EclecticIQ Platform user guide

Publish and share intel with outgoing feeds — 4/4

Last generated: January 12, 2018

Table of contents

User guide to EclecticIQ Platform

This user guide helps you configure the main options of the platform, as well as familiarize with EclecticIQ Platform, so that you can start collecting and analyzing potential threats efficiently.

Scope

The user guide to EclecticIQ Platform aims at providing clear and to-the-point help to get you acquainted with the threat intelligence platform, so that you can configure it as needed, and you can use it to collect and analyze intelligence on potential threats, as well as share it and collaborate with other analysts.

Although it is not a complete reference manual, this guide shows end-users how they can use the platform and its rich feature set to collect data, to analyze and investigate potential threats, and to collaborate and share intelligence with other analysts.

Goal

Learn how to incorporate the platform in your daily workflow as a poweful tool to:

- Automate data ingestion
- View, edit, create, and delete platform entities
- Enrich entities with additional contextual details
- Analyze entities on the graph to identify potential threats and their relationships
- Search, filter, and slice data using rules
- Share your findings and collaborate

Audience

This document targets the following audience:

- Cyber threat intelligence analysts
- Cyber threat intelligence specialists

Feedback

No one reads manuals, ever. We know.
Yet, we strive to give you clear, concise, and complete documentation that helps you get stuff done neatly.

We are committed to crafting good documentation, because life is too short for bad doc.
We appreciate your comments, and we'd love to hear from you: if you have questions or suggestions, drop us a line and share your thoughts with us!

The Product Team

Configure outgoing feeds

Configure outgoing feeds to publish cyber threat intelligence through the platform to instrument external tools and devices, and to share intelligence with selected recipients within the organization, as well as with external third-parties.

EclecticIQ Platform uses outgoing feeds to publish and share cyber threat intelligence in multiple formats through a number of configurable transport channels.

- You can share intelligence with co-workers and teams within the organization, as well as with external recipients such as clients and consumers.
- You can use outgoing feeds to route data to external devices to initiate follow-up actions based on the data type being transmitted, and on the receiving system or device.

Outgoing feeds are a powerful tool to disseminate intelligence and to promote constructive collaboration, as well as to programmatically act on intelligence by automating tasks in your security toolchain.

Once it is set up and it is running, an outgoing feed provides a data stream that the intended recipients can consume. For example, an external device can receive platform data through an outgoing feed, and it can react to it by initiating predefined actions such as closing open ports or blacklisting malicious IP addresses and domain names.

A minimal outgoing feed configuration includes:

- A *data source*: the data source of an outgoing feed is always a dataset.
  You can configure as many datasets as necessary to act as sources for an outgoing feed.
- A *transport type*: the vehicle carrying the data.
  Typically, this is a communications protocol like TAXII, HTTP, FTP, IMAP, or Syslog.
- A *content type*: the outgoing data format the platform is publishing through the outgoing feed.
  For example, STIX, JSON, CSV, or plain text.
- An *update strategy*: the condition(s) defining how content is selected for inclusion in the outgoing feed.
  For example, you can choose to include in an outgoing feed only new entities, or both new and existing entities.

This article describes how to configure the **general options** for outgoing feeds to publish EclecticIQ Platform data. These options are identical for all outgoing feeds.

To configure transport type and content type, as well as any other specific options for a particular outgoing feed, follow the links under Configure transport and content for specific outgoing feeds.

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.

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 TLP filters

- **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.
- **Filter TLP** includes in the ourtgoing feed any entities flagged with the selected TLP color code, as well as entities whose TLP color indicates that they are suitable for progressively broader audiences.
  For example, if you select green, the feed includes entities with TLP set to green and 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.

Anonymize data

In this section you can define specific fields and data to be either excluded from the outgoing feed, or replaced with other data. Data anonymization enables you to remove sensitive data from the published content, or to replace it with other non-sensitive information that can be safely disclosed.

Anonymization works only at entity level. It is not possible to anonymize data inside observables. You can anonymize entity data before publishing it through an outgoing feed in one of the following ways:

- You can flag data to be *skipped*: the data is excluded from the outgoing feed.
- You can flag data to be *replaced*: the data is replaced with the specified replacement data before being published through the outgoing feed.

Skip paths

In this field you can define specific entity fields, that is, specific locations in the entity JSON data structure whose data values you want to exclude from the outgoing feed.
Any values related to the paths you define in this field are ignored.

- **Skip paths**: from the drop-down menu select one or more options to define which fields and related values in the entity data structure you want to exclude from the outgoing feed content.

  The available options represent and map to corresponding JSON paths in the JSON data structure representing entities in the platform.
  The JSON path root is the top-level `data` field, and it is implicit in the JSON paths the menu options map to.

  Skip paths defines the place in the entity data structure where you want to look for specific data values that you do not want to publish with the outgoing feed.
  The platform searches for the specified entity fields and the corresponding values, and it strips the data before publication. This action applies to all entities published through the outgoing feed.

  From the drop-down menu select the entity field(s) to ignore:

Path option	JSON path	Entity type
Information source, Identity	`information_source.identity`	All
Information source, References	`information_source.references[]`	All
Title	`title`	All
Affected assets, Properties affected	`affected_assets[].nature_of_security_effect_properties_affected`	Incident
Observables	`observable`	Indicator
Sightings	`sightings`	Indicator
Raw events	`raw_events`	Sightings
Security control, Identity	`security_control.identity`	Sightings
Security control, References	`security_control.references[]`	Sightings
Resources, Infrastructure	`resources.infrastructure`	TTP
Resources, Persona	`resources.persona`	TTP

Replace paths

This feature allows defining specific entity fields and specific data patterns related to those fields that the rule should replace with user-defined values, before publishing the data through the outgoing feed.

To replace values in one or more entity fields with other values that are suitable for publication do the following:

- Click **✚ Add** or **✚ More** to add a filtering option.

- **Path**: from the drop-down menu select an option to define which field in the entity data structure you want to search for values in.

  The available options represent and map to corresponding JSON paths in the JSON data structure representing entities in the platform.
  The JSON path root is the top-level `data` field, and it is implicit in the JSON paths the menu options map to.

  Path defines the place in the entity data structure where you want to look for a specific data value that you want to exclude from publishing. This option works together with a specified regex to set the data pattern the rule should use to retrieve the desired matching value in the field defined in **Path**.

  From the drop-down menu select the entity field(s) to ignore:

Path option	JSON path	Entity type
Information source, Identity	`information_source.identity`	All
Information source, References	`information_source.references[]`	All
Title	`title`	All
Affected assets, Properties affected	`affected_assets[].nature_of_security_effect_properties_affected`	Incident
Observables	`observable`	Indicator
Sightings	`sightings`	Indicator
Raw events	`raw_events`	Sightings
Security control, Identity	`security_control.identity`	Sightings
Security control, References	`security_control.references[]`	Sightings
Resources, Infrastructure	`resources.infrastructure`	TTP
Resources, Persona	`resources.persona`	TTP

- **Pattern**: define a regex to specify the data pattern the rule should apply to search for the desired data value you want to replace.
  Wildcards are currently not supported.

  Pattern supports only the **Elasticsearch regular expression syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#regexp-syntax)`.

  The main peculiarities of the Elasticsearch query regex syntax are:

  - Anchors (`^` and `$`) are implied at the beginning and at the end of the regex. You do not need to include them in the regex you input.
  - If you insert explicit anchor characters in the **Value** field, they are interpreted as literal values.
  - You need to escape special characters (`.` `?` `+` `*` `|` `{` `}` `[` `]` `(` `)` `"` `\`).
    To escape a special character, prepend a backslash `\` to it. Example: `\{ \}`

> ✔ At this moment, Elasticsearch regular expression syntax **optional operators** (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#_optional_operators) are not supported.

- **Value**: enter the literal value that should replace the string matching the regex data pattern in the outgoing feed. This is the actual value that is published through the outgoing feed.
- Click ✚ **Add** or ✚ **More** to add new rows/new input fields as needed.

Example:

```
// Path: where to look for the values to replace
// Option: Resources, Persona
data.resources.persona

// Pattern: value(s) matching the regex are replaced
\[Aa\]l\?ateleco\*

// Value: value replacing the original value matching the regex
The Swedish Chef
```

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 run**: saves the current configuration for the feed, and it executes is right away; that is, the feed task to ingest (incoming feeds) or disseminate (outgoing feeds) intelligence is triggered upon saving the feed configuration.
- **Save and new**: saves the current configuration for the feed, and it opens a new empty form to start configuring a new feed.
- **Save and duplicate**: saves saves the current configuration for the feed, and it opens a pre-populated copy of the same feed configuration, which you can use as a template to speed up manual work.

Configure transport and content for specific outgoing feeds

- Configure Amazon S3 push transport and content
- Configure email transport and content
- Configure FTP upload transport and content
- Configure HTTP download transport and content
- Configure Mount point upload transport and content
- Configure SFTP upload transport and content
- Configure Syslog push transport and content
- Configure TAXII inbox transport and content

- Configure TAXII poll transport and content
- Exchange data between platforms

Start and stop feeds

Enable and disable feeds, as well as manually trigger a feed task run or stop a running feed.

