

Heureka

Version 2022.4 Release Notes

November 2022



CONTENTS

- Enhancements 1**
 - Daily Risk Summary Report 1
 - Automated Search Alert 1
- Bug Fixes & Improvements..... 2**
 - Recollect Failed Files* 2
 - Custom Index Extraction Size*..... 2
 - Search Schedule Options*..... 3
 - Security and Stability* 3
- Other Notable Changes 4**
 - License Validation*..... 4

Enhancements

Daily Risk Summary Report

It would be good to know when an endpoint's risk score is a concern without having to log into the interface every day to check. This is why the new Daily Risk Summary Report was created. When enabled, Heureka examines the total risk scores of all the endpoints daily. If any endpoints exceed the threshold for minimum acceptable risk, an email will be sent to all active company admin accounts with the list of violations. If no endpoints exceed the threshold, then an email is not sent.

Please see the Daily Risk Summary Report section on the System Configuration page to enable/disable the report and/or set the risk threshold.



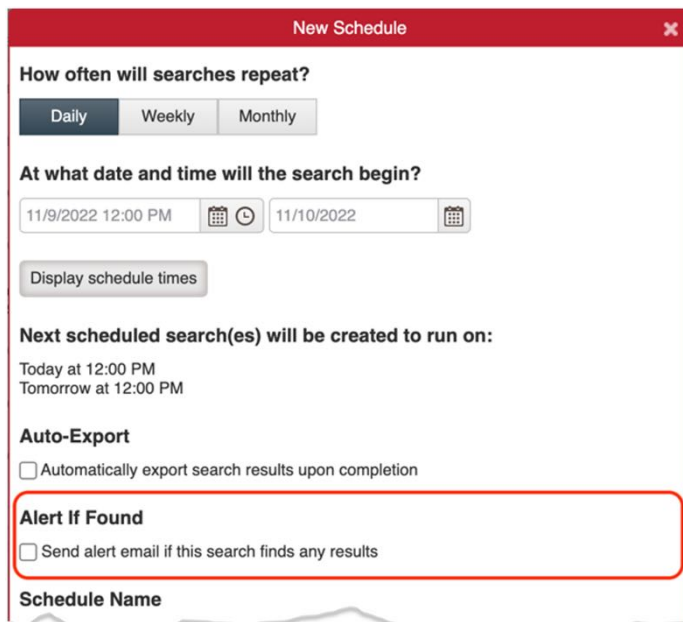
Daily Risk Summary Report ⓘ

Enable Report

Risk score threshold

1,000

Automated Search Alert



New Schedule [X]

How often will searches repeat?

Daily Weekly Monthly

At what date and time will the search begin?

11/9/2022 12:00 PM [Calendar] [Clock] 11/10/2022 [Calendar]

Display schedule times

Next scheduled search(es) will be created to run on:

Today at 12:00 PM
Tomorrow at 12:00 PM

Auto-Export

Automatically export search results upon completion

Alert If Found

Send alert email if this search finds any results

Schedule Name

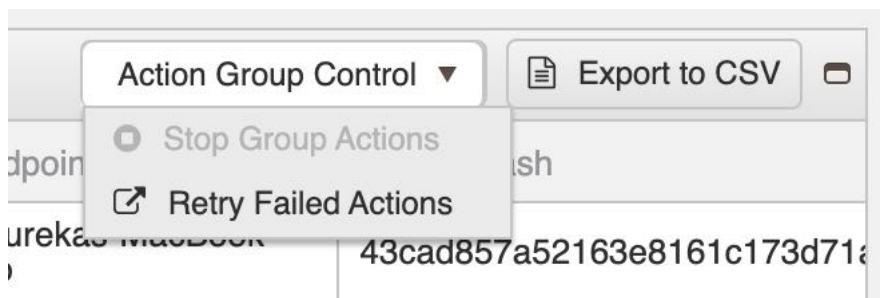
A common use of the automated search functionality is to search for things that should not be present on endpoints. There is a new option on scheduled searches to send an alert email to all company admin accounts when a search finds any matching files. This option can be enabled or disabled at any time in the Search Schedules grid. Please see the section **Search Schedule Options** in this document for more details.

Bug Fixes & Improvements

Recollect Failed Files

Sometimes when there are large collect actions, some of the endpoints have file collects that fail for various reasons, such as network timeouts. In the past, retrying these failed actions was a tedious task of finding the file you want to retry in the search results and creating a new collect action. Heureka has added a new feature to the collect result interface to aid in this.

If the collect action is complete but has failures, a new option in the Action Group Control dropdown will allow you to create a new collect action with the same options as the failed action that only includes the failed files.



Custom Index Extraction Size

During indexing, Heureka endpoints attempt to extract the full text of a file to enable keyword searching and content classification. Previously, this extraction was limited to the file's first 8,388,608 bytes (8 MiB). Given that the average file size today is less than 512k, not a lot of space is typically needed to store extracted text in the index.

However, in circumstances where customers are indexing vast quantities of large files, the index Heureka creates can get rather large. Furthermore, if the data customers need to classify a file is typically found at the beginning of a file, then extracting up to 8 MiB of text may be wasteful. In those circumstances, reducing the amount of extracted text may be desirable.

Lastly, there are some circumstances where customers do not want keyword searching or Heureka classification of files. In those circumstances, the limit can be set to zero to enable metadata-only indexing and searching.

A new configuration variable has been added to the endpoint config to enable smaller text extraction sizes. Adding the following to your agent.config file allows you to control the extraction size to a value between 0 and 8388608.

```
endpoint.max.text.extraction.size=<number of bytes>
```

Search Schedule Options

The Scheduled Search options for Auto-Export and Alert if Found are now easily enabled and disabled via the Search Schedules Grid.

Search Schedules + New Schedule							
Name	Next / Last Search	Starts on	Ends	Job	Start Time	Auto Export	Alert If Found
Alert Test	Last: 2 months ago	Fri Aug 26 2022	Wed Aug 31 2022	Heureka Test	12:00 pm	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Schedule Test	Last: 7 months ago	Wed Mar 02 2022	Thu Mar 31 2022	Heureka Test	09:00 am	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BWP Schedule Daily	Last: 5 years ago	Thu Sep 21 2017	Sat Sep 23 2017	Schedule System	10:00 am	<input type="checkbox"/>	<input type="checkbox"/>

Security and Stability

This release also contains various security and stability improvements.



Other Notable Changes

License Validation

For customers who use a Heureka Appliance on-premises, you may notice this new version of the Heureka Appliance trying to connect to <https://license.cloud.heurekasoftware.com> periodically. This call just transmits your license information to Heureka for validation. In the interest of data transparency, the following data is shared with Heureka for this operation:

- The hostname of the appliance
- The total active endpoint count
- The total active index size
- The license key in use

This information is needed to evaluate license key activations. This data is private and will not be shared with anyone outside of Heureka. Please contact us if you have any concerns.



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.

Heureka, Inc
PH. 800.310.0981
info@heureka.com