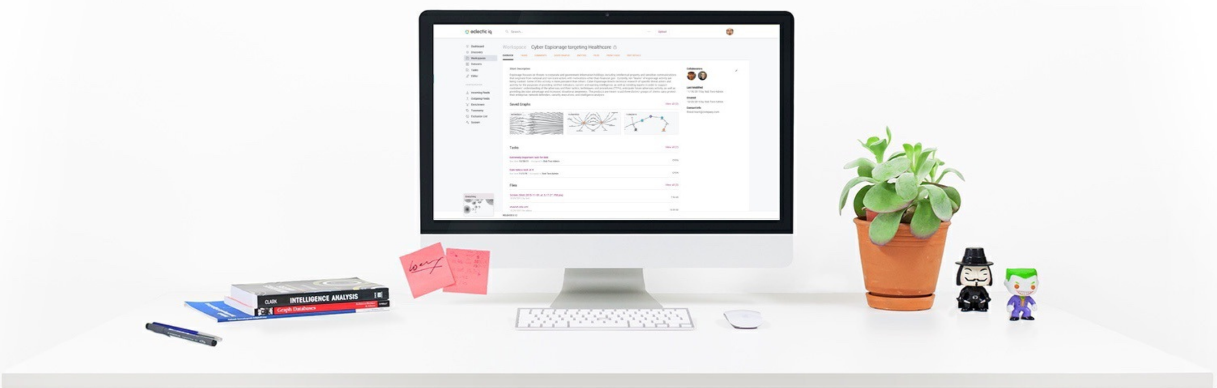
EclecticIQ Platform App for Splunk

Integrate EclecticIQ Platform with Splunk Enterprise — Installation and configuration

Last generated: March 06, 2018



Last generated on Mar 6, 2018

Table of contents

Splunk integration

EclecticIQ Platform App for Splunk enables Splunk users to ingest large quantities of threat intelligence by integrating EclecticIQ Platform feeds with Splunk Enterprise.

Splunk integration	
App	EclecticIQ Platform App for Splunk
Version	2.0.0
For	Splunk Enterprise 6.x
Splunk compatibility	Splunk Enterprise 6.3 and later
Platform compatibility	EclecticIQ Platform 1.14.4, 2.0.x, 2.1.x
Last changed	January 2018
Type	SIEM integration
Integration	app/bidirectional
Description	The app integrates EclecticIQ Platform feeds with Splunk Enterprise. Outgoing feeds transmit relevant data to a Splunk instance for analysis and for further filtering to identify potential threats that may target your organization.
Download	**Splunkbase** `(https://splunkbase.splunk.com/app/3408/)`
Authors	EclecticIQ, SOC Prime, SMT

Release notes

Version 2.0.0 — App revamp: EclecticIQ Platform App for Splunk is available as **SA for EclecticIQ**, the core app, and **TA for EclecticIQ**, an additional module.

- **SA for EclecticIQ** works with *Splunk Enterprise*.
  Everything you need is bundled with the installation package and the related files.
- **TA for EclecticIQ** can only be used in combination with SA for EclecticIQ; it does not work as a standalone app.
  TA for EclecticIQ adds EclecticIQ integration to *Splunk Enterprise Security*.

New and changed in SA for EclecticIQ

- Support for the **Splunk KV store** `(http://dev.splunk.com/view/webframework-developapps/sp-caaaezk)`

- Support for distributed environments and **search head clustering** (http://docs.splunk.com/documentation/splunk/6.6.5/distsearch/shcarchitecture)
- Dashboard query performance improvements
- Support for workflow actions on events — for example, look up an observable representing an IP address.

New in TA for EclecticIQ

- Four threat lists populated with data pulled from the platform and sent to Splunk through EclecticIQ Platform App for Splunk/SA-EclecticIQ
- Four saved searches speed up the threat list creation process
- A macro enables weighing/scoring threat list items
- A ready-to-use **correlation search** (https://docs.splunk.com/documentation/es/4.7.4/admin/correlationsearchoverview) to report sightings as **notable events** (http://dev.splunk.com/view/enterprise-security/sp-caaafa9).

Product compatibility

- Compatible with Splunk Enterprise 6.3 and later
- Compatible with EclecticIQ Platform 1.14.4, 2.0.x, 2.1.x

Contact

If you want to send us your feedback or if you need any support with the app, you can contact EclecticIQ at splunk@eclecticiq.com.

To request further documentation, contact EclecticIQ at splunk@eclecticiq.com.
To suggest a feature request and to report bugs, send an email to splunk@eclecticiq.com.

About EclecticIQ Platform App for Splunk

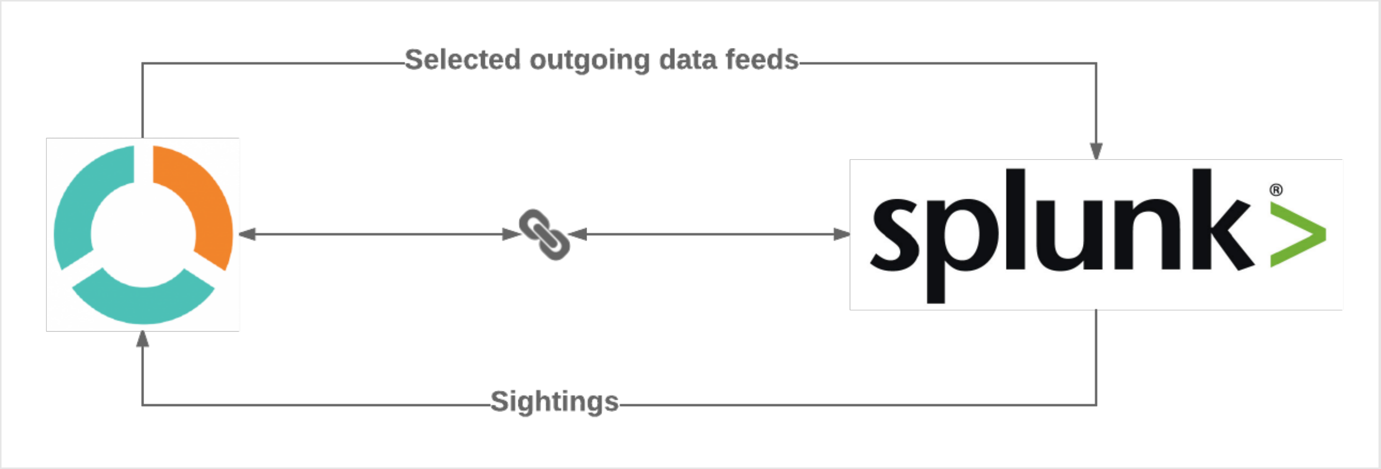
EclecticIQ Platform App for Splunk is an app for Splunk Enterprise. It enables Splunk users to ingest large quantities of threat intelligence by integrating EclecticIQ Platform feeds with Splunk.

EclecticIQ Platform ingests cyber threat data in different formats from multiple sources. The platform deduplicates, normalizes, and enriches source data with additional contextual details, and then it uses outgoing feeds to output relevant information to Splunk, where it can be analyzed and filtered by a set of rules to identify matching threats that may target your organization.

This process generates sightings and alerts that Splunk feeds back to EclecticIQ Platform, providing a rich threat intelligence dataset that allows you to efficiently tune your SIEM prevention and detection system.

EclecticIQ Platform App for Splunk consists of two modules:

- **SA for EclecticIQ**: the core app, it works with *Splunk Enterprise*.
  Everything you need is bundled with the installation package and the related files.
  It includes:
  - A default set of dashboard gauges to make it easier for Splunk users to monitor feed data collection, as well as to analyze and triage any *indicators of compromise* (IoCs) the data analysis process may yield;
  - Scripts to automate threat intelligence download and sighting upload tasks;
  - Workflow actions to quickly retrieve more details about observables and sightings in EclecticIQ Platform.
- **TA for EclecticIQ**: an add-on module for SA for EclecticIQ.
  The additional TA for EclecticIQ app extends the core app functionality set by adding EclecticIQ integration with *Splunk Enterprise Security*.



Quick start guide

Compatibility

- EclecticIQ Platform App for Splunk 2.0.0.
- Compatible with Splunk Enterprise 6.x (6.3 and later)
- Compatible with EclecticIQ Platform 1.14.4, 2.0.x, 2.1.x
- Supports Python 2.6.6 or higher 2.x.x version.
  Not supported: Python 3.x.x.