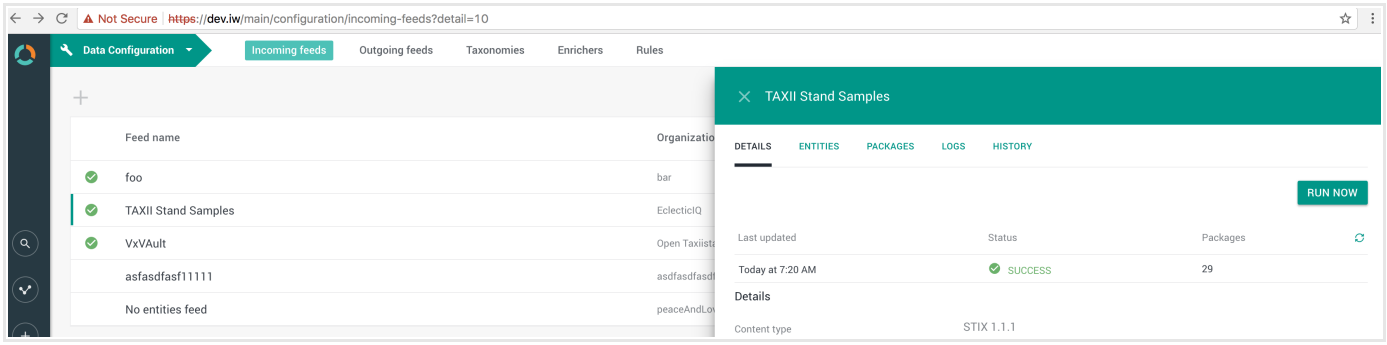
After configuring a feed, you can set a schedule to automate feed execution over time. If you do not set an execution schedule, the feed does not run, that is, it does not fetch or publish any data.

Manually start a feed

You can manually start an incoming or an outgoing feed run in one of the following ways:

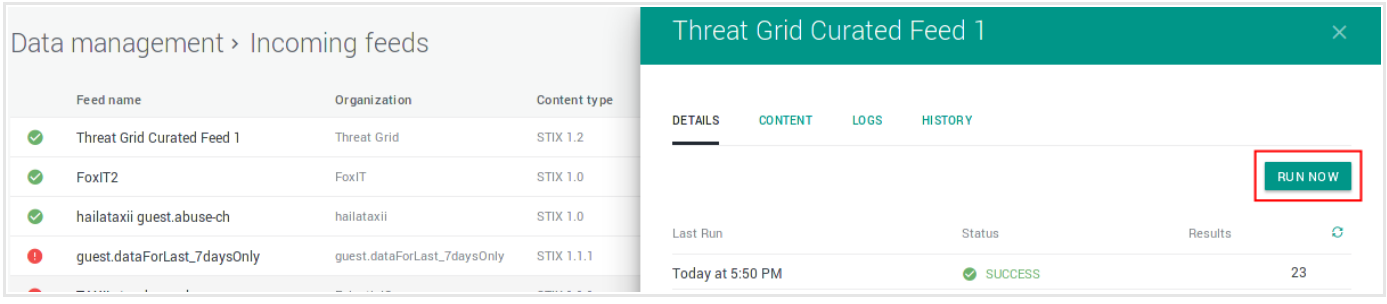
On the outgoing feed overview page

- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to run an incoming or an outgoing feed.
- On the feed overview page, click the ⋮ icon corresponding to the feed you want to run.
- From the drop-down menu select **Run now**.



On the outgoing feed entity detail pane

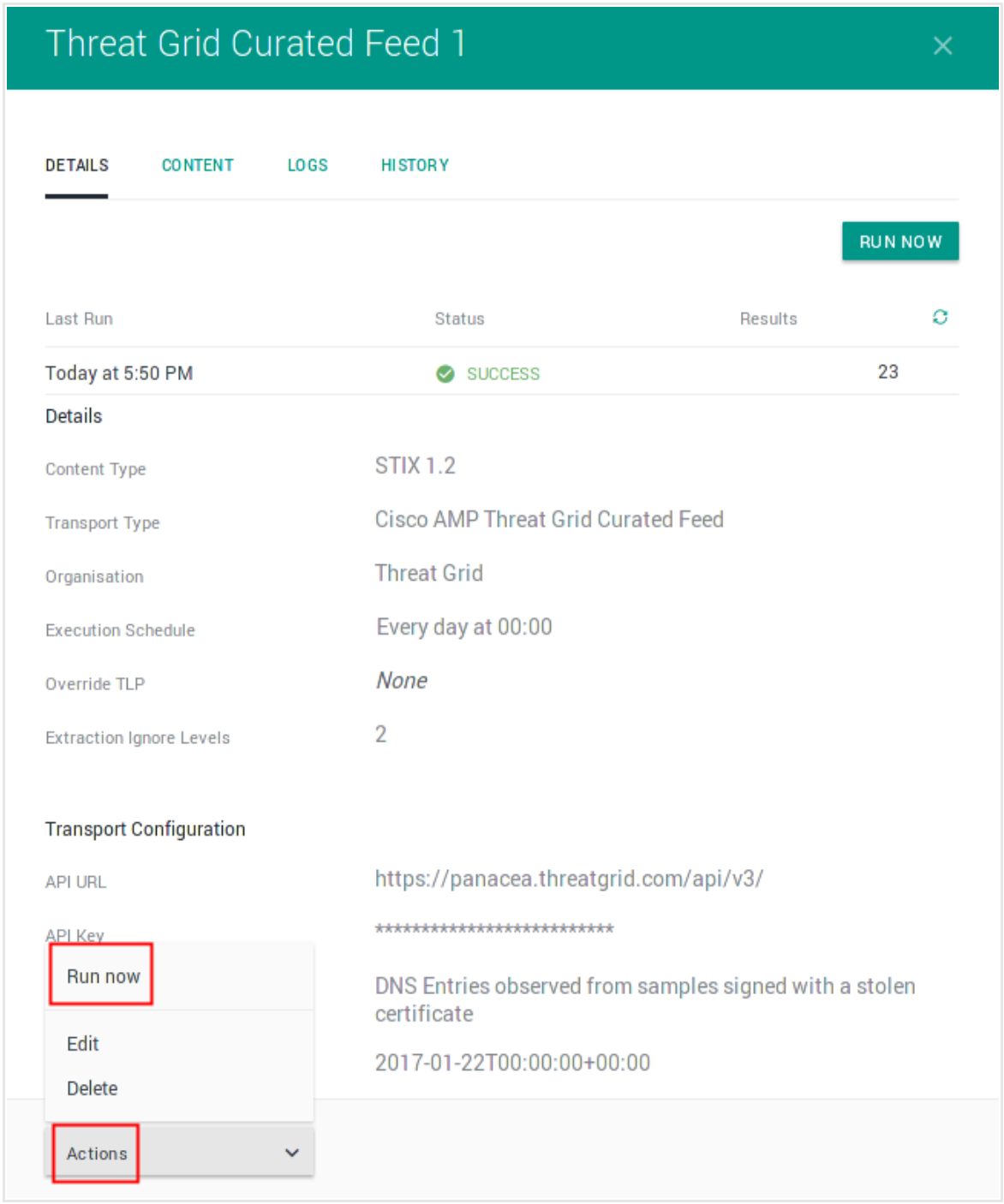
- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to run an incoming or an outgoing feed.
- On the feed overview page, click anywhere on the row corresponding to the feed you want to run.
- On the **Details** tab on feed detail pane click **Run now**.



Through the Actions menu

- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to run an incoming or an outgoing feed.
- On the feed overview page, click anywhere on the row corresponding to the feed you want to run.

- On the **Details** tab on feed detail pane, scroll to the bottom of the pane, and then click **Actions**.
- From the pop-up menu select **Run now**.



Manually stop a feed

You can either manually suspend/disable or stop/terminate a running incoming or outgoing feed.

Suspend and disable a running feed

To disable an active feed, do the following:

- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to run an incoming or an outgoing feed.
- On the feed overview page, click anywhere on the row corresponding to the feed you want to run.
- On the **Details** tab on feed detail pane click **Disable**.
  You can enable the disabled feed at any time by clicking **Enable**.

You can disable feed execution also by setting the feed execution schedule to **None**:

- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to suspend an incoming or an outgoing feed.
- On the feed overview page, click the ⋮ icon corresponding to the feed you want to run.
- From the drop-down menu select **Edit**.
- On the feed configuration page, go to the **Schedule** section, and then set **Execution schedule** to **None**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Alternatively:

- Go to **Data configuration > Incoming feeds** or to **Data configuration > Outgoing feeds**, depending on whether you want to run an incoming or an outgoing feed.
- On the feed overview page, click anywhere on the row corresponding to the feed you want to run.
- On the feed detail pane, scroll to the bottom of the pane, and then click **Actions**.
- From the drop-down menu select **Edit**.
- On the feed configuration page, go to the **Schedule** section, and then set **Execution schedule** to **None**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Stop and terminate a running feed

To stop the execution of a running feed and kill the task, do the following:

- On the left-hand navigation sidebar, click ⚙ **> System jobs > Running**.
- On the **System jobs > Running** overview page, browse to the running task(s) you want to terminate, and then click the corresponding ■ **Terminate** button to instantly stop executing the selected task(s).

Configure Amazon S3 push transport and content

Set up and configure transport and content types for Amazon S3 push outgoing feeds to securely transfer data to selected Amazon S3 buckets.

To configure the general options for the Amazon S3 push outgoing feed, see Configure outgoing feeds.

About Amazon S3 push

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
Amazon S3 push	The feed publishes entities and observables in the selected content type to the specified destination location on the designated Amazon S3 bucket. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
Amazon S3 push	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON
	Plain text value
	STIX 1.2

Configure the transport type

The Amazon S3 push transport type for outgoing feeds publishes data in the supported content types to the specified location on the designated Amazon S3 bucket.

- **Transport type**: from the drop-down menu select **Amazon S3 push**.

Under **Transport configuration** set the Amazon S3 push transport type options:

- **Secret key**: sign up to Amazon Web Services, and then create one or more accounts, as necessary, to use their S3 data storage service. The secret key is part of your authentication credentials to log in to and access Amazon S3 services.
- **Access key**: along with your secret key, the access key enables you to authenticate to access Amazon S3 services.
- **Bucket**: the name of the Amazon S3 bucket to use as a target location for the outgoing feed published content.
  Buckets `(https://docs.aws.amazon.com/amazons3/latest/dev/usingbucket.html)` are data containers in the S3 environment.
  Buckets are region-specific, and their names need to comply with standard DNS naming conventions.
  The default format of the URL to access a bucket is *https://${bucket_name}.s3-${aws-region}.amazonaws.com*
- **Path**: the path to the target directory where the outgoing feed published content is stored, relative to the bucket root.
  Example: */intel/actors/hacktivists*

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **Amazon S3 push** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.

- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..

- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure FTP upload transport and content

Set up and configure transport and content types for FTP upload outgoing feeds to publish selected platform data to an FTP server.

To configure the general options for the FTP upload outgoing feed, see Configure outgoing feeds.

About FTP upload

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
FTP upload	The feed publishes entities and observables in the selected content type to the specified destination location on an FTP server. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
FTP upload	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON

Transport type	Allowed content types
	Plain text value
	STIX 1.2

Configure the transport type

The FTP upload transport type for outgoing feeds publishes data in the supported content types to the specified location on the target FTP server.

- **Transport type**: from the drop-down menu select **FTP upload**.

Under **Transport configuration** set the FTP transport type options:

- **FTP server URL**: the target `ftp://` location on the FTP server to upload the outgoing feed content to, so as to make it available for retrieval.
  Example: *ftp://ftp.server.com/feeds/outgoing/folder*
- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated server location.
- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.
- **Include documents attached to entities**: select this checkbox to to include in the outgoing feed also any attachments to the entities such as MS Word documents or PDF files.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **FTP upload** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.

- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.

- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*

- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure HTTP download transport and content

Set up and configure transport and content types for HTTP download outgoing feeds to publish selected platform data to an HTTP server.

To configure the general options for the HTTP download outgoing feed, see Configure outgoing feeds.

About HTTP download

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
HTTP download	The feed publishes entities and observables in the selected content type through the platform API. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

HTTP endpoints

The default platform API endpoints for HTTP download outgoing feeds are:

- `https://${platform_host}/api/open-outgoing-feed-download/` for publicly accessible outgoing feeds. These feeds publish content that all platform users can access.
- `https://${platform_host}/api/outgoing-feed-download/` for non-publicly accessible outgoing feeds. These feeds publish content that only the intended recipients can access.

You can append additional elements to the URL to retrieve specific content from an HTTP download outgoing feed:

- `https://${platform_host}/api/open-outgoing-feed-download/{feed_id}/runs/latest`: replace `{feed_id}` with the outgoing feed ID reference to retrieve all packages from the latest outgoing feed task run.
  - The feed ID is the integer value in the `&detail={integer}` URL element in the URL pointing to the **Details** tab of the outgoing feed detail pane.

- `https://${platform_host}/api/open-outgoing-feed-download/{feed_id}/runs/{run_id}`: replace `{feed_id}` with the outgoing feed ID reference and `{run_id}` with the desired outgoing feed task run identifier value to retrieve all packages form a specific outgoing feed task run.
  - To retrieve the task run ID, do the following:
    - On the top navigation bar click ⚙ **> System jobs > Succeeded** .
    - On the successfully completed system job overview, look for the desired task run ID under the **ID** column.
- `https://${platform_host}/api/open-outgoing-feed-download/{feed_id}/runs/{run_id}/content-blocks/latest`: replace `{feed_id}` with the outgoing feed ID reference and `{run_id}` with the desired outgoing feed task run identifier value to retrieve the latest/most recent package from a specific outgoing feed task run.
- `https://${platform_host}/api/open-outgoing-feed-download/{feed_id}/runs/{run_id}/content-blocks/{block_id}`: replace `{feed_id}` with the outgoing feed ID reference, `{run_id}` with the desired outgoing feed task run identifier value, and `{block_id}` with the desired content block ID reference to retrieve a specific package from a specific outgoing feed task run.
  - To retrieve the content block ID, do the following:
    - In the web browser address bar, enter the URL pointing to the list of all content blocks in the specified outgoing feed: `https://${platform_host}/api/open-outgoing-feed-download/{feed_id}`
    - The `data.content_block` JSON array lists the URLs pointing to all the content blocks belonging to the outgoing feed.
    - The content block ID is the integer value at the end of the URL.

Example:


```
{
  "data": {
    "content_blocks": [
      "/private/open-outgoing-feed-download/12/runs/ff7458fg-c63b-4f94-a811-ffa87a254d98/content-blocks/98",
      "/private/open-outgoing-feed-download/12/runs/678bf255-0835-4994-a0ed-d98ac98aaa58/content-blocks/44",
      "/private/open-outgoing-feed-download/12/runs/c4a394e9-0a8f-42ca-ad4b-72cc3762afd7/content-blocks/32",
      "/private/open-outgoing-feed-download/12/runs/bf711b50-c2a1-4f5t-994f-ec1c481ace3d/content-blocks/11"
    ],
    "id": 4,
    "name": "Download CSV Line per entity"
  }
}
```


The same URL format applies to the `https://${platform_host}/private/outgoing-feed-download/` for non-publicly accessible HTTP download outgoing feeds.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
HTTP download	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON
	Plain text value
	STIX 1.2

Configure the transport type

The HTTP download transport type for outgoing feeds publishes data in the supported content types to the specified location on the target HTTP download.

- **Transport type**: from the drop-down menu select **HTTP download**.

Under **Transport configuration** set the HTTP transport type options:

- **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).

> **Warning:**
> Before deleting a group, check that is not an authorized group in an outgoing feed configuration.
> Deleting a group that is currently selected as an authorized group to access the outgoing feed content breaks the outgoing feed functionality.
>
> If you need to remove such a group:
>
> - First, remove it from the **Authorized group** selection in the relevant outgoing feed(s).
> - Then, proceed to delete the group.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **HTTP download** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.

- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure Mount point upload transport and content

Set up and configure transport and content types for Mount point upload outgoing feeds to publish selected platform data to a specific location on a local or network unit.

To configure the general options for the Mount point upload outgoing feed, see Configure outgoing feeds.

About Mount point upload

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
Mount point upload	The feed publishes entities and observables in the selected content type to the specified destination location on a local or network unit. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
Mount point upload	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON

Transport type	Allowed content types
	Plain text value
	STIX 1.2

Configure the transport type

The Mount point upload transport type for outgoing feeds publishes data in the supported content types to the specified location on a local or network unit.

- **Transport type**: from the drop-down menu select **Mount point upload**.

Under **Transport configuration** set the mount point transport type options:

- **Mount point path**: the path to the local or network unit to save the outgoing feed content to, so as to make it available for retrieval.
  Example: */media/feeds/outgoing/folder*

Warning:
You need to *explicitly whitelist mount point paths* to make them accessible to outgoing feeds.
If you do not whitelist the mount point path an outgoing feed should access to retrieve data for publication, the feed will not be able to produce any content.
To whitelist a mount point path open the platform settings file:

```
$ sudo vi /opt/eclecticiq/etc/eclecticiq/platform_settings.py
```

Look for the `MOUNT_POINT_PUSH_ALLOWED_DIRECTORIES` parameter.
It is a list that takes valid directory paths as list elements.
Each path in the list points to a location an outgoing feed can access to fetch the data to be published.
Outgoing feeds can access files and directories *inside* the specified location, based on the configured access rights of the available assets and resources.

Add as many paths to the list as necessary, then save the file and exit.
Example:

```
# Whitelist specific dirs; specific file types; everything inside a dir subdirs
MOUNT_POINT_PUSH_ALLOWED_DIRECTORIES = [ "/mnt/", "/media/", "/media/pirated-movies/" ]
```

Restart the *platform-api* service to make the changes effective:

```
$ sudo supervisorctl restart platform-api
```

- **Include documents attached to entities**: select this checkbox to to include in the outgoing feed also any attachments to the entities such as MS Word documents or PDF files.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **Mount point upload** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.

- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure email transport and content

Set up and configure transport and content types for Send email outgoing feeds to publish selected platform data as email attachments.

To configure the general options for the Send email outgoing feed, see Configure outgoing feeds.

About Send email

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
Send email	The feed publishes entities and observables in the selected content type as email attachments to the intended recipients. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
Send email	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON

Transport type	Allowed content types
	Plain text value
	STIX 1.2

Configure the transport type

- **Transport type**: from the drop-down menu select **Send email**.

Under **Transport configuration** set the email transport type options:

- **Mail subject**: enter a short, descriptive subject for the email notifications delivered through the outgoing feed.
- **Platform groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users. All the members of the selected group(s) will receive email notifications with the outgoing feed data.
- **Platform users**: if you want to further limit the outgoing feed email recipients to only some members of the selected group(s), from the drop-down menu select one or more users. In this case, only the selected users belonging to the designated platform groups receive the outgoing feed email notifications.
- **Include documents attached to entities**: select this checkbox to to include in the outgoing feed also any attachments to the entities such as MS Word documents or PDF files.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **Send email** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.

- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..

- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure SFTP upload transport and content

Set up and configure transport and content types for SFTP upload outgoing feeds to publish selected platform data to a SFTP server.

To configure the general options for the SFTP upload outgoing feed, see Configure outgoing feeds.

About SFTP upload

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
SFTP upload	The feed publishes entities and observables in the selected content type to the specified destination location on a SFTP server. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
SFTP upload	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON

Transport type	Allowed content types
	Plain text value
	STIX 1.2

Configure the transport type

The SFTP upload transport type for outgoing feeds publishes data in the supported content types to the specified location on the target SFTP server.

- **Transport type**: from the drop-down menu select **SFTP upload**.

