EclecticIQ Platform release notes

Product release notes and information

Last generated: March 06, 2018

Table of contents

Release notes for the EclecticIQ Platform

This section groups the release notes that are published to provide information about EclecticIQ Platform releases.

Here you can find an overview of the release notes that are published to complement the EclecticIQ Platform product releases.

In general, release notes contain information on new product features, enhancements, bug fixes, deprecated features (when applicable), and any known issues. They usually apply to specific product versions and/or releases.

Release notes

Browse the table for the topics you want to look up.
You can also use the drop-down menu on the left-hand navigation sidebar to access the articles or to go to a different section.

Title	Excerpt
EclecticIQ Platform release notes 0.12.4	Release 0.12.4 — The release notes for EclecticIQ Platform accompany product releases. They provide last-minute information on new product features, enhancements, bug fixes, deprecated featur...
EclecticIQ Platform release notes 0.13	Release 0.13 — The release notes for EclecticIQ Platform provide last-minute information on new product features, enhancements, bug fixes, deprecated features (when applicable), and known iss...
EclecticIQ Platform release notes 0.14.1 — hotfix	Release 0.14.1 — This EclecticIQ Platform hotfix release addresses specific platform issues.
EclecticIQ Platform release notes 0.14.2 — hotfix	Release 0.14.2 — This EclecticIQ Platform hotfix release addresses specific platform issues.
EclecticIQ Platform release notes 0.14	Release 0.14 — The release notes for EclecticIQ Platform accompany product releases. They provide last-minute information on new product features, enhancements, bug fixes, deprecated features...
EclecticIQ Platform release notes 0.15	Release 0.15 — Spotlight: new auditing feature, a cleaner UI, and improved database performance. More good stuff: easier batch uploading and ingestion with archives, enricher improvements, an...
EclecticIQ Platform release notes 0.16	Release 0.16 — Spotlight: pop-up tooltips, faster queries and graph reindexing. Moreover: cleaner UI, pagination on poll requests, default outgoing feed.
EclecticIQ Platform release notes 1.10.0	Release 1.10.0 — Spotlight: Flashpoint enrichers, system health monitor, running job monitor, incoming feed performance improvements.
EclecticIQ Platform release notes 1.11.0	Release 1.11.0 — Spotlight: Flashpoint enrichers, AnubisNetworks Infections Cyberfeed incoming feeds, ingestion performance improvements, and upgrades to Elasticsearch 2.3.5 and Kibana 4.5.

Title	Excerpt
EclecticIQ Platform release notes 1.12.0	Release 1.12.0 — Spotlight: new FlashPoint Thresher enricher, filter extracts by extract classification, PostgreSQL upgrade to version 9.5, database syncing optimization.
EclecticIQ Platform release notes 1.13.0	Release 1.13.0 — Spotlight: money mule TTPs, entity auto-tagging, syslog transport type for outgoing feeds, improved email delivery, distribute report entities with attachments, search entiti...
EclecticIQ Platform release notes 1.14.0	Release 1.14.0 — Spotlight: autosave your work, undo and redo actions on the graph, build custom enricher extensions, get intel from the new PassiveTotal enrichers.
EclecticIQ Platform release notes 1.14.1	Release 1.14.1 — Spotlight: out-of-the-box support for Farsight DNSDB and Cisco AMP Threat Grid Curated Feed enrichers, and FireEye iSIGHT Threat Intelligence incoming feed.
EclecticIQ Platform release notes 1.14.2	Release 1.14.2 — Spotlight: out-of-the-box support for DomainTools Hosted Domains, DomainTools Reputation, DomainTools Suspicious Domains, Recorded Future, and Unshorten-URL enrichers.
EclecticIQ Platform release notes 1.14.3	Release 1.14.3 — Spotlight: installation on Ubuntu Server, out-of-the-box support for DomainTools Malicious Server Domains enricher, DomainTools Retrieve Parsed Whois Observables enricher, Ce...
EclecticIQ Platform release notes 1.14.4	Release 1.14.4 — Spotlight: out-of-the-box support for Crowdstrike as an incoming feed and an enricher, and for BFK as an incoming feed; install on CentOS and RHEL from a TAR archive.
EclecticIQ Platform release notes 1.8.0	Release 1.8.0 — Spotlight: revamped notifications, LDAP authentication and authorization, item history, and configurable time zone.
EclecticIQ Platform release notes 1.9.0	Release 1.9.0 — Spotlight: duplicate data deduplication, Elasticsearch Sightings enricher, and support for ingesting AnubisNetworks Infections Cyberfeed intelligence.
EclecticIQ Platform release notes 2.0.2	Release 2.0.2 — Spotlight: the main focus of this release is on maintenance and bug fixing.
EclecticIQ Platform release notes 2.0 (Yay!)	Release 2.0 — Spotlight: a brand new UI redesigned from scratch with context-aware navigation; IOC-centric analysis with observables; enhanced intel reporting, out-of-the-box support for CIRC...
EclecticIQ Platform release notes 2.1.0	Release 2.1.0 — Spotlight: an automated platform installation script for CentOS and Ubuntu; an improved public API; a downloadable SDK to facilitate custom extension building; new feature tha...
EclecticIQ Platform release notes 2.1.1	Release 2.1.1 — Spotlight: this release main focus is on maintenance and bug fixing.

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

EclecticIQ Platform release notes 2.1.1

Release 2.1.1 — Spotlight: this release main focus is on maintenance and bug fixing.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	2.1.1
Release date	2018-03-05

Highlights

EclecticIQ Platform 2.1.1 is a maintenance release. It does not alter any core platform components, and it does not introduce new features; instead, it addresses bugs, solves known issues, and improves existing features with minor enhancements.

What's changed

Enhancements

More flexible user and group management

An organization may want to be able to delegate some, but not all, administrative tasks to a team admin user role.
To this end, we implemented additional permissions to enable an organization to delegate some administration tasks, without giving the team admin role full administrator rights.
In this way, a team admin role can manage team members and groups without requiring the `is_admin: True` permission.

With this enhancement, the following new permissions are available:

- `modify user-groups`
- `modify user-roles`

Roles and permissions

- The default team admin role includes the `modify user-groups` permission. It does not include the following permissions: `modify roles`, `modify groups`, `modify users`.

- A sysadmin role can create, enable, disable, and remove users in the platform through the GUI and by making a request to the API. The default sysadmin role includes the following permissions: `modify user-groups`, `modify roles`, `modify groups`, `modify users`.
- An analyst role can interact with platform data and platform workflows, but they have no additional permissions allowing them to modify users, groups, or roles.

User modification and permissions

- To modify user details in user profiles, a role needs the following permissions: `modify users`, `modify user-groups`.
- Roles lacking the `modify groups` permission cannot access the **Edit** and **Delete** options on the **Groups** view and on group detail panes.
- Non-admin roles (`is_admin: False`) with the `modify users` permission can now select the **Active** checkbox on the new user creation form to enable the newly created user.
- Non-admin roles (`is_admin: False`) with the `modify user-groups` permission, and lacking the `modify groups` and `modify roles` permissions, can add and remove users to and from groups.
- Non-admin roles (`is_admin: False`) lacking the `modify users` permission cannot create users via API requests.

Maintenance upgrade

We added maintenance upgrade documentation for CentOS and Ubuntu to the *Install* section to describe the upgrade process steps for maintenance releases.
The maintenance upgrade documentation applies to platform versions 2.1.x.

Important bug fixes

The following section gives an overview of the *most important bug fixes* to provide context and scope.

Feeds

- Ingestion timestamp filtering works as expected.

Observables

- The observable search tab fetches expected results, based on the corresponding search query input.
- It is possible to update observables from inside the observable detail pane.

Entities

- Adding multiple entities to a dataset does not affect platform performance.

System

- Neo4j starts successfully after a platform upgrade.

Security

- To prevent cross-site vulnerability, **Select a spec** input is now available as a drop-down menu.

Known issues

- After completing an installation of EclecticIQ Platform 2.1.1 using the install script provided, the list of systemd-managed services is repeated twice in the */opt/eclecticiq/etc/eclecticiq/platform_settings.py* platform settings configuration file.

  The issue does not affect platform functionality, and it will be addressed in the next minor release 2.1.2.

```
# CentOS list

SYSTEMD_SERVICES = [
    'elasticsearch',
    'logstash',
    'postfix',
    'neo4j',
    'postgresql-10',
    'redis',
    'statsd',
    'kibana',
]
```

```
# Ubuntu list

SYSTEMD_SERVICES = [
    'elasticsearch',
    'logstash',
    'postfix',
    'neo4j-service'
    'postgresql@10-main'
    'redis-server'
    'statsd',
    'kibana',
]
```

- The platform does not work correctly if the workspace module is disabled.
- **Skip** and **Replace** paths do not work on outgoing feeds for HTML reports.
- The UI is slower when you load more than 100 entities on the graph.
- Title modification of an entity is not reflected in the result table.
- Filtering by source is not working for rules creation.
- Creating an indicator with more than 100 observables returns an error.
- Labels on the graph are not positioned correctly.
- When running with the **Replace** strategy an outgoing feed producing STIX content, feed runs with identical STIX content may generate different hash IDs.
- Manually adding a **Sighting** characteristic to an exposed entity does not affect the **Sighting** attribute of that entity on the **Exposure** view,
- Intel set was renamed to **Datasets**, but the GUI may still display some *intel set* leftover captions.
- Entity relation is not displayed in the graph in the **Neighborhood** tab.
- Tags only search for exact matches.
- Performance issues with MS Edge and MS Internet Explorer web browsers.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 2.1.0

Release 2.1.0 — Spotlight: an automated platform installation script for CentOS and Ubuntu; an improved public API; a downloadable SDK to facilitate custom extension building; new feature that saves your work and remembers surfed pages in the platform.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	2.1.1
Release date	2018-01-12

Highlights

Version 2.1! We bring you a ton of platform upgrades with helpful new UI elements. And a ton of new improvements to make the platform easier and more intuitive.

Upgrades

- **Python 3.6 Upgrade** Upgrading all production deployments (Centos, Ubuntu, AMI etc.) to Python 3.6.
- **PostgreSQL 9.6 → 10.x Upgrade** Upgrading all production deployments to PostgreSQL 10. Read https://www.postgresql.org/docs/10/static/release-10-1.html to know more.
- **Elastic Stack 5.6 Upgrade** Upgrading all production deployments to Elastic Stack 5.6. Read https://www.elastic.co/guide/en/elasticsearch/reference/5.6/release-notes-5.6.0.html to know more.
- **Neo4j 3.0 Upgrade** Upgrading all production deployments to Neo4j 3.0 Upgrade. Read https://neo4j.com/release-notes/neo4j-3-0-0/ to know more.

All-in install script

From this release installing the platform is much easier, thanks to the provided documentation-driven install script. Run the script from the command line, and follow the prompts. And if you feel like taking a break for a GTA V or Horizon Zero Dawn game; no sweat, and enjoy it. You can resume the install process at a later time from where you left it. (14235)

What's new

SDK

- Our SDK provides a structured framework to build your extensions, to implement transport and content types for custom feeds, as well as to create new enrichers, based on your organization needs and requirements.

Feeds

- Incoming and outgoing feeds remember the patterns and actions to ease the user journey. (12697)
- You can now run a feed immediately after saving it. (12709)
- **New archive format** - Besides the *.zip* format, manual file upload and incoming feeds support extracting compressed files also from *.rar* archives, with or without password protection.

Observables

- You can now delete extracted and unlinked observables from the platform. (14571, 12278)

UI

- Levels are introduced to help manage log configuration. (5186)
- The platform remembers the state of the pages. (14129)

What's changed

Public API

- Our public API includes a number of endpoints exposing services such as the authentication mechanism, as well as access to the platform assets and resources, such as entities, observables, enrichment tasks, and data sources.

Enhancements

Search

- Search is enhanced for better results (14130)

Observables

- New lists are introduced in the observable **Neighborhood** tab to show how the observable is related to the intelligence in the platform.

Fixed bugs

The following sections give an overview of selected bug fixes to provide context and scope. The lists are not exhaustive. If you have any questions about a specific bug fix, feel free to contact us at support@eclecticiq.com.

Feeds

- Mount point download can no longer make requests to internal resources using incoming and outgoing feeds. (14277)
- SFTP incoming feed is working as expected. (14920)
- Maliciousness property for Proofpoint incoming feed is fixed and works as expected. (15088)
- Spycloud enricher, Capec, Crowdstrike indicator feed, and Threat grid curator feed work as expected. (15119, 15120, 15121, 15122)
- CSV schema now contains meta.taxonomy column for both entity-based and extract-based CSV.

Rules

- In Discovery rule modal, packages are renamed to entities for consistency. (14673)

Entities

- To provide clarity, only latest version of related entities is displayed. (14707)

Notifications

- Email notification for workspaces is configurable. (14800)

UI

- Notifications are moved to bottom left of the page, a box pops up notifying you of all the creations, updates, and changes in the platform. You can also look at the bell icon to see all the notifications.

System

Among the system-related issues we fixed:

- Wget installed version is now correct. (14464)

Known issues

- Platform does not work correctly if the workspace module is disabled.
- *Skip* and *Replace* paths isn't working on outgoing feeds for HTML reports.
- UI is slower when you load more than 100 entities on the graph.
- Title change of an entity is not reflected in the result table.
- Filter by source is not working for rules creation.
- Creating an indicator with more than 100 observables returns an error.
- Labels on the graph are not positioned correctly.
- Performance issues with MS Edge and MS Internet Explorer web browsers.
- Adding too many entities to a dataset is slow.
- Hashes are different for same STIX content.
- Manually adding a *Sighting* characteristic to an exposed entity does not affect the *Sighting* attribute of that entity on the *Exposure* view.
- Intel set was renamed to *Datasets*, but the GUI may still display some *intel set* leftovers.
- Entity relation is not displayed in the graph in the *Neighbourhood* tab.
- Filtering is not working for ingestion timestamp.
- Tags only search for exact matches.

Danger:
Due to breaking changes, the following enrichers and incoming feeds are *not working* on EclecticIQ Platform release *1.14.4 (and earlier) until release 2.0.2 included*:

- Enrichers:
  - FireEye iSIGHT
  - Intel 471
  - Recorded Future
- Incoming feeds:
  - BFK API
  - Cisco Threat Grid Curated Feed
  - Cisco Threat Grid Samples API
  - Crowdstrike Falcon Intelligence Indicator Feed
  - Crowdstrike Falcon Intelligence Reports Feed
  - Crowdstrike Falcon Intelligence Threat Actor Feed
  - FireEye iSIGHT Intelligence Report API

To restore full functionality for these enrichers and incoming feeds, upgrade to EclecticIQ Platform release *2.1.0* or later.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 2.0.2

Release 2.0.2 — Spotlight: the main focus of this release is on maintenance and bug fixing.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	2.0.2
Release date	2017-12-11

For a more detailed list of changes, enhancements and new features, refer to the sections below.

Upgrade to the latest release

Warning:
During the upgrade to release 2.0.2 you need to reinstall two extensions.
Reinstall the extensions:

- *After* installing the platform upgrade package on CentOS/RHEL or Ubuntu Server.
- *Before* migrating the databases on CentOS/RHEL or Ubuntu Server.

Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

Before upgrading, make sure you:

- Back up core data such as platform configuration files and databases
- Familiarize with the upgrade procedure

After installing the platform upgrade, make sure you:

- Migrate the PostgreSQL and Neo4j databases, as well as the Elasticsearch indices
- Run the fixtures to initialize and to bootstrap the platform
- Run a final check to verify that the upgrade completed successfully.

You can find more details about these steps in the *upgrade procedure* section for CentOS/RHEL or for Ubuntu Server.

Reinstall extensions

After upgrading to EclecticIQ Platform 2.0.2 you need to reinstall the following extensions:

- *eclecticiq-extension-core*: **eclecticiq-extension-core-2.0.2.tar.gz**
- *eclecticiq-extension-reports*: **eclecticiq-extension-reports-2.0.2.tar.gz**

The procedure is a standard remove-reinstall one:

- Download the current version of *eclecticiq-extension-core* and *eclecticiq-extension-reports*: **eclecticiq-extension-core-2.0.2.tar.gz** and **eclecticiq-extension-reports-2.0.2.tar.gz**, respectively.
- Remove the previous version of *eclecticiq-extension-core* and *eclecticiq-extension-reports*.
- Install the latest version of *eclecticiq-extension-core* and *eclecticiq-extension-reports*.

Follow the steps below to install the extensions and to bootstrap them, so that the platform can load them correctly.

Download the current extension

- Go to the EclecticIQ Platform Extensions repository at https://downloads.eclecticiq.com/Extensions/.
- Browse to the extension you want to install, and click its name.
- On the extension page, **General** tab, browse to the **Downloads** section, and then click the extension package name to download it.
  Extension package name format: *eclecticiq-extension-{extension_name}-{platform_release}.tar.gz*
  Example:
  - *eclecticiq-extension-anubis-1.0.tar.gz*: Anubis Cyberfeed incoming feed for EclecticIQ Platform release 1.14.x.
  - *eclecticiq-extension-anubis-2.0.tar.gz*: Anubis Cyberfeed incoming feed for EclecticIQ Platform release 2.0.x.
- Save the extension package to a local directory.

Switch to eclecticiq

- Switch to the `eclecticiq` user by running the following command(s):

```
$ su - eclecticiq
```

Activate venv

- Activate a Python virtual environment:

```
$ source /opt/eclecticiq/platform/api/bin/activate
```

- Export the platform settings configuration to create the necessary environment variables:

```
(api) $ export EIQ_PLATFORM_SETTINGS="/opt/eclecticiq/etc/eclecticiq/platform_settings.py"
```

Remove the previous extension

You may need to remove an extension for several reasons: to upgrade it to a newer release, to reinstall it in order to address functionality issues, or because you do not need it any longer.

To remove an extension, run the standard `pip uninstall` command, and then specify only the name of the extension, without platform release number, and without extension archive file type.

```
$ pip uninstall eclecticiq-extension-${extension-name}

# Example: uninstall eclecticiq-extension-arcsight-2.0.tar.gz
$ pip uninstall eclecticiq-extension-arcsight
```

Extension naming	cheatsheet
Default naming format	`eclecticiq-extension-${extension-name}-${platform-release}.tar.gz`
Install extension	`eclecticiq-extension-${extension-name}-${platform-release}.tar.gz`
Uninstall extension	`eclecticiq-extension-${extension-name}`

Install the current extension

- Install the downloaded extension with **pip install** (`https://pip.pypa.io/en/stable/reference/pip_install/`):

```
$ pip install eclecticiq-extension-${extension-name}-${platform-release}.tar.gz

# Example:
$ pip install eclecticiq-extension-anubis-2.1.0.tar.gz
```

Reload Supervisor configurations

Warning:
When you edit or update Supervisor configurations, run `systemctl restart supervisor` and `supervisorctl reload`, so that Supervisor can pick up and reload any updated configurations to the platform with the latest changes.

After editing Supervisor-managed configuration (*.ini*) files restart, and then reload Supervisor, so that it can pick up all changes and apply them:

```
$ systemctl restart supervisord

$ supervisorctl reload
```

```
$ systemctl restart supervisor

$ supervisorctl reload
```

This applies to all Supervisor-managed programs, applications, extensions, and services in the platform.

Load the fixtures

- As a final step, load the fixtures to complete the installation, and to bootstrap the extension:

```
(api) $ eiq-platform-script database load-fixtures
```

The extension is ready for use in the platform.

Platform documentation

The platform documentation is shipped together with the platform installation packages. When you install or upgrade the platform, the documentation is included in the process.

However, you may occasionally wish to install the documentation separately. For example, to update to a more recent version of the help.

To install the platform documentation on *CentOS* and *RHEL*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ yum install -y eclecticiq-platform-docs-{version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ yum install -y eclecticiq-platform-docs-2.0.1-1

# Install the latest version of the documentation
$ yum install -y eclecticiq-platform-docs
```

To install the platform documentation on *Ubuntu Server*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ apt-get install -y eclecticiq-platform-docs={version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ apt-get install -y eclecticiq-platform-docs=2.0.1-1

# Install the latest version of the documentation
$ apt-get install -y eclecticiq-platform-docs
```

The default install location for the platform documentation is */opt/eclecticiq/platform/docs*.