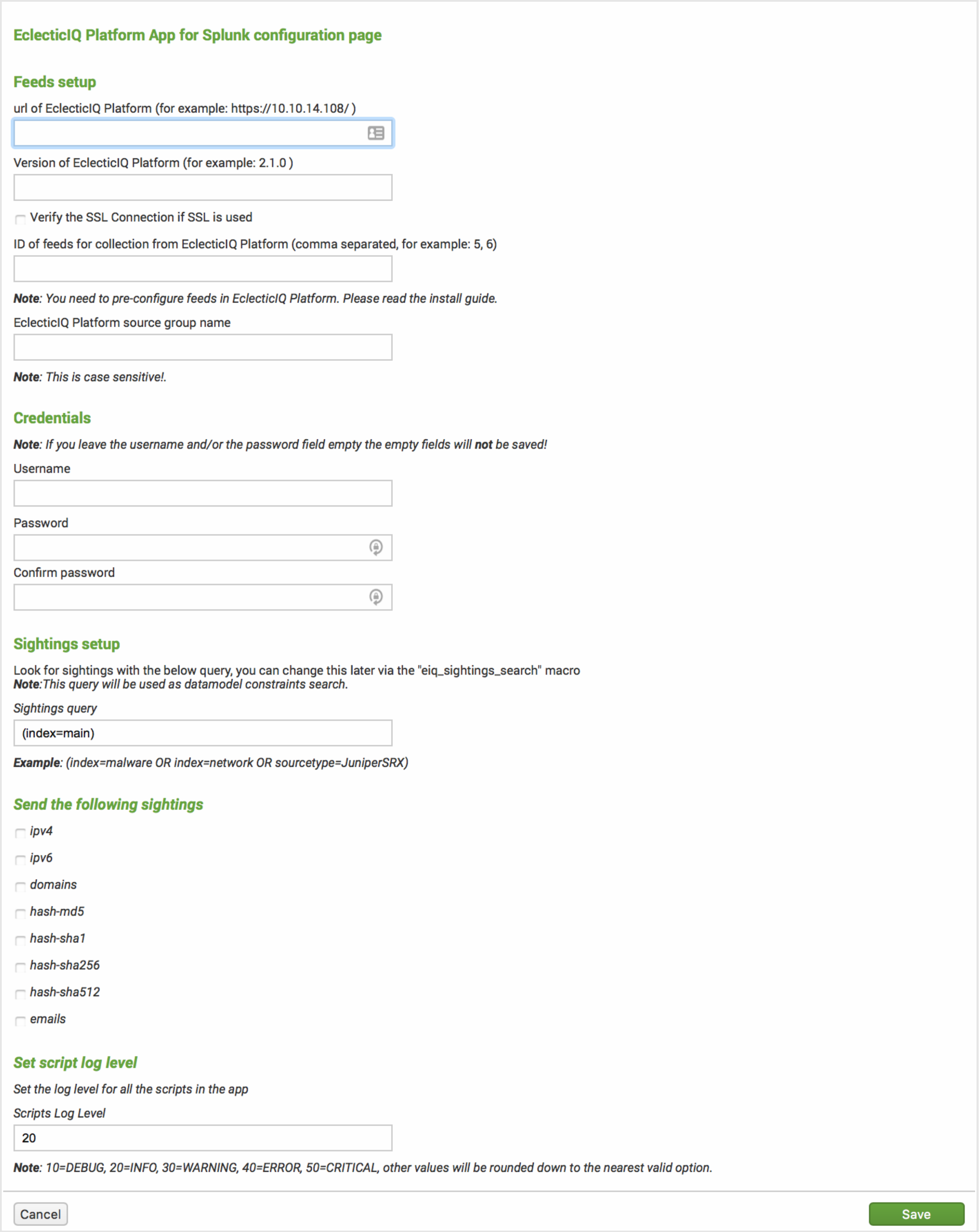
Install

EclecticIQ Platform App for Splunk is developed specifically for Splunk Enterprise.
Everything you need to use the app is bundled with the installation package and the related files.
If you are using Splunk Enterprise, you do not need to install the script and configuration files.

- Verify that the Splunk Enterprise server you want to install EclecticIQ Platform App for Splunk on is compatible with the app.
- Verify that the default Python version on the target system is compatible with the app.

Configure

After restarting Splunk, you can proceed to configuring EclecticIQ Platform App for Splunk.



EclecticIQ Platform App for Splunk configuration page

Feeds setup

url of EclecticIQ Platform (for example: https://10.10.14.108/)

Version of EclecticIQ Platform (for example: 2.1.0)

☐ Verify the SSL Connection if SSL is used

ID of feeds for collection from EclecticIQ Platform (comma separated, for example: 5, 6)

***Note**: You need to pre-configure feeds in EclecticIQ Platform. Please read the install guide.*

EclecticIQ Platform source group name

***Note**: This is case sensitive!.*

Credentials

***Note**: If you leave the username and/or the password field empty the empty fields will **not** be saved!*

Username

Password

Confirm password

Sightings setup

Look for sightings with the below query, you can change this later via the "eiq_sightings_search" macro
***Note**:This query will be used as datamodel constraints search.*

Sightings query

(index=main)

***Example**: (index=malware OR index=network OR sourcetype=JuniperSRX)*

Send the following sightings

☐ *ipv4*

☐ *ipv6*

☐ *domains*

☐ *hash-md5*

☐ *hash-sha1*

☐ *hash-sha256*

☐ *hash-sha512*

☐ *emails*

Set script log level

Set the log level for all the scripts in the app

Scripts Log Level

20

***Note**: 10=DEBUG, 20=INFO, 30=WARNING, 40=ERROR, 50=CRITICAL, other values will be rounded down to the nearest valid option.*

You can configure EclecticIQ Platform App for Splunk from the connected Splunk Enterprise instance:

- In the Splunk management console go to **Apps**.
- From the app list select **EclecticIQ Platform App for Splunk**.
- On the displayed dialog window click **Continue to app setup page**.

On the **EclecticIQ Platform App for Splunk configuration** page, define the following configuration options:

- **Feeds setup**
  - **URL of EclecticIQ Platform**: enter either the domain name or the IP address of the platform instance.
    Example: *https://corp.eiq-platform.com/*; *https://10.0.2.128/*
  - **Version of EclecticIQ Platform**: enter version number of the platform instance.
    Example: *2.1.0*
  - **Verify the SSL connection if SSL is used**: select this checkbox to verify the SSL certificate used by the platform.
  - **ID of feeds for collection from EclecticIQ Platform**: enter a comma-separated list of outgoing feed IDs that the Splunk instance can download from the platform. Example: *11*; *5,9,13,78*
  - **EclecticIQ Platform source group name**: enter the name of the platform group to use as a platform data source for the Splunk instance.

> The source outgoing feeds and the source group need to be already configured in the platform.

- **Credentials**
  - **Username**: enter a valid user name to sign in to the platform.
  - **Password**: enter a valid password associated with the platform user name.
  - **Confirm password**: type again the password to confirm it.

- **Sightings setup**
  - **Sightings query**: a **Splunk query** `(http://docs.splunk.com/documentation/splunk/6.6.5/searchtutorial/)` to look for sightings in specific Splunk indices and data sources.
    Example: *(index=botnet OR index=malware AND sourcetype=JuniperSRX OR sourcetype=Firepower4100)*
  - **Send the following sightings**: select one or more checkboxes to specify the data types you want search for and collect in Splunk.
    This generates sightings that are then sent on to the platform for ingestion.
    After ingestion and processing, they are stored in the platform as observables.
    Currently supported observable types:
    - *domain*
    - *email*
    - *hash-md5*
    - *hash-sha1*
    - *hash-sha256*
    - *hash-sha512*
    - *ipv4*
    - *ipv6*
  - **Set script log level**: set the severity level of the messages logging app script events.
    Log severity levels:
    - *DEBUG (10)*
    - *INFO (20)*
    - *WARNING (30)*
    - *ERROR (40)*
    - *CRITICAL (50)*

> This option does not enable log file ingestion in Splunk.
> To feed the script log file into Splunk, enable the **`[monitor://${path}]` stanza** `(https://docs.splunk.com/documentation/splunk/6.6.5/admin/inputsconf)` in the *$SPLUNK_HOME/etc/apps/SA-EclecticIQ/default/inputs.conf* file, and then set the appropriate `index` and `sourcetype` values.

- Click **Save** to save your configuration.
- You can change the job schedules in the following configuration file: *$SPLUNK_HOME/etc/apps/SA-EclecticIQ/default/inputs.conf*
  - *eiq_collect_feeds.py* is the script that collects outgoing feed data from EclecticIQ Platform.
  - *eiq_send_sightings.py* is the script that sends sightings to EclecticIQ Platform.

After correctly configuring EclecticIQ Platform App for Splunk to integrate and work with Splunk, the corresponding dashboard view should become populated with relevant results.

Uninstall

To uninstall EclecticIQ Platform App for Splunk/SA for EclecticIQ, run the following command(s):

```
$ SPLUNK_HOME/bin/splunk remove app SA-EclecticIQ
```

Or:

```
$ rm -rf SPLUNK_HOME/etc/apps/SA-EclecticIQ
```

After completing the uninstallation, restart Splunk:

```
$ SPLUNK_HOME/bin/splunk restart
```

End of the EclecticIQ Platform App for Splunk quick start guide

Beginning of the EclecticIQ Platform App for Splunk integration guide

EclecticIQ Platform integration with Splunk

(Through EclecticIQ Platform App for Splunk)

Before you start

Before you start installing the app, take a moment to review the preliminary requirements and the main steps of the process.

