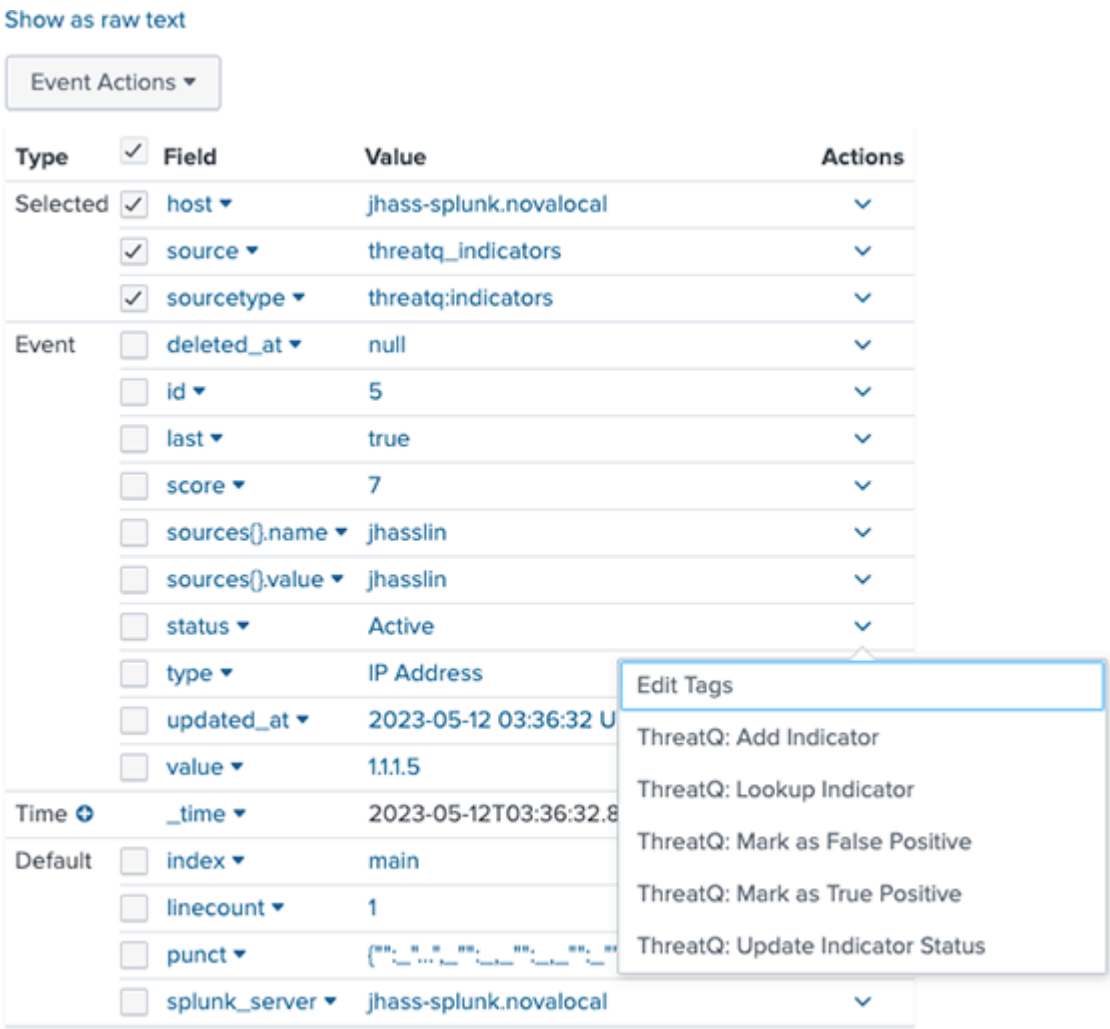
ATTRIBUTE	DESCRIPTION
Splunk Sighting Timestamp	When the latest sighting for this indicator was recorded in Splunk.
Match Count	The total count of all sightings recorded for this indicator.

ATTRIBUTE	DESCRIPTION
Event Count	The last run match count for this indicator.
Source	**Splunk** will be added as the **Source** for this indicator.

Workflow Actions

Roles Required: Admin, Splunk_System_Role, ess_admin.

The **ThreatQuotient App** provides five user workflow actions to the analysts for providing interactivity with the ThreatQuotient platform from Splunk. As shown on the diagram below, the actions can be invoked on any Splunk event by expanding the event view and clicking on the down arrow in the column below **Action**.



The actions are described below.

ACTION	DESCRIPTION

ACTION	DESCRIPTION
ThreatQ: Add Indicator	This workflow action adds the indicator to ThreatQ. You are presented with UI inputs that allow you to select indicator type, status and source. If the data and type do not match, an error is reported. Successful completion of this workflow action results in the indicator being successfully added to the ThreatQ Threat Library.
ThreatQ: Lookup Indicator	This workflow action searches for an indicator in ThreatQ and pulls additional context for that indicator. If the indicator does not exist in ThreatQ, an error is reported.
ThreatQ: Mark as False Positive	This workflow action adds the attribute key-value `False Positive: True` to the indicator in ThreatQ. If the indicator does not exist in ThreatQ, an error is reported.
ThreatQ: Mark as True Positive	This workflow action adds the attribute key-value `True Positive: True` to the indicator in ThreatQ. If the indicator does not exist in ThreatQ, an error is reported.
ThreatQ: Update Indicator Status	This workflow action updates the status of the indicator in ThreatQ. This action supports all statuses, including custom, that exist on the ThreatQ instance. You can view additional information and settings for this action on the application and the add-on by clicking on the **Settings** dropdown and selecting **Alert Actions** under the Knowledge heading. You can review and edit sharing permissions, action status, usage, and view log events.

