Heureka

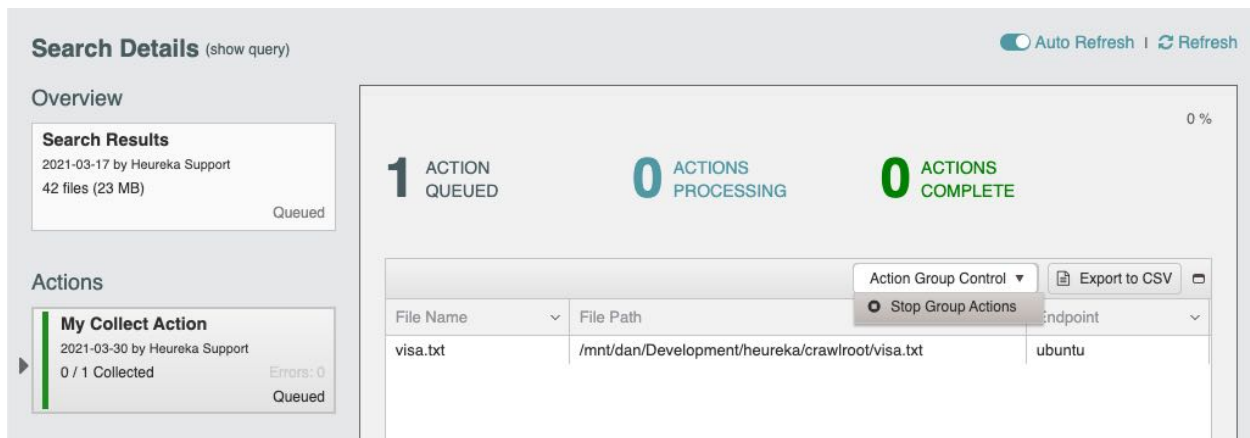Version 2021.2 Release Notes

April, 2021

CONTENTS

Enhancements

Prune Deleted Files From Index

When the endpoint indexes files and notices that a file that was previously present is no longer there, it marks the file as deleted in the index. Deleted files can be included in searches from the web interface. Prior to this update, deleted files remained in the index forever. This will cause the index to grow over time, especially if volatile filesystems are included in the crawl path.

This enhancement will remove deleted files from the index after a configurable number of days. The default is to keep deleted files for 30 days.

Cancel Collect

Prior to this update, there was no easy way to cancel a collect action. This enhancement allows a collect action to be canceled from the search interface.
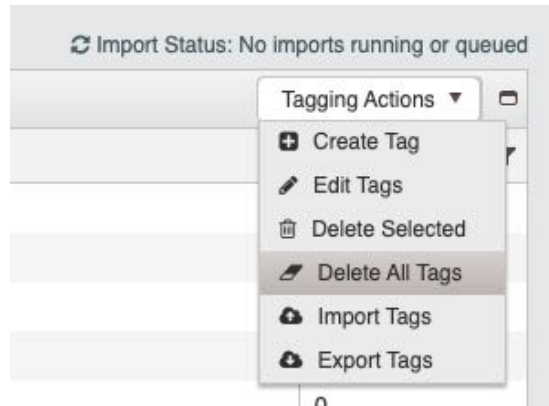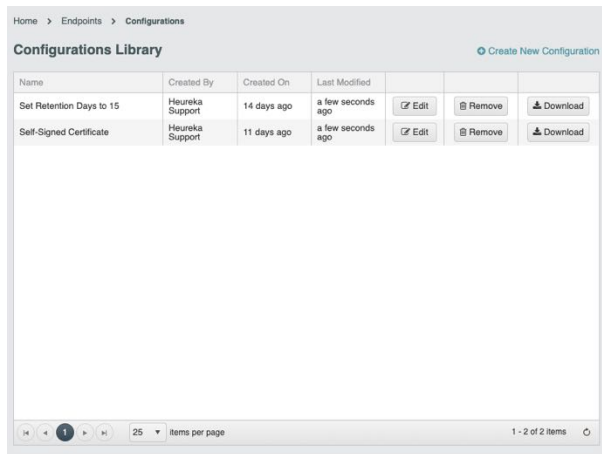

Delete All User Defined Tags

There are times in which a user may want to remove all User Defined Tags and start over. On the tagging interface, there is now an option to delete all tags. We recommend that users export their tags before deletion just in case they ever want to put them back.

Agent Configuration Management

To facilitate centralized management of endpoints, there is a new feature which allows snippets of configuration parameters to be saved and then pushed to endpoints. This eliminates the need to manually change the endpoint configuration files manually. In addition to configuration, certificates can be sent to endpoints as well. This enables customers the ability to rotate their certificates.

Once defined, these templates can be applied to one or more endpoints.

Bug Fixes & Improvements

macOS Big Sur and Apple Silicon Support

In order to support the new Apple M1 processor found in Macintosh computers, Apple made substantial changes to the operating system starting with macOS Big Sur. These changes required updates to be made to the Heureka endpoint software to support both Big Sur and the Apple M1 architecture.

Apple Installer Notarization

Apple now requires that all software installers, even ones not distributed by the App Store, to be notarized by Apple. The macOS installer is now notarized, which means it was submitted to Apple to be scanned for malicious content and code-signing issues, so customers know it is safe and trustworthy.

Agent Configuration Log Level

Some of the libraries on the endpoint software was not properly recognizing the logging level property in the agent configuration. This fix ensures the endpoint software is logging at the requested levels.

Integrations

H5 Classification Engine

H5 is a software product that specializes in classifying file content. Some of our customers use Heureka to do the initial indexing and classification, submit the files to H5 for further classification, export the resultant tags from H5, and then import them into Heureka. To facilitate a more streamlined process, Heureka has collaborated with H5 to provide a means for Heureka endpoints to use H5 classifiers directly. This means that H5 tagging can be natural result of Heureka's indexing and classification.

Heureka

Heureka is a technical leader in endpoint search, identify and classification software. Our goal is to bring order to unstructured data by identifying risk while helping you realize the value of unstructured data across all endpoints.