Requirements

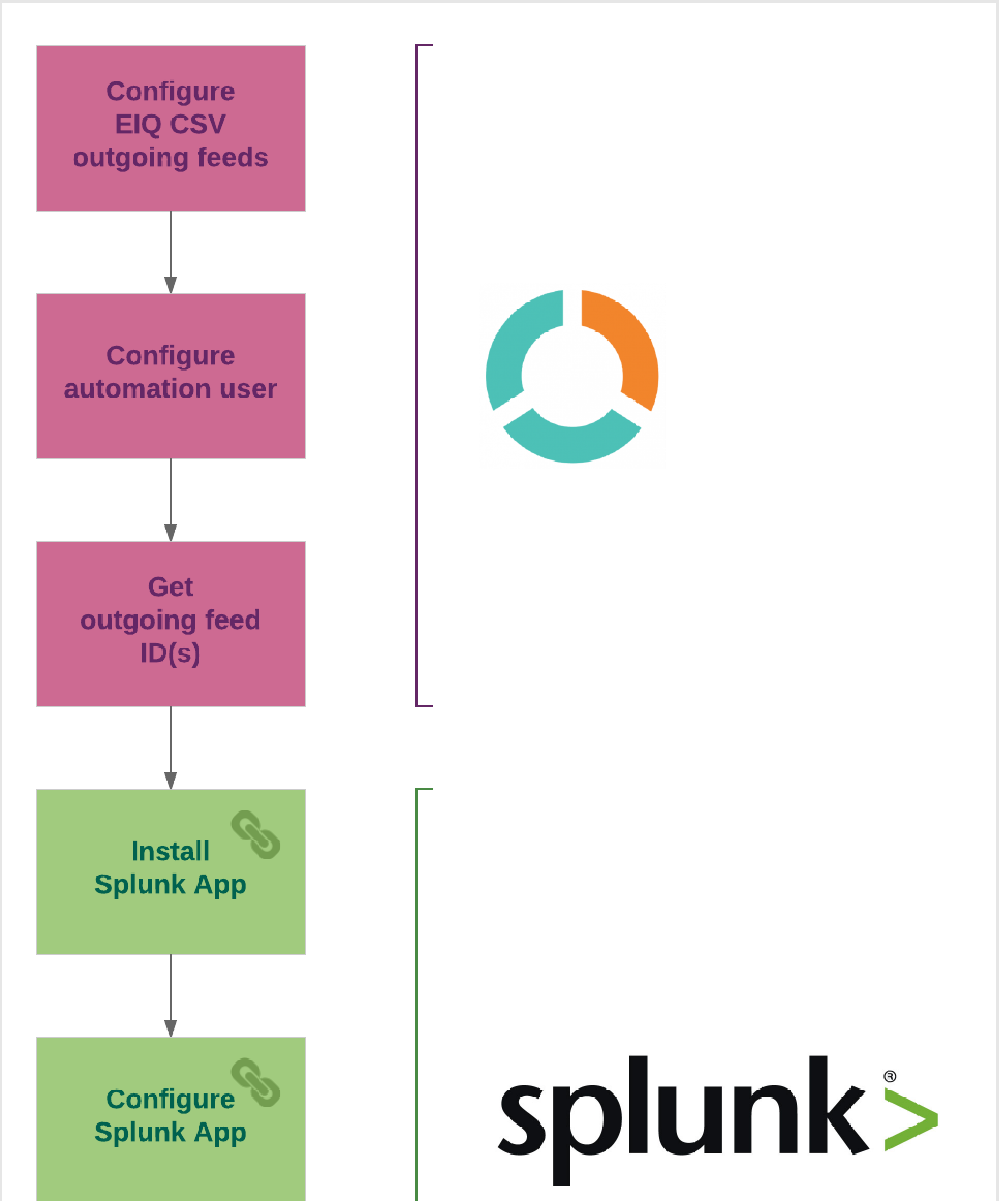
- An EclecticIQ Platform installation.
- A Splunk server installation.
- Splunk **Common Information Model (CIM)** `(https://splunkbase.splunk.com/app/1621/)` add-on needs to be **installed** `(https://docs.splunk.com/documentation/cim/latest/user/install)` on the Splunk server.
- Install and set up EclecticIQ Platform App for Splunk on a Splunk server that has network access to the EclecticIQ Platform server: these servers need to communicate and exchange data.
- Compatible with Splunk Enterprise 6.x (6.3 and later)
- Compatible with EclecticIQ Platform 1.14.4, 2.0.x, 2.1.x

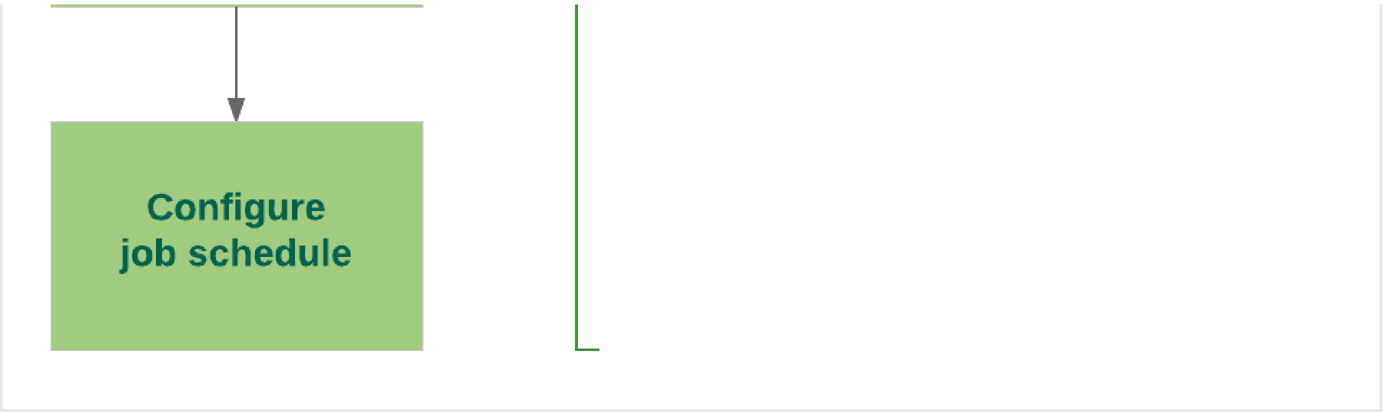
- Supports Python 2.6.6 or higher 2.x.x version.
  Not supported: Python 3.x.x.

Process outline

The diagram sums up the main steps to set up and configure a platform integration with Splunk:

- First, you set up the outgoing feed sending data from the platform to Splunk.
- Then, you install and configure SA for EclecticIQ to enable the integration between the platform and Splunk.





Configure EclecticIQ CSV outgoing feeds

EclecticIQ Platform outgoing feeds enable sharing and distributing cyber threat intelligence in several formats. Share knowledge and promote collaboration to support an ecosystem where partners work together to identify threats, and define an effective course of action to ensure their assets are protected.

This section describes how to configure **HTTP download** transport type / **EclecticIQ Observables CSV** content type outgoing feeds, so that the platform can send observables to Splunk and it can receive sightings from Splunk through EclecticIQ Platform.

Configure the general options

✔ Input fields marked with an asterisk are required.

- On the top navigation bar, select **Data configuration > Outgoing feeds**.
- On the top-left corner of the page click the ✚ icon to open the outgoing feed editor.

The **Outgoing feeds** page displays an overview of the configured outgoing feeds to publish and distribute selected intelligence from the platform to external parties, services, and systems.

On the **Create outgoing feed** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.
- **Sign content with private key**: select this checkbox to automatically sign the content of the outgoing feed with a private PGP key.
  If you have not yet set a PGP private key in the platform, **Click here for the Private Key settings** to go to **System settings > Private key**, where you can set it before continuing with the feed configuration.

To set a PGP private key to sign outgoing feed content with, do the following:

- On the left-hand navigation sidebar, click ⚙ **> System settings > Private Key**.
- Click **Edit settings** to display the **Edit private key settings** page.
- In the **Private key** input field copy-paste the private PGP key you want to add to sign outgoing feed data packages with.
  Include in the pasted content the leading `-----BEGIN PGP PRIVATE KEY BLOCK-----`and the trailing `-----END PGP PRIVATE KEY BLOCK-----` lines.
- Click **Save** to store your changes, or **Cancel** to discard them.

To change PGP private key, you first need to remove the currently registered one:

- On the **Edit private key settings** page, browse to **Delete private key settings**, and then click **Delete settings**.
- On the confirmation dialog, click **Delete** to confirm the action.