Under **Transport configuration** set the SFTP transport type options:

- **SFTP server URL**: the location on the SFTP server where the data source for the feed is made available (incoming feeds) or where the feed content is being published to (outgoing feeds).
  It needs to adhere to the following format: *sftp://${sftp_server}:${port}/${path_to_target_directory}*
  Example: *sftp://sftp.server.com:22/source-data/for-the-feed*
- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated server location
- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location
- **Use SSH key**: select this checkbox to enable logging in through SSH to apply this security layer to the outgoing feed.
  - **SSH private key**: paste into this field the private SSH key you want to use to access the target location where the SFTP upload outgoing feed should publish content to.
    Example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA3Tz2mr7SZiAMfQyuvBjM9Oi..Z1BjP5CE/Wm/Rr500P
RK+Lh9x5eJPo5CAZ3/ANBE0sTK0ZsDGMak2m1g7..3VHqIxFTz0Ta1d+NAj
wnLe4nOb7/eEJbDPkk05ShhBrJGBKKxb8n104o/..PdzbFMIyNjJzBM2o5y
5A13wiLitEO7nco2WfyYkQzaxCw0AwzlkVHiIyC..71pSzkv6sv+4IDMbT/
XpCo8L6wTarzrywnQsh+etLD6FtTjYbbrvZ8RQM..Hg2qxraAV++HNBYmNW
kbJ+q+rsJxQlaipn2M4lGuQJEfIxELFDyd3XpxP..Un/82NZNXlPmRIopXs
2T91jiLZEUKQw+n73j26adTbteuEaPGSrTZxBLR..yssO0wWomUyILqVeti
+PK+aXKwguI6bxLGZ3of0UH+mGsSl0mkp7kYZCm..OTQtfeRqP8rDSC7DgA
kHc5ajYqh04AzNFaxjRo+M3IGICUaOdKnXd0Fda..QwfoaX4QlRTgLqb7AN
ZTzM9WbmnYoXrx17kZlT3lsCgYEAm757XI3WJVj..WoLj1+v48WyoxZpcai
uv9bT4Cj+lXRS+gdKHK+SH7J3x2CRHVS+WH/SVC..DxuybvebDoT0TkKiCj
BWQaGzCaJqZa+POHK0klvS+9ln0/6k539p95tfX..X4TCzbVG6+gJiX0ysz
Yfehn5MCgYEAkMiKuWHCsVyCab3RUf6XA9gd3qY..fCTIGtS1tR5PgFIV+G
engiVoWc/hkj8SBHZz1n1xLN7KDf8ySU06MDggB..hJ+gXJKy+gf3mF5Kmj
DtkpjGHQzPF6vOe907y5NQLvVFGXUq/FIJZxB8k..fJdHEm2M4=
-----END RSA PRIVATE KEY-----
```

  - **SSH key password**: if your SSH key is password-protected, enter here the password to unlock the SSH key.
    If your SSH key is not password-protected, you can leave this field empty.
- **Host authentication mode**: select this checkbox to automatically add and save the new host name and the new host key to the local Paramiko `HostKeys` dictionary.

Configure the content type

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..

- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure Syslog push transport and content

Set up and configure transport and content types for Syslog push outgoing feeds to publish selected platform data to a Syslog server.

To configure the general options for the Syslog push outgoing feed, see Configure outgoing feeds.

About Syslog push

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
Syslog push	The feed publishes entities and observables in CSV or ArcSight CEF format to the specified Syslog server. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
Syslog push	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV

Configure the transport type

The Syslog push transport type for outgoing feeds publishes data in the supported content types to an external Syslog server for log aggregation.

- **Transport type**: from the drop-down menu select **Syslog push**.

Under **Transport configuration** set the Syslog push transport type options:

- **Syslog server host**: specify the IP address or the host name of the server handling syslog message log communications.
- **Syslog server port**: specify the port number of the server handling syslog message log communications. Make sure the port is open, and that data traffic through the port is not blocked by, for example, a firewall.

Typical port settings for the TCP protocol:

- *601* for syslog-conn
- *6514* for syslog over TCP with TLS

Typical port settings for the UDP protocol:

- *514* for syslog
- **Protocol**: from the drop-down menu select the transmission protocol, either **TCP** or **UDP**.

Configure the content type

- **Content type** from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **Syslog push** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ Observables CSV

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.

- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

ArcSight CEF

The **ArcSight CEF** `(https://www.protect724.hpe.com/docs/doc-1072)` content type is suitable for machine consumption. Typical use cases include feeding an ArcSight CEF outgoing feed to a SIEM system such as **ArcSight ESM** `(https://saas.hpe.com/en-us/software/siem-security-information-event-management)` or to a Syslog server for further processing.

The **ArcSight CEF** `(https://www.protect724.hpe.com/docs/doc-1072)` content type does not have any specific configuration parameters.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

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 menu.

Configure TAXII inbox transport and content

Set up and configure transport and content types for TAXII inbox outgoing feeds to publish selected platform data through the TAXII inbox service.

To configure the general options for the TAXII inbox outgoing feed, see Configure outgoing feeds.

About TAXII inbox

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
TAXII inbox	The feed publishes entities and observables in the selected content type to the TAXII inbox service configured for the feed. You can retrieve the content by accessing the TAXII inbox service endpoint configured for the feed in the platform, and by specifying the name of the collection the outgoing feed belongs to, as well as the feed name. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
TAXII inbox	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest

Transport type	Allowed content types
	EclecticIQ JSON
	Plain text value
	STIX 1.2

Configure the transport type

The TAXII inbox transport type for outgoing feeds publishes data in the supported content types through the TAXII inbox service.

- **Transport type**: from the drop-down menu select **TAXII inbox**.

> **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII inbox** transport type requires Cabby. For further details, see the **official Cabby documentation** (https://cabby.readthedocs.org/en/latest/), the **Cabby public repo on GitHub** (https://github.com/eclecticiq/cabby), and the **Cabby download page** (https://pypi.python.org/pypi/cabby/).

Under **Transport configuration** set the TAXII inbox transport type options:

- **Auto discovery**: enter the URL pointing to a **TAXII discovery service** (https://taxiiproject.github.io/about/#how-do-you-communicate-available-taxii-services-and-their-use) that feed consumers can send a request to in order to determine the available TAXII services they can access — including the TAXII inbox outgoing feed — and poll them for updates.
  Example: *http://hailataxii.com/taxii-discovery-service*
- **Inbox service URL**: enter the URL pointing to the location of the **TAXII data collections** (https://taxiiproject.github.io/documentation/sample-use/#data-collections) available through the TAXII inbox service.
  Example:
  https://example.com/taxii-inbox
- **Destination collection name**: enter an existing collection name as the target container for the outgoing feed data.
  Example:
  collection.Default
- **Taxii version**: select the TAXII version your system supports:
  - Either **1.0** (https://taxiiproject.github.io/releases/1.0/)
  - Or **1.1** (https://taxiiproject.github.io/releases/1.1/)
- **EclecticIQ authentication URL**: the URL pointing to the EclecticIQ Platform instance, including the endpoint that takes the user name and password inputs to send them to the authentication mechanism.
  Example: *http://${platform_host}/api/auth*
- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.
- **SSL certificate authentication**: if the TAXII server requires an SSL certificate to authenticate and to authorize access to the corresponding TAXII services, select this checkbox to fill out the required information.
  - **SSL certificate**: copy-paste the content of a valid SSL certificate to authenticate.
    SSL certificate file format: PEM
    Example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxDTALBgNVBAgMBFV0YWgxDzANBgNV
BAcMBkxpbmRvbjEWMBQGA1UECgwNRGlnaUNlcnQgSW5jLjERMA8GA1UECwwIRGln
aUNlcnQxHTAbBgNVBAMMFGV4YW1wbGUuZGlnaWNlcnQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8+To7d+2kPWeBv/orU3LVbJwDrSQbeKamCmo
wp5bqDxIwV20zqRb7APUOKYoVEFFOEQs6T6gImnIolhbiH6m4zgZ/CPvWBOkZc+c
1Po2EmvBz+AD5sBdT5kzGQA6NbWyZGldxRthNLOs1efOhdnWFuhI162qmcflgpiI
WDuwq4C9f+YkeJhNn9dF5+owm8cOQmDrV8NNdiTqin8q3qYAHHJRW28glJUCZkTZ
wIaSR6crBQ8TbYNE0dc+Caa3DOIkz1EOsHWzTx+n0zKfqcbgXi4DJx+C1bjptYPR
BPZL8DAeWuA8ebudVT44yEp82G96/Ggcf7F33xMxe0yc+Xa6owIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAB0kcrFccSmFDmxox0Ne01UIqSsDqHgL+XmHTXJwre6D
hJSZwbvEtOK0G3+dr4Fs11WuUNt5qcLsx5a8uk4G6AKHMzuhLsJ7XZjgmQXGECpY
Q4mC3yT3ZoCGpIXbw+iP3lmEEXgaQL0Tx5LFl/okKbKYwIqNiyKWOMj7ZR/wxWg/
ZDGRs55xuoeLDJ/ZRFf9bI+IaCUd1YrfYcHIl3G87Av+r49YVwqRDT0VDV7uLgqn
29XI1PpVUNCPQGn9p/eX6Qo7vpDaPybRtA2R7XLKjQaF9oXWeCUqy1hvJac9QFO2
97Ob1alpHPoZ7mWiEuJwjBPii6a9M9G30nUo39lBi1w=
-----END CERTIFICATE REQUEST-----
```

