Heureka

Version 2022.1 Release Notes

February, 2022

☀ Heureka

CONTENTS

Bug Fixes & Improvements

This release has focused on automation and stability improvements.
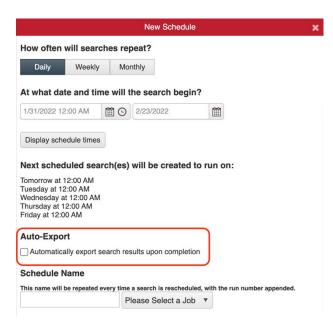
Dynamic Date Range Search

There is a new option for searching that allows you to specify dynamic date ranges instead of having to use specific dates. For example, you can search for all documents with a document date between five years ago and six months ago.

This will make scheduled searches for date ranges much more useful in finding data that, for example, violates data retention policies.

Auto-Export Search Results

There is a new option on scheduled searches to automatically export search results to a CSV when the search is complete.

The exported results are stored on the same secure FTP server used to download collected files. This will make it easier to automate importing search results from Heureka into other workflows.

Delete Scheduled Searches

Before this release, you could only deactivate a scheduled search. Now you can delete the searches you no longer need to clean up the search list.

Bug Fixes & Improvements (Continued)

Re-Expand Search Criteria for Scheduled Searches

To explain this feature, let's talk about how searches work prior to this release using an example. You create a new scheduled search that uses the endpoint group called "Workstations". The Workstations endpoint group contains endpoints A and B. The first scheduled search will expand the Workstations group into the A and B endpoints. Now let's say you edit the Workstations endpoint group to remove A and add C. All subsequent scheduled searches will continue to search A and B because we did not re-expand the endpoint group. We just reused the original definition of the Workstations endpoint group.

With this new feature, all the criteria groups (such as the endpoint groups) are re-expanded for each subsequent scheduled search. This means that, given the previous example, subsequent searches would search endpoints B and C.

Settable Search Timeout

Have more control over when long-running searches time out. When searching an endpoint group that contains an endpoint that never comes online, an endpoint will continue to stay in the "Queued" state for ten days until the system marks the unreachable endpoint as "Suspended". This can make it difficult to know when a search is truly complete.

There is now a new setting where you can set how long to wait before suspending an unresponsive endpoint during a search operation.

Tagging Data on Collect Load Files

We have added tagging data to the load files generated during collection. The default format is JSON, but if a specific export target is selected (Relativity, Logikcull, Etc.) we try to format the tag data to match what that export target expects. For example:

JSON: `{ "TAG1" : "Value 1", "TAG2" : "Value 2" }`

Relativity: `TAG1;TAG2`

Bug Fixes & Improvements (Continued)

Relativity Tagging Support on Search Export

Tag data exported from the search result screen in CSV format will contain tags formatted to match a target format, such as Relativity. You can set the export target format on the settings screen.

Search Export Tag Format ⊘

Column format when exporting Search Results to CSV:

Relativity ▾

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.