Transport and content

Under **Transport type** and **Content type**, select the appropriate options to configure transport and content for the specified outgoing feed.

- **Transport type**: from the drop-down menu select **HTTP download** as the appropriate transport type to implement the integration between Splunk and the platform.
- **Content type**: from the drop-down menu select **EclecticIQ Observables CSV** and configure the appropriate parameters under **Content configuration**, when applicable.
- **Dataset**: from the drop-down menu select one or more datasets as data sources for the outgoing feed.
- **Update strategy**: from the drop-down menu select the preferred method to update the data:
    - **Append**: every time the outgoing feed task runs, only new data from the latest task run, that is, only new entities, is appended to the existing data.
      When the outgoing feed task runs, it includes only new entities.
    - **Replace** every time the outgoing feed task runs, it publishes only new data.
      When the outgoing feed task runs, it produces new content that can include new, as well as existing entities.
    - **Diff**: every time the outgoing feed task runs, new data is compared against existing data to identify any differences between the two datasets at observable-level — any observable added to or removed from the entities in the set — or at entity-level — any entities added to or removed from the set.
      Depending on the selected CSV content option, each row in the CSV output contains information about one entity or one observable.
      An extra diff column is added to the output to indicate if a row, and therefore either an entity or an observable, was added to or removed from the set.
      This option allows you to identify any changes in a feed between two task runs without downloading the whole feed.

Set a schedule

Under **Schedule — Execution schedule** you can define how often you want to automatically run the feed task:

- **None**: scheduled feed execution is disabled. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.
- **Every [n] minutes**: the feed task runs automatically once every *[n]* minutes, where *[n]* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.
- **Every hour, [n] minutes past the hour**: the feed task runs automatically once an hour every hour at the specified minute offset from the hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.
- **Every [n] hours**: the feed task runs automatically once every *[n]* hours, where *[n]* defines the time interval in hours between two consecutive feed task runs.
  You define how long the time interval between feed executions should be by selecting the number of hours from the corresponding drop-down menu.
- **Every day at [time]**: the feed task runs automatically once a day at the specified time.
  You define the time of the day when the task should run from the corresponding drop-down menus.

- **Every [n] days**: the feed task runs automatically once every *[n]* days, where *[n]* defines the time interval in days between two consecutive feed task runs.
  You define how long the time interval between feed executions should be by selecting the number of days from the corresponding drop-down menu.
- **Every week on [day of the week] at [time]**: the feed task runs automatically once a week on the designated day, at the specified time.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menus.
- **Every month on [day of the month] at [time]**: the feed task runs automatically once a month on the designated day of the month, at the specified time.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menus.
  Keep in mind that not all months of the year have 30 or 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated with the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

  You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
  When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
  For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.
- The **Filter TLP color** options allow including in the feed data only an entity subset, based on the selected **TLP** `(https://www.us-cert.gov/tlp)` value.
  If you set a TLP color as a filter, the feed includes all the entities flagged with the selected TLP color code, as well as the entities whose TLP color indicates that they are suitable for progressively broader audiences. For example, if you select green, the feed includes entities with a TLP color set to green and entities with a TLP color set to white.

Set reliability and relevancy

- **Source reliability**: from the drop-down menu select an option to flag the feed or enricher content with a predefined reliability value to help other users assess how trustworthy the data source is.
  Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code).`
  Example: *B - Usually reliable*
- **Relevancy threshold (%)** allows you to set a filter to include in the feed only entities whose relevancy is higher than the value defined here.

Set observable filters

Observable filters work independently of each other: there are no explicit or implicit Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the outgoing feed content only entities whose observable states match at least one of the selections defined here.

- **Include only observables with link names**: from the drop-down menu select one or more link name options to include in the outgoing feed content only observables with the specified link name value(s) describing specific types of relationship between observables and their parent entities.

  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.
  This filter option does not apply to enrichment observables.
- **Include observables without a link type**: select this checkbox to include in the outgoing feed content also observables without a defined link type/link name. These observables may or may not have relationships with other entities or other observables; in the former case, the relationships are undefined; therefore, they have lower intelligence value than link-named ones.
  This filtering applies to bundled observables, that is, to observables that are included inside entities. It does not apply to enrichment observables.
- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed content only entities with observables whose types match at least one of the selections defined here.
- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the outgoing feed content only entities with enrichment observables whose types match at least one of the selections defined here.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

Besides committing the current data by clicking **Save**, you can also click the downward-pointing arrow on the **Save** button to display a context menu with additional save options:

- **Save and new**: saves the current data for the active item, and it allows you to start creating a new item of the same type right away. For example, a dataset, a feed, a rule, a workspace, or a task.
- **Save and duplicate**: saves the current data for the active item, and it creates a pre-populated copy of the same item, which you can use as a template to speed up manual work.

Configure transport and content types

Transport type	Allowed content type
HTTP download	EclecticIQ Observables CSV

HTTP download

ℹ The HTTP download transport type requires basic access authentication.

If you want to make the outgoing feed data available through an HTTP URL, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intended recipient groups in the **Authorized groups** drop-down menu.
- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

Configure the content type

When you set up an outgoing feed from the platform to the destination Splunk instance, you need to configure the following content type parameters.

From the drop-down menu select the following option to define the output data structure in the CSV output:

- **EclecticIQ Observables CSV**: in the resulting CSV with column headers, each row holds information referring to one observable.
  For example, an IP address, a hash, an email address, and so on.

  Currently supported observable types:

  - *domain*
  - *email*
  - *hash-md5*
  - *hash-sha1*
  - *hash-sha256*
  - *hash-sha512*
  - *ipv4*
  - *ipv6*

Warning:
If you select **EclecticIQ Observables CSV**, you need to choose at least one observable type from the **Observable types** drop-down menu, and at least one enrichment observable type from the **Enrichment observable types** drop-down list.

Create an automation user and group

It is a good idea to have one or more dedicated users and user groups, as necessary, to handle automation tasks that interact with external products or components of your system.
Automation groups bring together automation users, and they act as global controllers of the permissions the automation users require to operate.
Automation users handle automation and integration tasks such as authentication, data transmission through feeds and enrichers, or automatic entity creation as a follow-up action on a specific event.

Create an automation role

To add a new automation role, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**

- Under **User management > Roles**, click ✚ *(Create role)*
  The role editor is displayed.

✔ Input fields marked with an asterisk are required.

- Under **Create role**, define the following configuration settings:
  - **Name**: a descriptive name for the automation role.
    Example: *Systems integrator*
  - **Description**: a short description of the automation role and its purpose.
    Example: *Allows implementing data exchange interoperability between the platform and an external system.*
  - **Permissions**: from the drop-down menu select the actions the role is allowed to perform.

    Alternatively:
    - Start typing a permission name in the autocomplete text input field.
    - Select one or more filtered permissions from the list.
  - To revoke one or more permissions for the role, click the ✖ icon corresponding to the permission you want to remove, or the ✖ icon next to the drop-down arrow in the input field to remove all permissions at once.
  - Click **Save** to store your changes, or **Cancel** to discard them.

About permissions

- Permissions are associated with roles. Roles act as containers for sets of permissions defining the scope of the actions roles are authorized to perform.
- Permissions are predefined in the platform, and they are not editable or configurable. You can either grant them to roles, or revoke them.
- Permission names strive to be self-explanatory:
  Format: *${type of action} ${object of the action}*
  Example: *modify entities*
- Permissions allow two types of action:
  - **modify**: a modification permission that allows write operations.
  - **read**: a read permission that grants access to data without allowing any modifications.

To get an overview of the available permissions available on the platform, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**
- Under **User management > Permissions**, the permission overview is displayed as a table, where each permission is assigned a row.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

Whereas role-based permissions define what *actions* users are allowed to perform, group-based **Allowed sources** define what platform *data*, *assets*, and *resources* users are allowed to access.

Create an automation group

The automation group should include all the data sources — incoming feeds, enrichers, and groups — the automation users in the group need to access.

To add an automation user group, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**
- Under **User management > Groups**, click **+** *(Create group)*
  The user group editor is displayed.

Input fields marked with an asterisk are required.

- Under **Create group**, define the following configuration settings:
  - **Name**: a descriptive name for the automation user group.
    Example: *Integration automation group*
  - **Description**: a short description of the automation user group and its purpose.
    Example: *Automation group for integrations with external systems and services through incoming and/or outgoing feeds*
  - **Allowed sources**: click **+ Add** or **+ More** to add new rows as needed, where you can enter additional criteria.
    - **Sources**: from the drop-down menu select one or more data sources the automation user group and its members can access to fetch data from.
      Data sources can be existing incoming feeds, enrichers, as well as other user groups.