Performing Workflow Actions by Non-Admin Users

Users can perform workflow actions from Splunk to ThreatQuotient without admin capability by performing following steps.

1. Navigate to **Settings > Advance search > Search macros**.
2. Apply the app filter to **ThreatQuotient Add-on for Splunk**.

3. Edit the **workflow_action_using_conf** macro and set it to **True**.
4. Go to the backend and create the **credentials_storage.conf** in the local folder.

   If local folder is not available then create new folder and name it to "local"

5. Now provide the below information in the **credentials_storage.conf** file:

```
sample of credentials_storage.conf:
[credentials]
username = <username>
password = <password>
server_url = <server_url>
threatq_splunk_url  = < threatq_splunk_url >
client_id = < client_id>
[proxy_credentials]
proxy_enabled = <boolean>
proxy_password = <proxy_password>
proxy_port = <proxy_port>
proxy_type = <proxy_type>
proxy_url = <proxy_url>
proxy_username = <proxy_username>
```

6. Restart Splunk.

Scaling the App

The primary objective of this App is to find evidence of sightings and report those sightings back to ThreatQ. The sightings are discovered using the **matching algorithm** that works either in the **Raw Matching** or **Datamodel Matching** mode, which will take a set of indicators from ThreatQ, a set of events from Splunk, and find which indicators (and how many times) appear in the events.

The best way to scale the App is to run multiple saved searches for matching. This section details performance testing results that supports this recommendation and how to implement this scaling based on your matching preferences.

Performance Testing

Performance testing was conducted to determine how many Splunk Events the application can handle with the default configuration.

The matching algorithm, by default, runs every 30 minutes in a saved search, so it is important that it **completes in under 30 minutes on average** just to keep up with incoming load.

Datamodel Matching Mode

Test Environment: Dedicated Box with 16 cores and 32GB of ram.

Test Summary Result: The limit is 15 million events per 30 minutes per single saved search.

Recommendation: Users should utilize multiple searches using the **datamodel matching** mode. If your data is mapped to multiple Splunk data models from the CIM Support table, each data model is handled by a separate saved search. In such an instance, you would need to deploy your search head in a cluster and ensure that these saved searches are distributed in that cluster. You can run up to five of them, thus potentially scaling your App to handle five times the traffic.

Test Details: The table provided below illustrates that testing determined that the algorithm runtime started to exceed the 30 minute mark with 15 million Splunk events. **Thus, for a single saved search, this represents the upper limit of how much data this algorithm can handle every 30 minutes**.

TOTAL INDICATORS FROM TQ	TOTAL RAW EVENTS IN SPLUNK	TOTAL INDICATORS MATCHED	TIME TO COMPLETE (S) MACHINE SPECS: (16 CORE, 32GB RAM)
100,000	500,000	0	29.282
100,000	500,000	10,000	36.92
100,000	1,000,000	20,000	77.649
500,000	1,000,000	0	99.473
500,000	1,000,000	10,000	130.991
1,000,000	1,000,000	0	166.517
1,000,000	1,000,000	25,000	261.362
1,000,000	5,000,000	0	420.111
100,000	5,000,000	10,000	619.047
1,000,000	10,000,000	10,000	1,316.541
1,000,000	**15,000,000**	**10,000**	**1,866.059**
1,000,000	50,000,000	25,000	6,554.610

Raw Matching Mode

Test Environment: Dedicated Box with 16 cores and 32GB of ram.

Test Summary Result: The limit is 1 million events per 30 minutes per separate saved search.

Recommendation: For the raw matching mode, the App by default will only be able to run one saved search. In order to extend it to multiple searches, you will have to break apart this one saved search into multiple, and then, distribute these saved searches in the Splunk cluster of search heads. You can do this by running a separate saved search for:

- Splunk index for events
- ThreatQuotient indicator types

For using a fixed Splunk index for the saved search, you can modify the default saved searches for matching as shown below.

Splunk Search for Listing TQ Indicators

```
index=<my_index> `threatq_match_sourcetypes` source- type!="threatq:indicators" |
threatqmatchiocs indicator_types- ='IP Address, FQDN'(threatq_match_indicators saved
search) index=<my_index> `threatq_match_sourcetypes` source- type!
="threatq:indicators" | threatqmatchiocs is_update=true
(threatq_update_matched_indicators saved search)
```

Compare the above saved searches with the defaults as shown in the Save Search Documentation table. The macro `threatq_match_indices` is replaced by passing an actual index to the saved search. Now, you can make multiple copies of the default saved search, run them on the same schedule, and have each saved search get events from a different Splunk index.

To use the similar technique for ThreatQuotient indicator types, you can pass an additional argument to the `threatqmatchiocs` module as shown below. This allows you to make the saved search use only a specific indicator type. Again, as before, you can then make multiple copies of the saved searches and have each one handle only specific ThreatQuotient indicator types. You are free to pass a single indicator type, or a comma separated list as shown below.