Fixed bugs

- When accessing Kibana, the user can only see the data they have access to (*14617*)
- Users can now enrich the observable successfully (*14406*)
- Outgoing feeds now passes all the transport-related parameters needed for auto discovery (*14397*)
- Mount point download completes successfully (*14472*)
- PDF files uploaded by admin are readable to other users (*14490*)

- Report content type run successfully for outgoing feeds (*14509*)
- Users can be added/deleted using a private API with a token generated through the public API (*14651*)

Known issues

- Updating an entity may erroneously return a *created new entity* message (*7246*)
- Exposure count inconsistencies before and after sorting (*9595*)
- After editing the title of an entity on the entity detail pane, the change is not reflected in the entity result table (*9673*)
- Audit trail logging may unexpectedly throw errors (*10148*)
- Ingesting very large packages between two platform instances throws a memory error during data serialization (*10152*)
- Deleting entities from PostgreSQL instead of the UI may cause the graph to stop working (*10405*)
- A TLP override value for a feed does not propagate to the entities in the feed (*10529*)
- Memory usage may spike when creating content for outgoing feeds (*10557*)
- When creating a new entity rule, not all applicable data sources may be available for selection (*10925*)
- The **Matches** tab on entity and observable rule detail panes throws and error (*11952*)
- The *back* button on the user management page does not work as expected (*12005*)
- Selecting 100 or more observable, and then creating an indicator from the selected items throws an HTTP 400 error (*12071*)
- Web browser built-in password manager does not prompt users to save the login credentials to access the platform (*12094*)
- Sorting items by maliciousness classification does not work as expected (*12115*)
- UI cosmetic issues when displaying the web-based UI in Firefox and MS Edge (Windows, Mac OS X) (*12401*)
- Time displayed on charts is out of sync with system time (*12440*)
- **Send email** outgoing feed task does not return any error message to users when it fails (*12445*)
- Pagination does not reset correctly after changing the number of items to display per page (*12461*)
- Creating an entity with a POST API call, and then immediately deleting it does not remove it from Elasticsearch (*12485*)
- Proxy password encoding issue (*12521*)
- Cosmetic issue affecting the entity detail pane **Actions** menu (*12556*)
- Missing sort option for entity table columns on incoming and outgoing feeds (*12618*)
- Missing validation on some inpout fields (*12670*)
- Missing user icon to flag user-created observables (*12678*)
- Signing in to the platform may take too long (*12706*)
- Outgoing feed anonymization **Skip paths** group selections do not produce the expected results (*12713*)
- Observable tree structure view does not reflect the actual parent-child relationships of the displayed items (*12732*)
- Usability issue affecting PDF viewing inside the platform (*12737*)
- Editing a manually uploaded entity removes it from the uploaded entity view (*12766*)

- Opening an outdated version of an entity from the version tab in the entity detail pane displays the selected outdated entity in full page instead of inside the detail pane (*12773*)
- Double-clicking an entity in a group of entities with different types displays an empty entity detail pane (*12785*)
- Moving or resizing widgets on the dashboard to rearrange them may occasionally not work as expected; minor cosmetic issues affecting dashboard widgets (*12784*, *12813*, *12837*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 2.0 (Yay!)

Release 2.0 — Spotlight: a brand new UI redesigned from scratch with context-aware navigation; IOC-centric analysis with observables; enhanced intel reporting, out-of-the-box support for CIRCL, CVE and Shodan enrichers; AWS S3 and CVE incoming feeds, CAPEC support.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	2.0.0
Release date	2017-10-02

Highlights

Version 2.0! We changed the whole first digit in our versioning system, and since we were at it we threw in a platform release sporting a completely redesigned UI. Plus a ton of new features and improvements under the hood to make it easier and more intuitive to add data sources, analyze ingested information, and share it with fellow analysts and other parties. (*5624*)

Revamped UI 2.0

The *new UI* aims at improving navigation and discoverability, while keeping you focused on the data that matters to you:

- The dashboard is more intuitive. It offers a structured overview of the available platform intel, and any pending user tasks.
  Not happy with the layout? Click ✎ on the top-left corner to rearrange the widgets as you please.

- Context-aware navigation makes it easier to find your way inside the platform, and it keeps clicking as limited as possible:
  - The left-hand navigation sidebar enables you to search for and create entities, access workspaces and user tasks, as well as your user profile and the system settings.
  - The top navigation bar keeps things neat and organized by grouping options under two main groups:
    - **Intelligence** keeps you focused on intel analysis and collaboration.

      Within **Intelligence**, you can select **All intelligence**, or you can directly jump to the **All workspaces** overview to select a workspace where you or your team organize and structure a specific platform intel subset.
    - **Data configuration** lets you configure data sources, data dissemination channels, as well as the business rules to manage intel acquisition and distribution as needed.
  - Redesigned, user-friendlier quick filters ( ) allow highlighting and isolating specific clusters of information to zero in on during an analysis.

IOC-centric analysis with observables

Remember when Pluto was demoted, and then reinstated as a dwarf planet ? We felt the same about observables. Analysts can now use *observables* to perform IOC-centric and incident-centric analysis:

- Observables behave like standalone items: you can add and ingest observables as distinct items, besides adding them to the entities they are related to.
- The observable **Link name** field enables you to label observable relationships: depending on the parent entity they are related to, observables can take predefined **Link name** values that define the relationships between observables and their parent entities. These labels add context, and they help understand the role of an observable relative to the parent entity it refers to.

  For example, an observable can represent a vulnerability, a targeted victim, a malicious piece of infrastructure, and so on. It can be observed outside the organization, or sighted within the organization.

  This additional information enables analysts assess the intelligence value and the relevance of observables, which makes triaging easier.
- The observable detail pane, similar to the entity detail pane, provides a clear view of the observable details, its relationships with other observables, and the neighboring threat landscape.
- On the entity detail pane, **Observables** tab, you can show or hide the new tree structure view to inspect observable relationships with entities and with other observables in an intuitive way.
- On the entity and the observable detail pane, **Observables** tab, you can directly go to an observable external data source.
  Clicking the link to an external resource on the **Observables** tab opens the target on a new tab.
- Since observables are indexed you can browse, search for, and find observables.

> If you upgrade the platform from a previous version, rewire observables to make them platform 2.0-compliant.

Enhanced intel reporting

A new *rich text editor* enables threat analysts to author *intelligence reports* easily and efficiently, and to distribute them through outgoing feeds:

- The intel report editor guides analysts in the report writing process, so that they can leverage platform intelligence without leaving the editor.
- They can then publish the entire intel report or only a report digest in HTML format through outgoing feeds.

Command palette (beta)

Click stress? No worries, we got you covered. Ditch the mouse and browse through commands like a ninja with the **Command palette**:

- Press **CTRL + SHIFT + P** to display the **Command palette**.
- Press ↑ **Pg up** or ↓ **Pg dn** to scroll through the platform commands.
  Alternatively, press **TAB** or **SHIFT + TAB**.
- The command palette includes search with autocomplete: start typing a command name to get a result list with commands containing your typed input.
- To select a command, select it, and then press **ENTER**, or click it.
  For example, manually add a new observable.
- Press **ESC** to close the **Command palette**.

More new features and new user guide

Among the new goodies we added to this release:

- You get notified when enrichers are automatically disabled. For example, this can happen with open source data sources enforcing caps and limits, or when requests repeatedly time out. The notification message prompts you to re-enable the enricher, so that it can resume normal operation.
- New enrichers and incoming feeds to poll data from CIRCL and Shodan.

The documentation has changed:

- A new **User guide** replaces the previous *Getting started* guide, as well as most user-targeted how-to articles.
  This is part of an ongoing effort to consolidate and simplify documentation to make it user-friendlier.
- We are gradually moving to a continuous documentation delivery approach:
  - From this release, the documentation package is decoupled from the platform installation packages.
    You can download the documentation package separately from the same location the platform install packages are available from, and install it separately.
  - The documentation is going to be updated more often than the platform. You may want to check the standard platform download location from time to time to download the latest doc package.
  - The documentation versioning format is *${platform_version}-${documentation_version}*.
    Example: *2.0.1-1*

The platform documentation is shipped together with the platform installation packages. When you install or upgrade the platform, the documentation is included in the process.

However, you may occasionally wish to install the documentation separately. For example, to update to a more recent version of the help.

To install the platform documentation on *CentOS* and *RHEL*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ yum install -y eclecticiq-platform-docs-{version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ yum install -y eclecticiq-platform-docs-2.0.1-1

# Install the latest version of the documentation
$ yum install -y eclecticiq-platform-docs
```

To install the platform documentation on *Ubuntu Server*, so that it is available in-product as a help resource, do the following:

```
# {version_number} format: 0.0.0-0
$ apt-get install -y eclecticiq-platform-docs={version_number}

# Install a specific version of the documentation
# by specifying the release number:
$ apt-get install -y eclecticiq-platform-docs=2.0.1-1

# Install the latest version of the documentation
$ apt-get install -y eclecticiq-platform-docs
```

The default install location for the platform documentation is */opt/eclecticiq/platform/docs*.

For a more detailed list of changes, enhancements and new features, refer to the sections below.

Upgrade to the latest release

Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

Before upgrading, make sure you:

- Back up core data such as platform configuration files and databases
- Familiarize with the upgrade procedure

After installing the platform upgrade, make sure you:

- Migrate the PostgreSQL and Neo4j databases, as well as the Elasticsearch indices
- Run the fixtures to initialize and to bootstrap the platform
- Run a final check to verify that the upgrade completed successfully.

You can find more details about these steps in the *upgrade procedure* section for CentOS/RHEL or for Ubuntu Server.

Rewire observables to v.2.0

> Rewiring observables to v.2.0 is a one-off task you need to perform only when upgrading EclecticIQ Platform from v.1.14.x to 2.0.

After successfully upgrading EclecticIQ Platform from version 1.14.x to 2.0, you need to run `eiq-platform-script bulk-refresh-extracts`.

Run this script only after booting up the platform, and after starting all platform components. The platform needs to be fully up and running for the observable refresh script to work correctly.

From v.2.0 observables are powerful tools to drive IOC-centric analysis. Observables ingested and created with previous versions of the platform need to be rewired and upgraded to v.2.0, so that the platform can, among others, index them and make them searchable.

The script reparses existing observables to update their format to platform 2.0-compliant.

Run the script from the terminal or the command line:

```
$ export EIQ_PLATFORM_SETTINGS=/opt/eclecticiq/etc/eclecticiq/platform_settings.py
$ /opt/eclecticiq/platform/api/bin/eiq-platform-script bulk-refresh-extracts --workers=4
```

`workers`

It is a mandatory parameter.
It takes an integer as a value.
If you do not specify any value, it defaults to `1`.

It defines the number of workers the script should concurrently run in parallel.
The process is resource-intensive, and it takes some time to complete: gauge the number of workers based on your system resources.
`4` workers is a rule-of-thumb value to run the script with a limited impact on normal platform operation.
You can increase the number of workers as needed, based on your system resources.

Logging

- After initializing, the script starts discovering items to process, and outputting log information to the terminal.
- After successfully completing, it notifies you with the following message: `all entities processed`.

Errors

- If the user terminates the script before it completes, the script returns `Aborted!`.
- If an error occurs during execution, the script returns `an unexpected worker error occurred`, along with traceback information.

In case of errors, you may want to check the traceback information, as well as the `first_entity_id` and `last_entity_id` values in the log block preceding the error message: they correspond to the first and last entities in the last successfully processed batch before the error.

Example:

```
{"event": "sending batch to search", "first_entity_id": "00209576-bd04-48be-a4f0-c9a865b2b0c0",
"last_entity_id": "0024eceb-fb14-44ee-8e8d-6dad0ce58849", "level": "info", "logger":
"eiq.platform.scripts.bulk_refresh_extracts", "timestamp": "2017-09-01T16:26:44.685313Z",
"worker_pid": 9332}
```

What's new

Enrichers

- **CIRCL** enricher to retrieve all the IP addresses associated with the input SSL certificate `hash-sha1` fingerprints (*12188*)
- **CIRCL** enricher to retrieve all the domain names associated with the input SSL certificate `hash-sha1` fingerprints (*12188*)
- **CVE** enricher to retrieve information about common software and hardware vulnerabilities, along with the corresponding exposures, based on the input **`cve`** `(https://cve.mitre.org/cve/identifiers/)` observables (*10455*)
- The **Shodan** enricher takes a wealth of input observable types to help you discover which of your devices are connected to the Internet, where they are located, and who is using them (*12257*)
- You get notified when an enricher is automatically disabled. Click the enricher name on the notification message to go to the corresponding configuration page, where you can re-enable the enricher (*10107*, *10108*)
- An enrichment option is added to the observable context menu (*13169*)
- Enrichments show notifications displaying the status of an ongoing job (*13026*)

Feeds

- **CAPEC XML** is a new incoming feed content type to retrieve **Common Attack Pattern Enumeration and Classification (CAPEC)** `(https://capec.mitre.org/)` information. Ingested data is processed and saved as **TTP entities** `(https://stixproject.github.io/data-model/1.2/ttp/ttptype/)`
  The STIX ID is based on the CAPEC ID — the default naming convention of a standard CAPEC-ingested TTP starts with the *[CAPEC-${numeric reference}]* prefix — and it is idempotent across uploads (*10460*)
- **CVE Search API** is a new incoming feed transport type to retrieve complete CVE (Common Vulnerability and Exposures) records from the CVE database hosted by CIRCL (Computer Incident Response Center Luxembourg). CVE information is ingested as a STIX package containing an exploit target (*10455*, *10620*)
- MISP to EclecticIQ Platform data mapping schemas as a preparatory step to supporting MISP ingestion into the platform (*11681*)
- The **OpenPhish** and the **PhishMe Intelligence** incoming feeds enable you to ingest phishing URLs and richer phishing intelligence
- **S3** is a supported transport mechanism for incoming and outgoing feeds, so that you can store and retrieve data to and from AWS S3 (*12075*)

Observables

- You can now search for observables in the same way as you search for entities (*8812*)
- Observables feature a detail pane, just like entities, where you can review related observables, as well as neighborhood relationships (*8445*)

UI

- The **Command palette** enables you to scroll through and to select platform commands using the keyboard (*9500*)
- Quick filters are more intuitive and easier to use to perform quick searches on the fly (*8964*)
- A new horizontal navigation bar enables you to make multiple selections, and to apply bulk actions to the selected items in search results, on dataset views, on entities detail panes, and on observable detail panes (*8961*)
- When your user session is about to expire, you get notified, and your work is automatically saved.
  When your user session expires, you get notified, and you are prompted to sing in again (*7693*)

- You are notified if an incorrect value is entered in the platform (*12670*)
- A graph can be exported as an image (*13008*)

What's changed

Enhancements

Observables

- The information displayed for enrichment observables now incldues the source extract for an enrichment observable — for example, the source IP address of a domain name observable — and the date of the most recent enrichment for that observable (*8824*)

UI

- Enter UI v.2.0 (*5624*)
- TLP options and captions are consistent throughout the UI (*10601*)

Fixed bugs

EclecticIQ Platform 2.0.0 includes more than a hundred bug fixes to improve stability, robustness, interoperability with external systems and applications both upstream and downstream in the system chain.

UI bug fixes address cosmetic, as well as functional issues, to get rid of known usability hiccups, and to improve consistent behavior across the UI.

The following sections give an overview of selected bug fixes to provide context and scope. The lists are not exhaustive. If you have any questions about a specific bug fix, feel free to contact us at support@eclecticiq.com.

Enrichers

Among the enricher-related issues we fixed:

- Enricher success rate visibility
- Enrichers were erroneously included in the system job overview
- Entity creation could cause enrichers to fail
- `extracts-unique` enricher search index errors
- Missing **Source reliability** default value for enrichers
- PassiveTotal passive DNS enricher not working as expected
- Splunk enricher not working as expected

Entities

Among the entity-related issues we fixed:

- Adding entities to a task

- Creating, editing, and updating entities in the entity editor/entity builder; accessing draft entities in the entity editor/entity builder
- Deleting entities from UI and PostgreSQL
- Downloading entities as original or exporting them as JSON
- Entity rule content criteria inconsistency
- Exposure override settings inconsistency
- Filtering entities by origin
- **Impact** characteristic of incidents not keeping loss estimation value after saving
- Modifying entity and extract rules
- Removing entities from datasets

Graph

Among the graph-related issues we fixed:

- Deleted items persist and are visible on the graph
- Item grouping on the graph
- Item visibility on the graph
- Items loaded and disappearing on the graph
- **Path** visibility on the graph
- Unwanted **Undefined** relationships on the graph

Ingestion and dissemination

Among the ingestion and dissemination-related issues we fixed:

- Deleting feeds
- Entity ingestion hiccups and inconsistencies, occasionally
- Manual file upload for users who do not belong to any group
- Indicators can be removed from datasets while editing (*12641*)
- Content type can be changed in incoming feed after adding a collection (*13106*)

Observables

Among the observable-related issues we fixed:

- Filtering by observable in **Exposure** not working as expected
- Filtering observables
- Manually adding observables to indicators
- Observable rules not working as expected, occasionally
- Opening the observable detail pane when the graph is open
- Removing ignored observables on the active view
- Search action triggered by clicking an observable
- Sorting observables by number of connections

System

Among the system-related issues we fixed:

- Adding a user to a user group from the group detail pane

- Elasticsearch would occasionally hang or crash upon processing badly-formed queries
- Packages are successfully ingested using real data (*13002*)
- Email messages are successfully uploaded to the platform (*12982*)

UI

Among the UI-related issues we fixed:

- Cosmetic and functional issues affecting buttons, icons, menus, missing notifications, auto-discovery, quick filters, item sorting on the active view, user information display on feed views, pagination

Known issues

- Updating an entity may erroneously return a *created new entity* message (*7246*)
- Exposure count inconsistencies before and after sorting (*9595*)
- After editing the title of an entity on the entity detail pane, the change is not reflected in the entity result table (*9673*)
- Audit trail logging may unexpectedly throw errors (*10148*)
- Ingesting very large packages between two platform instances throws a memory error during data serialization (*10152*)
- Deleting entities from PostgreSQL instead of the UI may cause the graph to stop working (*10405*)
- A TLP override value for a feed does not propagate to the entities in the feed (*10529*)
- Memory usage may spike when creating content for outgoing feeds (*10557*)
- When creating a new entity rule, not all applicable data sources may be available for selection (*10925*)
- The **Matches** tab on entity and observable rule detail panes throws and error (*11952*)
- The *back* button on the user management page does not work as expected (*12005*)
- Selecting 100 or more observable, and then creating an indicator from the selected items throws an HTTP 400 error (*12071*)
- Web browser built-in password manager does not prompt users to save the login credentials to access the platform (*12094*)
- Sorting items by maliciousness classification does not work as expected (*12115*)
- UI cosmetic issues when displaying the web-based UI in Firefox and MS Edge (Windows, Mac OS X) (*12401*)
- Time displayed on charts is out of sync with system time (*12440*)
- **Send email** outgoing feed task does not return any error message to users when it fails (*12445*)
- Pagination does not reset correctly after changing the number of items to display per page (*12461*)
- Creating an entity with a POST API call, and then immediately deleting it does not remove it from Elasticsearch (*12485*)
- Proxy password encoding issue (*12521*)
- Cosmetic issue affecting the entity detail pane **Actions** menu (*12556*)
- Missing sort option for entity table columns on incoming and outgoing feeds (*12618*)
- Missing validation on some inpout fields (*12670*)
- Missing user icon to flag user-created observables (*12678*)
- Signin in to the platform may take too long (*12706*)

- Outgoing feed anonymization **Skip paths** group selections do not produce the expected results (*12713*)
- Observable tree structure view does not reflect the actual parent-child relationships of the displayed items (*12732*)
- Usability issue affecting PDF viewing inside the platform (*12737*)
- Editing a manually uploaded entity removes it from the uploaded entity view (*12766*)
- Opening an outdated version of an entity from the version tab in the entity detail pane displays the selected outdated entity in full page instead of inside the detail pane (*12773*)
- Double-clicking an entity in a group of entities with different types displays an empty entity detail pane (*12785*)
- Moving or resizing widgets on the dashboard to rearrange them may occasionally not work as expected; minor cosmetic issues affecting dashboard widgets (*12784*, *12813*, *12837*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.14.4

Release 1.14.4 — Spotlight: out-of-the-box support for Crowdstrike as an incoming feed and an enricher, and for BFK as an incoming feed; install on CentOS and RHEL from a TAR archive.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.4
Release date	2017-07-21

Highlights

With this release, EclecticIQ Platform extends out-of-the-box support to the following intel providers (*11357*):

- BFK, incoming feed
- Crowdstrike Falcon Intelligence Indicator, incoming feed
- Crowdstrike Falcon Intelligence Indicator, enricher

A new platform installation option is available for CentOS and RHEL OSs:

- Install the platform from a TAR archive

You can now upgrade the platform also on Ubuntu Server:

- Upgrade the platform from the APT repository

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Feeds

- **BFK** is available as a data source through incoming feeds (*11425*, *11664*)
- **Crowdstrike Falcon Intelligence** is available as a data source through incoming feeds (*11665*)
- **Crowdstrike Falcon Intelligence** is available as a data source through enrichment (*11666*)

- It is now possible to delete or purge an incoming feed (*11388*, *11539*):
  - *Delete the feed* to remove the incoming feed configuration.
    The platform stops ingesting and processing data from the designated data source for the feed.
    Existing data linked to the feed are preserved, such as previously ingested and processed entities and relationships.
  - *Purge the feed* to remove the incoming feed configuration, and any data ingested through or linked to the feed.
    The platform stops ingesting and processing data from the designated data source for the feed.
    Data linked to the feed are completely removed as well, such as entities previously ingested through the feed.

What's changed

Enhancements

Entities

- Indicator wrappers, that is, empty indicators wrapped around CybOX observables whose CybOX `idref`s point to external observables that have not yet been ingested and processed, are ignored and excluded from search and from the graph when the observable `idref`s they contain are successfully resolved to the actual observables they represent (*11630*)

Feeds

- Ingestion improvements in Fox-IT incoming feeds (*11935*)

System

- The default number of workers was raised to 17 for the platform API, and to 4 for OpenTAXII (*11936*)
- Upgrade the platform to a more recent release on Ubuntu Server (*11495*)
- Install the platform on CentOS and RHEL from a TAR archive (*11284*, *11842*, *11869*)
- Improved interoperability with the Postfix email server component (*11500*)
- Improved interoperability with external authentication mechanisms such as LDAP, AD, and SAML (*11812*, *11927*)

UI

- Usability improvements in the scheduler (*10676*)
- When a form detects missing data, an error message is displayed, but the fields with the missing data would not be highlighted to the user (*12047*)

Fixed bugs

Feeds

- The date selector to filter entity display by dates in incoming feeds would not work correctly (*11709*)
- The FireEye iSIGHT Intelligence Report incoming feed would stop working after upgrading the platform (*12182*)

Ingestion and dissemination

- Uploading a password-protected *zip* file to the platform would fail (*11839*)
- Uploading an email body content as *eml* file would fail (*12008*)
- After a non-resolved observable `idref` embedded in a wrapper indicator is resolved to the actual observable it represents, the fully resolved wrapped observable would not always be deleted from Elasticsearch (*12090*)

System

- LDAP users whose user name contains a comma character would not be able to sign in to the platform (*11951*)
- It would not be possible to edit or update the permissions of AD-synced role groups from within the platform (*12138*)

UI

- Fixed several issues to improve usability, as well as look and feel (*11718*, *11789*, *11828*, *11931*, *11950*, *11965*, *11988*, *11991*, *12013*, *12048*, *12092*, *12100*, *12105*, *12107*, *12112*)

Known issues

- Drop-down menus near the header and footer sections are partially covered by the header and footer areas — IE 11 only (*6693*)
- After editing the title of an entity on the entity detail pane, the change is not reflected in the entity result table (*9673*)
- After completing clearing the graph canvas and refreshing the graph page, previsouly deleted entities are displayed again (*12128*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.14.3

Release 1.14.3 — Spotlight: installation on Ubuntu Server, out-of-the-box support for DomainTools Malicious Server Domains enricher, DomainTools Retrieve Parsed Whois Observables enricher, Censys, and ThreatCrowd enrichers.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.3
Release date	2017-06-23

Highlights

Cyber threat analysts need access to a diverse pool of resources to design threat models, build scenarios, as well as test and validate them. With this release, EclecticIQ Platform extends out-of-the-box support for the following enrichers:

- Censys
- DomainTools Malicious Server Domains
- DomainTools Retrieve Parsed Whois Observables
- ThreatCrowd

Besides LDAP, you can now authenticate and authorize users also through SAML.

And since Ubuntu is a much loved Linux distro, we threw in Ubuntu support as well: from this release, you can install and run EclecticIQ Platform also on Ubuntu Server 16.04 (Xenial).

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Enrichers

- **Censys** enricher: it enriches *asn*, *city*, *company*, *country*, *country_code*, *geo-lat*, *geo-long*, *hash-md5*, *hash-sha1*, *hash-sha256*, *ipv4*, and *postcode* observable types by providing additional context about geographic and geolocation details, hashes, and ASN details. It makes it easier to discover relationships between events, actors, and targets (*11250*)
- **DomainTools Malicious Server Domains** enricher: it enriches *domain* and *host* observable types with a list of malicious domain names related to the same primary or secondary name server. It includes configurable thresholds to assign maliciousness confidence levels to the processed domains and hosts, and to ignore non-malicious domains/hosts (*11255*)
- **DomainTools Retrieve Parsed Whois Observables** enricher: it enriches *domain*, *host*, and *ip* observable types with Whois information. The JSON output includes the most recent Whois record for the requested domain or IP range, as well as parsed, structured data such as registrant, registrar, contacts, and so on. It helps searching for, indexing, and cross-referencing data in a set of Whois records (*10745*)
- **Splunk** enricher: based on the search queries defined in the enricher, the enricher looks for matching data in the specified Splunk instance. Matching data is extracted and saved to the platform as sightings. It supports *domain*, *email*, *hash-md5*, *hash-sha1*, *hash-sha256*, *hash-sha512*, *host*, *ipv4*, *ipv6*, and *uri* observable types (*11244*)
- **ThreatCrowd** enricher: it enriches *domain*, *email*, *hash-md5*, *hash-sha1*, *hash-sha256*, *hash-sha512*, *host*, *ipv4*, *ipv6*, and *malware* observable types with suspicious and potentially malicious domains, IP addreses, email addresses, file hashes, and antivirus detections, so that you can explore relationships between events, actors, and targets (*10624*)

Feeds

- Two EclecticIQ Platform instances can use outgoing and incoming feeds to exchange observables in EclecticIQ JSON format (*10960*, *11227*, *10959*, *11653*)

System

- Platform users can now authenticate also through SAML (*11153*)

What's changed

Enhancements

Datasets

- After adding an entity to a static dataset, more recent versions of the same entity are automatically included in the same dataset (*10956*)

Entities

- When deleting an entity, the original package it was ingested from is not also automatically deleted (*11159*)

Feeds

- Incoming feed package ingestion status is displayed on the GUI (*11115*)
- Package ingestion processing improvements to retrieve more data from ingested packages, as well as trigger a new processing attempt for failed ingested packages (*10961*, *11463*)
- Besides a timestamp, entities published through outgoing feeds include also their STIX ID (*10957*)
- Entities published through outgoing feeds always include a `"type": "information-source"` field (*10958*)
- Performance improvements in the **Diff** strategy for outgoing feeds (*11135*)

System

- Ubuntu Server 16.04 (Xenial) is a supported OS (*9512*)
- When a platform user signs in with LDAP, it is not possible to change their password or other user profile properties, as long as they remain signed in (*11215*)
- Cabby 0.1.18 was released, and it is shipped with this platform release (*11734*)

UI

- Terminology as well as look and feel in incoming and outgoing feed areas is more consistent and symmetric (*10863*, *11238*, *11594*, *11719*)

Fixed bugs

Graph

- Graph ingestion edge case issue may cause the process to crash and throw an ingestion exception due to escaped special characters in a CSV source file (*11043*)
- Graph ingestion issue causing a read timeout error when ingesting large (> 5000 entities) JSON packages (*11044*)

Ingestion and dissemination

- The feed scheduler would not allow to set intervals shorter than an hour to plan feed task runs (*9911*)
- MAEC objects would not be parsed correctly during ingestion (*10775*)
- The **Farsight DNSDB** enricher fails and it is automatically disabled when enriching a non-existing invalid IPv6 address (*10823*)
- OpenTAXII would occasionally crash when processing XML files with specific encoding (*10928*)
- Deduplication race condition when two workers try to ingest identical entities concurrently (*11039*, *11328*, *11414*)
- Deduplication identical entities inside the same package during ingestions is logged (*11040*)
- Deduplication concurrency issue when exchanging data between two platform instances (*10809*)
- Timestamp comparison during ingestion may occasionally fail if the value of one of the timestamps is `null` (*11045*)
- MISP package ingestion may fail or only partially succeed when ingesting a large MISP STIX package with many children (*11046*)
- Observables in EclecticIQ JSON format exchanged between two EclecticIQ Platform instances would not be exported correctly from the source instance (*11714*)
- Entities in EclecticIQ JSON format exchanged between two EclecticIQ Platform instances would not be ingested correctly in the target instance (*11753*)
- Regex patterns in CybOx observables (attributes: `pattern_type="Regex" condition="FitsPattern"`) may be parsed as URIs instead of being interpreted (*10777*)

System

- Issue affecting the proper status display of Logstash (*11234*)
- Group and role syncing from AD through LDAP would not work correctly (*11557*)

UI

- Fixed several issues to improve usability, as well as look and feel (*11050*, *10760*, *10774*, *10778*, *11043*, *11104*, *11253*, *11327*, *11417*, *11428*, *11451*, *11475*, *11513*, *11631*, *11719*, *11781*)

Known issues

- The date selection filter on the incoming feed detail pane, **Entities** tab, does not work correctly (*11709*)
- When a detail pane is temporarily inactive (in the background) behind an active pop-up modal dialog (on the foreground), the detail pane closes (*11718*)
- Assigning a **Targeted victim** characteristic in a TTP a name value containing the *"&"* character causes the TTP creation to fail (*11789*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.14.2

Release 1.14.2 — Spotlight: out-of-the-box support for DomainTools Hosted Domains, DomainTools Reputation, DomainTools Suspicious Domains, Recorded Future, and Unshorten-URL enrichers.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.2
Release date	2017-05-25

Highlights

This release focuses on integration with a new set of data sources to enhance EclecticIQ Platform interoperability, and to make it easier for you to hook up the platform with an expanding range of intelligence providers (*10116*).

We added a wealth of new enrichers to augment observable intelligence value with additional context information about vulnerability and exploits, suspicious and/or malicious domains and hosts: **DomainTools Hosted Domains**, **DomainTools Reputation Enricher**, and **DomainTools Suspicious Domains**, **Recorded Future**, and **Unshorten-URL**.

Incoming feeds offer a new transport type to ingest data about vulnerabilities and phishing campaigns: **PhishMe Intelligence API**.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Enrichers

- **DomainTools Hosted Domains**, **DomainTools Reputation Enricher**, and **DomainTools Suspicious Domains** are implemented as enrichers (*10742*, *10744*, *10790*, *10791*)
  - **DomainTools Hosted Domains** enriches IPv4 observables by returning all the domain names hosted on the input IP addresses.
  - **DomainTools Reputation Enricher** enriches domain and host name observables with whois lookup information and maliciousness confidence levels based on the user-defined threshold values.
  - **DomainTools Suspicious Domains** enriches IPv4 observables with suspicious domains related the input IP addresses, and it includes configurable thresholds to assign maliciousness confidence levels to the processed IP addresses, and to ignore non-malicious IPs.
- **Recorded Future** is implemented as an enricher to enhance intelligence value and help assess, among others, IP address and domain name reputation, and maliciousness confidence level of potential threats (*10818*, *11191*, *11194*) **Recorded Future** enricher supports and enriches the following observable types:
  - *domain*
  - *hash-md5*
  - *hash-sha1*
  - *hash-sha256*
  - *hash-sha512*
  - *ipv4*
  - *ipv6*
- **Unshorten-URL** enricher returns observables with the original expanded URLs corresponding to the shortened ones generated by services such as goo.gl, fb.me, t.co, bit.ly, and TinyURL. This enables analysts to correlate the original URLs with other intelligence that mentions them (*10202*, *10619*)

Feeds

- **PhishMe Intelligence API** is a new incoming feed transport type to retrieve report information about malware associated with phishing campaigns. Feed data is ingested in STIX 1.1 format (*10793*)

What's changed

Enhancements

Feeds

- The **TAXII poll** transport type for incoming feeds supports selecting the maximum number of days to poll at a time under **Days per poll**. This enables polling in batches, instead of a single batch starting from the selected initial date (*10626*)

System

- LDAP integration was improved to work with Microsoft Active Directory (*10309*)

UI

- Terminology as well as look and feel in incoming and outgoing feed areas is more consistent and symmetric (*10863*, *11115*)

Fixed bugs

Download

- Manual email attachment download would lack the *.eml* file extension (*10708*)

Enrichers

- Fixed a minor issue affecting the **Farsight DNSDB** enricher (*10707*)
- The maliciousness confidence level of enriched observables would not be updated after running enrichers that can change observable state (*10747*)
- The **VirusTotal** enricher would not enrich entities correctly (*10748*)

Entities

- Upon creation of a new version of an entity belonging to a static dataset, it would not be possible to completely delete the previous version (*10956*)

Feeds

- The feed scheduler configuration section would not allow to run feed tasks when the interval between runs was shorter than one hour (*9911*)
- The **Cisco AMP Threat Grid Curated Feed** transport type for incoming feeds supports only STIX as a content type. However, users could choose more than one format for the content type (*10458*, *10672*)
- After revoking an outgoing feed task run, the downloaded package counter would be reset (*10567*)
- It would not be possible to schedule a 90-day interval between feed task runs to fetch incoming feed content (*10614*)
- Fixed an edge case issue where content creation for an outgoing feed would fail (*10753*)
- The **FireEye iSIGHT Intelligence Report API** transport type for incoming feeds would start running normally, and then it would abort unexpectedly (*10918*)

System

- Logstash logs would not be available in Kibana (*10633*, *11009*)

UI

- Fixed several issues to improve usability, as well as look and feel (*11050*, *10760*, *11104*)

Upload

- Manual PDF upload would fail (*10585*)

Users and groups

- When creating a new user group, **Source reliability** and **TLP** values would not be saved correctly (*10587*)
- Fixed an issue affecting user access to resources based on TLP filtering (*10931*)

Known issues

- Deduplication concurrency issue when exchanging data between two platform instances (*10809*)
- Deduplication race condition when two workers try to ingest identical entities concurrently (*11039*)
- Deduplication of identical entities inside the same package is not logged (*11040*)

- Graph ingestion edge case issue may cause the process to crash and throw an ingestion exception due to escaped special characters in a CSV source file (*11043*)
- Graph ingestion issue causing a read timeout error when ingesting large (> 5000 entities) JSON packages (*11044*)
- MISP package ingestion may fail or only partially succeed when ingesting a large MISP STIX package with many children (*11046*)
- Regex patterns in CybOx observables (attributes: `pattern_type="Regex" condition="FitsPattern"`) may be parsed as URIs instead of being interpreted (*10777*)
- Timestamp comparison during ingestion may occasionally fail if the value of one of the timestamps is `null` (*11045*)
- The **Farsight DNSDB** enricher fails and it is automatically disabled when enriching a non-existing invalid IPv6 address (*10823*)
- Issue affecting the proper status display of Logstash (*11234*)
- Some UI issues affecting usability, as well as look and feel (*10774*, *10778*, *11253*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.14.1

Release 1.14.1 — Spotlight: out-of-the-box support for Farsight DNSDB and Cisco AMP Threat Grid Curated Feed enrichers, and FireEye iSIGHT Threat Intelligence incoming feed.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.1
Release date	2017-04-03

Warning:
UPDATE MAY 12, 2017 — This release was updated with a hotfix to address some issues. Please check the updated notes under Upgrade to the latest release:

- Repair report descriptions
- Check the Logstash configuration file
- Restart Logstash

Log files are now stored in a new partition:

- Until release 1.14.1, not hotfixed: `/opt/eclecticiq/logs/`
- From release 1.14.1 hotfixed: `/var/log/`:
  - `/var/log/eclecticiq/`: EclecticIQ Platform logs
  - `/var/log/elasticsearch/`: Elasticsearch logs
  - `/var/log/logstash/`: Logstash logs
  - `/var/log/nginx/`: Nginx logs
  - `/var/log/postgresql/`: PostgreSQL logs
  - `/var/log/redis/`: Redis logs

Production VM images *do not include Neo4j*.
To manually install Neo4j on a production VM, follow the installation instructions in the platform help, and refer to the **official Neo4j documentation** `(https://neo4j.com/docs/operations-manual/current/installation/linux/)`.

Highlights

This EclecticIQ Platform hotfix release addresses one or more specific issues. For further details about the fixes, see What's new and Fixed bugs.

We did not only fix bugs 🐞, though: we also added a couple of cool new features and we just could not wait for the next standard product release, so we packed them in this hotfix release (*9025*).

EclecticIQ Platform ships with three new data ingestion sources out of the box: **Cisco AMP Threat Grid Curated Feed**, **Farsight DNSDB**, and **FireEye iSIGHT Threat Intelligence**.

Cisco AMP Threat Grid Curated Feed is implemented as an incoming feed. It provides a wealth of curated information about banking Trojans, network streams, suspicious IP addresses, domain names, and DNS entries.

Farsight DNSDB is implemented as an enricher to feed the platform additional context such as suspicious domain names and IP addresses.
The Farsight DNSDB enricher performs passive DNS lookup, and it returns domain names associated with an IP netblock, or IP addresses associated with a domain name. Enriched data is saved as observables. The context the enricher provides helps to map domain names to IP addresses over time, and to correlate domain names using the same suspicious name server infrastructure.

FireEye iSIGHT Threat Intelligence is implemented as an incoming feed to fetch relevant intelligence reports as STIX. The reports are available on a subscription basis; they provide more context and valuable insights to better understand the possible threats that may target your organization.

Besides email attachments, the IMAP email fetcher incoming feed can now ingest also email body content. When you choose to ingest email body content, it is saved as a report whose title is the email subject, the description is the email body text, and the estimated threat start time is the email sent date.

Last but not least, two or more EclecticIQ Platform instances can talk to each other. Interoperability across platform instances enables you to exchange intelligence and route it to other components of the system more efficiently.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.
- After completing the standard upgrade procedure, upgrading to EclecticIQ Platform 1.14.1 requires a couple of extra steps:
  - Run `eiq-platform-script fix-report-descriptions`.
  - Check the Logstash configuration file.
  - Restart Logstash.

Repair report descriptions

Run this script only after booting up the platform, and after starting all platform components. The platform needs to be fully up and running for the cleanup script to work correctly.

The script addresses and solves a STIX data model mismatch affecting report entities created by earlier versions of the platform, where a STIX report description field would not be correctly parsed.

Run the script from the terminal or the command line:

```
$ export EIQ_PLATFORM_SETTINGS=/opt/eclecticiq/etc/eclecticiq/platform_settings.py
$ /opt/eclecticiq/platform/api/bin/eiq-platform entity fix-report-descriptions
```

The script looks for any existing reports whose description fields need to be repaired, and it generates a log summarizing the actions it carried out:

```
{
  "event": "discovering report entities to fix",
  "level": "info",
  "logger": "eiq.platform.scripts.fix_report_descriptions",
  "timestamp": "2017-04-04T09:01:52.556581Z"
}

{
  "event": "found reports",
  "level": "info",
  "logger": "eiq.platform.scripts.fix_report_descriptions",
  "n": 0,
  "timestamp": "2017-04-04T09:02:07.194916Z"
}

{
  "event": "updating entities",
  "level": "info",
  "logger": "eiq.platform.scripts.fix_report_descriptions",
  "timestamp": "2017-04-04T09:02:07.195160Z"
}

{
  "event": "done",
  "level": "info",
  "logger": "eiq.platform.scripts.fix_report_descriptions",
  "timestamp": "2017-04-04T09:02:07.195277Z"
}
```

Check the Logstash configuration file

You may need to access the resource by running first `sudo su -` to obtain root privileges.

- Open the Logstash `input.conf` file:

```
$ cat /etc/logstash/conf.d/input.conf
```

In the upgraded release 1.14.1 the configuration file should be empty:

```
input {

}
```

Restart Logstash

You may need to access the resource by running first `sudo su -` to obtain root privileges.

- Close the configuration file, and restart Logstash:

```
systemctl restart logstash
```

- Check the Logstash status:

```
systemctl status logstash
```

The status request should return `Active: active (running).`

- Sign in to the platform UI, and initiate any loggable actions to populate the Logstash log.
  For example, run a feed or an enricher task.
- Check the tail of the Logstash log:

```
$ tail -f /var/log/logstash/logstash.log
```

It should return the most recently logged events.

What's new

- Cisco AMP Threat Grid Curated Feed incoming feed (*9023*)
- Farsight DNSDB enricher for passive DNS lookup (*7484*, *10200*)
- FireEye iSIGHT Threat Intelligence incoming feed to fetch intelligence reports as STIX (requires FireEye iSIGHT Intelligence subscription) (*9030*, *10242*)

What's changed

Enhancements

Feeds

- Outgoing feeds performance improvements (*10337*)
- Implemented STIX 1.2 support for the **Cisco AMP Threat Grid Curated Feed** and **Cisco AMP Threat Grid Sample Feed API** incoming feeds (*9023*, *10332*)
- The **IMAP email fetcher** incoming feed can ingest email body content, besides email attachments. It is now possible to select if the feed should ingest email attachments or the email body content. Ingested email body content is saved as a report (*10115*, *10445*)
- The UI of the execution scheduling section of feeds has been simplified to make it user-friendlier (*9911*)

System

- Improved SQL performance (*10291*)
- Improved memory management when creating content in outgoing feeds (*10207*)
- Interoperability between EclecticIQ Platform instances: different instances of the platform can now communicate by exchanging data in JSON and STIX formats (*9811*, *9815*, *9818*. *10087*, *10139*)

Fixed bugs

Enrichers

- **Max low confidence threat score** and **Min high confidence threat score** in the Cisco AMP Threat Grid enricher are mandatory input fields, but they were not marked as such in the UI (*9522*)
- It would not be possible to save user-created extract queries in the Elastic Sightings enricher (*10498*)
- Addressed some issues affecting the VirusTotal enricher (*9925*, *10073*, *10088*, *10126*)
- Addressed some issues affecting the Elastic Sightings enricher (*10009*)

Entities

- Occasionally, it would not be possible to open entities with a large number of relationships (in the order of magnitude of several tens of thousands) (*9056*)

Feeds

- Outgoing feeds: **Verify SSL** option was added to the TAXII inbox transport type (*9810*)
- Outgoing feeds: when using the TAXII inbox transport type with TAXII 1.0, it is not possible to select a destination collection because TAXII 1.0 does not support collection selection (*9897*, *10191*)
- Outgoing and incoming feeds: when using the TAXII inbox transport type with STIX 1.2 as the content type to exchange data between two platform instances, the incoming feed may not be able to process the incoming data correctly (*9902*)
- Incoming feeds: addressed an issue that would occasionally cause Threat Grid incoming feed requests to time out (*10147*)

Misc

- Addressed a PDF ingestion issue (*9978*)
- Addressed an issue concerning the update of blob IDs after ID ref resolution (*10067*)

Rules

- Addressed an issue concerning regex processing in extract rules (*9903*)

Upload

- Occasionally, a successful PDF upload would not result in a successful content creation (*10504*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 1.14.0

Release 1.14.0 — Spotlight: autosave your work, undo and redo actions on the graph, build custom enricher extensions, get intel from the new PassiveTotal enrichers.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.14.0
Release date	2016-12-31

Highlights

Winter tastes like orange and cinnamon. EclecticIQ Platform release 1.14.0 tastes like autosave, undo/redo to your heart's content, and BYOE (Build Your Own Enrichers).

When working with data, these are possibly the worst user scenarios ever:

- The Death Star blows up the planet you're working from.
- You lose unsaved work.

We're gathering intelligence to address the former issue, but we got you covered right now from the risk of losing unsaved work: autosave saves the day and your data.

Autosave

Autosave automatically saves a copy of your work in progess, be it a graph view, a taxonomy entry, an entity, and so on, in case you are about to be logged out because of a session timeout, or if connection to the host server(s) is lost unexpectedly.
Context-sensitive pop-up dialog windows inform you about the issue, and notify you about saving your work in progress.

You can resume your work from where you left it as soon as the system becomes available again: upon signing in, a message notifies you about your previously saved work.
If an edit conflict occurs because in the meantime another user has modified the same content, you can decide what to do with one click: you can keep your changes and discard the other user's edits, keep the other user's changes and discard yours, or do what we all know is by far the best thing to do at the end of the day: procrastinate, create a copy of the data and call off the final decision to mañana.

Undo and redo

You can also get sloppier and get away with it, too: unleash the power of oops ! Well, at least as long as you're in the graph, thanks to the new *undo/redo* feature. On the graph you can undo the last action, as well as redo the previously undone action. Very handy, especially when examining scenarios with complex relationships.

Autorefresh

The graph view *automatically refreshes* when you edit an entity or its extracts: when the graph is open, an entity is loaded on the graph canvas, and you edit the entity or its extracts on the corresponding detail pane, the graph view is updated to reflect the changes.

Configure session timeout

The web-base UI features a new section where you can *configure the user session timeout interval*. To access this option, go to **System > Server > General/Server settings > Edit settings** .

Observables

Entity extracts + enrichment extracts = Observables

Entity extracts and enrichments/enrichment extracts now live together on one tab called **Observables** in the entity detail pane. This UI change features a cleaner layout, and it is your one-stop-shop to clearly examine all the observable elements related to an entity, regardless their source being the entity or external enrichment data. You can filter the observables listed on this tab by origin — entity extracts, enrichment process extracts, or manually added by users — as well as based on other criteria like maliciousness or specific observable data types.

Enrichers

We added *new enrichers* to help you draw an accurate picture of the threat scenario under investigation, where you can clearly see the tree and the forest. The new PassiveTotal enrichers augment entities with extra context to help you cross-reference domain names vs IP addresses, retrieve whois details, and look up geolocation information.

Besides the built-in, ready-to-use enrichers that ship with the platform, you can *create your own custom enricher extensions*. We provide a boilerplate that you can use as a scaffold to build your custom enricher, and documentation to cover the tricky parts. Just kidding, there are no tricky parts. But the doc is there, just in case.

Help

On a closing note: EclecticIQ Platform ships with *built-in help*. Who knew? That's why we moved the help link outside the user profile drop-down menu and turned it into a **(?)** icon on the header bar next to the notification icon and the avatar picture.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Features and functionality

Discovery

- You can now edit an existing discovery rule, and then click **Save and Re-Run for All Time** to run it again and discover all relevant entities *since the beginning of time*; that is, all discovered entities, not only those added since the previous successful execution of the same rule (*8336*)

Enrichers

- Four new enrichers are available to poll data from. The data generates meaningful extracts that augment entity intel value and relevance:
  - The PassiveTotal **Passive DNS** `(https://api.passivetotal.org/api/docs/#api-dns)` enricher returns extracts containing cross-reference information about domain names and the IP addresses they refer to (*8378*)
  - The PassiveTotal **Get WHOIS** `(https://api.passivetotal.org/api/docs/#api-whois)` enricher returns extracts containing cross-reference information about domain names and the individuals or entities who own them (*8379*)
  - The PassiveTotal **IP/Domain** `(https://api.passivetotal.org/api/docs/#api-enrichment-getv2enrichmentquery)` enricher returns extracts containing geolocation information about IP addresses (*8380*)
  - The PassiveTotal **Malware** `(https://api.passivetotal.org/api/docs/#api-enrichment-getv2enrichmentmalwarequery)` enricher returns extracts containing malware information related to the queried host or domain (*8381*)

Extracts

- You can remove a specific occurrence of an extract from the entity it is related to, when the extract occurrence is no longer relevant (*8108*)

Graph

- Undo the last action and redo the previously undone action (*6355*)

Groups

- The group detail pane has a new **Users** tab that shows the group members. You can filter users, as well as act on them by selecting the desired options from the context menus (*8504*)

Observables

- You can create and add new observables to entities from the **Observables** tab in the entity detail pane (*8184*)
- On the **Observables** tab in the entity detail pane you can see the number of connections an observable has to other entities (*8604*)
- On the **Observables** tab in the entity detail pane you can filter observables by level 1 or 2 to reduce unwanted noise and to focus only on the relevant observables (*8781*)

System

- It is possible to configure the user session timeout interval in the UI through **System > Server > General/Server settings > Edit settings** (*8590*, *8591*)
- If the connection to the API is lost, the current screen locks and a message is displayed while the platform automatically attempts to reconnect (*8592*)

Documentation

- Documentation is now available also as PDF (*7676*, *8371*, *8372*)

New

- Rules in the getting started documentation
- How to work with the PassiveTotal enrichers in the *How to* section
- Build custom enricher extensions to implement ad-hoc integrations

- Integrations with external systems and services:
  - Cisco AMP OpenDNS integration
  - Cisco AMP Threat Grid integration
  - Flashpoint integration
  - Intel 471 integration
  - PassiveTotal integration
  - Splunk integration
  - VirusTotal integration
- Hardware requirements for system administrators in the *RPM installation and configuration* guide

Updated

- Discovery in the *Getting started* guide
- Configure the enricher section in *How to work with the Elasticsearch sightings enricher*
- How to install the platform via an RPM package , the shorter how-to version of the *RPM installation and configuration* guide
- RPM installation and configuration guide
- Reindex Elasticsearch in the *Bootstrap* and *Upgrade* sections of the *RPM installation and configuration* guide

What's changed

Enhancements

Discovery

- Improved handling of deleted discovery rules (*8616*)

Enrichers

- Fixtures for enrichers now include a preset source reliability value, which users can modify at any moment (*8518*)

Entities

- During entity ingestion, any entity raw attachments, such as embedded CybOX objects or embedded images, undergo a deduplication check (*8095*)
- Entity extracts are now called *observables*. You can view any observables related to an entity on the **Observables** tab in the entity detail pane. (*8415*, *8447*)

Graph

- On the graph, the **Layout** menu was redesigned to make it more efficient and user-friendly (*6377*)
- On the graph, an **(i)** icon is displayed next to the **Layouts** menu header: hover the mouse over it or click it to view a short explanation of the available graph layout formats (*8756*)

- The graph view refreshes when you edit an entity or its extracts: when the graph is open, an entity is loaded on the graph canvas, and you edit the entity or its extracts on the corresponding detail pane, the graph view is updated to reflect the changes (*7941*)
- Graph ingestion of observables was improved (*8762*)
- We upgraded KeyLine from version 2.11 to version 3.2. This introduces a number of improvements to the graph, including extensive control over the time bar events, more granular control of node hierarchy, and WebGL as the default API for WebGL-enabled browsers (*6522*)

Ingestion

- In case a connection problem or an error occurs, pending payload data is sent to a queue, so that its ingestion can be resumed as soon as the system is available again (*8757*)

Processes

- We added a nightly build step to our CI cycle to improve, among others, QA and testing processes (*6059*)

Rules

- Entity extract rules were refactored to improve processing speed (*8217*)

System

- Implemented support for gzip-compressed HTTP responses in Cabby (*8492*)
- Improved management of Elasticsearch index mapping during migrations, for example, to upgrade to a newer platform release (*8239*)
- Improved management of task runs with no task object (*7780*)

UI

- A dialog window is displayed to notify users when the current session is about to expire. User work in progress is automatically saved. A notification confirming that your work was saved is displayed on the login screen as well (*7693*, *8276*, *8589*, *8624*, *8758*, *8760*)
- When a user changes their password, a notification is displayed to notify them about the successful or failed outcome of the action (*8678*)
- **Enrich** and **Run now** actions, previously available as clickable buttons on the detail panes of incoming/outgoing feeds and discovery rules, are now incorporated as menu options in the **Actions** menu (*8586*)
- The built-in help menu option was moved outside the user avatar drop-down menu. Now it is a clickable **(?)** icon on the header bar next to the notification icon and the avatar profile picture (*8400*, *8465*, *8503*, *8508*)
- Improved behavior of filter menus to provide a more consistent and predictable user experience across the platform GUI (*8585*)
- Pagination can remember a user's page size selection (*8567*)
- Whitespace is correctly preserved in the entity descriptions of incoming entities (*8611*)
- The **Exposure** feature was refactored to improve modularity (*6762*)
- The UI areas providing information and control over incoming and outgoing feeds were refactored to improve usability (*8750*)
- UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*8427*)

Deprecated

N/A

Fixed bugs

Entities

- When creating a TTP entity including CAPEC information, an unnecessary dot character (“.”) would be visible on the entity detail pane (*8252*)
- Deleting an entity through the **Actions > Delete** menu option on the entity detail pane would leave the detail pane open, instead of automatically closing it (*8253*)
- When creating an incident entity including **Impact** characteristics, user-entered data would not be saved correctly (*8538*)
- A sighting with an empty security control characteristic section would still produce a security control observable related to the entity (*8895*)

Entity builder

- The **Targeted victim** form on the CIQ editor would not correctly check for required fields (*8459*)

Feeds

- Occasionally, an outgoing feed task may hang after correctly completing a run (*8593*)
- An output feed using the **EIQ Extracts CSV** output content type would not automatically flag exported entities as **Detection**, **Prevention**, or **Sighting** in **Exposure**, even if the outgoing feed in question is associated with one of these options (*8282*)
- Content update strategy options in outgoing feeds using the same dataset(s) as source and whose content type is set to **EclecticIQ Extracts CSV** would not always yield consistent results (*9000*)

Graph

- Occasionally, grouping elements on the graph would fail; at each subsequent click, numbers displayed on the graph would double (*8142*)
- Occasionally, grouping elements on the graph would produce unexpected results (*8643*)
- Occasionally, loading entities containing special characters in the name would fail (*8605*)
- Occasionally, loading entities on the graph would produce unnamed, undefined relationship elements (*8556*)
- When changing the visibility of a workspace from private to public, a graph pinned to the workspace before the visibility change would not be available anymore (*8226*)

Observables

- It would not be possible to delete an observable obtained through enrichment (*8573*)

Rules

- Occasionally, when creating a new entity rule the rule may fail to execute (*8587*)
- Occasionally, creating or editing an entity or an extract rule would fail (*8751*, *8872*)
- Rule content criteria would not always produce the expected results (*8883*, *8929*)

System

- It would not be possible to restart PostgreSQL and automatically start autorecovering it without first restarting also the *platform-api* service and Celery workers (*8271*)
- Fixed a JavaScript compatibility issue in IE 11 concerning multiple definitions of a property in strict mode (*8690*)

UI

- Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*7534*, *7766*, *7846*, *8012*, *8317*, *8327*, *8328*, *8349*, *8392*, *8428*, *8430*, *8450*, *8457*, *8461*, *8497*, *8502*, *8519*, *8534*, *8539*, *8540*, *8541*, *8545*, *8549*, *8551*, *8597*, *8601*, *8603*, *8610*, *8623*, *8653*, *8654*, *8666*, *8669*, *8680*, *8686*, *8687*, *8691*, *8754*, *8768*, *8774*, *8775*, *8799*, *8808*, *8820*, *8823*, *8827*, *8844*, *8847*, *8860*, *8861*, *8866*, *8873*, *8875*, *8877*, *8878*, *8884*, *8886*, *8887*, *8889*, *8890*, *8891*, *8915*, *8928*, *8934*, *8935*, *8939*, *8940*, *8969*, *8971*, *8979*, *8980*, *8982*, *8984*, *8986*, *8994*, *8997*)

Upload

- Occasionally, it would not be possible to manually upload a PDF or an XML file (*8596*)

Workspaces

- It would not be possible to change a workspace from private to public using the lock icon on the workspace header (*9004*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 1.13.0

Release 1.13.0 — Spotlight: money mule TTPs, entity auto-tagging, syslog transport type for outgoing feeds, improved email delivery, distribute report entities with attachments, search entities by taxonomy

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.13.0
Release date	2016-10-21

Highlights

A new release, and a wealth of new goodies. You can set up rules to automatically tag entities upon ingestion based on the specified rule criteria, as well as filter out less relevant entity extracts, so that you can concentrate on the more important ones without any added noise. Entity rules were extended to give you more granular control over the data you want to exclude or retrieve. Moreover, you can now search entities also by taxonomy name.

A new CIQ standard-based editor is available, so that fraud and risk teams can create TTP entities to describe money mules and their behaviors. This enables them to use the platform feature set to investigate potential frauds and to detect fraudulent behaviors.

The GUI got some love, too, with a focus on the entity editor to make it easier to manually create new entities.
On the entity detail pane, besides manually exporting an entity to JSON, you can now export it to STIX as well.

We implemented the syslog transport type for outgoing feeds, so that you can send the output to a syslog server, for example to consolidate and centralize cyber intel logging.

We tightened the screws and bolts around email delivery to make it more robust by introducing Postfix as a mail transfer agent. Postfix runs as a systemd-managed service, and its health state is included in the platform system health monitor.

elasticdump, an Elasticsearch Node module, was upgraded from version 0.16.2 to version 3.0.0.
Before installing elasticdump 3.0.0, remove version 0.16.2:

```
$ yum remove elasticdump
```

This upgrade introduces a change to the *elasticdump* installation procedure: instead of using `yum`, **globally install** `(https://www.npmjs.com/package/elasticdump#installing)` elasticdump 3.0.0 as a Node js module:

Upgrade to the latest release

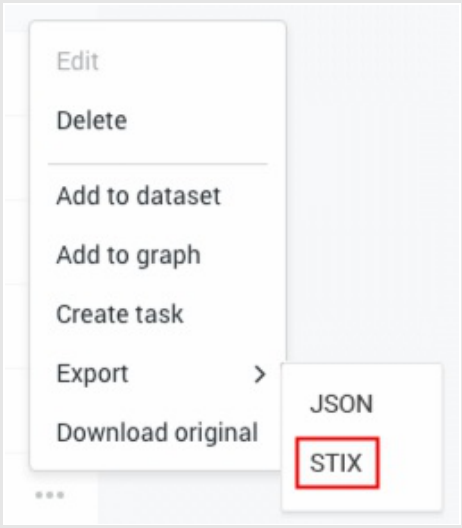
- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Features and functionality

Entities

- A new CIQ standard-based editor allows fraud and risk teams to create TTP entities describing money mules to identify potentially fraudulent behaviors (*8072*)
- When a report entity has attached documents, it is possible to send it on to a recipient along with its attachments. Currently, this feature is supported by email, FTP, and mount point transport types, and it is available for report entities in JSON and STIX formats (*5025*)
- From the **Actions** menu on the entity detail pane it is now possible to export an entity also to STIX XML format (*7039*)



- The `/private/discovery/_search` API endpoint returns all discovered entities, that is all the entities whose `discovery.ignore` field is set to `False`.
  To exclude an entity from discovery, make a `POST` API call to `/api/entities/${entity_id}/meta` and pass `discovery.ignore: True`. (*7150*)
  The field is included in the `meta` entity section:

```
meta: {
  discovery: {
    rules: [id, ...],
    task_runs: [id, ...],
    ignore: False
  }
}
```

Extracts

- It is possible to automatically flag extracts for detection/prevention when the corresponding value is directly extracted from a CybOX object embedded in a STIX Indicator (level 1 extract).
  When this value is indirectly derived from the CybOX payload, for example a domain extract derived from a CybOX object containing a URI, the extract is not flagged for detection/prevention, and the derived extract is marked as an indirectly related extract to the corresponding source indicator (*7922*)
- When ingesting new data through an incoming feed or by uploading a document, it is possible to exclude from ingestion extracts that are derived/inferred from sources other than an embedded CybOX object. When this option is enabled, only the extracts that can be directly acquired from the input are added to the ingestion queue (*7923*)
- Extract classification rule criteria include new options to create rules based on the direct (level1)/indirect (level 2) extract properties (see *7922*) (*7928*)

Feeds

- It is possible to configure a syslog transport feed to send outgoing feed data and event log messages to a syslog server or a SIEM product like ArcSight to centralize cyber intel collection (*7550*, *7781*)

Graph

- On the graph filter pane you can also filter and group the items displayed on the graph by extract state (*7940*)

Notifications

- It is possible to configure notifications to select and deselect which events you want to be notified about (*8096*)

Search

- Tags are searchable: it is possible to search for entities sharing the same tag. Click a tag to automatically run a search based on it, and to display the results (*7910*)
- It is possible to look up entities by taxonomy label, for example based on an Admiralty code or a Kill chain phase (*8094*)
  Search by using the following filters:
  - `tags`: prepend `tags:` to the search term(s) to look up custom tags and taxonomy entries
  - `meta.tags`: prepend `meta.tags:` to the search term(s) to look up custom tags

System

- Postfix takes care of email handling tasks to ensure smoother and more robust operation. You can configure email settings in the GUI through **System > Server > Email > Email settings** , and by specifying other configuration options like host and SMTP in the `/etc/postfix/main.cf` file (*7443*)

Tags

- It is possible to configure custom rules to automatically assign one or more predefined tags to ingested entities (*7290*)

Configuration files

- Dynamic script execution in Elasticsearch is deprecated and should not be used (*7853*)
  In `/etc/elasticsearch/elasticsearch.yml` disable **dynamic scripting** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-scripting.html#enable-dynamic-scripting)` by either removing the `script.inline` property from the configuration file, or by setting it to `false`:

```
script.inline: false
script.indexed: true
```

- New configuration file to set up Postfix email server settings: `/etc/postfix/main.cf`

Documentation

New:

- Default users in the installation guide
- Run a final check in the installation guide, bootstrap section
- Run a final check in the installation guide, upgrade section
- How to create a money mule TTP
- Example of an empty placeholder entity in the *How to enrich entities with extracts* article
- How to back up and restore a PostgreSQL database
- HTTP status codes in the *How to retrieve outgoing feeds* article

Updated:

- Entity editor in the getting started guide
- Configuration files in the installation guide
- Install from the YUM repository in the installation guide, RPM install section
- Install the new package in the installation guide, upgrade section
- Backup guidelines in the installation guide, backup section
- Install the platform in the *How to install the platform via an RPM package* article
- Upgrade Kibana to version 4.5 in the *How to upgrade Elasticsearch and Kibana* article
- Update the config files in the *How to upgrade Elasticsearch and Kibana* article
- Filtering and enriching in the *How to enrich entities with extracts* article
- idref resolution — Nested objects in the *How to enrich entities with extracts* article
- Enriching entities via extracts in the *How to enrich entities with extracts* article

What's changed

Enhancements

Entities

- The author of an entity is displayed on the entity detail pane, so that it is possible to track entity authorship and notify entity authors when changes or updates occur (*7026*)
- Deduplication optimization of incoming feed entities (*7868*)
- Relationship naming logic overall improvement to generate clearer relationship names. Relationships pointing to external, i.e. not yet available in the platform, reference are clearly described in the corresponding headers (*7984*)

- When creating a new entity with the entity editor, or when editing relationships on the **Neighborhood** tab on the entity detail pane, you can now select an option from the drop-down menu to assign the relationship a descriptive title. You can add new entries to the drop-down menu by typing them in the input field, and then by pressing **ENTER**. To remove an entry from the list, click the corresponding ✖ icon (*7985*)

Entity editor

- The **Incident** entity creation form was redesigned and reorganized (*8003*)
- Minor redesign of the other entity creation forms to make it easier to enter entity characteristics (*8063*)

Extracts

- Extract rule refactoring (*7933*)

Feeds

- TAXII poll transport type fpr incoming feeds supports custom HTTP headers, so that it behaves like the same transport type fpr outgoing feeds (*7193*)
- The ArcSight CEF output format for outgoing feeds underwent changes to allow certification of the CEF output (*8068*)

Graph

- Relationship titles, if assigned while creating or updating an entity, are displayed on the graph (*7986*)

Notifications

- Platform users can configure their notifications to receive only selected ones (*7074*)

Rules

- Entity rules — extract classification rules in previous releases — were extended to allow for more flexibility, as well as the ability to drill down with greater detail (*8143*)

System

- Cabby supports JWT token caching (*4163*)
- Email setup is easier and more robust. It is powered by Postfix, and a **postfix** entry has been added to the system health monitor (*7743*)
- elasticdump was upgraded from version 0.16.2 to version 3.0.0 (*7836*)
- HTTP status code responses for feeds downloaded via HTTP transport are clearer (*8088*):
  - HTTP 404 is returned when the outgoing feed task run does not execute
  - HTTP 200 is returned when the outgoing feed task run executes, and an empty list is returned because the feed does not include any new/updated content block
  - HTTP 200 is returned when the outgoing feed task run executes, and a populated list with new/updated content blocks is returned
- Before creating a new Elasticsearch mapping template during an installation procedure, all previous versions of the mapping template are removed to ensure only the new mapping is applied (*8203*)

UI

- UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*7506*, *7542*, *7597*, *7599*, *7606*, *7648*, *7651*, *7755*, *7782*, *7794*, *7830*, *7872*, *7936*, *7937*, *7938*, *7993*, *8003*, *8006*, *8016*, *8063*, *8066*, *8067*)

Deprecated

- On the left-hand navigation sidebar **Extract classification** was renamed to **Rules** (*7290*)
- On the entity detail pane, the **Enrichments** tab was renamed to **Extracts**. Now it shows all the extracts related to the entity (*8092*)

Fixed bugs

Datasets

- Bulk-removing all entities from a static dataset would not remove all the selected entities (*7917*)

Feeds

- Addressed some compatibility issues between Soltra Edge and STIX (*8018*)

Graph

- On the graph, loading all the entities of an extract would return a 404 HTTP status code in the browser console (*8260*)

Logging

- When a database transaction failed, error logging could occasionally fail because of incorrect exception handling (*4327*)

System

- The platform API would not properly handle exceptions in some edge cases (*7777*)
- The platform would lack a default configuration for the TAXII domain, which the OpenTAXII interface requires in order to work correctly (*7964*)
- Deduplication could cause a database deadlock in some edge cases (*8132*, *8286*)

Tags

- It would not be possible to search by tag name for tagged entities ingested through an incoming feed (*7745*)

UI

- Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*6421*, *6695*, *6819*, *7030*, *7272*, *7542*, *7662*, *7971*, *8041*, *8042*, *8043*, *8057*, *8058*, *8059*, *8060*)

Workspaces

- Files attached to a workspace would be erroneously removed upon changing the visibility status of the workspace from private ro public (*7972*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.12.0

Release 1.12.0 — Spotlight: new FlashPoint Thresher enricher, filter extracts by extract classification, PostgreSQL upgrade to version 9.5, database syncing optimization.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.12.0
Release date	2016-09-08

Highlights

We keep expanding the platform core feature set. More flexibility and more intel sources, as well as powerful extract filtering on the graph to clear the view without sacrificing insight in the cyber threat scenario under inspection.

Under **Enrichment > Catalog** you can find a new enricher: Flashpoint Thresher. Polls data from the Flashpoint API. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables with Flashpoint torrent thresher data.

On the graph you can filter and group entity extracts on extract classification, as well as on extract classification state, for example *safe*. Especially when inspecting multiple entities, each one having many extracts, this feature helps unclutter the view. You can ungroup the extracts at any moment to display the exploded view.

At UI level, the autodiscovery URL configuration for incoming feeds using the **TAXII poll** transport type underwent a usability makeover to simplify TAXII feed setup.

PostgreSQL was upgraded from version 9.4 to version 10.1.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Features and functionality

- *Enrichers* — The new FlashPoint Thresher enricher is available in the enricher catalog (*7156*)
- *Entities* — In the entity editor you can now define Snort test mechanisms for indicators (*7842*)
- *Extracts* — On the graph you can now view whether an extract is safe or malicious (*7529*)
- *Feeds* — Outgoing feeds now support also Snort rules (*7843*)
- *Feeds* — The **Update strategy** of outgoing feeds has a new **Diff** option. At the moment, **Update strategy > Diff** is available for CSV and JSON content types. **Diff** compares two datasets, and it returns only the changed data at extract level. An *Added* or *Removed* flag on each line populated with extract information indicates whether the corresponding extract data is new or if it has been deleted (*7849*)
- *Graph* — The right-click context menu on the graph features a new **Add to dataset** option to add the selected entities and extracts to the specififed dataset on the fly (*6356*)
- *Graph* — The right-click context menu on the graph features a new **Create task** option to make it easier to create tasks to follow up on the selected entities and extracts on the graph (*6368*)
- *Graph* — You can filter and group extracts by extract classification and extract classification state (*7940*)
- *UI* — A branded favicon is visible on the browser tab where the active platform instance is running. This makes it easy to identify the platform tab When several tabs are open at the same time (*7020*)

Configuration files

- *Utilities and commands* — The `manage enqueue_entities_to_graph` command was renamed to `manage reindex_graph` (*7946*)

Reindex graph until release 1.11.0:

```
$ /opt/eclecticiq/platform/api/bin/manage enqueue_entities_to_graph
```

Reindex graph from release 1.12.0:

```
$ /opt/eclecticiq/platform/api/bin/manage reindex_graph
```

Documentation

New:

- *How-tos* — Ingestion section and its sub-sections in How to enrich entities with extracts.
- *How-tos* — How to work with the Flashpoint Thresher enricher.
- *How-tos* — How to reindex the graph database.

Updated:

- *Get started* — Entity types
- *Get started* — Create a new entity
- *How-tos* — How to enrich entities with extracts
- *How-tos* — How to monitor the platform
- *Troubleshooting* — Neo4j does not start or is very slow

What's changed

Enhancements

- *Entities* — On the TTP entity detail pane the new **Attack patterns** field is displayed. It shows extra context and additional details about the TTP **CAPEC attack patterns** `(https://capec.mitre.org/index.html)` like CAPEC attack ID reference, the attack name, and a short description. You can enter and edit this information in the entity editor (*7821*)
- *Entities* — The wrapping of empty indicators referencing observables through `idref`s has been improved (*7855*)
- *Extracts* — Also the graph database can now ingest entity extract metadata (*7311*)
- *Extracts* — It is now possible to selectively fetch and sort specific extract rules through the `/extract-rules/` endpoint by using the `classification` filter (*7912*)
- *Graph* — On the **Histogram** tab on the graph, the **Group** functionality features additional grouping options: (*6365*)
  - *Confidence*
  - *Reliability*
  - *Source*
  - *TLP*
  - *Type*
- *Indexing* — Elasticsearch indexing performance has improved, especially in terms of speed (*7884*)
- *System* — PostgreSQL was upgraded from version 9.4 to version 10.1 (*7166*)
- *System* — `EntityPublishedCounter` now supports pagination and standard filtering. It also features two new fields: `destination_name` and `outgoing_feed`. They help create links to existing outgoing feeds. If the destination outgoing feed does not exist any longer, the `outgoing_feed` is empty. `destination_name` can be sorted and filtered (*7751*)
- *System* — Backgrounding the migration run and piping the output to a file (*7769*)
- *Search* — The search index module was refactored to improve Elasticsearch performance and speed (*7851*))
- *UI* — The autodiscovery URL configuration for incoming feeds using the **TAXII poll** transport type underwent a usability makeover to simplify setting up TAXII feeds (6127)
- *UI* — UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*6365*, *7020*, *7308*, *7852*, *7898*, *7913*)

Deprecated

N/A

Fixed bugs

- *Extract classification* — An extract classification rule to blacklist only email addresses would not worlk as epxected (*7883*, *7891*)
- *Extracts* — Report headers including file names in reports titles generated from text files inside an uploaded archive would produce redundant noisy extracts (*7541*)
- *Extracts* — Refreshing the extracts associated with an entity could sometimes not work as expected, resulting in a failure of the reindexing process (*7881*)
- *Extracts* — Delete matching extract rules would not work correctly, resulting in some matching extracts not being deleted (*7896*)
- *Feeds* — An outgoing feed with CSV content type, extact per line output, and a large amount of entities in the CSV output would negatively affect PostgreSQL (*7877*)
- *Feeds* — Intel 471 incoming feeds would fail to run (*7894*)
- *Graph* — The graph would display duplicate relationships (*7106*)
- *Graph* — Graph images in reports would not be synced correctly when updating the graph (*7856*)
- *Mapping* — Incorrect STIX index mapping (*7867*)
- *Notifications* — In case of errors in an outgoing feed form, errors would not be displayed in direct notifications (*7535*)
- *System* — Sometimes errors could occur during a data migration, for example after updating the platform to a newer release (*7960*)
- *UI* — Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*6695*, *7030*, *7272*, *7280*, *7287*, *7361*, *7570*, *7599*, *7606*, *7665*, *7713*, *7783*, *7863*, *7870*, *7918*, *7947*, *7961*)
- *Upload* — It would be possible to manually upload the same file multiple times, which would result in entity duplication (*7652*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.11.0

Release 1.11.0 — Spotlight: Flashpoint enrichers, AnubisNetworks Infections Cyberfeed incoming feeds, ingestion performance improvements, and upgrades to Elasticsearch 2.3.5 and Kibana 4.5.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.11.0
Release date	2016-08-18

Highlights

This release focuses mainly on product maintenance and consolidation.

We upgraded the third-party components Elasticsearch and Kibana to versions 2.3.5 and 4.5, respectively, and we concentrated on enhancing and improving existing functionality.

We added the Flashpoint AggregINT and Flashpoint Blueprint enrichment sources to the enricher catalog.

The EclecticIQ Platform can ingest a new intel source as an incoming feed: **AnubisNetworks Infections Detection Cyberfeed** `(https://www.anubisnetworks.com/products/threat-intelligence/cyberfeed)` provides rich, contextualized threat intelligence for incident response and situational response. The feed offers access to the following intel channels:

- *Infection detection bank trojans*
- *Infection detection DNS malware*
- *Compromised systems website analysis*
- *Compromised systems malware analysis*

Regex syntax in extract classification rules is more restrictive: This field supports only **Elasticsearch regular expression syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#regexp-syntax).`
For further details, see the section describing the **Value matches** field.

Danger:
Before upgrading the platform, check any existing extract classification rules, either active or inactive, you may have created.

Before you proceed to upgrade the platform, edit and update all existing extract classification rules, both active and inactive, so that they comply with the **Elasticsearch regular expression syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#regexp-syntax)`, otherwise any existing rule customization may be lost.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

Features and functionality

- *Enrichers* — The catalog features two new enrichment sources: Flashpoint AggregINT and Flashpoint Blueprint (*7157*)
- *Extract classification* — For any rule in **Extract classification** it is possible to view a list with existing matches in the platform, and users can carry out actions on the reported matches (*7383*, *7468*)
- *Feeds* — A new content type is available to ingest incoming feeds: the compromised systems feed of the AnubisNetworks Infections Detection Cyberfeed, an intel source that provides infection detection information on banking Trojans and DNS malware (*6895*)

Third-party products

- We upgraded the following components:
  - *Elasticsearch* — from version 1.7.1 to version 5.6.7.
  - *Kibana* — from version 4.1.1 to version 5.6.8.
- Elasticsearch requires the **ignore plugin** `()`.

> At the end of the Elasticsearch upgrade, you need to migrate Elasticsearch indices. Make sure you plan the upgrade so that you can factor in enough downtime for this operation. Depending on the size of your database, *it can take from several hours to a few days* .

Configuration files

- New property added to `/opt/eclecticiq/etc/eclecticiq/platform_settings.py` as per release 1.10.0:

```
NEO4J_BATCHING_URL = 'http://127.0.0.1:4008'
```

- New property added to `/opt/eclecticiq/etc/eclecticiq/platform_settings.py` as per release 1.10.0:

```
SUPERVISORD_HOSTS = '127.0.0.1:9001'
```

Documentation

New:

- *How-tos* — How to upgrade Elasticsearch and Kibana
- *How-tos* — How to configure a different database in OpenTAXII
- *Troubleshooting* — Common proxy issues
- *Troubleshooting* — Common ingestion issues
- *Troubleshooting* — Broken dashboard gauges
- *Troubleshooting* — Errno 111 Connection refused
- *Cheatsheets* — Redis cheatsheet
- *Cheatsheets* — Search cheatsheet
- *Cheatsheets* — Supervisor cheatsheet
- *Cheatsheets* — systemd cheatsheet

Updated:

- *Installation* — Config and log files
- *Installation* — Configure Elasticsearch section in Configure the platform
- *Installation* — Define the environment variables under Bootstrap the platform has been removed, since it is no longer necessary to set environment variables.
- *Installation* — Bootstrap Neo4j section in Bootstrap the platform
- *Installation* — Export the settings under Upgrade the platform has been removed, since it is no longer necessary to set environment variables.
- *Installation* — Remove deprecated packages section in Upgrade the platform
- *Installation* — Back up the Neo4j database section in Backup guidelines
- *Installation* — Data recovery section in Backup guidelines
- *How-tos* — The section about **Value matches** under Add an extract classification rule in Extract classification
- *How-tos* — How to configure Anubis Cyberfeed incoming feeds
- *How-tos* — Set the environment variables under Bootstrap the platform in the How to install the platform via an RPM package quick guide has been removed, since it is no longer necessary to set environment variables.

What’s changed

Enhancements

- *Entity editor* — When creating a new entity in the editor, it is now possible to select a save-to-draft or a publish option from the drop-down menus to speed up repetitive entity creation work (*6515*)
  To save the entity as a draft without publishing it right away click **Draft**, and then and choose one of the following options:
  - **Save draft and new**: saves the current entity as draft and creates a new empty entity.
  - **Save draft and duplicate**: saves the current entity as draft and creates a copy to use as a template.
    To save the entity and publish it right away click **Publish**, and then choose one of the following options:
  - **Publish and new**: saves and publishes current entity, and it creates a new empty entity.
  - **Publish and duplicate**: saves and publishes current entity, and it creates a copy to use as a template.
- *Feeds* — Feed update task performance improvements (*7294*)
- *Ingestion* — Performance improvements for calls made by collection management services to poll TAXII collections data changes or data updates (*7507*)
- *System* — Elasticsearch has been upgraded to **version 2.3.5** `(https://www.elastic.co/guide/en/elasticsearch/reference/2.3/release-notes-2.3.5.html)` (*6520*)
- *System* — Kibana has been upgraded to **version 4.5** `(https://www.elastic.co/guide/en/kibana/current/releasenotes.html)` (*6520*)
- *System* — Kibana now includes all the index patterns used in the platform: (*7438*)
  - *stix*
  - *logstash-**
  - *statsd-**
  - *draft-entities*
  - *documents*
- *UI* — UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*6856*, *7095*, *7096*, *7269*, *7274*, *7422*, *7462*, *7517*, *7543*, *7544*, *7567*, *7581*, *7592*, *7600*, *7626*, *7655*, *7664*, *7679*, *7746*, *7758*)

Deprecated

- *Feeds* — Extract IDs are not included any longer in JSON format outgoing feeds, since they are not relevant in exports (*7112*)
- *System* — Before installing or upgrading to this release of the platform, remove the following deprecated packages:
  - `platform-opentaxii`
- *System* — When installing, upgrading or bootstrapping the platform, it is no longer necessary to set environment variables manually.

Fixed bugs

- *Enrichers* — When configuring the PyDat enricher, it would not be possible to set a private network IP address in the **API URL** input field (*7801*)
- *Entities* — A user belonging to more than one group would not be able to publish a previously created draft entity if they are reassigned to be part of only one group before attempting to publish the draft entity (*7285*)
- *Entity editor* — Modifying an entity in the entity editor by changing its observable type value, by adding more observable types to the existing one(s), or by adding a URL observable type would not be applied upon saving (*7604*, *7728*, *7771*)
- *Extract classification* — Ignoring an extract that had previously already been flagged as either safe or malicious would throw an error (*7388*)
- *Extract classification* — A newly created extract classification rule would not work as expected when the rule source was set to the default admin group (*7666*)
- *Extract classification* — Deleting multiple extract classificaiton rules would require a web page hard refresh after each deletion to work as expected (*7785*)
- *Feeds* — SSL validation on incoming feeds would not work as expected (*7773*)
- *Feeds* — The paginated fetch query for outgoing feeds would not work as expected (*7793*)
- *Graph* — The menu option that allows loading all the extracts of an entity on the graph canvas would sometimes fail to load all the extract (*7803*)
- *Indexing* — Fixed some issues affecting Elasticsearch indexing (*6432*, *7613*, *7672*, *7689*)
- *Ingestion* — Sometimes, ingestion errors would not be properly intercepted and stored into the `processing_status` field of a blob. This would cause ingestion to unexpectedly abort (*7709*)
- *Search* — On the **Upload** section, search would not work as expected (*7719*)
- *Taxonomy* — Modifying an editable taxonomy entry would throw an error (*7222*)
- *Taxonomy* — Creating two taxonomies and promoting them both to parent for each other would create a circular reference and an infinite loop (*7423*)
- *UI* — Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*6051*, *6294*, *6543*, *6572*, *6574*, *6583*, *6878*, *6930*, *7003*, *7004*, *7034*, *7062*, *7122*, *7176*, *7177*, *7179*, *7181*, *7281*, *7287*, *7310*, *7358*, *7593*, *7601*, *7607*, *7629*, *7653*, *7656*, *7659*, *7668*, *7678*, *7694*, *7698*, *7712*, *7713*, *7715*, *7717*, *7727*, *7740*, *7757*, *7765*, *7767*, *7774*, *7787*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.10.0

Release 1.10.0 — Spotlight: Flashpoint enrichers, system health monitor, running job monitor, incoming feed performance improvements.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.10.0
Release date	2016-07-15

Highlights

This release introduces new features and enhances existing ones. Because less is more, but more is better .

The new **Jobs** tab, which you can access by clicking **System > Jobs**, offers an overview of platform background tasks. You can filter tasks by status, as well as manually terminate running tasks, if necessary.

We added the Flashpoint AggregINT and Flashpoint Blueprint sources to the enricher catalog.

As for intel ingestion, we tweaked incoming feeds to improve performance, resulting in more efficient data deduplication and ingestion speed.

The graph embedded in the **Neighborhood** tab on the entity detail pane is refreshed upon selecting the tab. Click it to view updated neighborhood relationships for the selected entity on the graph.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

- *Enrichers* — The enricher catalog supports a new source: Flashpoint Blueprint.
  Polls data from the Flashpoint API. It provides information based on geolocation and IP ranges, as well as on country scope. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, state actors involved in cyberwarfare, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables like city/country name or IP address hit, latitude/longitude or IP address hit, forum name and thread title related to a hit, user name uniquely matched to an IP address hit. (*7157*)

- *Enrichers* — The enricher catalog supports a new source: Flashpoint AggregINT.
  Polls data from the Flashpoint API. It provides information on malware, hosts, domains, IP addresses, and hashed files. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, communities in conflict, state actors involved in cyberwarfare, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables like forum name, forum room name, user name of the author of a post (as actor-id), post content, thread title, UTC date and time of a post in **ISO 8601** `(https://en.wikipedia.org/wiki/iso_8601)` **(RFC 3339)** `(https://tools.ietf.org/html/rfc3339)` format. (*7158*)
- *System* — It is now possible to check and monitor basic system health, either via the **System** health bar on the web-based GUI status bar, or by making an API call (*4036*, *4643*)
- *System* — The new **Jobs** tab, which you can access by clicking **System > Jobs**, offers an overview of platform background tasks (*6967*, *7120*)
- *Documentation*
  - New:
    - Check system health
    - Work with enrichers
  - Updated:
    - Enrich entities with extracts
    - Extract classification
    - Monitor the platform for system administrators
    - Configure and monitor the platform through the web-based GUI
    - Bootstrap Elasticsearch
    - Bootstrap Neo4j

What's changed

Enhancements

- *Entities* — When exporting an entity to a JSON file, any sighting relationships the entity may have are included in the export (*7108*)
- *Entities* — The query responsible for populating the **Extracts** section on the **Overview** tab of the entity detail pane has been optimized to reduce data loading time (*7419*)
- *Extracts* — Entity data deduplication has been improved to make it more efficient (*7491*)
- *Feeds* — The look and feel of the feed configuration option sections for incoming and outgoing feeds have been redesigned to improve user-friendliness (*5825*, *6546*, *6981*)
- *Graph* — Clicking the embedded graph on the **Neighborhood** tab on the entity detail pane opens the entity neighborhood relationship view on the graph (*6868*)
- *Notifications* — An error message is displayed when users manually try to upload a duplicate file (*6675*)

- *Notifications* — A notification message is displayed when proxy settings are changed or updated to remind users to restart the process: *Proxy configuration updated. The process needs to be restarted in order for these settings to be applied.* (*6286*)
- *Notifications* — If the Neo4j service is down and users try to add entities to the graph, an error message is displayed to notify the issue: *Error adding items to graph* (*7477*)
- *UI* — UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*6472*, *6774*, *7365*, *7373*, *7540*)

Deprecated

- n/a

Fixed bugs

- *Datasets* — Manually removing an entity from a dataset would not behave as expected (*7362*)
- *Datasets* — Manually adding a newly created entity to an existing dataset, or to a new dataset created on the fly would not behave as expected, or it would throw an error (*7366*, *7430*, *7431*, *7432*, *7448*, *7464*, *7528*)
- *Enrichers* — Links to the VirusTotal web site source in the **Enrichments** tab on the entity detail pane would not behave as expected (*6995*)
- *Entities* — It would not be possible to edit an existing entity name when the name is very long (> 50 characters)(*6862*)
- *Entities* — Downloading en entity as original would generate a file with extension *.undefined* instead of the correct file extension for the original file (*7217*)
- *Entities* — When creating a sighting entity, it would not be possible to add related extracts to it because the action would trigger an error (*7279*)
- *Feeds* — When trying to ingest again failed blobs because of content type mismatch, upon reingestion with the appropriate content type selection the originally failed blobs would be rejected as duplicates (*7483*)
- *Search* — After manually entering a search string in the search box and clicking the search button to run it, the search string would be removed (*5859*)
- *UI* — Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*6322*, *7001*, *7283*, *7284*, *7293*, *7300*, *7324*, *7313*, *7360*, *7363*, *7370*, *7372*, *7389*, *7391*, *7433*, *7434*, *7436*, *7455*, *7479*, *7481*, *7494*, *7532*)
- *Upload* — Uploading a file with binary/non-text content as text would be erroneously ingested and saved as a report entity (*6301*)
- *Users* — User creation or deuplication would throw an error and it would not possible to save the changes (*7437*)
- *Workspaces* — It would be possible to create workspaces with the same name even if workspace names need to be unique (*7180*, *7429*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.9.0

Release 1.9.0 — Spotlight: duplicate data deduplication, Elasticsearch Sightings enricher, and support for ingesting AnubisNetworks Infections Cyberfeed intelligence.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	1.9.0
Release date	2016-06-15

Highlights

This release has an emphasis on maintenance, but that does not mean we got less enthusiastic: besides carrying out standard maintenance tasks like bug fixing and screw tightening, we built new features and revamped existing ones as well.

Incoming data deduplication now includes basic entity-level deduplication on entity content. Besides data deduplication at file level to filter out duplicate packages, the same process is carried out also at entity level. Think of a scenario where a package repeatedly embeds the same TTP definition. Instead of spawning multiple duplicate entities in the platform, duplicate instances of the definition are ignored and excluded from ingestion. The result is less noise and cleaner data.

Rules replaces and expands **Exclusion list**. Entity and observable rules allows for granular control over entity observable filtering by flagging observables as malicious, safe, and irrelevant. Configurable rules help you filter out unwanted and/or unnecessary data, so that you can focus on the most relevant potential threats that can affect your organization.

The EclecticIQ Platform can ingest a new intel source as an incoming feed: **AnubisNetworks Infections Detection Cyberfeed** `(https://www.anubisnetworks.com/products/threat-intelligence/cyberfeed)` provides rich, contextualized threat intelligence for incident response and situational response.

Besides external intelligence, you may wish to access and search also intelligence within your organization. The **Elasticsearch sightings** enricher allows you to do just that. You can configure the enricher to index and search an Elasticsearch instance outside the platform, for example one that aggregates organization-wide log data. Based on the rule criteria you define, returned hits are automatically saved to the platform as sightings.

We revamped the **Upload** area, where you can submit supported file types and compressed archives for upload and ingestion to the platform. Same functionality, slicker look.

Upgrade to the latest release

- Follow the standard *upgrade procedure* for CentOS/RHEL or for Ubuntu Server.

What's new

- *Extracts* — Entity extracts ingested via the ThreatGRID enricher can be automatically flagged as *malicious* upon ingestion (*6773*)
- *Extracts* — **Rules** replaces and expands **Exclusion list**. Entity and observable rules allows for granular control over entity observable filtering by flagging observables as malicious, safe, and irrelevant. Configurable rules help you filter out unwanted and/or unnecessary data, so that you can focus on the most relevant potential threats that can affect your organization. (*7129*)
- *Enrichers* — You can configure the new *Elasticsearch sightings* enricher to run customizable searches in an external Elasticsearch instance, for example one responsible for centralized log aggregation within the organization. Based on the search critieria defined for the enricher, any matches the enricher retrieves are used to automatically create a sighting in the platform (*6087*)
- *Feeds* — A new content type is available for incoming feeds: AnubisNetworks Infections Detection Cyberfeed, an intel source that provides infection detection information on banking Trojans and DNS malware (*6994*, *7125*)
- *Feeds* — Enhancements to the Intel 471 incoming feed to improve feed configuration and modification (*6742*)
- *Documentation*
  - New troubleshooting section. The articles in this part of the documentation focus on specific known issues that may occur while installing, configuring, or using the platform, and they suggest workarounds or mitigating alternatives.
  - New articles on troubeshooting SELinux issues and MS Edge certificate error message (*6699*), backup guidelines for the platform configuration files and databases, and guidelines on monitoring the platform.

What's changed

Enhancements

- *Editor* — The built-in WYSIWYG text editor that is available, for example, in the **Analysis** field of the entity editor has been replaced with a new one to offer a smoother and more pleasant writing experience (*6914*)
- *Entities* — Improved content extraction when handling entity attachments from CybOX raw artifacts and data URIs (*7151*)
- *Feeds* — Clearer STIX/JSON package naming STIX packages are created in outgoing feeds (*7111*)
- *Search* — By default, Elasticsearch search queries that do not resolve time out after 20 seconds This prevents Elasticsearch from hanging in case a query does not resolve (*7090*)
- *Tasks* — The task detail pane displays an overview of the task stakeholders under **Stakeholders**, so that you know whom you need to notify with task update messages (*6786*)
- *Upload* — The **Upload** area features a revamped look and feel (*6429*)
- *UI* — UI alignment to improve UI consistency, and to provide a more consistent and predictable user experience across the platform GUI (*6970*)

Deprecated

- **Exclusion list** is not available anymore as per this release. This feature has been replaced by **Rules**.

Fixed bugs

- *Discovery* — In **Discovery**, filtering results by rule would throw a 400 error (*6756*)
- *Enrichers* — Enrichers would not be automatically disabled after a failure, but they would remain active in a failed status (*6963*)
- *Entities* — When exporting to CSV the entities returned by a search, TLP values would not be exported correctly and would be replaced by *null* in the CSV file (*6956*)
- *Entities* — When creating and then saving an entity in the entity editor, a user-populated **Impact** field would not properly retain its content (*7032*)
- *Entities* — When creating and then saving an entity in the entity editor, an empty **Analysis** field would be automatically populated with JSON data (*7033*)
- *Entities* — In MS IE 11, when creating, saving, and then editing an entity in the entity editor, previously saved content would not be properly retained (*7139*)
- *Extracts* — When creating an entity and adding extracts to it, not all allowed extracts types would be available for selection (*7000*)
- *Feeds* — Content block URLs in outgoing feeds would be broken if no domain is name configured by default (*6283*)
- *Relationships* — It would not be possible to save a newly manually created relationship between entities (*7018*)
- *Graph* — After deleting an entity from the graph, the deleted entity would be restored on the graph (*7058*)
- *Graph* — Entity details would not be displayed in the entity detail pane on the graph (*7063*)
- *Search* — On a search result page, it would be possible to select, and then successfully deselect, a dataset (*6997*)
- *UI* — Fixed several bugs that would cause unexpected behavior on user actions or user selections, as well as a number of cosmetic issues (*6436*, *6673*, *6750*, *6753*, *6781*, *6782*, *6861*, *6866*, *6869*, *6892*, *6903*, *6958*, *6960*, *6961*, *6992*, *6997*, *7005*, *7007*, *7010*, *7011*, *7019*, *7031*, *7032*, *7035*, *7048*, *7060*, *7076*, *7083*, *7087*, *7093*, *7136*, *7219*, *7270*, *7271*)
- *Workspaces* — Removing a dataset from an archived workspace would throw a 403 error (*6506*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 1.8.0

Release 1.8.0 — Spotlight: revamped notifications, LDAP authentication and authorization, item history, and configurable time zone.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

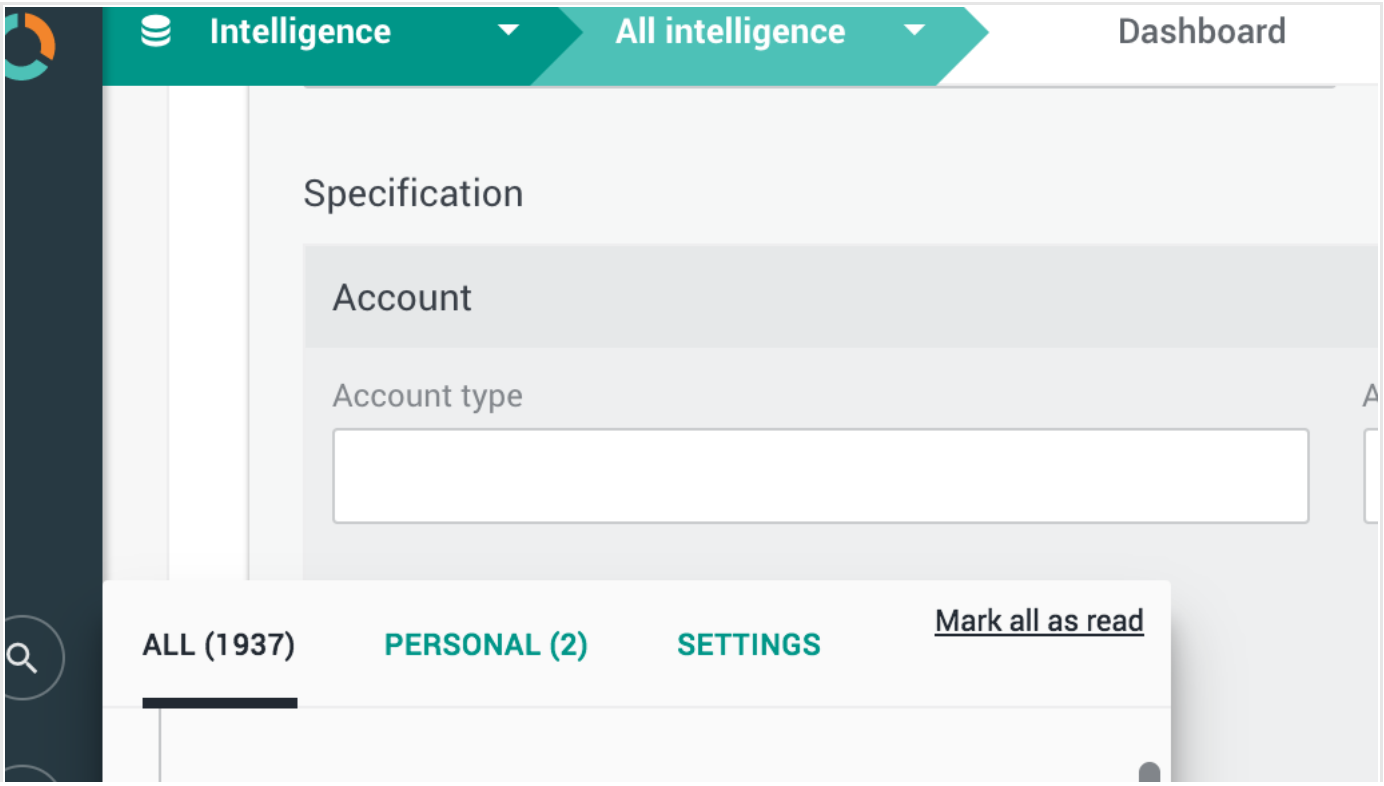
These release notes apply to the following product:

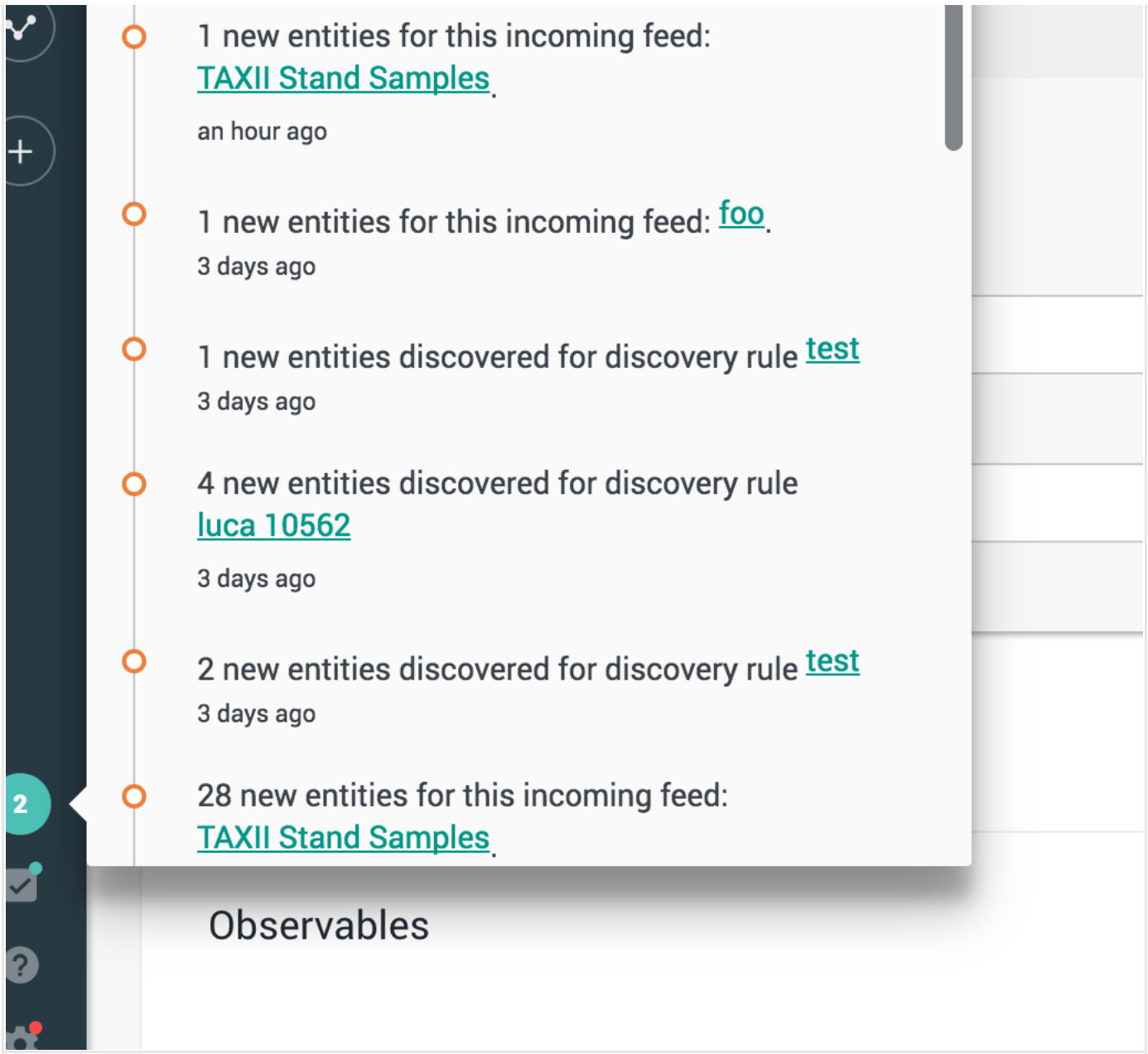
EclecticIQ Platform	
Release version	1.8.0
Release date	2016-05-12

Highlights

Features

We gave platform notifications a full facelift: the new notification center is now your one-stop-shop to review general, platform user-wide, as well as direct notifications for a specific user. To display the notification center drop-down, click the notification icon next to the profile avatar image:





You can control user authentication and authorization through LDAP.

Enters history: we started to gradually roll out this feature, and we plan to extend it in future platform releases. **History** is currently available for workspaces, incoming and outgoing feeds, enrichers, groups, roles, and users.

You can now set a specific time zone in the platform to display time values in your location time zone.

Last but not least, we hunted down some cosmetic issues affecting the UI like truncations and word alignment on text strings.

What's new

- *File submission* — You can submit files through the API to scan them for possible threats
- *History* — The **History** feature is currently available for workspaces, incoming and outgoing feeds, enrichers, groups, roles, and users
- *LDAP support* — Control access through LDAP authentication and LDAP authorisation

- *Notifications* — The notification center offers easy access to general and personal notifications. Notification messages are also displayed in a pop-up in the relevant platform area, where applicable. Direct user notifications for important messages concerning processes and configuration that may require user review or user action
- *Time zone* — It is possible to set the preferred time zone system-wide, as well as per user

What's changed

Enhancements

- *Dashboard* — When you customize the dashboard, you can select and deselect all gauges with one click
- *Documentation* — Added a section describing platform monitoring tools and how to use them
- *Enrichers* — The enricher catalog was now includes also the *Fox-IT InTELL Portal*
- *Entities* — On the entity detail pane, it is easier to share the entity direct link
- *Entities* — The platform ships with a script that allows automating sighting reporting from an outgoing feed
- *Entries* — When creating a new platform entry like a workspace, an enrichment rule, a feed and so on, saving the current entry and creating a new one of the same type right away is quicker and easier
- *Feeds* — When creating an incoming or an outgoing feed, the feed content type and the transport type are related: the selected content type affects the allowed transport types available in the corresponding drop-down menu
- *Feeds* — The ArcSight CEF format schema for outgoing feeds was fine-tuned to improve performance
- *File extraction* — It is possible to save a file as an entity attachment
- *File upload* — It is possible to save a file as an entity attachment
- *History* — A context-specific audit history is available; audit history is available for process and configuration items; the **System > Audit** section now includes a **Message** column to display audit trail messages that provide context and information about the audit entries
- *Notifications* — Improved user feedback through pop-up notifications in the **Upload** section

Deprecated

- *Graph* — On the graph, the **Remove** context-sensitive menu option has been renamed to **Remove from graph**
- *Ingestion* — The `supervisor intel-search-indexer` process was renamed to `search-ingestion` to better clarify its purpose

Fixed bugs

- *Dashboard* — Some dashboard gauges would be duplicates (*6538*)
- *Datasets* — Mixed static and dynamic datasets would be allowed (*6052*)
- *Discovery* — Editing and saving changes to a discovery rule would not apply the changes correctly (*6298*)
- *Enrichment* — In the entity detail pane, the enricher sort order of the **Enrich** drop-down menu on the **Enrichment** tab would not be correct (*6315*)
- *Enrichment* — The undo delete action for an enrichment rule would not work as expected (*6795*)
- *Entities* — Aborting an entity creation in the entity editor would redirect to the previously browsed page instead of the entity overview page (*5934*)
- *Entities* — After deleting a sighting of an entity, the entity would still be flagged as sighted (*6167*)
- *Entities* — The sighted status of an entity would not be updated automatically (*6317*)
- *Entities* — Filtering draft entities by user would not work as expected (*6419*)
- *Entities* — Clicking a draft entity in the entity editor would return an error in the console (*6475*)
- *Entities* — (*IE 11*) In the entity detail pane, switching among the available tab views may cause the browser to hang (*6576*)
- *Entities* — (*IE 11*) It would not be possible to create entities with characteristics because the operation would return an error in the console (*6577*)
- *Entities* — When creating an entity, an empty `information_source` object in the source would not be ignored as expected (*6587*)