      Whereas role-based permissions define what *actions* users are allowed to perform, group-based **Allowed sources** define what platform *data*, *assets*, and *resources* users are allowed to access.
    - **TLP**: from the drop-down menu select a **Traffic Light Protocol** `(https://www.us-cert.gov/tlp)` color to filter data accordingly.
    - Click **+ Add** or **+ More** to add new rows as needed, where you can enter additional criteria.
  - **Source reliability**: from the drop-down menu select a value to filter data source reliability, so as to allow access only to data whose sources meet the specified reliability criteria.
  - Click **Save** to store your changes, or **Cancel** to discard them.

Save options

Besides committing the current data by clicking **Save**, you can also click the downward-pointing arrow on the **Save** button to display a context menu with additional save options:

- **Save and new**: saves the current data for the active item, and it allows you to start creating a new item of the same type right away. For example, a dataset, a feed, a rule, a workspace, or a task.
- **Save and duplicate**: saves the current data for the active item, and it creates a pre-populated copy of the same item, which you can use as a template to speed up manual work.

Create an automation user

To add an automation user, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**

- Under **User management > User**, click ✚ *(Create user)*
  The user editor is displayed.

✔ Input fields marked with an asterisk are required.

In the user editor define the following configuration settings:

- **First name**: enter a name that provides a short description of the automation user and its purpose.
- **Last name**: enter a name that provides a short description of the automation user and its purpose.
- **User name**: enter the designated user name to identify the user, when signed in to the platform.
  Choose a name that helps understand what the automation user does.
  Example: *platform-to-platform connector*; *platform-splunk connector*
- **Email**: an email address associated with the automation user. You can use this address to send and to receive automated notifications.
- **Active**: select this checkbox to enable the user immediately after saving the newly created user profile.
  Active users can sign in to the platform and carry out actions, based on their permissions.
- **Administrator**: select this checkbox to elevate the user's role to administrator.
  When the checkbox is selected, the user has full administrator rights and permissions.
- **Contact info**: n/a
- **PGP public key**: the user's **PGP public key** `(https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp)`, if available.
- **Locale**: from the drop-down menu select the appropriate **locale** `(https://en.wikipedia.org/wiki/locale_(computer_software))` settings for the user interface.
- **Use system timezone**: select this checkbox to override any locale-specific time zone setting with the system-defined time zone.
  When this setting is enabled, the platform retrieves the time from the host server, and it displays it in the format defined in the host server configuration.
- **Preferred timezone**: this option is available when **Use system timezone** is deselected. From the drop-down menu select the preferred time zone you want to use as a reference to display date and time in the platform for the current user profile.
- **Groups**: from the drop-down menu select one or more groups to assign the new user to.
  Alternatively, search for a group by starting typing a group name in the autocomplete text input field.
  Groups allow managing user access to platform data, assets, and resources.
- To remove the user from one or more groups, remove the relevant entries by clicking the ✖ corresponding to the group you want to remove the user from.
- **Roles**: it works like **Groups**, the only difference being that instead of adding the user to one or more groups, this option assigns one or more roles to the user.
  Roles allow managing what users are authorized to do in the platform.
- Click **Save** to store your changes, or **Cancel** to discard them.

Authentication

The basic authentication mechanism is based on **JSON web tokens** `(http://jwt.io/)`.
See the authentication section for further details and examples.

Get the feed ID

You can access and download content from an outgoing feed by specifying its ID.
A feed ID is included in the outgoing feed URL as a URL parameter.

Get the feed ID through the GUI

To get the feed ID through the platform GUI, do the following:

- On the top navigation bar, select **Data configuration > Outgoing feeds**.
- On the top-left corner of the page click the ✚ icon to open the outgoing feed editor.
- On the **Outgoing feeds** overview, browse to the feed whose ID you need to retrieve, and then click the corresponding row.
- The outgoing feed URL is loaded on the web browser address bar. For example:
  `https://${platform_host}/#/configuration/outgoing-feeds?detail=78&tab=detail`
- The `detail` URL parameter holds the feed ID.
  In the example URL, `detail=78` indicates that the selected outgoing feed ID is `78`.
  When you make an API call to retrieve the feed content, you need to include the ID value in the API endpoint.

Get the feed ID through the API

Make an API call to download a list of all available public outgoing feeds.
This call returns a JSON object with an array listing all available public outgoing feeds with HTTP transport type.

API endpoint	`/open-outgoing-feed-download/`
API method	`GET`
HTTP headers	`"Content-Type: application/json"`, `"Accept: application/json"`, `"Authorization: Bearer ${token}"`
API request	`GET` + `"Content-Type: application/json"` + `"Accept: application/json"` + `"Authorization: Bearer ${token}"` + `${platform_host}/private/open-outgoing-feed-download/`
API response	`{ "data" : [ ${open_outgoing_feed_array} ] }`

API request outgoing feeds

cURL call

```
curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/open-outgoing-feed-download/

# copy-paste version:
curl -X GET -v --insecure -i -H "Content-Type: application/json" -H "Accept: application/json" -H
"Authorization: Bearer ${token}"
```

API response outgoing feeds

```
{
  "data": [

    {
      "id": 1,
      "link": "/private/open-outgoing-feed-download/1",
      "name": "Default outgoing feed"
    },

    {
      "id": 16,
      "link": "/private/open-outgoing-feed-download/18",
      "name": "Public feed with electrolytes"
    },

    {
      "id": 25,
      "link": "/private/open-outgoing-feed-download/25",
      "name": "XYZ"
    }

  ]
}
```

Get a specific outgoing feed

Make an API call to download the details of a specific outgoing feed.
This call returns a JSON object containing the details of a specific public outgoing feed with HTTP transport type.
To select the public outgoing feed whose details you want to retrieve, include the feed ID in the API request endpoint.

API endpoint	`/open-outgoing-feed-download/${feed-id}/`
API method	`GET`
HTTP headers	`"Content-Type: application/json"`, `"Accept: application/json"`, `"Authorization: Bearer ${token}"`
API request	`GET` + `"Content-Type: application/json"` + `"Accept: application/json"` + `"Authorization: Bearer ${token}"` + `${platform_host}/private/open-outgoing-feed-download/${feed-id}/`

API response	`{ "data" : { ${specific_feed_details} } }`

API request specific outgoing feed

cURL call

```
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/open-outgoing-feed-download/18

# copy-paste version:
$ curl -X GET -v --insecure -i -H "Content-Type: application/json" -H "Accept: application/json"
-H "Authorization: Bearer ${token}" https://${platform_host}/private/open-outgoing-feed-
download/18
```

API response specific outgoing feed

The response details include an array listing the successful feed executions.

The paths in the `content_blocks` array have the following format:

`/private/open-outgoing-feed-download/${feed-id}/runs/${run-id}/content-blocks/${content-block-id}`

- A *run* is a feed execution to publish the feed content.
- A *content block* is a data blob whose format depends on the content type defined for the feed. For example, JSON, CSV or STIX.

```
{
  "data": {

    "content_blocks": [
      "/private/open-outgoing-feed-download/18/runs/0ad2edd4-8a7b-4894-b8b3-aee90a22ebaa/content-
blocks/32",
      "/private/open-outgoing-feed-download/18/runs/5fdeff71-93af-43a5-b94e-c4ab857a749c/content-
blocks/33",
      "/private/open-outgoing-feed-download/18/runs/40e31ada-06e6-4647-a287-4c9b54841619/content-
blocks/34",
      "/private/open-outgoing-feed-download/18/runs/0f56ec9c-cc1e-4aae-afd0-f693f412ad55/content-
blocks/35",
      "/private/open-outgoing-feed-download/18/runs/d842dd68-8ecf-4ecf-b073-a591d361cf26/content-
blocks/36",
      "/private/open-outgoing-feed-download/18/runs/eed28e1e-4352-42a5-8b1f-cfc918b0e0ab/content-
blocks/37",
      "/private/open-outgoing-feed-download/18/runs/f830aa7b-4ddc-4725-b13c-7cbe445f306d/content-
blocks/40",
      "/private/open-outgoing-feed-download/18/runs/a11bb585-720a-4c56-b650-90cb9d6a69e5/content-
blocks/41",
      "/private/open-outgoing-feed-download/18/runs/6e677f4b-c91d-49dd-9c39-70266987b863/content-
blocks/42"
    ],

    "id": 18,
    "name": "Public feed with electrolytes"
  }
}
```

Install and configure EclecticIQ Platform App for Splunk

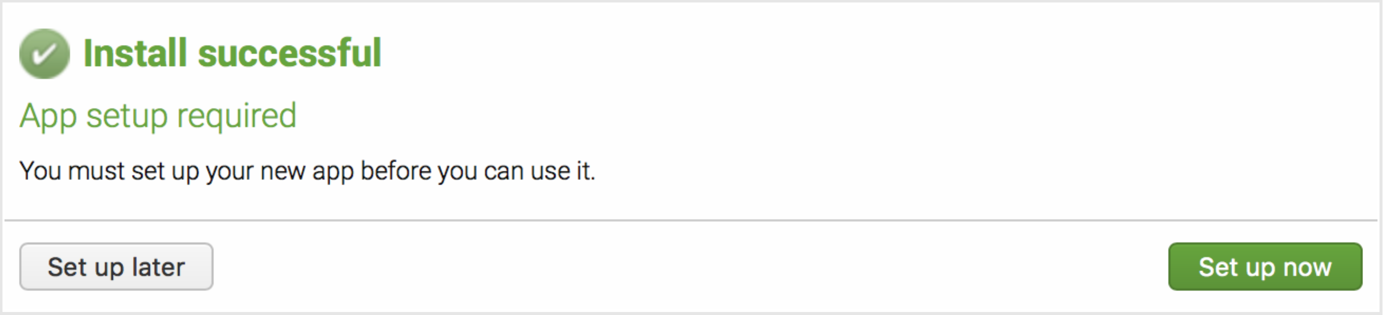
EclecticIQ Platform App for Splunk is a native application that installs directly on your Splunk instance.
This section describes how to download and install EclecticIQ Platform App for Splunk, as well as how to configure Splunk to work with the app.