Splunk Search for Listing TQ Indicators

```
index=<my_index> `threatq_match_sourcetypes` source- type!
="threatq:indicators" | threatqmatchiocs indicator_types- ='IP
Address, FQDN'(threatq_match_indicators saved search)
index=<my_index> `threatq_match_sourcetypes` source- type!
="threatq:indicators" | threatqmatchiocs is_update=true
indicator_types='IP Address, FQDN'(threatq_update_matched_ indicators
saved search)
```

Test Details: The table provided below illustrates that testing determined that the algorithm runtime started to exceed the 30 minute mark with 1 million Splunk events. **Thus, for a single saved search, this represents the upper limit of how much data this algorithm can handle every 30 minutes**.

TOTAL INDICATORS FROM TQ	TOTAL RAW EVENTS IN SPLUNK	TOTAL INDICATORS MATCHED	TIME TO COMPLETE (S) MACHINE SPECS: (16 CORE, 32GB RAM)
100,000	500,000	0	885.36
100,000	500,000	10,000	899.75
100,000	**1,000,000**	**20,000**	**1,932.04**
500,000	**1,000,000**	**0**	**1,926.62**
500,000	**1,000,000**	**10,000**	**2,020.56**
1,000,000	1,000,000	0	2,174.18
1,000,000	1,000,000	25,000	2,294.39
1,000,000	5,000,000	0	11,354.64
10,000	50,000,000	0	35,233.185 (9 hr 47 min)

Dashboards

Threat Dashboards

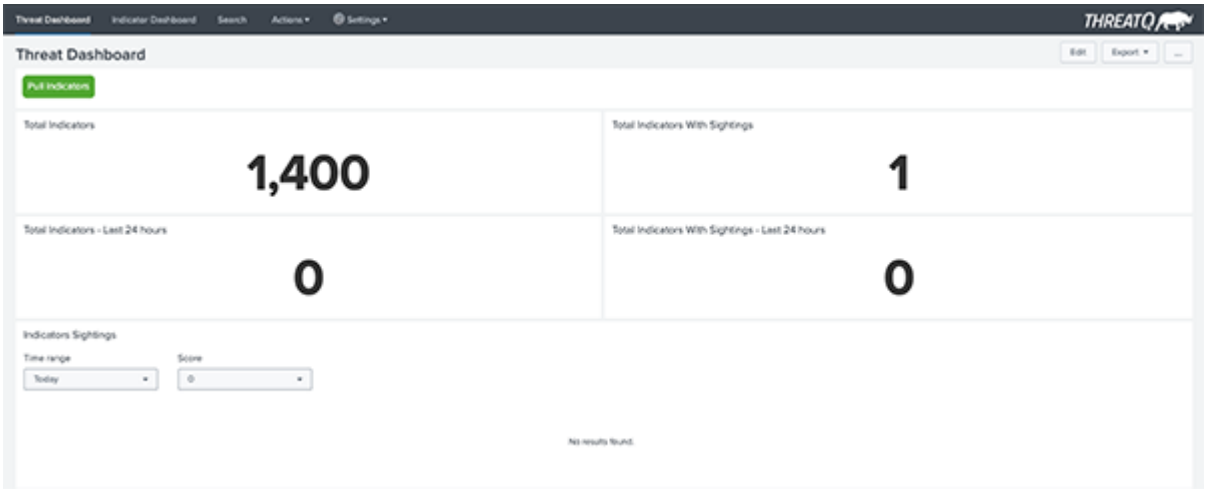
Roles Required: Admin, Power, Splunk_System_Role, User, can_delete, ess_user, ess_analyst, ess_admin.

The Threat Dashboard displays indicator sighting-related information such as:

- Cumulative Counts
- Score Breakdown
- Type Breakdown
- Source Breakdown
- Adversaries Breakdown
- Static Table View
- Top 10 By Sightings
- Indicators Malware Family Distribution
- Indicators with Sightings Malware Family Distribution

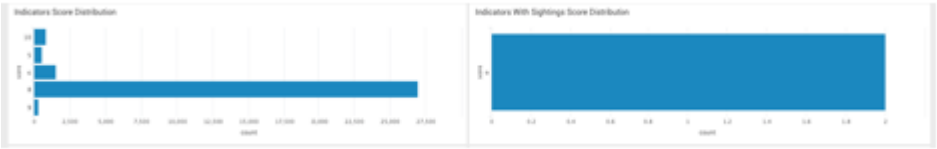
Cumulative Counts

The top section of the dashboard shows total count for all ThreatQ indicators in the **master lookup table** (on the left) and the **match lookup table** (in the right) (all time and the last 24 hours). It is important to note that the data displayed as Sightings are not the total sightings; rather it is the total number of indicators for which evidence of sightings has been found. Example screen capture below.



Score Breakdown

The next section shows the distribution of indicator scores for indicators in master and match lookup tables as bar charts. Example screenshot below. These charts do not have a time filter. The counts for individual score breakdown represent the cumulative indicator count. As an example, notice that there are two indicators with sightings each with score 9 (which matches up with the cumulative sightings count of 2 in the chart above).



