



# EclecticIQ Platform release notes

## Product release notes and information

Last generated: May 26, 2017



©2017 EclecticIQ

All rights reserved. No part of this document may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without written permission from the author, except in the case of a reviewer, who may quote brief passages embodied in critical articles or in a review.

Trademarked names appear throughout this book. Rather than use a trademark symbol with every occurrence of a trademarked name, names are used in an editorial fashion, with no intention of infringement of the respective owner's trademark.

The information in this book is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

©2017 by EclecticIQ BV. All rights reserved.  
Last generated on May 26, 2017

Table of contents

Table of contents	2
EclecticiQ Platform release notes 1.14.2	3
Highlights	3
Upgrade to the latest release	3
What's new	3
What's changed	4
Enhancements	4
Fixed bugs	5
Known issues	6
Contact	6

# 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:

<b>EclecticIQ Platform</b>	
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.

## 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](mailto:support@eclecticiq.com)

 The Support Team