EclecticIQ Platform App for Splunk consists of two modules:

- **SA for EclecticIQ**: the core app, it works with *Splunk Enterprise*.
  Everything you need is bundled with the installation package and the related files.
- **TA for EclecticIQ**: an add-on module for SA for EclecticIQ.
  The additional TA for EclecticIQ app extends the core app functionality set by adding EclecticIQ integration with *Splunk Enterprise Security*.

Download and install the core app

- Download the *eclecticiq_platform_app_for_splunk-2.0.0.tar.gz* file from **Splunkbase** `(https://splunkbase.splunk.com/app/3408/).`
- Save the archive locally.
- In the Splunk management console go to **Apps > Manage Apps**, and then click **Install app from file**.
- Browse to the location where the *eclecticiq_platform_app_for_splunk-2.0.0.tar.gz* file is stored, and then click **Upload**.
- After successfully completing the upload and the installation, restart Splunk.



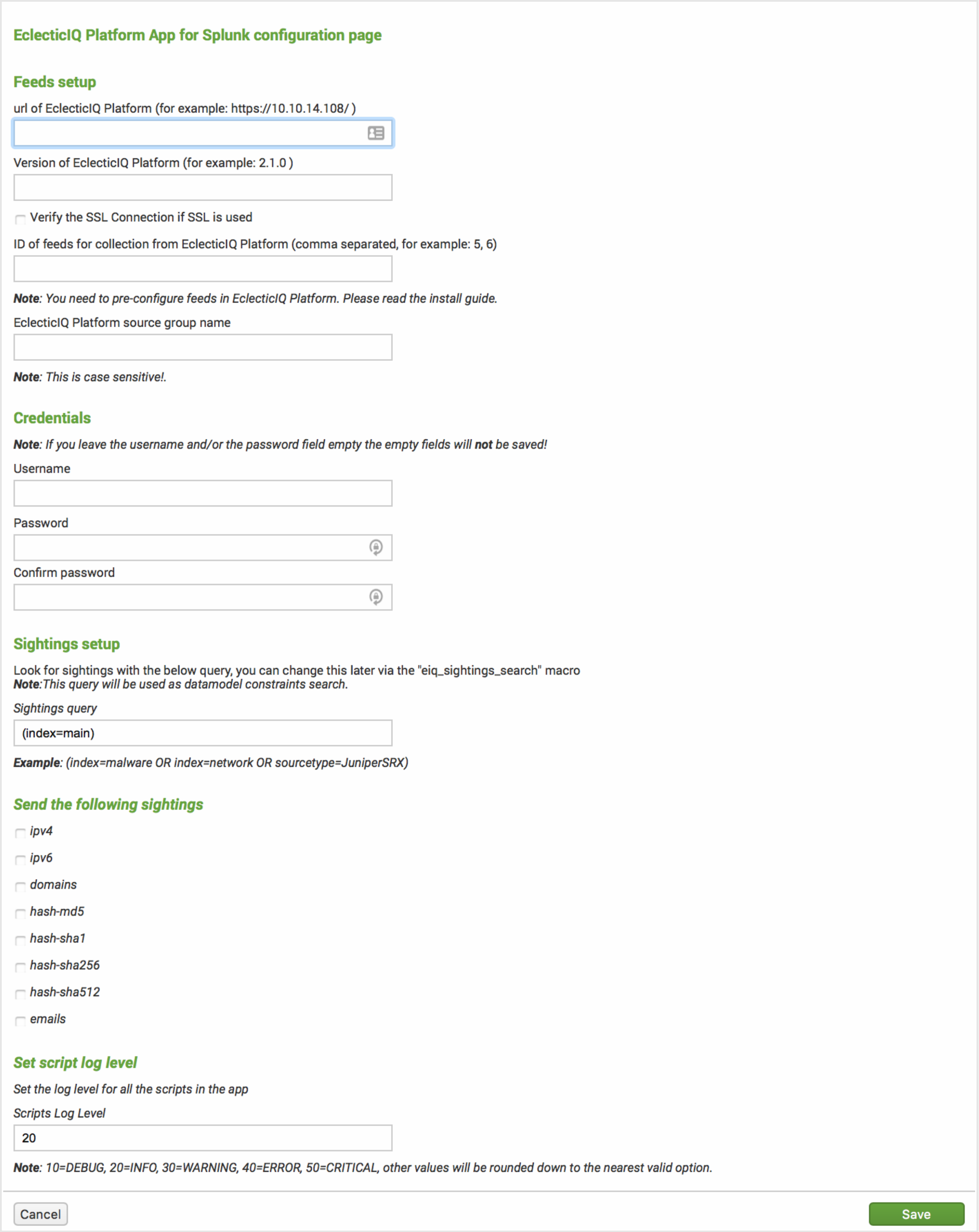
Install successful

App setup required

You must set up your new app before you can use it.

Configure the core app

After restarting Splunk, you can proceed to configuring EclecticIQ Platform App for Splunk.



EclecticIQ Platform App for Splunk configuration page

Feeds setup

url of EclecticIQ Platform (for example: https://10.10.14.108/)

Version of EclecticIQ Platform (for example: 2.1.0)

☐ Verify the SSL Connection if SSL is used

ID of feeds for collection from EclecticIQ Platform (comma separated, for example: 5, 6)

Note: *You need to pre-configure feeds in EclecticIQ Platform. Please read the install guide.*

EclecticIQ Platform source group name

Note: *This is case sensitive!.*

Credentials

Note: *If you leave the username and/or the password field empty the empty fields will **not** be saved!*

Username

Password

Confirm password

Sightings setup

Look for sightings with the below query, you can change this later via the "eiq_sightings_search" macro
Note:*This query will be used as datamodel constraints search.*

Sightings query

(index=main)

Example: *(index=malware OR index=network OR sourcetype=JuniperSRX)*

Send the following sightings

☐ *ipv4*

☐ *ipv6*

☐ *domains*

☐ *hash-md5*

☐ *hash-sha1*

☐ *hash-sha256*

☐ *hash-sha512*

☐ *emails*

Set script log level

Set the log level for all the scripts in the app

Scripts Log Level

20

Note: *10=DEBUG, 20=INFO, 30=WARNING, 40=ERROR, 50=CRITICAL, other values will be rounded down to the nearest valid option.*

You can configure EclecticIQ Platform App for Splunk from the connected Splunk Enterprise instance:

- In the Splunk management console go to **Apps**.
- From the app list select **EclecticIQ Platform App for Splunk**.
- On the displayed dialog window click **Continue to app setup page**.

On the **EclecticIQ Platform App for Splunk configuration** page, define the following configuration options:

- **Feeds setup**
  - **URL of EclecticIQ Platform**: enter either the domain name or the IP address of the platform instance.
    Example: *https://corp.eiq-platform.com/*; *https://10.0.2.128/*
  - **Version of EclecticIQ Platform**: enter version number of the platform instance.
    Example: *2.1.0*
  - **Verify the SSL connection if SSL is used**: select this checkbox to verify the SSL certificate used by the platform.
  - **ID of feeds for collection from EclecticIQ Platform**: enter a comma-separated list of outgoing feed IDs that the Splunk instance can download from the platform. Example: *11*; *5,9,13,78*
  - **EclecticIQ Platform source group name**: enter the name of the platform group to use as a platform data source for the Splunk instance.

ℹ The source outgoing feeds and the source group need to be already configured in the platform.

- **Credentials**
  - **Username**: enter a valid user name to sign in to the platform.
  - **Password**: enter a valid password associated with the platform user name.
  - **Confirm password**: type again the password to confirm it.