Type Breakdown

This section shows the distribution of indicator types for indicators in master and match lookup tables as pie charts. As the score distributions above, these are cumulative distributions. Example screenshot below. Hovering over each portion of the pie chart will display the indicator count for that specific portion.

Source Breakdown

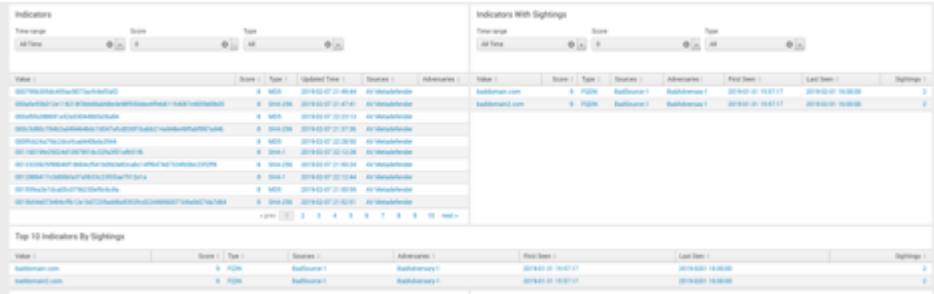
This section shows the breakdown of indicators and sighted indicators by sources. Example screenshot below. One thing to note here is that all indicators must have at least one source, but some indicators may have more than one. For this reason, the cumulative counts in the charts below may exceed the total number of indicators and sighted indicators in the lookup tables.

Adversaries Breakdown

This section shows the breakdown of indicators and sighted indicators by adversaries. Example screenshot below. One thing to note here is that not all indicators have adversaries; although some indicators may have more than one. Depending upon how many indicators have adversaries, the total cumulative counts in the charts below may be less or more than the total indicators and sighted indicators in the lookup tables. For the example dataset below, there is only one adversary assigned to a few indicators, and those same indicators are sighted.

Static View Table

This section shows all indicators and sightings in static tables - time filters are provided and defaulted to the last 24 hours. Score and type filters are also available for both. This information gives a threat analyst a single place to view all sightings in Splunk. In the screenshot below, notice there are two indicators sighted, each with 2 sightings.

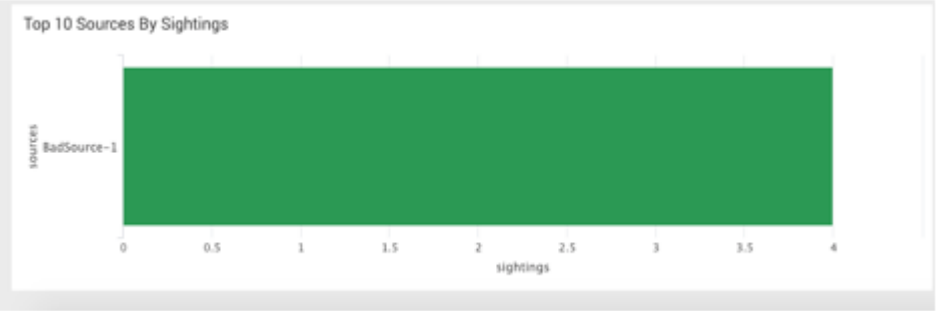


Top 10 By Sightings

The final section displays top 10 indicators by sightings, top 10 sources by sightings and top 10 adversaries by sightings in the form of a static table, bar chart and bar chart respectively. This information gives an analyst a quick view of the indicator's sources and adversaries with the most matches within Splunk.

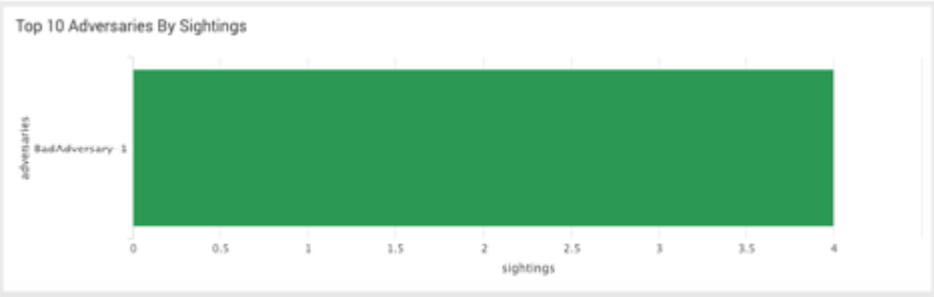
Sources

Example screenshot below. Notice the source BadSource-1 appears as the top source with sightings corresponding to the sighted indicators as displayed in the static table above. Also notice that the sightings count is 4, which corresponds to 2 sightings each for the sighted indicators.