  - **SSL key**: copy-paste the content of a valid SSL key to authenticate.
    SSL key file format: PEM
    Example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA3Tz2mr7SZiAMfQyuvBjM9Oi..Z1BjP5CE/Wm/Rr500P
RK+Lh9x5eJPo5CAZ3/ANBE0sTK0ZsDGMak2m1g7..3VHqIxFTz0Ta1d+NAj
wnLe4nOb7/eEJbDPkk05ShhBrJGBKKxb8n104o/..PdzbFMIyNjJzBM2o5y
5A13wiLitEO7nco2WfyYkQzaxCw0AwzlkVHiIyC..71pSzkv6sv+4IDMbT/
XpCo8L6wTarzrywnQsh+etLD6FtTjYbbrvZ8RQM..Hg2qxraAV++HNBYmNW
kbJ+q+rsJxQlaipn2M4lGuQJEfIxELFDyd3XpxP..Un/82NZNXlPmRIopXs
2T91jiLZEUKQw+n73j26adTbteuEaPGSrTZxBLR..yssO0wWomUyILqVeti
+PK+aXKwguI6bxLGZ3of0UH+mGsSl0mkp7kYZCm..OTQtfeRqP8rDSC7DgA
kHc5ajYqh04AzNFaxjRo+M3IGICUaOdKnXd0Fda..QwfoaX4QlRTgLqb7AN
ZTzM9WbmnYoXrx17kZlT3lsCgYEAm757XI3WJVj..WoLj1+v48WyoxZpcai
uv9bT4Cj+lXRS+gdKHK+SH7J3x2CRHVS+WH/SVC..DxuybvebDoT0TkKiCj
BWQaGzCaJqZa+POHK0klvS+9ln0/6k539p95tfX..X4TCzbVG6+gJiX0ysz
Yfehn5MCgYEAkMiKuWHCsVyCab3RUf6XA9gd3qY..fCTIGtS1tR5PgFIV+G
engiVoWc/hkj8SBHZz1n1xLN7KDf8ySU06MDggB..hJ+gXJKy+gf3mF5Kmj
DtkpjGHQzPF6vOe907y5NQLvVFGXUq/FIJZxB8k..fJdHEm2M4=
-----END RSA PRIVATE KEY-----
```

  - **SSL key password**: enter the SSL password or passphrase for the SSL key. This field is masked.
- **Verify SSL**: if the TAXII server requires an SSL certificate to authenticate and to access the corresponding TAXII services, you can select this checkbox to test the SSL connection and to verify that it works correctly.
  - **SSL CA bundle file path**: enter the path to the CA bundle file containing the root, intermediate, and public certificates for SSL authentication.
- Click **Save** to store your changes, or **Cancel** to discard them.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **TAXII inbox** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.

- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Configure TAXII poll transport and content

Set up and configure transport and content types for TAXII poll outgoing feeds to publish selected platform data through the TAXII poll service.

To configure the general options for the TAXII poll outgoing feed, see Configure outgoing feeds.

About TAXII poll

> Assign unique names to TAXII feeds: TAXII inbox and TAXII poll incoming and outgoing feeds should all have unique names within the platform.

This feed source enables intelligence dissemination through the following channels:

Feed	Published data
TAXII poll	The feed publishes entities and observables in the selected content type to the platform TAXII server. You can retrieve the content by accessing the TAXII poll service endpoint configured in the platform, and by specifying the name of the outgoing feed. By default, the TAXII poll endpoint is `https://${platform_host}/taxii/poll`. Each time the outgoing feed task runs, it generates a data package containing zero or more entities, depending on the outgoing feed update strategy, and on the feed data source containing data that match the feed configuration.

To view and to retrieve outgoing feed content, do the following:

- On the top navigation bar click **Data configuration > Outgoing feeds**.
- On the **Data configuration > Outgoing feeds** page, click anywhere on the row corresponding to the outgoing feed whose content you want to view or retrieve.
  The feed detail pane slides in from the side of the screen.
- On the outgoing feed detail pane click the **Content** tab.
- On the **Content** tab, click the name of a package to download it.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
TAXII poll	ArcSight CEF
	EclecticIQ Entities CSV

Transport type	Allowed content types
	EclecticIQ Observables CSV
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON
	Plain text value
	STIX 1.2

Configure the transport type

The TAXII poll transport type for outgoing feeds publishes data in the supported content types to through the TAXII poll service.

- **Transport type**: from the drop-down menu select **TAXII poll**.

Under **Transport configuration** set the TAXII poll transport type options:

- **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).
- **Collection name**: enter the name of the **TAXII data collection** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)` you want to use to group the outgoing feed content.
  The data collection name can be max. 1024 characters long, and its XML schema should comply with the **xsd:anyURI** `(https://www.w3.org/tr/xmlschema11-2/#anyuri)` data type.
  Example: *MalwareDomainList_Hostlist*

> **Warning:**
> Before deleting a group, check that is not an authorized group in an outgoing feed configuration.
> Deleting a group that is currently selected as an authorized group to access the outgoing feed content breaks the outgoing feed functionality.
>
> If you need to remove such a group:
>
> - First, remove it from the **Authorized group** selection in the relevant outgoing feed(s).
> - Then, proceed to delete the group.

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **TAXII poll** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

ArcSight CEF

The **ArcSight CEF** (https://www.protect724.hpe.com/docs/doc-1072) content type is suitable for machine consumption. Typical use cases include feeding an ArcSight CEF outgoing feed to a SIEM system such as **ArcSight ESM** (https://saas.hpe.com/en-us/software/siem-security-information-event-management) or to a Syslog server for further processing.

The **ArcSight CEF** (https://www.protect724.hpe.com/docs/doc-1072) content type does not have any specific configuration parameters.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.

- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.

- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.

- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Outgoing feeds reference

Reference section with lookup information on supported outgoing feed content types and transport types.

Available outgoing feeds

The overview lists and points to the articles on the available outgoing feeds. Each article describes how to configure the specific options for each outgoing feed.
Typically, outgoing feeds use different *transport types* and *content types*. General configuration options are identical across all outgoing feeds.

Title	Excerpt
Configure Amazon S3 push transport and content	Set up and configure transport and content types for Amazon S3 push outgoing feeds to securely transfer data to selected Amazon S3 buckets.
Configure email transport and content	Set up and configure transport and content types for Send email outgoing feeds to publish selected platform data as email attachments.
Configure FTP upload transport and content	Set up and configure transport and content types for FTP upload outgoing feeds to publish selected platform data to an FTP server.
Configure HTTP download transport and content	Set up and configure transport and content types for HTTP download outgoing feeds to publish selected platform data to an HTTP server.
Configure Mount point upload transport and content	Set up and configure transport and content types for Mount point upload outgoing feeds to publish selected platform data to a specific location on a local or network unit.
Configure SFTP upload transport and content	Set up and configure transport and content types for SFTP upload outgoing feeds to publish selected platform data to a SFTP server.
Configure Syslog push transport and content	Set up and configure transport and content types for Syslog push outgoing feeds to publish selected platform data to a Syslog server.
Configure TAXII inbox transport and content	Set up and configure transport and content types for TAXII inbox outgoing feeds to publish selected platform data through the TAXII inbox service.
Configure TAXII poll transport and content	Set up and configure transport and content types for TAXII poll outgoing feeds to publish selected platform data through the TAXII poll service.
Exchange data between platforms	Configure TAXII feeds to enable data exchange between two platform instances.

Content types

These are the data formats the platform can process through feeds.
Under *Feed type* **in** defines an input format that incoming feeds ingest; **out** defines an output format that outgoing feeds publish.

Content type	Feed type	Description
Anubis Cyberfeed JSON	in	JSON format representing entity data as JSON objects.
ArcSight CEF	out	The Common Event Format is a text-based standard for log records proposed by ArcSight. It allows sharing, consuming, and parsing event information across devices such as SIEM platforms and Syslog servers.
Cisco Threat Grid Samples JSON	in	JSON format representing entity data as JSON objects.
EclecticIQ Entities CSV	out	Comma separated CSV format for tabular data representation of entities.
EclecticIQ Observables CSV	out	Comma separated CSV format for tabular data representation of observables.
EclecticIQ HTML Report	out	Default HTML format to publish EclecticIQ intel reports.
EclecticIQ HTML Report Digest	out	Default HTML format to publish EclecticIQ intel report digests.
EclecticIQ JSON	in, out	JSON format representing entity data as JSON objects.
Intel 471	in	Intel 471 reports. Bundled observables are linked to the parent report entity. API endpoint: *https://api.intel471.com/v1/reports/{}*
PDF	in, out	Standard PDF format, preferably native (not scanned).
STIX 1.0	in, out	STIX data model **v. 1.0** `(http://stixproject.github.io/data-model/1.0/).`
STIX 1.1	in, out	STIX data model **v. 1.1** `(http://stixproject.github.io/data-model/1.1/).`
STIX 1.1.1	in, out	STIX data model **v. 1.1.1** `(http://stixproject.github.io/data-model/1.1.1/).`
STIX 1.2	in, out	STIX data model **v. 1.2** `(http://stixproject.github.io/data-model/1.2/).`
Text/Plain text value	in, out	Plain text format. This content type allows you to enter free text and literals, wildcards (where supported), as well as JSON paths to point to specific entity property fields, and regex patterns to filter data.

Content type	Feed type	Description
Threat Recon	in	Threat Recon JSON output returned by the **Threat Recon API** `(https://threatrecon.co/api)`. Threat Recon focuses on providiung information about indicators.
STIX 1.1.1	in	FireEye iSIGHT Intelligence Report API outputs reports in STIX 1.1.1 format. Reports concern threat topics such as vulnerabilities, malware, threat actors, stategies, tactics, and techniques.
BFK Threat Intelligence JSON	in	BFK reports and NIDs (Network Intrusion Detections) are saved as JSON report entities; they concern threat topics such as threat actors, targeted victims, tactics, and techniques.
Crowdstrike indicator JSON	in	Indicators retrieved from the Falcon Intelligence platform such as compromised devices, malicious domains, hashes, and so on starting from the specified polling date.
CAPEC XML	in, out	Categorizied and enumerated attack patterns, attack mechanisms, strategies, tactics and techniques retrieved from the **CAPEC** `(https://capec.mitre.org/about/index.html)` catalog.
Crowdstrike report JSON	in	Reports retrieved from the Falcon Intelligence platform in JSON format and as PDF attachments.
Crowdstrike actor JSON	in	Threat actor entities, related TTPs, indicators, and campaigns, as well as related observables to represent actor ID, target country, target industry, and targeted victim(s).
CVE Search JSON	in	Exploit target entities retrieved from **CIRCL CVE Search** `(https://www.circl.lu/services/cve-search/)`. The entity ID is derived from the **CVE ID** `(https://cve.circl.lu/)`. API endpoint: *https://cve.circl.lu/api/last*.
Intel 471 IOC Feed	in	Indicators of compromise such as IP addresses, malicious URLs, and MD5 and SHA-256 hashes. Intel 471 focuses on providing first-hand information related to threat actors and groups. API endpoint: *https://api.intel471.com/v1/search/{}*.
OpenPhish Feed Text	in	Phishing URLs are saved as indicators. The signaled phishing activities are saved as TTPs related to the corresponding indicators. API endpoint: *https://openphish.com/feed.txt*.
Proofpoint Message	in	Indicators and observables focusing on email threats such as phishing, spoofing, email malware, and impostor email/fraudulent messages API endpoint: *https://api.emaildefense.proofpoint.com/v1*.

Transport types

These are the supported communications protocols the platform uses to publish data through outgoing feeds.

Transport type	Feed type	Description
FTP upload	out	Custom feed to publish data through an FTP server.

Transport type	Feed type	Description
HTTP download	out	Custom feed to publish data through an HTTP server. By default, the outgoing feed content is available through the following platform API endpoints: `/private/open-outgoing-feed-download/` for public outgoing feeds, and `/private/outgoing-feed-download/` for private outgoing feeds.
Mount point upload	out	Custom feed to publish data from a location on a local or network unit.
Send email	out	Custom feed to publish data as email attachments.
Syslog push	out	Custom feed to share data with other devices using the Syslog protocol. Usually, Syslog messages are centralized to a Syslog server.
TAXII inbox	out	Custom feed using the TAXII inbox service to publish data.
TAXII poll	out	Custom feed using the TAXII polling service to publish data.
Amazon S3 push	out	Custom feed to publish data to the designated Amazon S3 **bucket** `(https://docs.aws.amazon.com/amazons3/latest/dev/usingbucket.html).`
SFTP upload	out	Custom feed to publish data through an SFTP server.

Exchange data between platforms

Configure TAXII feeds to enable data exchange between two platform instances.

You can exchange data between two platform instances using TAXII feeds. This is what you need to implement this platform-to-platform integration:

- A group and a user with access rights to both platform instances.
- Basic authentication
- 1 TAXII outgoing feed
- 1 TAXII incoming feed
- 2 platform instances

Let's call the publishing platform instance *Alice*. This is the *data source*.
And let's call the recipient platform instance *Barbara*. This is the *intended recipient* and the *consumer* of the feed content.

> Assign unique names to TAXII feeds: TAXII inbox and TAXII poll incoming and outgoing feeds should all have unique names within the platform.

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 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: *TAXII integration group*
  - **Description**: a short description of the automation user group and its purpose.
    Example: *Automation group for integrations through TAXII services*
  - **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.
      The 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 carry out, group-based **Allowed sources** define *what* users can act on, that is, what platform data they 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 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 actions of the corresponding roles.
- 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 carry out, group-based **Allowed sources** define *what* users can act on, that is, what platform data they are allowed to access.

It is a good idea to assign a role as few permissions as the role requires to accomplish its purpose.
The role you need for a platform-to-platform integration through a TAXII feed should be able to read data sources, feeds, and TAXII services:

- *read configurations*
- *read content-blocks*
- *read content-types*
- *read destinations*
- *read discovery-services*
- *read entities*

- *read extracts*
- *read incoming-feeds*
- *read intel-sets*
- *read outgoing-feeds*
- *read poll-services*
- *read services*
- *read sources*
- *read transports*

These are guidelines, and therefore not mandatory. You may need to tweak role permissions based on trial and error hands-on experience to best suit your environment.

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*
- **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.
- 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.
- Click **Save** to store your changes, or **Cancel** to discard them.

> For a platform-to-platform integration through a TAXII feed, you should assign the automation user to the dedicated automation user group and role.

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.

Alice: create a TAXII outgoing feed

To configure the general options for the TAXII poll outgoing feed, see Configure outgoing feeds.

Configure transport and content types

Under **Transport and content** you define *what* you want to publish and *how*, that is, the data content type and the data transport type.

Transport type	Allowed content types
TAXII poll	ArcSight CEF
	EclecticIQ Entities CSV
	EclecticIQ Observables CSV

Transport type	Allowed content types
	EclecticIQ HTML Report
	EclecticIQ HTML Report Digest
	EclecticIQ JSON
	Plain text value
	STIX 1.2

Configure the transport type

The TAXII poll transport type for outgoing feeds publishes data in the supported content types to through the TAXII poll service.

Under **Transport configuration** set the TAXII poll transport type options:

- **Public**: default setting: deselected.
  Leave it deselected to make the outgoing feed available only to the automation user group you previously created.
- **Authorized groups**: from the drop-down menu select the automation user group you previously created.
- **Collection name**: enter the name of the **TAXII data collection** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)` you want to use to group the outgoing feed content.
  The data collection name can be max. 1024 characters long, and its XML schema should comply with the **xsd:anyURI** `(https://www.w3.org/tr/xmlschema11-2/#anyuri)` data type.
  Example: *MalwareDomainList_Hostlist*

Configure the content type

- **Content type**: from the drop-down menu select the appropriate content type for the data you want to publish through the outgoing feed.
  The selected content type for the feed should match the source data format.
  This can vary, depending on the dataset source(s) you retrieve the data from.
  The **TAXII poll** transport type enables fetching data in the following formats:
  - ArcSight CEF
  - EclecticIQ Entities CSV
  - EclecticIQ HTML Report
  - EclecticIQ HTML Report Digest
  - EclecticIQ JSON
  - EclecticIQ Observables CSV
  - Plain text value
  - STIX 1.2

Under **Feed content** you can define the data source and the update strategy for the outgoing feed:

- **Datasets**: from the drop-down menu select one or more existing datasets to use as sources to populate the outgoing feed content.
  For the feed not to be empty, at least one selected dataset should contain entities and observables in the same format as the configured *content type* for the feed.
- **Update strategy**: from the drop-down menu select the preferred method to populate the outgoing feed with data before publishing it:
  - **Append**: every time the outgoing feed runs, it fetches only new unpublished data — new entities and observables ingested after the previous execution of the feed — to generate the content to publish through the feed.
  - **Replace** every time the outgoing feed runs, it fetches new and existing data — new and existing entities and observables included in the previous execution of the feed — to generate the content to publish through the feed.
  - **Diff**: this option is available *only* for the **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** content types.

    Every time the outgoing feed runs, new data is compared against existing data to identify any differences between the two datasets at *entity-level* — any entities added to or removed from the set when **EclecticIQ Entities CSV** is the designated content type for the feed — or at *observable-level* — any observable added to or removed from the entities in the set when **EclecticIQ Observables CSV** is the designated content type for the feed.

    Depending on the selected CSV content option, each row in the CSV output contains information about one entity being added or removed, or one observable being added or removed.
    An extra diff column is added to the output CSV to indicate if a row, and therefore either an entity or an observable, has been added to or removed from the set.

    This option allows you to identify any changes in a feed between two executions without downloading the whole feed every time.

ArcSight CEF

The **ArcSight CEF** `(https://www.protect724.hpe.com/docs/doc-1072)` content type is suitable for machine consumption. Typical use cases include feeding an ArcSight CEF outgoing feed to a SIEM system such as **ArcSight ESM** `(https://saas.hpe.com/en-us/software/siem-security-information-event-management)` or to a Syslog server for further processing.

The **ArcSight CEF** `(https://www.protect724.hpe.com/docs/doc-1072)` content type does not have any specific configuration parameters.

EclecticIQ Entities CSV

The EclecticIQ Entities CSV content type outputs CSV files with column headers where each row holds data describing one entity.
For example, an indicator, a TTP, and so on.

The EclecticIQ Entities CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at entity-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

EclecticIQ Observables CSV

The EclecticIQ Observables CSV outgoing feed outputs CSV files with column headers where each row holds data describing one observable.
For example, an IP address, a hash, a geographic location name, and so on.

The EclecticIQ Observables CSV content type enables comparing two different outputs from the same outgoing feed to diff them, and to examine any changes at observable-level.
This is a quick and inexpensive way to check for feed content changes and updates since the previous feed run.
To do so, under **Update strategy** select **Diff**.

> **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 menu.

EclecticIQ HTML Report

The EclecticIQ HTML Report content type outputs intel reports in HTML format.
Use this content type to publish and disseminate cyber threat analysts' intelligence reports, so that the intended audience can retrieve them.

Intel reports are published as HTML files. When the transport type is **Send email**, the HTML report is sent as attachment to an email message.

Under **Content configuration** set the EclecticIQ HTML Report content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the reports, if applicable.
  To create standard terms of use content to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include logo**: select this checkbox to include a logo image to brand the intel reports, if applicable.
  To add a default logo for inclusion in intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand intel reports with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include contact information**: select this checkbox to include in the intel reports any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to intel reports do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated intel report.

EclecticIQ HTML Report Digest

The EclecticIQ HTML Report Digest content type outputs a HTML format document containing an intel report digest. Typically, an intel report digest includes summaries of approximately 5 to 8 intel reports, with links to the full reports.

Intel report digests are published as HTML files. When the transport type is **Send email**, the HTML report digest is sent as attachment to an email message.

Report digests are useful to communicate a quick overview of the main hot topics an analyst team is focusing on. Each report digest includes the following content:

- **Source**: the intel report producer. For example, an organization, an agency, or a specific department.
- **Date**: the creation date of the original intel report the digest is taken from.
- **STIX ID**: a clickable link with the STIX ID of the intel report for easy lookup.
- **Previous version STIX ID**: the STIX ID of the previous version of the same intel report, if available.
- **Intents**: one or more tags or labels to define the purpose of the threats, techniques, actors, and so on the intel report focuses on.
- **Tags**: one or more tags and/or taxonomy entries to assess intelligence value indicators such as source reliability, type of threat, threat actor details, targeted victim details, and so on.
- **Summary**: a brief account of the main points the original intel report the digest is taken from touches upon.

Under **Content configuration** set the EclecticIQ HTML Report Digest content type options:

- **Include following tags and taxonomy** : from the drop-down menu select one or more tags and taxonomy entries to include in the *Tags* section of the generated report digest content.
  You can select individual tags, free tags that are not part of a taxonomy, as well as parent and child tags that are part of a taxonomy.
  If you select a parent tag, all the corresponding children are added to the *Tags* report section as well.
- **Include terms of use**: select this checkbox to include a terms of use section in the report digests, if applicable.
  To create standard terms of use content to add to intel reports and to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default terms of use** input field, type or copy-paste the terms and conditions that apply to the intel reports and to report digests.
  - Click **Save** to store your changes, or **Cancel** to discard them.

- **Include logo**: select this checkbox to include a logo image to brand the report digests, if applicable.
  To add a default logo for inclusion in report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Specify a URL for your company logo used in the email template** input field, enter a URI pointing to the logo image you want to brand report digests with.
    - Max image size: *200 x 200 px*
    - Max file size: *320 KB*
    - Allowed formats: *.png*, *.jpg*
    - Example: *https://awesome-logos.com/images/logos/mind-blowing-logo.png*
  - Click **Preview and test** to display an image preview of the selected logo under **Logo preview**.
  - Click **Save** to store your changes, or **Cancel** to discard them.
- **Include contact information**: select this checkbox to include in the report digests any relevant contact information report recipients may use to request assistance or further details, if applicable.
  To add default contact information to add to report digests do the following:
  - On the left-hand navigation sidebar, click ⚙ **> System settings > Intel report** .
  - In the **Edit intel report settings > Default contact information** input field, type or copy-paste any applicable contact details such as a contact person, their email address, Skype user or phone number, (snail) mail address, and so on.
  - Click **Save** to store your changes, or **Cancel** to discard them..
- **Root URL of EclecticIQ platform installation** : enter the base URL of the data source platform instance to link relevant items in the intel report content back to that platform instance.
  If you leave the field field empty, it is automatically populated with the host name value specified in ⚙ **> System settings > General > Hostname**.
- **Additional information**: enter any additional information you want to include at the end of the generated report digest.

EclecticIQ JSON

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the `data.information_source.identity.name` value in the entity JSON structure:

```
{
  "data": {
    "information_source": {
      "type": "information-source",
      "identity": {
        "name": "${producer_identity}", // ex.: 'EclecticIQ'
        "type": "identity"
      }
    }
  }
}
```

Plain text value

The plain text value content type is suitable for machine consumption. Typical use cases include feeding a plain text value outgoing feed to an external compatible device to instrument further processing or to trigger a response action.

The plain text value content configuration options set up a rule to define the eligible data pool to produce the outgoing feed content from.

The rule works like this:

- **Field to check a conditional value in** works together with **Only use entities that match this conditional value** to select the entities to use as a data pool source for the outgoing feed content.
- **Field to take values from** selects the values in the data pool that should be fetched and included in the outgoing feed content.

The rule flow works like this:

- The **Field to check a conditional value in** condition looks for a specific JSON path pointing to a specific entity field in the entity JSON structure.
- When the rule find a JSON path, that is, an entity field matching **Field to check a conditional value in**, it searches it for values matching the **Only use entities that match this conditional value** condition.
  This condition takes a literal or a regex, and it searches the specified JSON path key for any values matching the input data pattern.
- If the previous conditions yield matches, the **Field to take values from** condition points to a specific entity field whose value is fetched and included in the outgoing feed content.

Under **Content configuration** set the **Plain text value** content type options to define the rule behavior:

- **Field to take values from**: specifies the location in the entity JSON structure where the values to include in the feed are stored.
  Enter a JSON path pointing to the entity field whose value you want to fetch and include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Field to check a conditional value in**: this condition works together with **Only use entities that match this conditional value** to filter specific entities.
  Enter a JSON path pointing to the entity field you want to use as a filter to select entities whose content you want to include for publication in the outgoing feed.
  - The JSON path can start at either the top-level `data` or at the `meta` JSON field. Therefore, the first member at the beginning of a JSON path needs to be `data` or `meta`.
  - The JSON path is a string that points to a location, that is, a field inside a JSON object. It defines *where* in the entity structure the rule should look for a corresponding data value.
  - The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  - Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
- **Only use entities that match this conditional value**: this condition works together with **Field to check a conditional value in** to filter specific entities for the feed.
  Enter a string to define the value to match. Matching values are fetched and included in the outgoing feed content.

Example

You can configure this rule to send relevant data to an external Snort or Suricata instance, where they can be further processed or used to initiate a specific response action:

- **Field to check a conditional value in**: *data.test_mechanisms.test_mechanism_type*
- **Only use entities that match this conditional value**: *snort*
- **Field to take values from**: *data.test_mechanisms.rules.value*

The rule uses these conditions to:

- Look for platform entities containing Snort rules: *data.test_mechanisms.test_mechanism_type: snort*
- If the previous condition yields matching entities, the rule looks in those entities to see if they contain this field: *data.test_mechanisms.rules.value*
- If they do, the rule fetches the *data.test_mechanisms.rules.value* value to include it in the outgoing feed content.

  Matching values are added to the outgoing feed, one value per line.
  The value in question should be a valid Snort rule for the resulting feed data to be meaningful.

  Example:

```
alert tcp $HOME_NET any -> [72.20.35.70,72.20.35.120] 6661 (msg:\"ET CNC Shadowserver Reported CnC
Server Port 6661 Group 1\"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,www.shadowserver.org; threshold: type limit, track by_src, seconds 360, count 1;
classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2405018; rev:3633;)
```

STIX 1.2

The STIX 1.2 content type is suitable for machine consumption. Typical use cases include feeding a STIX 1.2 outgoing feed to an external STIX-compatible device to instrument further processing or to trigger a response action.

Under **Content configuration** set the **STIX 1.2** content type options:

- **Override producer**: select this checkbox to replace the original producer identity with the **Producer** name defined for the platform in the STIX settings.
  Leave it deselected to include the original producer of the information.
  This setting changes the following nested XML element in the entity STIX structure:

```
<stixCommon:Identity>
  <!-- Producer identity, for example 'EclecticIQ' -->
  <stixCommon:Name>EclecticIQ</stixCommon:Name>
</stixCommon:Identity>
```

Barbara: create a TAXII incoming feed

To configure the general options for the TAXII poll incoming feed, see Configure incoming feeds.

Configure transport and content types

Transport type	Allowed content types
TAXII poll	CAPEC XML
	EclecticIQ JSON
	EclecticIQ JSON (Legacy)
	Email message
	PDF
	STIX 1.0
	STIX 1.1
	STIX 1.1.1
	STIX 1.2
	Text

- From the **Transport type** drop-down menu, select **TAXII poll**.
- From the **Content type** drop-down menu, select the appropriate content type for the data you want to ingest through the incoming feed.
  The selected content type for the feed should match the data source format.
  This can vary, depending on the intel sources you retrieve the data from.
  The **TAXII poll** transport type enables fetching data in the following formats:
  - *CAPEC XML*
  - *EclecticIQ JSON*
  - *EclecticIQ JSON (Legacy)*
  - *PDF*
  - *STIX 1.0*
  - *STIX 1.1*
  - *STIX 1.1.1*
  - *STIX 1.2*
  - *Text*
- **Accept password protected archives**: select this checkbox to specify a global password to open any archives retrieved through the incoming feed.

  If the archives are password-protected, enter it in the **Archive password** field. The specified password acts as a master password, and it is used to try to unlock and access any archives retrieved with the feed.

  Supported archive formats: *.rar*, *.tar*, *.tar.bz2*, *.tar.gz*, *.tar.bz2*, *.tar.z*, *.zip*

Configure the transport type

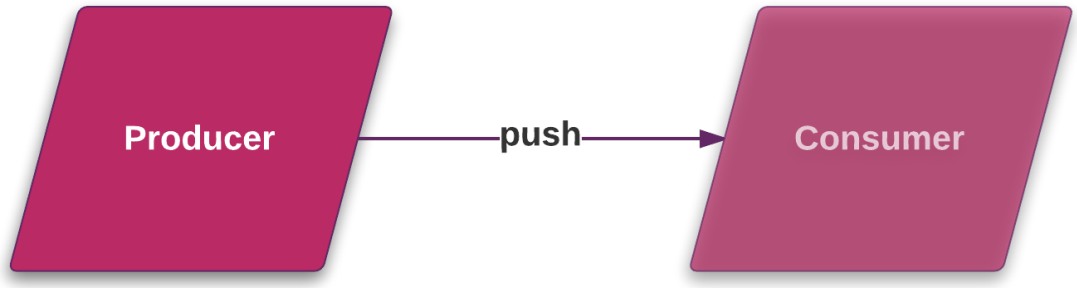
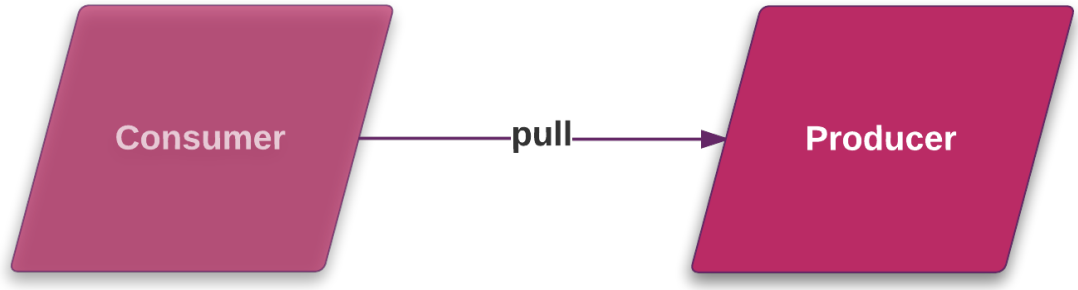
Under **Transport configuration**, configure the following settings:

- **Auto Discovery**: enter the URL of the TAXII discovery service configured in the data source platform instance, that is, Alice's discovery service.
  The data recipient platform instance, that is, Barbara, can send a request to this URL to determine Alice's available services, and to poll for updates.
  Example: *https://${platform_alice}/taxii-discovery-service*
- **Polling service URL**: enter the URL of the TAXII poll service configured in the data source platform instance, that is, Alice's polling service.
  The data recipient platform instance, that is, Barbara, can send a request to this URL to poll the service for updated content.
  Example: *https://${platform_alice}/taxii-poll-service*
- **Collection name**: enter the name of the data collection you want to poll and use as a source for the feed.
  The collection you define here needs to be available through the auto-discovery or the polling services.
  The name of the collection should correspond to the one specified under **Collection name** in the TAXII outgoing feed configuration in the data source platfom instance (Alice).
  Example: *MalwareDomainList_Hostlist*
- **TAXII version**: specify the TAXII version the data source service, that is, Alice's TAXII poll service, uses to publish data.
  Example: *1.1*
- **Ingest messages starting from**: select an initial date if you want to fetch content from the intel provider/data source starting from a specific date in the past.
- **Days per poll**: if you select a start date to poll data from, you can enter an integer to specify the maximum number of days to poll at a time.
  This enables polling in multiple smaller batches, instead of a single batch, starting from the selected initial date.
  This option works only if you select an ingestion start date.
- **Basic authentication**: select this checkbox since the data source platform instance, that is, Alice, is set up to require basic authentication to grant access to its TAXII services.
- **Username**: enter the user name of the automation user profile you set up for this integration.
  Example: *platform-to-platform connector*
- **Password**: enter the password associated with the automation user profile you set up for this integration.
  Example: *3@7-y0ur-v3gg135*
- **EclecticIQ authentication URL**: enter the authentication URL of the data source platform instance, that is, Alice's URL endpoint responsible for taking user name and password inputs to send them to the authentication mechanism.
  Example: *https://${platform_alice}/api/auth*

About TAXII services

After configuring a TAXII server, you can set up TAXII services. A TAXII service is a specialized data handler that implements a specific TAXII capability.
The platform supports the following TAXII services:

Service type	Description
Collection management service	TAXII consumers can use a TAXII collection management service to request information about, subscribe to, and cancel subscriptions to TAXII data collections (TAXII outgoing data feeds and TAXII datasets). Binding: TAXII HTTP 1.0, TAXII HTTPS 1.0

Service type	Description
Discovery service	A TAXII discovery service allows TAXII consumers to obtain information about the availability and use of TAXII services like collection management, inbox, and polling. Binding: TAXII HTTP 1.0, TAXII HTTPS 1.0
Inbox service	The TAXII inbox service allows TAXII consumers to accept push messages initiated by a TAXII producer. This service can be based on a subscription model, or it can be an unsolicited payload a producer pushes to a consumer. Binding: TAXII HTTP 1.0, TAXII HTTPS 1.0 
Poll service	The TAXII poll service allows TAXII consumers to request TAXII data collection content from a TAXII producer, usually through TAXII outgoing feeds. Binding: TAXII HTTP 1.0, TAXII HTTPS 1.0 

TAXII data collections — structured TAXII data feeds, and unstructured TAXII datasets — are typical examples of inbox and poll service content.

View TAXII services

To access an overview of the existing and configured TAXII services in the platform do the following:

- On the left-hand navigation sidebar click ⚙ **> STIX and TAXII > TAXII**.
- The **TAXII** view shows the currently configured TAXII services for the platform.
  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.
- To view the configuration information of a TAXII service, click the ⋮ icon on the row corresponding to the TAXII service whose configuration you want to review.
- From the drop-down menu select **View**.
  The TAXII settings page shows the current configuration of the specified service.

Alternatively:

- On the **TAXII** view click anywhere on the row corresponding to the TAXII service whose configuration you want to review.
  The TAXII settings page shows the current configuration of the specified service.

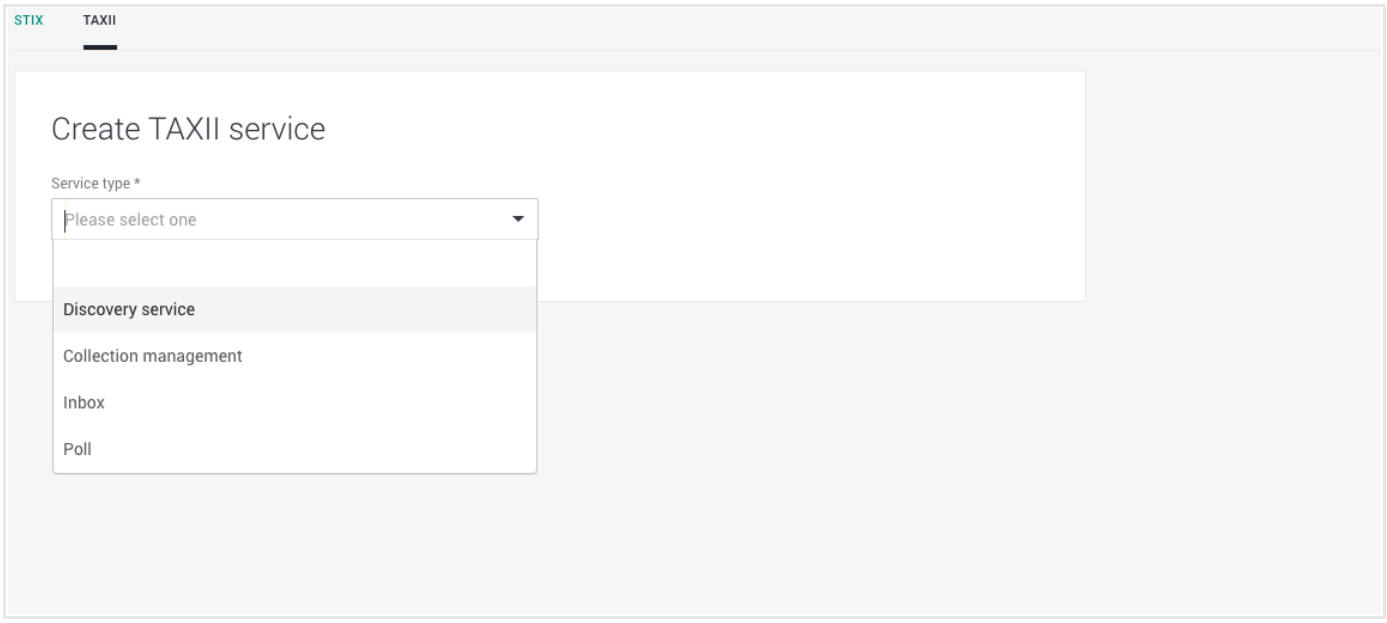
Add a TAXII service

Configure the general options

- On the left-hand navigation sidebar click ⚙ **> STIX and TAXII > TAXII**.
- On the **TAXII** view click the ✚ *(Add service)* icon.

Under **Create TAXII service** define the following configuration settings:

- **Service type**: from the drop-down menu select the TAXII service type you want to add.
- **Description**: a free-text description of the service. It should be descriptive and easy to remember.
  Example: *Polling from Ecorp threat db*.
- **Address**: the public endpoint the service can be reached at.
  It should be relative to the configured domain name identifying the machine hosting the TAXII server.
  Example: */taxii/services/poll*.
- **Protocol bindings**: from the drop-down menu select the the data exchange transport protocol.
  Allowed values: *HTTP*, *HTTPS*.
- **Authentication required**: select the checkbox to enable user authentication, or deselect it to allow anonymous/guest access.
- Click **Save** to store your changes, or **Cancel** to discard them.



Configure specific options per service

Besides the general options appicable to all TAXII services, each service type has additional, specific configuration options.

Discovery service

- **Advertised services**: when you set up a new *discovery service*, you need to select the TAXII services you want to advertise and make discoverable, so that consumers can access them as data sources.
  From the drop-down menu select one or more services.

Collection management

- **Outgoing feeds**: when you set up a new *collection management service*, you need to select the outgoing feeds you want to associate with and be managed by the service.
  From the drop-down menu select one or more outgoing feeds.

> **Warning:**
> You first need to configure outgoing feeds before making them available through this drop-down menu.

Inbox

This service has no extra configuration options besides the common settings for all TAXII services.

Poll

- **Max result count**: if you set this option to *-1*, a poll request also counts how many entities are available in the feed(s). If you set **Max result count** to a positive integer value, and if the total amount of available entities in the feed(s) exceeds this value, a poll request to the service informs the consumer that the total entity count in the feed(s) is higher than the maximum result count value you set here.
  You can use this option if you prefer to not disclose the total amount of entities accessible through the poll service.
- **Max result size**: this option controls pagination, that is, the number of results per page.
  We recommend limiting the number of pages by setting a relatively large number of results per page.
  For example, *200*.
- **Outgoing feeds**: when you set up a new *poll service*, you need to select the outgoing feeds you want to associate with and be managed by the service.
  From the drop-down menu select one or more outgoing feeds.

> **Warning:**
> You first need to configure outgoing feeds before making them available through this drop-down menu.