- **Sightings setup**
    - **Sightings query**: a **Splunk query** `(http://docs.splunk.com/documentation/splunk/6.6.5/searchtutorial/)` to look for sightings in specific Splunk indices and data sources.
      Example: *(index=botnet OR index=malware AND sourcetype=JuniperSRX OR sourcetype=Firepower4100)*
    - **Send the following sightings**: select one or more checkboxes to specify the data types you want search for and collect in Splunk.
      This generates sightings that are then sent on to the platform for ingestion.
      After ingestion and processing, they are stored in the platform as observables.
      Currently supported observable types:
        - *domain*
        - *email*
        - *hash-md5*
        - *hash-sha1*
        - *hash-sha256*
        - *hash-sha512*
        - *ipv4*
        - *ipv6*
    - **Set script log level**: set the severity level of the messages logging app script events.
      Log severity levels:
        - *DEBUG (10)*
        - *INFO (20)*
        - *WARNING (30)*
        - *ERROR (40)*
        - *CRITICAL (50)*

> This option does not enable log file ingestion in Splunk.
> To feed the script log file into Splunk, enable the **`[monitor://${path}]` stanza** `(https://docs.splunk.com/documentation/splunk/6.6.5/admin/inputsconf)` in the *$SPLUNK_HOME/etc/apps/SA-EclecticIQ/default/inputs.conf* file, and then set the appropriate `index` and `sourcetype` values.

- Click **Save** to save your configuration.

Download and install the add-on module

- Download the *eclecticiq_platform_add_on_for_splunk_es-1.0.0.tar.gz* file from **Splunkbase** `(https://splunkbase.splunk.com/app/3408/).`
- Save the archive locally.
- In the Splunk management console go to **Apps > Manage Apps**, and then click **Install app from file**.
- Browse to the location where the *eclecticiq_platform_add_on_for_splunk_es-1.0.0.tar.gz* file is stored, and then click **Upload**.
- After successfully completing the upload and the installation, restart Splunk.

Configure the add-on module

To enable TA for EclecticIQ, you need to add the JSON key/value pairs listed below to the *log_review.conf* file, `[incident_review]` stanza, `event_attributes` list.

- In a terminal session, copy the *log_review.conf* file from the */SA-ThreatIntelligence/default* dir to the */SA-ThreatIntelligence/local* dir:

```
$ cp $SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/default/log_review.conf
$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/log_review.conf
```

- Open *$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/log_review.conf*, browse to the `[incident_review]` stanza and to the `event_attributes` list.
  The `event_attributes` list cannot add custom JSON key/value pairs without risking losing existing data in the list.
- Copy-paste the following JSON key/value pairs and add them to the list.
  These data pairs need to be at the top of the list, that is, insert them immediately after `event_attributes = [`, and before the first `{` in the list.

```
{"field":"value_url_eiq",               "label":"EIQ platform value URL"},\
{"field":"meta.tlp_eiq",                "label":"EIQ TLP"},\
{"field":"meta__tlp_eiq",               "label":"EIQ TLP"},\
{"field":"meta.relevancy_eiq",          "label":"EIQ relevancy score"},\
{"field":"meta__relevancy_eiq",         "label":"EIQ relevancy score"},\
{"field":"meta.entity_url_eiq",         "label":"EIQ platform entity URL"},\
{"field":"meta__entity_url_eiq",        "label":"EIQ platform entity URL"},\
{"field":"feed_id_eiq",                 "label":"EIQ feed ID"},\
{"field":"entity.type_eiq",             "label":"EIQ entity Type"},\
{"field":"entity__type_eiq",            "label":"EIQ entity Type"},\
{"field":"entity.id_eiq",               "label":"EIQ entity ID"},\
{"field":"entity__id_eiq",              "label":"EIQ enitiy ID"},\
{"field":"value_eiq",                   "label":"EIQ sighting value"},\
{"field":"type_eiq",                    "label":"EIQ sighting type"},\
```

Example:

```
[incident_review]
event_attributes = [
  { "field":"value_url_eiq",        "label":"EIQ platform value URL" },
  { "field":"meta.tlp_eiq",         "label":"EIQ TLP" },
  { "field":"meta__tlp_eiq",        "label":"EIQ TLP" },
  { "field":"meta.relevancy_eiq",   "label":"EIQ relevancy score"},
  { "field":"meta__relevancy_eiq",  "label":"EIQ relevancy score"},
  { "field":"meta.entity_url_eiq",  "label":"EIQ platform entity URL"},
  { "field":"meta__entity_url_eiq", "label":"EIQ platform entity URL"},
  { "field":"feed_id_eiq",          "label":"EIQ feed ID"},
  { "field":"entity.type_eiq",      "label":"EIQ entity Type"},
  { "field":"entity__type_eiq",     "label":"EIQ entity Type"},
  { "field":"entity.id_eiq",        "label":"EIQ entity ID"},
  { "field":"entity__id_eiq",       "label":"EIQ enitiy ID"},
  { "field":"value_eiq",            "label":"EIQ sighting value"},
  { "field":"type_eiq",             "label":"EIQ sighting type"},
  {   ...   }
]
```

- Save the *log_review.conf* file.
- In Splunk, refresh the **Incident review** screen by pressing **F5**.
  The new fields are now visible with a notable event.

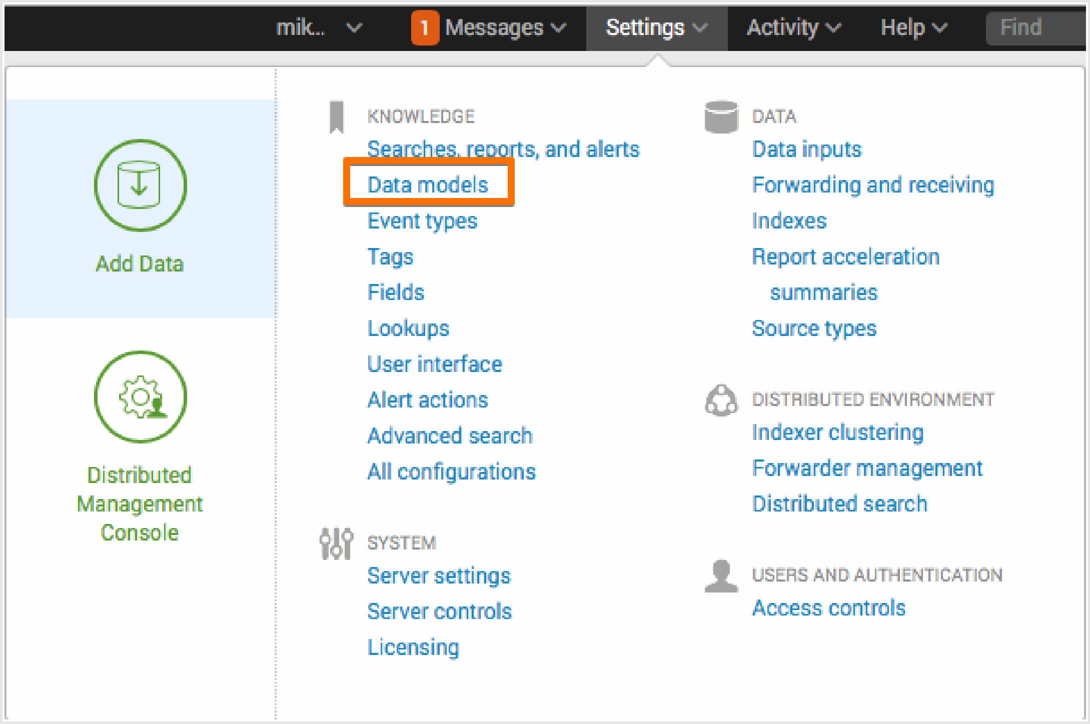
To obtain an information overview of the detected sightings and to add sighting fields to the *log_review.conf* file, `[incident_review]` stanza, enable **notable events** `(http://docs.splunk.com/documentation/es/4.7.4/admin/customizenotables)`, and the **correlation search** `(http://docs.splunk.com/documentation/es/4.7.4/tutorials/correlationsearch)` provided with the TA for EclecticIQ add-on module.