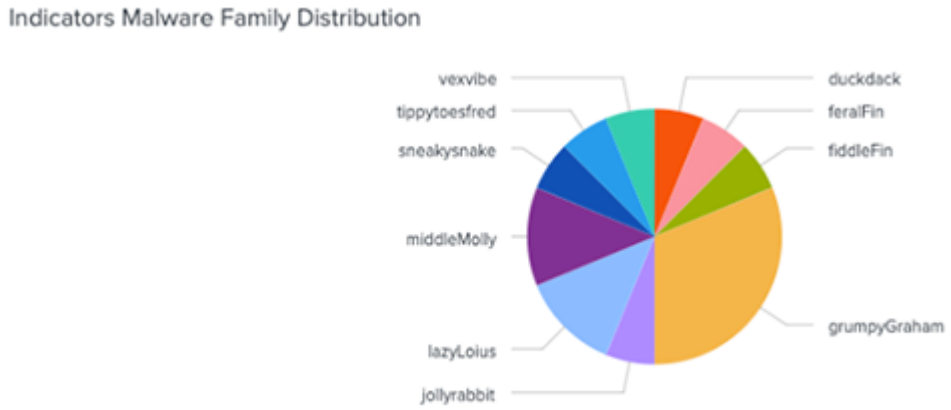
Adversaries

Example screenshot below. Notice the source **BadAdversary-1** appears as the top adversary with sightings corresponding to the sighted indicators as displayed in the static table above. Also notice that the sightings count is 4, which corresponds to 2 sightings each for the sighted indicators.



Indicators Malware Family Distribution

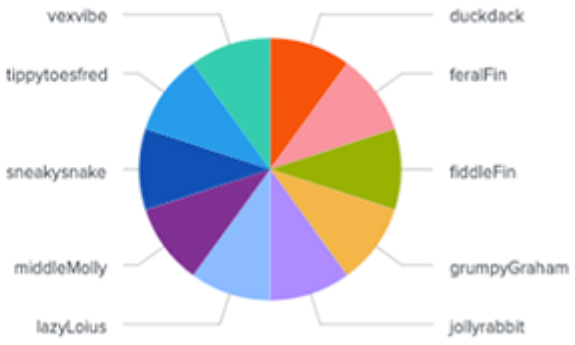
The Indicators Malware Family Distribution widget provides a pie with breakdown of indicator malware information.



Indicators with Sightings Malware Family Distribution

The Indicators with Sightings Malware Family Distribution widgets provides a pie chart breakdown of indicators with malware sightings.

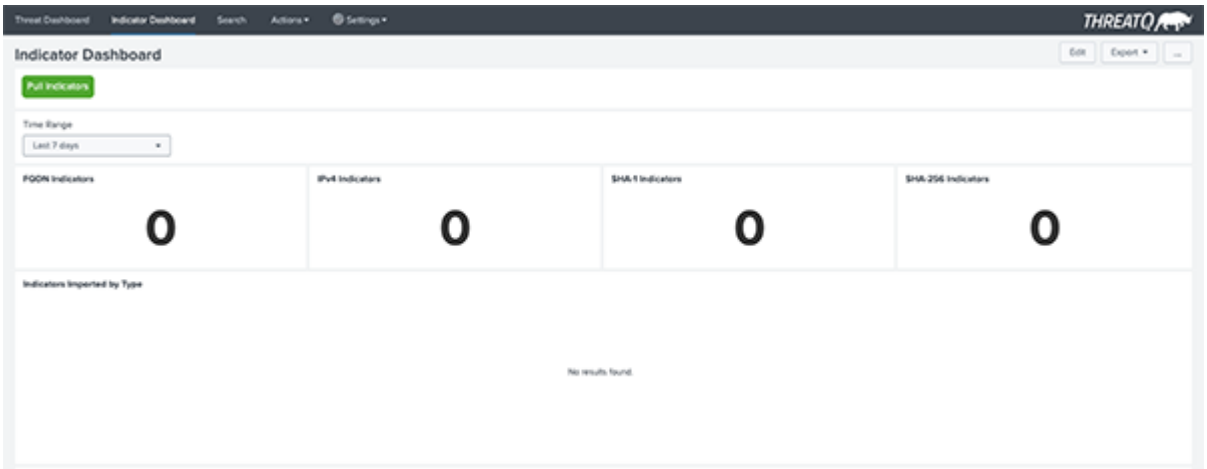
Indicators With Sightings Malware Family Distribution



Indicator Dashboards

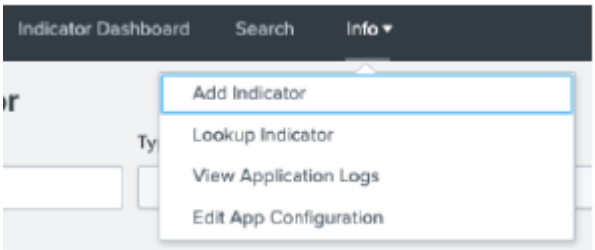
Roles Required: Admin, Power, Splunk_System_Role, User, can_delete, ess_user, ess_analyst, ess_admin.

The Indicator Dashboard displays indicator-related widgets, such as type counts and bar charts, for a user-specified time frame.



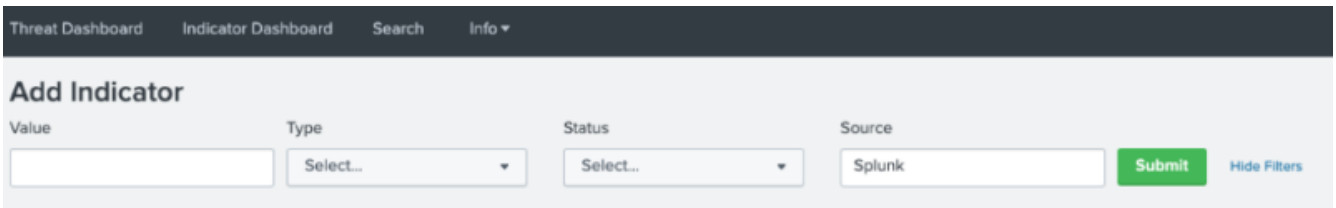
Info Tab

The Dashboard Info tab, located next to the Search Option, provides you with the ability to perform indicator and application log searches along with shortcuts to the Add Indicator and Edit App Configuration functions.