- *Entities* — Creating a Course of action entity in the entity editor would return an error in the console (*6744*)
- *Entities* — In the entity detail pane, the related workspace the entity belongs to would not be displayed (*6784*)
- *Entities* — Creating an Incident entity in the entity editor would return an error in the console (*6792*)
- *Entities* — Creating a Threat actor entity in the entity editor would return an error in the console (*6804*)
- *Entities* — Editing an entity in the entity editor and then saving it as a draft would return an error in the console (*6865*)
- *Exclusion* — Adding an extract to an exclusion list would return an error in the console (*6814*)
- *Extracts* — Flagging an extract with any state among the available ones would return an error in the console (*6297*)
- *Feeds* — When editing an incoming or an outgoing feed, multiple selections in an input field (where applicable) would not be saved (*6477*)
- *Feeds* — When editing an existing outgoing feed, no authorized groups would be displayed on the edit form (*6527*)
- *File attachments* — Removing an attachment would not work correctly (*6683*)
- *File download* — (*Firefox*) Downloading a file attached to a workspace would not work (*6544*)
- *Graph* — Undefined relations would be displayed on the graph (*6142*)
- *Graph* — Adding an extract to the graph would throw an error (*6316*)
- *Graph* — Outdated entity versions would be displayed on the graph (*6482*)
- *Graph* — Deleting entities from the graph would return errors in the console (*6508*)
- *Graph* — It would not be possible to correctly save a graph (*6726*)
- *Graph* — In the graph view, trying to open a workspace to select one or more workspace entities wold return an error in the console (*6803*)
- *Login* — Loggin in to the platform with invalid credential would return an incorrect error message (*6584*)
- *Logs* — (*IE 11*) Results would not be displayed on the log tab (*6284*)

- *Neighborhood* — When browsing back to the previous entity, the graph view on the **Neighborhood** tab would not be displayed correctly (*6303*)
- *Scheduler* — The Celery module responsible for task scheduling would not run as expected (*6107*)
- *Search* — (*Firefox*) When selecting a search pattern from the search cheatsheet, the selection would not populate the search input field (*6687*)
- *System* — An invalid namespace would not be properly validated in the platform settings (*6211*)
- *Tasks* — When creating a task, the mandatory **Assigned to** field would not be validated correctly in the UI (*6485*)
- *UI* — Pagination would be enabled also when no content is returned on a page (*6289*)
- *UI* — (*Firefox*) Right-clicking would open the browser context menu instead of the platform context menu (*6691*)
- *UI* — (*IE 11*) The calendar would not be displayed correctly (*6694*)
- *UI* — (*IE 11*) Right-clicking would open the browser context menu instead of the platform context menu (*6698*)
- *UI* — (*Windows 7 + IE 11*) The platform UI does not open (*6821*)
- *User profile* — When editing the currently signed in user profile, available groups and roles for the user would not be displayed on the form (*6431*)
- *Workspaces* — Archived workspaces would be included in workspace drop-down lists (*6447*)
- *Workspaces* — Clicking **Cancel** on a deletion confirmation pop-up dialog would cause a loop where the pop-up would be iteratively displayed again (*6767*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 0.16

Release 0.16 — Spotlight: pop-up tooltips, faster queries and graph reindexing. Moreover: cleaner UI, pagination on poll requests, default outgoing feed.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.16
Release date	2016-04-15

Highlights

Features

Automatically run newly ingested URLs through the VirusTotal public API.

The search cheatsheet drop-down overlay includes a new hint showing how to run searches by tag: `tags:*`.

The **Direct link to entity** option on the entity detail pane, **Overview** tab, makes entity link sharing a breeze.

Pop-up tooltips provide short contextual hints when you hover the mouse on the tooltip icon:

UI

We reviewed UI strings and UI messages to make them more consistent and to harmonize the tone of voice. The edits aim at removing ambiguities in phrasing and terminology to improve clarity and user-friendliness.

The default graph view is simpler and cleaner. When you open the graph, the **Time bar** and the **Histogram** are minimized to offer a distraction-free view of the entities on the graph.

Performance

As usual, we strive to tweak and tune platform performance to improve, among other things, task execution: with this release we offer shorter ingestion times for PostegreSQL queries, more efficient graph reindexing, and a faster enricher startup process.

We also optimized the existing TAXII services to include pagination support on poll requests, an optimized `count_only` poll query, and a default outgoing feed upon install to speed up getting up and running with the platform.

You can find a detailed overview of the changes included with this release in the following sections.

What's new

- *Enrichers* — It is now possible to automatically scan newly ingested URLs by running them through the VirusTotal public API (*6057*)
- *Entities* — On the entity detail pane, **Overview** tab, the confidence value assessing the reliability of the entity details is displayed, when available (*5844*)
- *Entities* — On the entity detail pane, **Overview** tab, the **Direct link to entity** option enables entity URL sharing with one click (*6123*)
- *Help* — On mouse hover, tooltips pop up to display short usage hints. Currently, these tooltips are available in the following sections: **Exclusion list > Add entry**, **Enrichment > Rules**, **Incoming feeds > Create**, **Outgoing feeds > Create** (*5346*)
- *UI* — Selection lists with multiple options include now **Select all** / **Unselect all** command options to enable easy one-click selection and deselection of all available list items (*5823*)

What's changed

Enhancements

- *Audit* — A **System > Audit** breadcrumb navigation aid is available in the platform audit section (*6255*)
- *Enrichment* — Enricher startup performance was improved (*5817*)
- *Entities* — On the entity detail pane under the entity title, the entity source is displayed (*5139*)
- *Graph* — Graph reindexing was improved, resulting in faster reindexing times (*6088*)
- *Graph* — When you open the graph, the **Time bar** and the **Histogram** are minimized to offer a distraction-free view of the entities on the graph (*6524*)
- *Ingestion* — The `count_only` poll request skips unnecessary processing when the expected response includes only the amount of available polled items (*5317*)
- *Ingestion* — Internationalized domain name extraction was improved (*5844*)
- *Ingestion* — under **Uploads > Upload a document** and **Incoming feeds > Create** it is now possible to define passwords for password-protected archives, so that they can be seamlessly ingested. Two input fields are available to enter archive passwords: **Archive password** on **Uploads > Upload a document** , and **Accept password protected archives** on **Incoming feeds > Create** (*6069*)

- *Search* — The `data.type:coa` query on the search cheatsheet drop-down overlay was renamed to `data.type:course-of-action` to better clarify its purpose (*6225*)
- *Search* — The search cheatsheet drop-down overlay includes a new hint showing how to run searches by tag: `tags:*` (*6274*)
- *System* — PostegreSQL query processing speed was improved (*6507*)
- *Tasks* — The **Run now** button allows to run a task, for example incoming and outgoing feeds, asynchronously. It becomes unavailable when task execution has already been initiated. In other words, it is not possible to manually initiate a task run if another task is already running (*5791*)
- *Tasks* — The **…** context menu to manipulate tasks on the **Tasks** page was restyled to improve ease of use (*6143*)
- *TAXII services* — The existing TAXII services were enhanced to include pagination support on poll requests, an optimized `count_only` poll query, and a default outgoing feed upon install to speed up getting up and running with the platform (*5314*, *5315*)
- *UI* — UI string and message cleanup across the UI to improve consistency and to offer a more uniform user experience (*3694*)
- *UI* — Pressing **ENTER** on a form while the input cursor is inside an input field saves the form content (*6247*)
- *UI* — The **Remove** context menu option on the graph was renamed to **Remove from graph** to avoid ambiguities between removing an item from the graph and actually deleting it from the platform database (*6516*)
- *Users* — The default user avatar is associated with a default image to improve its visibility on the UI (*5950*)
- *Users* — The **Edit user** form under **System > User management** was restyled to improve ease of use (*6247*)

Deprecated

- *Extracts* — Whereas the platform previously allowed both URL and URI extract types, URI extracts have now replaced all URL ones. The reason is that URI extract types are automatically created from entities. This approach provides a more efficient use of the platform automation capabilities (*6350*)

Fixed bugs

- *Discovery* — It would not be possible to save a new discovery rule if a workspace was selected under **Correlated workspaces types** (*6495*)
- *Entities* — When filtering results by entity type in the **Discovery** section, the list with the currently available entity types would be incomplete (*6287*)
- *Entities* — When creating a report entity, it would not be possible to attach a file to it (*6292*)
- *Entities* — It would not be possible to create a sighting from an entity (*6296*)
- *Entities* — When creating a report entity, it would not be possible to remove a previously uploaded attached file (*6318*)
- *Entities* — When creating a new entity, the **Source** field would not be validated correctly (*6441*)
- *Entities* — It would not be possible to open an entity from the **Content** tab of an incoming feed detail pane, or open an entity related through extracts from the **Neighborhood** tab of an entity detail pane (*6525*)
- *Feeds* — For an outgoing feed with FTP upload transport type, it would not be possible to successfully publish feed content (*6280*)

- *Feeds* — For an incoming feed with a TAXII inbox transport type, it would not be possible to create and run content through a TAXII push request (*6290*)
- *Feeds* — When creating a new incoming feed with the **TAXII poll** transport type, the **Autodiscovery** configuration option would not be available (*6417*)
- *Feeds* — When creating a new incoming feed, any extra headers in the feed configuration would not be validated correctly (*6461*)
- *Feeds* — When editing an existing outgoing feed, any fields holding multiple selections would not be saved correctly upon saving and exiting (*6477*)
- *Feeds* — When creating a new incoming or outgoing feed and setting an invalid URL in the transport configuration, the invalid URL would not be validated correctly (*6483*)
- *Feeds* — When creating a new outgoing feed including one or more authorized groups, they would not be displayed in the **Authorized groups** drop-down list when editing the same feed at a later time (*6527*)
- *Neighborhood* — After saving new related entities, the entity detail pane sections on the **Neighborhood** tab would not be populated accordingly (*6537*)
- *Search* — Applying filters to display a sub-set of the available content would sometimes hang without returning the filtered entries (*6351*)
- *Settings* — When configuring the STIX settings for the platform, the STIX namespace would not be validated correctly (*6211*)
- *UI* — Clicking the detail pane while its content is still loading would cause the detail pane to close (*6253*)
- *Workspaces* — Creating multiple worskpaces with the same name would not trigger a duplicate name error message (*5924*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 0.15

Release 0.15 — Spotlight: new auditing feature, a cleaner UI, and improved database performance. More good stuff: easier batch uploading and ingestion with archives, enricher improvements, and overall tighter nuts, bolts, and washers.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.15
Release date	2016-03-18

Highlights

Auditing

On the left-hand navigation sidebar click **System**. The new **Audit** tab offers a searchable overview of the platform events. You can filter the events you want to be returned in the audit view, and you can examine event details thoroughly in Kibana.

Automatic archive decompression

You can now upload or ingest multiple files at once by adding them to an archive, which you then upload or ingest through an incoming feed. For the supported archive formats, the platform automatically detects the archive type, and it extracts the files. The entities found in the files are shown in a view with the results of the operation.

- Supported archive formats: *.zip*, *.rar*, *.tar*, *.tar.gz*, *.tar.bz2*, *.tar.Z*.
- Each archive needs to contain only one file format.
- The file format of the files in the archive needs to match the specified content type for the incoming feed or the upload operation handling the ingestion.

UI

The UI underwent scrutiny to improve labeling consistency, and it is now more streamlined. The server and proxy settings sections have been redesigned to make them more intuitive and easier to use.

Performance

System optimization focused on reducing PostgreSQL processing time and improving SQL query ingestion. These tweaks contribute to speeding up entity ingestion into the platform and to decreasing the size of ingestion queues.

You can find a detailed overview of the changes included with this release in the following sections.

What's new

- *Documentation* — You can run full-text searches in the platform documentation
- *Enrichments* — The VirusTotal enricher can now retrieve full public reports (*6023*):
  - URL scan report
  - IP address scan report
  - Domain name scan report.

  When a VirusTotal report is available as the outcome of an enrichment task execution, the report includes:
  - Observable for the hashes, if it is not already existing
  - A permalink reference
  - When the scan detects a malicious item, a TTP entity is created.
- *Enrichments* — The OpenDNS enricher is available through the OpenResolve enricher task (*5355*)
- *Entities* — When an entity is created using the entity editor, it is validated against the corresponding schema in the backend before being further processed (*5613*)
- *Entities* — It is now possible to post a new entity along with any known extracts belonging to it (*5383*)
- *Feeds* — The user agent HTTP header for Intel 471 feeds and enrichments is `User-Agent:'EclecticIQ Platform'` (*5742*)
- *Feeds* — Users can edit the ingestion start date for an incoming feed to adjust the feed scope as necessary (*5792*)
- *Logging* — You can forward Logstash logs to an external system like **Syslog** `(http://www.syslog.org/)` by implementing an Elasticsearch plugin (*4668*)
- *Logging* — A new **Audit** tab is accessible through the **System** option. It displays a searchable event audit trail so that sysadmins can inspect the platform event sequence, for example for troubleshooting purpose (*5766*)
- *System* — Incoming feeds can use custom/internal CAs to verify SSL certificates for incoming feeds with TAXII polling transport type (*5298*)
- *System* — Authentication through client certificate: it is possible to configure Nginx to carry out client SSL verification (*5768*)
- *Tags* — The tag selection box has been reintroduced. The drop-down list is a tree structure displaying tag hierarchy (*5641*)
- *Tasks* — Users can delete existing tasks to prune the platform from unnecessary tasks (*5909*)

- *UI* — Content and transport types with extensions are reflected in the incoming and outgoing feed UI areas (*5558*, *6148*, *6156*, *6170*)
- *UI* — When a user is a member of one group only, the **Source** drop-down menus in the entity editor and in the file upload section are now automatically pre-populated with the group name (*5670*)
- *Upload* — You can upload plain text files to the platform (*5940*)
- *Upload* — Archive files that are ingested through incoming feeds and upload operations are automatically detected and decompressed (*6068*)

What's changed

Enhancements

- *Kill chain* — The kill chain implementation through a dedicated drop-down menu in the entity editor has been replaced by kill chain stage assignment through tagging (*5345*)
- *System* — PostgreSQL default configuration has been fine-tuned (*5764*)
- *System* — PostgreSQL SQL ingestion queries have been optimized (*5765*)
- *UI* — Form feedback is more consistent to provide a more familiar and predictable user experience (*4872*)
- *UI* — It is now possible to customize pagination to display 20, 50 or 100 entities per page. Navigation aids are available to go the first or the last page, as well as to the previous or the following page (*5365*)
- *UI* — Unauthorized user access to an entity with access restrictions triggers a message informing the user that they lack the necessary permissions to access the resource (*5392*)
- *UI* — In the proxy setting section it is now possible to define destinations that should bypass proxying; host names, IP addresses, and/or IP ranges need to be comma-separated (*5772*)
- *UI* — The proxy setting section has been redisegned to reduce complexity and improve user-friendliness (*5776*)
- *UI* — Server settings are now consolidated in one section in the UI (*5829*)
- *UI* — The TAXII poll transport label for the starting ingestion time of an incoming feed has changed from **Initial Since** to **Starting From** (*6104*)
- *UI* — Consolidated terminology for **Delete** and **Remove** action options in the **Actions** menu in the detail pane (*6122*, *6124*)

Deprecated

- *Discovery* — On the **Discovery > Entities** tab it is no longer possible to sort entities by workspace (*4621*)

Fixed bugs

- *Dashboard* — **Cybox observables per type** dashboard visualization would not include all available CybOX entities (*5473*)
- *Discovery* — After running a discovery rule task, the discovery rule table overview on the **Logs** tab in the discovery detail pane would not update correctly (*5813*)
- *Enrichments* — Deleted groups in enrichment rules would remain available as sources (*5926*)
- *Enrichments* — When creating or editing an enrichment rule, some entity types would not be available in the **Entity type** drop-down menu (*6163*)
- *Entities* — Entity detail pane content is not refreshed correctly to reflect changes to the entity (*5898*)
- *Entities* — In the entity editor, canceling an entity creation operation would redirect to the previously navigated page (*5934*)
- *Entities* — Adding a dynamic dataset to a workspace would prevent dataset entities from being displayed on the **Entities** tab in the workspace (*5947*)
- *Entities* — Deleting an intel dataset would leave orphan entities behind (*5949*)
- *Entities* — Pagination would not work correctly when trying to display more than 10 entities per page (*5890*, *6106*, *6034*)
- *Entities* — The `idref` resolution of nested CybOX observables would not resolve correctly (*6110*)
- *Entities* — It would not be possible to correctly create an exploit target entity (*6221*)
- *Exposure* — The exposure outgoing feed list would not be displayed (*5929*)
- *Feeds* — An incoming feed with HTTP transport type and configured to download PDF content would not correctly download all available PDF files for that feed (*5731*, *5732*)
- *Feeds* — When creating an outgoing feed, the one minute execution schedule option would not be displayed (*5873*)
- *Feeds* — Discovery service URLs in outgoing feeds would be incorrect (*5918*)
- *Feeds* — The default outgoing feed configuration would not have any defined extracts, and the CSV output with one extract per line would be empty (*5986*)
- *Feeds* — Editing a Fox-IT feed would cause the UI to freeze (*6012*)
- *Feeds* — An incoming feed with the Intel 471 transport type would display the incoming feed details only after performing a hard refresh (*6030*)
- *Feeds* — In outgoing feeds, authorized groups with the HTTP transport type would be represented with IDs instead of names (*6031*)
- *Feeds* — Password fields for incoming feeds would not be masked in the corresponding input fields (*6095*)
- *Feeds* — When creating a new incoming feed, it would not be possible to correctly define a TAXII inbox transport type (*6178*, *6180*)
- *Feeds* — Incoming feed creation would not pass schema validation (*6246*)
- *Feeds* — Editing an existing incoming feed would return the following error: `Run Status Failure: Invalid task parameters` (*6268*)
- *Graph* — Removing entities from the graph would throw an error in the web browser console (*6249*)
- *Graph* — Adding entities to the graph would cause the graph to hang without loading correctly (*6261*)

- *Installation* — When performing an RPM installation of the platform, the `gi-storage` directory ownership would be assigned to the `root` user. This would not allow the `eclecticiq` user to write to the directory (*6048*)
- *Logging* — It would not be possible to obtain log information from Kibana (*6234*)
- *Search* — When searching entities by tag, it would not be possible to retrieve any tagged entities (*6144*)
- *System* — Platform login password would not be correctly validated for minimum length requirement (*5917*)
- *System* — The system would automatically log users out after two hours (*5952*)
- *System* — Editing a user name by replacing it with an existing user name would not be correctly validated at UI level (*6050*)
- *System* — It would not be possible to save a TAXII domain in the platform system settings (*6113*, *6114*)
- *Tags* — Deleted tags from the taxonomy and existing entity tags would be represented with their IDs instead of their names (*5897*, *5900*)
- *Tasks* — During a task creation operation, adding entities to it, and then saving it would not retain all the input data (*5979*)
- *UI* — UI headers and other UI strings would overlap or be truncated (*5412*, *5885, *5914*, *5927*, *6121*, *6251*)
- *UI* — Groups and users in the email transport type for outgoing feeds would be displayed as IDs instead of names (*5928*)
- *UI* — Signing back in to the platform after a session expiration would prevent drop-down menu options from being displayed (*5945*)
- *UI* — When trying to delete an entity that cannot be deleted, for example because it has relationships with other objects in the platform, a 404 error would be displayed instead of a more informative error message (*6120*)
- *Upload* — Batch file upload would stall, resulting in a partial upload of only some files in the batch (*5461*)
- *Upload* — After uploading a file with entities, the platform entity count would not be updated correctly (*5403*, *5925*)
- *Upload* — When uploading a file without previously making a selection from the mandatory **Content type** and **Source** drop-down menus, validation for the missing input would not be carried out correctly (*6014*)
- *Upload* — Uploading a nested `idref` package XML would return the following error: `Unhandled rejection Error: Minified exception occurred` (*6126*)
- *Workspaces* — Adding a comment to an archived workspace would not be saved correctly (*5881*)
- *Workspaces* — During a workspace creation operation by the currrently signed in user, the creator would be automatically added as a collaborator, and the workspace creation would not be completed correctly (*5920*)
- *Workspaces* — During a workspace creation operation, drop-down menu filters would not reset correctly after clicking an area outside the drop-down input field (*5922*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 0.14.2 — hotfix

Release 0.14.2 — This EclecticIQ Platform hotfix release addresses specific platform issues.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.14.2
Release date	2016-03-04

Highlights

This EclecticIQ Platform hotfix release addresses one or more specific issues. For further details about the fixes, see What's new and Fixed bugs.

What's new

N/A

Fixed bugs

- When installing the platform from an RPM package, OpenTAXII would not install correctly due to an issue with its dependencies and the **anyconfig** `(https://pypi.python.org/pypi/anyconfig)` API (*6115*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 0.14.1 — hotfix

Release 0.14.1 — This EclecticIQ Platform hotfix release addresses specific platform issues.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.14.1
Release date	2016-03-01

Highlights

This EclecticIQ Platform hotfix release addresses one or more specific issues. For further details about the fixes, see What's new and Fixed bugs.

What's new

- Depending on the size of your database, *reindexing the graph database can take from several hours to a few days*.
  It is a good idea to reindex the graph database in a separate screen session, so that you can monitor the process.

The `graph reindex` command adds and enqueues entities, enrichments, and observables stored in the platform to the graph ingestion queue. Example:

```
$ sudo -u eclecticiq -i EIQ_PLATFORM_SETTINGS=/opt/eclecticiq/etc/eclecticiq/platform_settings.py
/opt/eclecticiq/platform/api/bin/eiq-platform graph reindex -o ${offset_value} -q ${queue_name}
```

Example:

```
$ sudo -u eclecticiq -i EIQ_PLATFORM_SETTINGS=/opt/eclecticiq/etc/eclecticiq/platform_settings.py
/opt/eclecticiq/platform/api/bin/eiq-platform graph reindex -o 0 -q queue:graph:inbound
```

Parameter	Description
`-?`	Shows the built-in help.
`-i ${item_type}`	Ex.: `entity`. Allowed values/Supported types: `entity`, `enrichment`, `extract`. When no item type is specified, the command reindexes all graph items of all supported item types.
`-q ${queue_name}`	Ex.: `queue:graph:inbound`. The queue to reindex and ingest again. If no queue is specified, the default queue for the process is the graph ingestion queue: `queue:graph:inbound`.
`-o ${offset_value}`	Ex.: `-o 10`. Offset value, integer. Default value: `0`. Typically, graph reingestion and reindexing selects all the entities IDs stored in the platform, sorts them in ascending order by `created_at`, and then adds all the IDs to the graph ingestion queue. If an offset value is defined, the process ignores the first *n* entities corresponding to the specified offset.
`-l ${limit_value}`	Ex.: `-l 200`. Capping value, integer. Default value: `100000`. Typically, graph reingestion and reindexing selects all the entities IDs stored in the platform, sorts them in ascending order by `created_at`, and then adds all the IDs to the graph ingestion queue. If a limit value is defined, only the first *n* entities corresponding to the specified limit are processed.

Fixed bugs

- When installing the platform from an RPM package, the *root* user would own the `gi-storage` temporary directory. Therefore, the *eclecticiq* user would not be allowed to access the directory in write mode (*6048*)
- A character escape issue in Neo4j would not allow to correcty ingest entities in CSV format (*6097*)
- When creating an entity, en error would be triggered if the start time is set before 1970, and no end time is defined (*6013*)

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 0.14

Release 0.14 — The release notes for EclecticIQ Platform accompany product releases. They provide last-minute information on new product features, enhancements, bug fixes, deprecated features (when applicable), and known issues. When a workaround exists to mitigate a known issue, it is reported here.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.14
Release date	2016-02-13

Highlights

New features and tools

The new **Exposure** feature, currently available as beta, gives you insight into how effectively you use your intelligence. Ingested entities with no follow-up actions are flagged as exposed. When an entity is exposed, it means that it is not used, for example to implement a course of action, intrusion detection or prevention measures. In this overview, you can review the entities, and then define the appropriate courses of action.

When you add entities to a dataset with **Actions > Add to dataset** in the entity detail pane, the **Filter by workspace** drop-down list enables filtering datasets based on the workspace they belong to.

You can now pre-process large MISP STIX files for ingestion with our command line package splitter utility.

We also introduced basic support for the **CIQ Identity Type** `(https://stixproject.github.io/data-model/1.2/stix-ciqidentity/ciqidentity3.0instancetype/)`.

UI fine-tuning

We applied some fine-tuning to the UI to make it more consistent and intuitive. In the entity detail pane, you can perform more actions on-the-fly, without leaving it. The graph area gained a couple of new features that make it easier to select and load specific entities, and to extract sub-sets on the graph canvas, based on entity or extract type.

Under-the-hood optimization

With this release, we implemented a number of enhancements and improvements in the backend. We improved data loading times from the database and on the graph, and we reduced the ingestion time for large packages. Query rules received a makeover as well, so they are more efficient now.

You can find a detailed overview of the changes included with this release in the following sections.

What's new

New features

Content

- New content types: the platform now supports Intel 471 incoming feeds (*4891*, *4892*)
- You can assess and flag ingested entities based on the **Admiralty System** `(https://en.wikipedia.org/wiki/admiralty_code)` (*5452*)
- Basic support for the **CIQ Identity Type** `(https://stixproject.github.io/data-model/1.2/stix-ciqidentity/ciqidentity3.0instancetype/)` (*4859*)

Functionality

- *Exposure* — The new **Exposure** feature, currently available as beta, gives you insight into how effectively you use your intelligence (*5077*)
- *Discovery* — The discovery service offers a new filter option to view specific entities, based on the selected rule (*4910*)
- *Entities* — In the entity detail pane, the **Actions > Add to dataset** option displays a pop-up dialog where you can filter datasets based on the workspace they belong to by making a selection in the **Filter by workspace** drop-down list (*5414*)
- *Entities* — You can create and view entity source **references** `(https://stixproject.github.io/data-model/1.2/stixcommon/referencestype/)`. They are links pointing back to the entity source to retrieve additional information, when available. In the entity builder, under **References**, a new blank URL input field automatically becomes available as soon as you fill out the default input field and press **ENTER**, or when you click an empty area near the available reference input field(s). In the entity detail pane, the **Reference** section lists the available source references for the entity (*5105*) (*5575)*
- *Entities* — In the entity detail pane, in the **Tasks** section, you can view a list of tasks related to the entity (*5409*)

- *Entities* — In the entity detail pane, on the **Neighborhood** tab, you can examine the entities that are directly related to the selected one, as well as the indirectly related entities, i.e. those related to the selected entity through extracts (*5421*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, you can assign states to entity extracts to flag them as unknown, safe or malicious with low, medium, or high confidence level, and to filter them by extract state (*5377*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, a new **State** column displays sighting indicator flags for the entity extracts. This allows you to quickly spot any entity extract sightings inside your environment (*5411*, *5369*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, you can sort extracts by state to quickly identify the most malicious items (*5367*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, the **Make Sighting** pop-up menu option allows you to create a sighting on the fly from an extract. In this way, you can immediately record information surrounding the sighting of an extract (*5457*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, the **Add to graph** pop-up menu option allows you to add an extract to the graph for further investigation (*5410*)
- *Extracts* — In the entity detail pane, under the **Extracts** section, the **Add to Exclusion List** pop-up menu option allows you to add an unnecessary or irrelevant extract to an exclusion list to reduce data noise (*5358*)
- *Graph* — The new right-click **Load entities** sub-menu allows you to select and load on the graph entities related to the currently selected one (*3953*)
- *Graph* — The new right-click **Load extracts** sub-menu allows you to load on the graph specific extract types related to the currently selected entity (*3952*, *5287*)
- *Incoming feeds* — You can define and set custom headers on incoming HTTP(S) feeds (*5334*)
- *Incoming feeds* — The HTTP transport type for incoming feeds follows redirect links to correctly return the desired target files from the corresponding sources (*5501*)
- *Licensing* — The EclecticIQ Platform now supports licensing and license management (*5371*)

Tools

- Large MISP STIX file splitter: this command line utility allows you to extract the embedded packages included in MISP STIX files, and to ingest them individually. This solves an issue that would occur when ingesting large MISP STIX packages (*5404*)
- The test STIX feeds that are shipped by default with the platform have been improved to make it easier for you to start using the platform right away after installing it (*5316*)

Enhancements

UI

- Signing in with invalid credentials triggers an informative error message to the user (*5594*)
- Newly created entities without a name are assigned a default one: *Unnamed* + *entity_type* (*5435*)
- When you change and then save the platform proxy settings, an alert message is displayed to notify that you need to restart all processes (*5679*)

Backend

- Ingestion performance optimization (*5538*)
- Graph ingestion improvement (*5243*)
- Improved domain extraction (*4183*)
- The Oracle JDK third-party product has been upgraded to version 8u72 (*5602*)

What's changed

Deprecated features

- In the entity editor, the **Pin to workspace** checkbox has been replaced by the **Add to dataset** checkbox. When you select the checkbox, a drop-down list allows you to choose one or more datasets you want to add the entity to (*5119*)
- The **Run now** button on the **Delivery** tab in the entity detail pane for outgoing feeds has been removed. You can find and execute this command in the entity detail pane, on the **Task logs** tab (*5364*)

Fixed bugs

Fixed a number of bugs and issues. Highlights:

- The **Status** column in the extract table in the entity detail pane has been renamed to **State** (*5456*)
- When editing exposure settings for an entity, the form overview would not update correctly after saving the changes (*5550*)
- When saving a graph, it is no longer necessary to enter a description (*5197*)
- After saving a graph, filters would be reset instead of storing the selections (*4833*)
- When creating an outgoing feed using the EclecticIQ CSV content type, an error would occur and the outgoing feed creation would fail (*5254*)
- When creating an outgoing feed, the feed content would not be created upon executing **Run now** on the **Task logs** tab in the detail pane (*4707*)
- When editing the ThreatGRID enricher to remove data from the input fields, an error would occur, and it would not be possible to amend the field content (*5083*)
- The incoming feed log tab content would not be refreshed accordingly when selecting a different incoming feed for display (*5413*, *5458*)
- PDF email attachments ingested through incoming feeds with an IMAP email fetcher transport type would not be added as entities (*5126*)
- Autodiscovery would not support SSL parameters like certificate, key and password (*5401*)

- When creating or editing an entity in the entity builder, it would not be possible to successfully save tags that are not included in the taxonomy (*5304*)
- When creating an entity in the entity builder, it would not be saved correctly (*5599*)
- It would not be possible to add a relationship to an existing or to a new entity (*5406*)
- Changing the user profile photo would occasionally trigger an error (*4029*)
- In Cabby, some TAXII incoming feeds would fail when no user name/password credentials are configured (*5423*)

Known issues

- At the moment, EclecticIQ Platform supports Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Last generated on Mar 6, 2018

EclecticIQ Platform release notes 0.13

Release 0.13 — The release notes for EclecticIQ Platform provide last-minute information on new product features, enhancements, bug fixes, deprecated features (when applicable), and known issues. When a workaround exists to mitigate a known issue, it is reported here.

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.13
Release date	2015-01-24

Highlights

We applied a few changes to the EclecticIQ Platform UI to address, among other things, a few UI-related bugs. Far from just putting some lipstick on the UI, we focused on improving usability, while keeping the changes visually subtle and non-disruptive.

Among the new features available with this release, we added ThreatGrid support as a feed and as an enricher, and we made sure the platform correctly ingests FS-ISAC, Fox-IT, and MISP STIX feeds.

In the entity editor, you can add any supported entity as a relationship, and you can attach documents to report entities, as well as download them.

You can find a detailed overview of the changes included with this release in the following sections.

What's new

New features

Entity editor

- It is possible to create associations among entities by establishing relationships (*4922*).
- In the entity builder, it is now possible to attach a document to a report (*4697*).
- If a report entity has attached documents, they can be downloaded and saved locally (*4698*).

Feeds

- Support for ThreatGrid feeds (*3388*).
- Support for FS-ISAC STIX/TAXII feed (*4864*).
- Support for `cybox:Related_Objects` in feed ingestion to establish relationships among CybOX objects (*3891*).

Functionality

- Support for **SELinux** `(http://selinuxproject.org/)` (*5192*, *4342*)

Enhancements

UI

- The entity detail pane was redesigned to improve usability (*4977*).

Functionality

- Large package ingestion is faster (*5424*).

Tooling

- A utility is available to split the embedded STIX packages in MISP XML files into separate XML files: `split-misp-stix-packages` (*5404*).
- **Cabby v. 1.0.9** `(http://cabby.readthedocs.org/)` released.
- **Cabby** `(http://cabby.readthedocs.org/)` is available as an RPM package (*4454*, *4456*)
- **OpenTAXII** `(http://opentaxii.readthedocs.org/)` is available as an RPM package (*4457*)

What's changed

Fixed bugs

Fixed a number of bugs and issues. Highlights:

- Creating a new outgoing feed with a dataset containing a report entity with an attachment would not result in generating the new content (*5112*).
- Incoming TAXII feeds created with an earlier platform version than release 0.13 would not work after upgrading the platform (*5203*).
- Fox-IT package timestamps would impact duplication detection (*5430*).
- When editing entities to add characteristics, some characteristics would not be correctly saved, and therefore they would not be available upon reopening the same entity to edit it at a later moment (*5109*).
- In the entity builder, it would not be possible to successfully create an indicator (*4979*).
- In the entity builder, it would not be possible to successfully create a report (*5061*).
- In the entity builder, it would not be possible to successfully create a campaign (*5253*, *5310*)

- When creating a sighting in the entity builder, it would not be possible to successfully create relationships using the relationship drop-down menu list (*5273*).
- In the entity detail pane, *Overview* tab, under *Title* > *Description*, `idref` entities providing no usable information would be displayed (*4604*).
- The *Intents* field in reports created with the entity builder would not be rendered correctly (*5059*).
- After uploading a PDF file, a report would not be generated (*5265*).
- Entities created with the *Threat Analyst* user role would not be visible in the platform (*4690*).
- When creating a new group, the *Source* and *TLP* fields would not be correctly validated to verify they contain valid input (*5088*).
- When clicking the user profile image to select the *Help* menu option, the action would not produce any result (*5065*).
- Clicking *Read More* on a long workspace description would not toggle the description area to display the entire text content (*5009*).
- In Cabby, some incoming TAXII feeds would fail when no user name/login information is configured (*5423*).

Deprecated features

N/A

Known issues

- Shared entity links can be accessed by any user in any group (*4157*).
- At the moment, the EclecticIQ Platform supports only Google Chrome as a web browser. If you use a different browser, platform behavior may produce unexpected results.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

EclecticIQ Platform release notes 0.12.4

Release 0.12.4 — The release notes for EclecticIQ Platform accompany product releases. They provide last-minute information on new product features, enhancements, bug fixes, deprecated features (when applicable), and any known issues. When a workaround exists to mitigate a known issue, it is reported here.

These release notes apply to the following product:

EclecticIQ Platform	
Release version	0.12.4
Release date	2015-11-26

Product overview

EclecticIQ Platform is powered by **STIX** `(https://stixproject.github.io/)` and **TAXII** `(http://taxiiproject.github.io/about/)` open standards.
It enables ingesting, consolidating, analyzing, integrating, and collaborating on intelligence from multiple sources.

EclecticIQ Platform	**Key features**
Feed management	Manage multiple cyber threat intelligence feeds from any source, in many different formats.
Enrichment	Enrich existing intelligence with external data sources, and refine it with de-duplication and pattern recognition.
Sharing	Investigate and identify threats together with partners as part of an information ecosystem.
Collaboration	Analyze and create intelligence in collaboration with other teams and departments.
Insights	Generate insight thanks to a high-fidelity, normalized view into your intelligence.
Integration	Understand how cyber intelligence relates to and how it can affect your organization and your environment.

What’s new

New features

- The platform is now available also as an RPM package. (*4458*)

- Besides CentOS, RPM packages now support also Red Hat Enterprise Linux 7.1. (*4725*)
- OpenTAXII is now available as an RPM package, with all relevant dependencies. (*4457*)
- New entity builder item to create incidents. (*1774*)
- New enricher: support for ThreatGrid feeds. (*2404*)
- New tab: Neighborhood to quickly inspect the context around an entity. (*2193*)
- New page: Entity detail. (*4701*)
- Add any supported entities as relationships to a newly created entity in the entity editor. (*4507*)
- Export to CSV feature to export selected listings from a search result table to CSV format. (*2409*)
- Report Entity attachments can be downloaded. (*4698*)
- Quick preview of attached documents before downloading them. (*4699*)
- Log configuration management for system administrators. (*2382*)

Enhancements

- Upgrade to Neo4j 2.3.1. (*4616*)
- Upgrade to Keylines 2.11. (*4355*)
- Updated *Getting started guide* built into the platform. (—)
- UI enhancements to improve consistency and usability. (—)
- Unused services are disabled. (*4344*)
- Improved memory usage by Redis. (*4341*)

What's changed

Fixed bugs

Fixed a number of bugs and issues. Highlights:

- Fixed: Action menu would not display after changing task status. (*4525*)
- Fixed: validation in Edit Entity Half Life field. (*3728*)
- Fixed: updated entity alias would still show the old alias value after changing it. (*3958*)
- Fixed: upon opening the Discovery overview, it would not refresh correctly to display new results. (*4008*)
- Fixed: incident entity types would not be saved in a graph. (*4181*)
- Fixed: upon opening the Outgoing feeds Content tab, it would not update its content. (*4324*)
- Fixed: in the Overview tab, newly added files would be displayed only after refreshing the page. (*4359*)

- Fixed: adding an observable to an entity would cause data loss upon pressing ENTER. (*4377*)
- Fixed: in the entity detail view, it would not be possible to edit the TLP value. (*4434*)
- Fixed: after adding a new user to a group, all the data entered in the input fields would be lost. (*4439*)
- Fixed: uploading a large PDF file (file size > 10 MB) would fail (*4446*)
- Fixed: after changing a static dataset to be dynamic, it would not be possible to revert it back to static. (*4656*)
- Fixed: referenced entities would not be displayed in the Tasks detail pane. (*3998*)

Deprecated features

N/A

Known issues

- Shared entity links can be accessed by any user in any group (*4157*)
- Content is not created in outgoing feeds (*4707*)
- Right-clicking on the graph canvas shows both the platform and the web browser context menus (Safari, Firefox) (*3203*)
  - *Workaround*: use Google Chrome as a web browser.
- User is signed out automatically when they right-click an area on the graph (Safari) (*4014*)
  - *Workaround*: use Google Chrome as a web browser.

Contact

For any questions about the content of this document or to request assistance, you can contact EclecticIQ at the following email address: support@eclecticiq.com

The Support Team

Cannot GET /_release-notes/Release%20notes%20splunk.html