eclectic iq

EclecticIQ Platform release notes

Product release notes and information

Last generated: March 06, 2018

Table of contents

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