Add Indicator

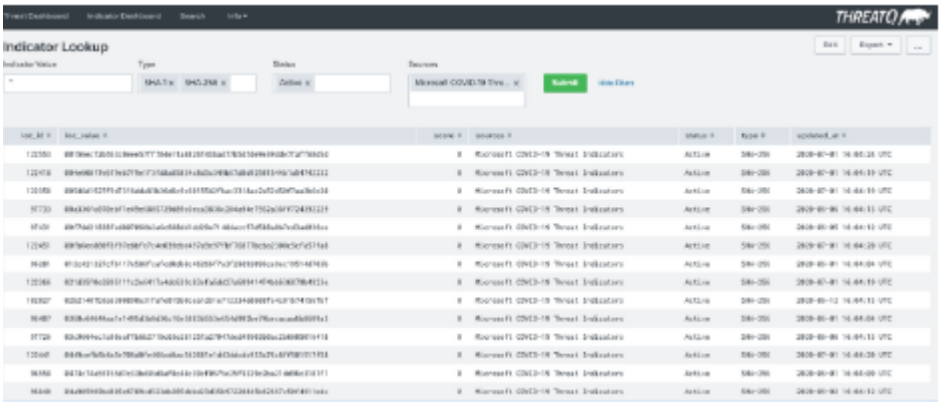
The Add Indicator option will open the Add Indicator input from within the dashboard. You can use this form to manually add indicators to ThreatQ.



Indicator Lookup

The Indicator Lookup option allows you to perform a search based on:

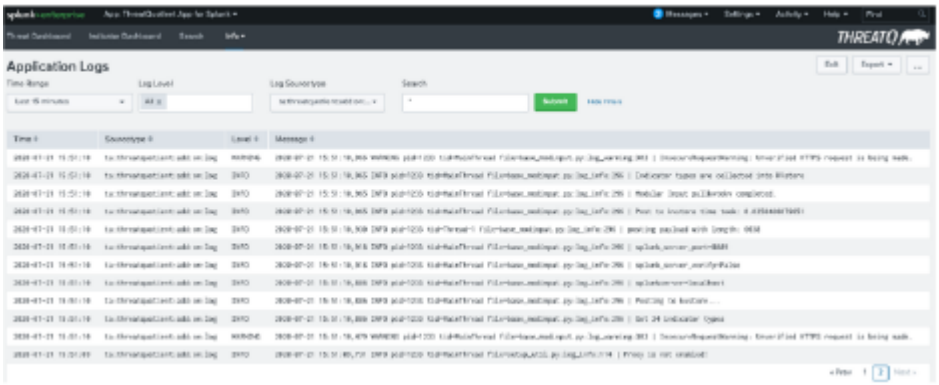
- IndicatorValue
- IndicatorType
- Status
- Source(s)



Application Log Search

The Application Log Search allows you to perform a search of logs based on:

- Time Range
- Log Level
- Log Source Type
- Search



Edit App Configuration

The Edit App Configuration will open the app's Setup page. See the configuration section of the Installing the App Component topic for more details.

Troubleshooting

- Use the log file below to troubleshoot the ThreatQuotient Add-on:

  `$SPLUNK_HOME/var/log/Splunk/ta_threatquotient_add_on_threatq_indicators.log`

- To find all unique indicators indexed in Splunk by the Add-On (Splunk App allows you to select a specific time range):

  `sourcetype="threatq:indicators" | dedup value`

- To review the data collected by data collection, use a query such as:

  `"index=your_index_name sourcetype=threatq_indicators"`

  - Confirm all the saved searches are enabled.
  - Confirm the macro is updated as per the settings.
  - The log file can be found at the following location:

    `/opt/splunk/var/log/splunk/scheduler.log`

- If the user changes macros for global score and status thresholds, the audit logs can be accessed using the following two saved searches:

  Splunk Search for Listing TQ Indicators

  `index=_internal threatq_score_filter sourcetype="splunkd_ui_access"`

  `index=_internal threatq_score_filter sourcetype="splunkd_access"`

- To disable Verify SSL Certification - App versions 2.6.0+

  1. Navigate to the following file: `$SPLUNK_HOME/etc/apps/ThreatQAppforSplunk/bin/threatq_const.py`
  2. Change the `VERIFY_SSL` to False.

- To disable Verify SSL Certification - Add-On versions 2.6.0+

  1. Navigate to the following file: `$SPLUNK_HOME/etc/apps/TA-threatquotient-add-on/bin/threatq_const.py`
  2. Change the `VERIFY_SSL` to False.