Configure data model acceleration

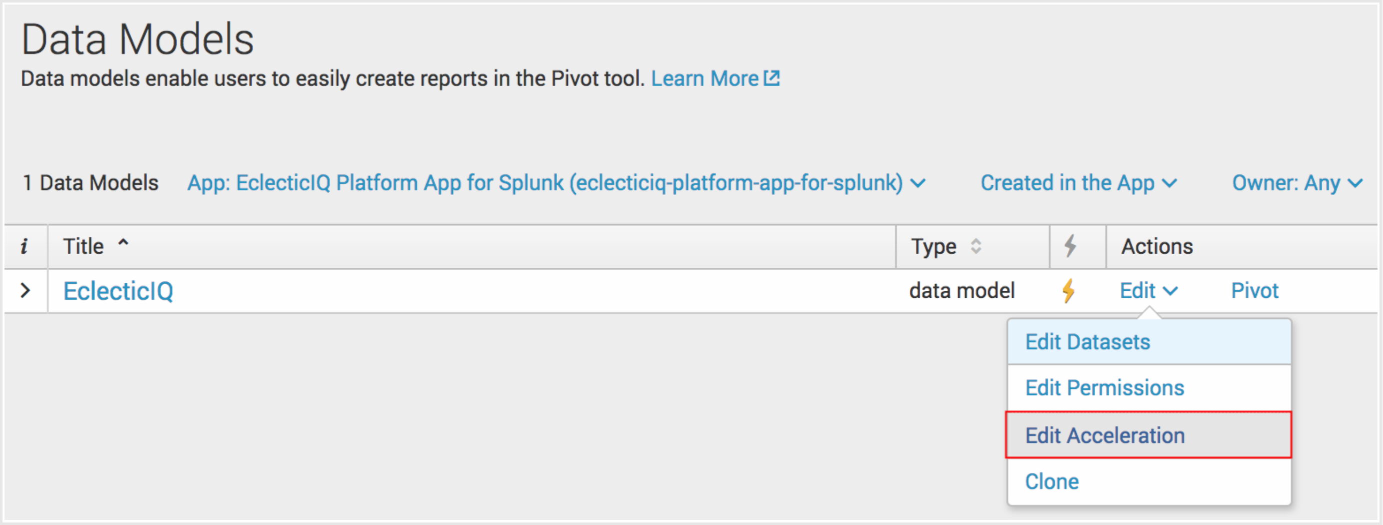
By default, **data model acceleration** `(https://docs.splunk.com/documentation/splunk/latest/knowledge/acceleratedatamodels)` is configured to speed up data models within 7 days.

To modify the data model acceleration settings, do the following:

- In Splunk, go to **Settings > Data models**.



- Browse to the **EclecticIQ** row, and then select the **Edit > Edit Acceleration** menu option.



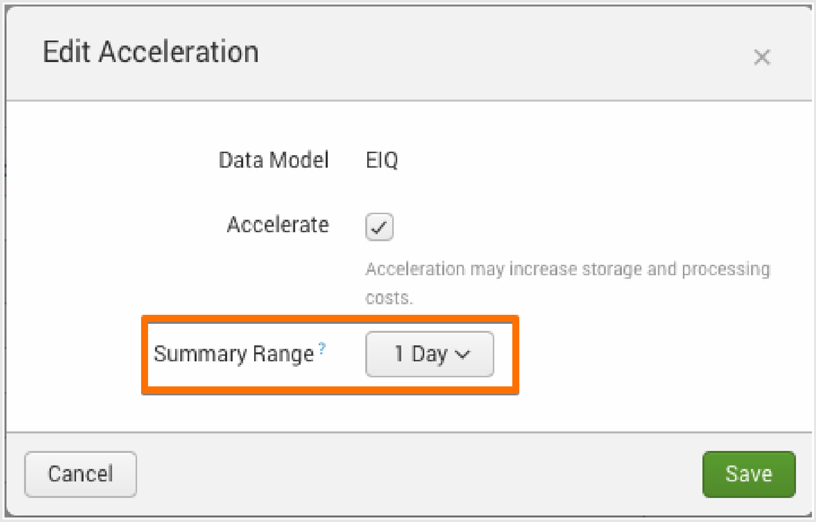
Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

1 Data Models | App: EclecticIQ Platform App for Splunk (eclecticiq-platform-app-for-splunk) | Created in the App | Owner: Any

i	Title	Type	⚡	Actions
>	EclecticIQ	data model	⚡	Edit Pivot

- In the displayed dialog window, make sure the **Accelerate** checkbox is selected.
- From the **Summary Range** drop-down menu, select the time interval you want data to base acceleration on.



Edit Acceleration

Data Model: EIQ

Accelerate: ☑

Acceleration may increase storage and processing costs.

Summary Range: 1 Day

- Click **Save** to save and store your edits.

Default job schedule

- *eiq_collect_feeds.py* is the script that collects outgoing feed data from EclecticIQ Platform.
  - *inputs.confs* stanza: `[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_collect_feeds.py]`
  - By default, the collection script is configured to run *every 2 minutes* — Cron schedule: `*/2 * * * *`
- *eiq_send_sightings.py* is the script that sends sightings to EclecticIQ Platform. To change the script execution schedule, edit the corresponding `interval` cron expression.
  - *inputs.confs* stanza: `[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_send_sightings.py]`
  - By default, the sighting script is configured to send sightings back to the platform *once a day at 01:00* — Cron schedule: `0 1 * * *`

Customize the job schedule

You can change the job schedules in the following configuration file: *$SPLUNK_HOME/etc/apps/SA-EclecticIQ/default/inputs.conf*

This is the default version of the file that ships with the app:

```
[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_send_sightings.py]
disabled = false
interval = 0 1 * * *
passAuth = splunk-system-user
send_index_as_argument_for_path = false

[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_collect_feeds.py]
disabled = false
interval = */2 * * * *
passAuth = splunk-system-user
send_index_as_argument_for_path = false

[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_setup_handler.py]
disabled = true
passAuth = splunk-system-user
send_index_as_argument_for_path = false

[monitor://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/logs/SA-EclecticIQ.log]
disabled = true
index = main
sourcetype = EclecticIQ:scripts
```

Scripts

Collection script

- *eiq_collect_feeds.py* is the script that collects outgoing feed data from EclecticIQ Platform.
    - *inputs.confs* stanza: `[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_collect_feeds.py]`
    - By default, the collection script is configured to run *every 2 minutes* — Cron schedule: `*/2 * * * *`

To change the script execution schedule, edit the corresponding `interval` cron expression.
When editing cron expressions, take note of the following:

- If the platform outgoing feed is configured as a **Diff** feed, the cron expression defining the script schedule should span over a shorter time interval than the outgoing feed execution schedule. This makes sure you do not miss feed updates.

  Example: if the outgoing feed is scheduled to run every 30 min, set the script schedule so that the script runs more often than that.
  For example, define a cron expression that runs the script every 15 minutes: `*/15 * * * *`
- If the platform outgoing feed is configured as a **Replace** feed, too many items in the feed payload may cause a timeout.
  In tests the script could process about 25-30 rows per second.
  Multiply this value times the session timeout value to obtain an estimate of the maximum amount of items you can publish through the feed.

  Example: a session timeout is set to 30 minutes.
  *30 minutes * 60 seconds * 25 rows per second = 45,000 entries per feed run*
  One block of data can hold max. 500 rows, so processing it can take about 20 seconds.
  To know exactly how long it takes to process a block of data, enable debug logging and inspect the log file: in debug mode, the script writes performance stats to the log.

The collection script writes downloaded data directly to the **Splunk KV store** `(http://dev.splunk.com/view/webframework-developapps/sp-caaaezk)` instead of a local CSV lookup file. This strategy prevents bundle replication problems with large feeds.

The collection script is **search head cluster** `(http://docs.splunk.com/documentation/splunk/6.6.5/distsearch/shcarchitecture)`-aware: in a search head cluster, the search head captain is the only cluster member responsible for downloading the feed content from the platform, and for updating the Splunk KV store.

The KV store is automatically replicated across the members of a search head cluster. This ensures that all the systems have the same information, and that the platform does not receive feed update requests from all the cluster members. Besides preventing potentially DDoS-like request overflows to the platform from large search head clusters, it also avoids unnecessary data replication and identical data conflicts among cluster members.

Sighting script

- *eiq_send_sightings.py* is the script that sends sightings to EclecticIQ Platform. To change the script execution schedule, edit the corresponding `interval` cron expression.
  - *inputs.confs* stanza: `[script://$SPLUNK_HOME/etc/apps/SA-EclecticIQ/bin/eiq_send_sightings.py]`
  - By default, the sighting script is configured to send sightings back to the platform *once a day at 01:00* — Cron schedule: `0 1 * * *`

To change the script execution schedule, edit the corresponding `interval` cron expression.
When editing cron expressions, take note of the following:

- *EclecticIQ_Sightings* is a preconfigured sighting collection search that runs every day at midnight — Cron schedule: `0 0 * * *`
  It is advisable to change the schedule of this search, so that *EclecticIQ_Sightings* runs before the *eiq_send_sightings.py* script. This ensures that only new sightings are forwarded for ingestion to the platform

For further details on Splunk cron expressions, see the official **Splunk documentation on cron expressions** `(http://docs.splunk.com/documentation/splunk/latest/alert/defineschedule dalerts#using_cron_expressions` and their **answers to common questions on cron expressions** `(https://answers.splunk.com/answers/120603/cron-expression-in-splunk.html).`

After correctly configuring EclecticIQ Platform App for Splunk to integrate and work with Splunk, the corresponding dashboard view should become populated with relevant results.