Change Log

COMPONENT	VERSION	UPDATES
App	3.3.0	• Added the **Splunk ES Threat Group Field** and **Splunk ES Threat Category Field** parameters to the app settings tab, allowing users to select the `master_lookup` fields used to populate `threat_group` and `threat_category` in Splunk Enterprise Security `*_intel` lookups. • Upgraded the Splunk SDK for Python to version 3.0.0. • Added support for the `FQDN` indicator type and the `url_domain` field when matching against the Web data model.
App	3.2.0	• Added support for regex-based and partial-value matching. • Introduced support for port-based matching. • Added support for custom data models in matching operations. • Enhanced matching capabilities to support multiple data model matches for a single IOC value. • Added **Match Count** (lifetime match count) and **Event Count** (last-run match count) fields to Sighting events. • Added a new dashboard panel displaying the count of events matched during the last run, grouped by matched data model. • Added support for Common Access Card (CAC) authentication in account configuration. • Updated the add-on builder to version 4.5.1.

COMPONENT	VERSION	UPDATES
		⚠ Version 3.2.0 for the App introduces support for unique sightings per data model, which requires an update to the `threatq_matched_indicators` lookup format. See the Upgrading the App to 3.2.0 section for steps on migrating your existing data to the new format before performing the standard upgrade steps.
Add-On	3.2.0	• Added CAC (Common Access Card) authentication support for account configuration. • Added extraction for port value

App	3.1.0	• Added support for OAuth authentication.
		• Added the following new configuration parameters under Account tab:
		  ◦ **Authentication Type** - select your authentication method: basic authentication or OAuth.
		  ◦ **Add Splunk Port to URL** - you can now include the Splunk instance's port number in the generated URL used in ThreatQ events as part of the attribute.

Add-On	3.1.0	• Added support for OAuth authentication. • Added the following new configuration parameter under Account tab: ◦ **Authentication Type** - select your authentication method: basic authentication or OAuth.

COMPONENT	VERSION	UPDATES
		• Added a new configuration parameter to the Add ThreatQ Indicators dialog box when creating a new input: ◦ **Response Page Size** - you can now define the number of indicators to retrieve per API request.
Add-On	3.0.3	• Updated the Splunk Add-on Builder to version 4.5.0.
App	3.0.2	• Added support for Splunk 10.0.x (Enterprise and Cloud).
Add-On	3.0.2	• Added support for Splunk 10.0.x (Enterprise and Cloud).
App	3.0.1	• Removed the `sort` parameter for the attributes API call used in **threatqconsumeindicatorsnew** and **threatqconsumeindicators** custom commands.
Add-On	3.0.1	• Resolved an issue with the App dashboard where the 24 hour count widget always displayed 0.
App	3.0.0	• Resolved Splunk cloud compatibility issues. • Added support to perform bulk indicator lookup. • Added two new configuration tabs: ◦ Splunk Custom Fields

COMPONENT	VERSION	UPDATES
		◦ Splunk Forwarder • Added the ability to fetch latest indicators from ThreatQ to Splunk through the App - see the **Splunk Forwarder** section under **Configuration** chapter for further details. • Renamed the **Custom Attributes** and **Custom Fields** parameters to **ThreatQ Custom Attributes** and **ThreatQ Custom Fields**. Relocated these updated fields to the new **Splunk Custom Fields** tab. • Added ThreatQ Custom Attributes • Added support to send custom fields to ThreatQ from Splunk. • Added support to send Datamodel name and latest raw event to ThreatQ. • Added support for Splunk Enterprise and Cloud versions 9.3.x and 9.4.x. • Updated the minimum ThreatQ version to 5.11.0
Add-On	3.0.0	• Resolved cloud compatibility issues. • Resolved a data case sensitivity issue. • Added support for Splunk Enterprise and Cloud versions 9.3.x and 9.4.x. • Updated the minimum ThreatQ version to 5.11.0
Guide Update	2.8.0 rev-A	• Added **User Capabilities** section to the **Role-Based Permissions** chapter.
App	2.8.0	• Resolved a connectivity issue by using requests library.

COMPONENT	VERSION	UPDATES
		• Updated Splunk compatibility versions to Splunk (Enterprise or Cloud) 9.1.x and 9.2.x.
Add-On	2.8.0	• Upgraded Add-on Builder framework version to 4.2.0. • Resolved a KV Store connectivity issue by replacing session key with credentials and requests library. • Updated Splunk compatibility versions to Splunk (Enterprise or Cloud) 9.1.x and 9.2.x.
App	2.7.0	• Updated the app for Splunk SDK updates. • Resolved application inspection warnings.
Add-On	2.7.0	• Updated the Builder framework version to 4.1.3. • Updated the Splunk compatibility versions for the add-on to Splunk Enterprise 9.0.x and 9.1.x.
App	2.6.0	• Added new **Configuration** tab for ThreatQ Account and App settings. The app can be configured to communicate directly with your ThreatQ instance. Previously, authentication with your ThreatQ instance was performed by the add-on. • Added Splunk Web URL field to the ThreatQ Account tab. • Added two new Threat Dashboard widgets: **Indicators Malware Family Distribution** and **Indicators with Sightings Malware Family Distribution**.

COMPONENT	VERSION	UPDATES
		• Resolved an issue where Add-on logs could not be viewed in the app. • Added Workflow Actions and Alert Actions from the add-on to the app. • Added new workflow action: **ThreatQ: Update Indicator Status** with options from the lookup. Options for the **ThreatQ Update Indicator Status** alert action will now populate from the lookup. This action supports all statuses, including custom, that can be pulled from the ThreatQ instance. • Removed the **ThreatQ: Add to Whitelist** workflow action. • Removed the **Verify SSL Certificate** checkbox under Configuration. • Splunk version 8.2.x has been removed from the compatibility list as it is no longer supported by Splunk.
Add-On	2.6.0	• Migrated Workflow Actions and Alert Actions to the app. • The Add-on is no longer required to be installed on the search head as a dependency for the app. • Removed usage of Proxy while checking KVStore status. • Restricted initial data collection to last 90 days. • Removed the **Verify SSL Certificate** checkbox under the KVStore configuration.
Add-On	2.5.1	• Minor bug fix.

COMPONENT	VERSION	UPDATES
App	2.5.0	• Upgraded the JQuery bundled with the app to version 3.5.0. • Fixed an issue where `threatq_update_retired_indicators` failed if ingested object attributes included the **$** and **.** special characters. Additional data validation has been added to the custom fields/attributes on the configuration page. • Updated app to support Splunk versions to 8.1.x and 8.2.x.
Add-On	2.5.0	• Updated the add-on to AOB 4.1.0. • Fixed an issue where indicators with null values would cause kvstore data to be belated. • Updated add-on to support Splunk versions to 8.1.x and 8.2.x.

App	2.4.1	• Fixed the following issues:
		  ◦ Updated_at information was not being populated in the kvstore.
		  ◦ The tstats search failed to execute in certain instances due to a typo in a search variable.
		  ◦ Updating the search to the Datamodel tstats search failed to disable older searches.
		  ◦ Custom fields with spaces were not handled correctly in the kvstore.
		  In some instances, existing custom attributes failed to load upon upgrading to version 2.4.1. If you encounter this issue, you

COMPONENT	VERSION	UPDATES
		should re-save your app configuration. ◦ The UI text in the Setup Dashboard page had a small typo.
Add-On	2.4.1	• The Whitelisted status has been removed as a default status when creating a new input configuration. The default status is now Active.
App	2.4.0	• Added **Datamodel tstat Search** option for Matching Algorithm Configuration. • Added new macro, `threatq_match_fields`, that will allow you to match on specific fields. • Added new macro for Raw Matching, `threatq_match_base_query`, that allows you to alter the base query for matching. • Added two new fields to the Splunk Setup Dashboard: ◦ **Custom Attributes Configuration** - Allows you to include custom attributes that will be exported from ThreatQ using a comma-separated list. ◦ **Custom Fields Configuration** - Allows you to include custom fields that will be exported from ThreatQ using a comma-separated list. • Updated the datamodel search queries to support chunking. The default chunk size is 50,000.
Add-On	2.4.0	• Fixed an issue where attempting to fetch import-timeout resulted in a 401 error in the heavy forwarder.

COMPONENT	VERSION	UPDATES
		• Added custom fields and custom attributes support to the KVStore.
App	2.3.0	• Fixed an issue which caused certain datamodel searches to not complete. • Fixed an issue where saved searches would fail if events had Chinese characters. • Upgraded the Splunklib.
App	2.2.0	• A Hostname configuration field has been added to the Setup page. This value will be used as a Source Attribute when calling consume endpoints. • Saved Searches have been staggered to prevent encountering concurrent search limitations. • Added a Malware family attribute field to the KVStore. • Added partial URL matching support for Datamodel searches. • Combined saved searches for Datamodel to have only a single search per Datamodel.
Add-On	2.3.0	• Fixed an authentication issue with the KVStore configuration. • Malware family data, if available for ThreatQ indicators, will now be stored in the KVStore. • The localhost Username and Password dependency for the KVStore data collection has been removed.
App	2.1.0	• Added new Indicator Dashboard.

COMPONENT	VERSION	UPDATES
		• Added ability to use KVStore for saving data. • Added Info tab to dashboards page with the following options/shortcuts: • Add Indicator • Lookup Indicator • View Application Logs • Edit App Configurations • Fixed an issue where no sightings were generated for domain object types within Splunk. • Fixed an issue with data listed in multi-valued fields.
Add-On	2.2.0	• Added new Splunk KVStore Rest configuration tab. This configuration tab is required if users save data to KVStore. • Additional options Enable Index and Pull all Indicators available under input configuration.
Add-On	2.1.0	• Import timeout is now configurable from UI. • Pagination support for initial import of ThreatQ data. • Updated default frequency for ThreatQ Exports from 300 to 900.

App	2.0.0	• Python 3 Support - ThreatQuotient App for Splunk is now compatible with Python 3. Supported versions include:
		  ◦ Splunk 7.2.x
		  ◦ Splunk 7.3.x
		  ◦ Splunk 8.X (Python 2)

COMPONENT	VERSION	UPDATES
		◦ Splunk 8.X (Python 3)
Add-On	2.0.0	• Python 3 Support - ThreatQuotient Add-on for Splunk is now compatible with Python 3. Supported versions include: ◦ Splunk 7.2.x ◦ Splunk 7.3.x ◦ Splunk 8.X (Python 2) ◦ Splunk 8.X (Python 3) • Resolved an issue where creating an indicator in Splunk would occasionally result in the creation of an indicator with an incorrect type within the ThreatQ platform.