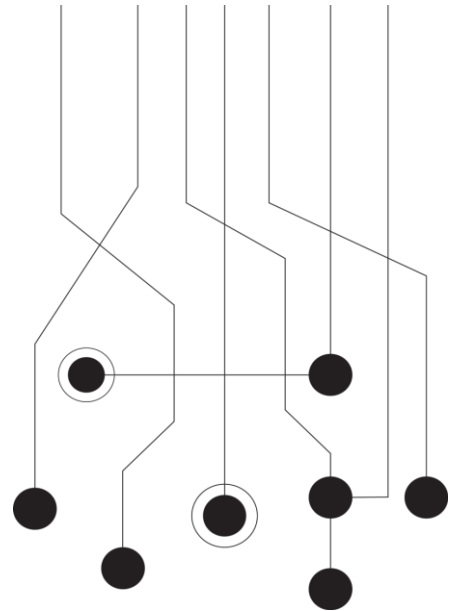




---

HEUREKA INTELLIGENCE PLATFORM



## Heureka Interrogate® Software Version 2.5

Rev. April 2016

The Crittenden Building  
1382 W 9th Street, Suite 400  
Cleveland, OH 44114 PH: 216.241.3443  
Email: [info@heurekasoftware.com](mailto:info@heurekasoftware.com)

# Table of Contents

Version 2.5 .....	3
Risk Dashboard.....	3
Using the Risk Dashboard .....	3
Current Risk.....	3
Last 30 Days (Historical) .....	3
Risk by Type.....	4
Endpoint View .....	4
Create Search from Selected Endpoints .....	4
Jobs View.....	4
Maximize/Minimize sidebar .....	4
Job List.....	5
Endpoint Status.....	5
Offline Status.....	5
Initial Crawl .....	5
Saved Searches List .....	5
Saved Search Overview.....	5
Breadcrumb Navigation .....	5
Search Name Information.....	6
Top 10 File Types Discovered.....	6
Search Criteria View .....	6
Search Criteria Overview .....	6
Search Criteria Area .....	6
Search Details Summary Overview .....	6
Search Details Summary .....	7
Login.....	7
Log Out.....	7
Configuration .....	7
Endpoint Info .....	7
User Management .....	8
My Information .....	9
Creating New Job .....	9
Interrogate Search .....	9
Running a Search.....	10
Search Details Summary .....	10
Status .....	10

Criteria.....	11
Results.....	11
Collect .....	12
Collect Files .....	12
Collected File Information.....	12
Reports.....	13

## Version 2.5

Welcome to **Interrogate**, your gateway to the Heureka Intelligence Platform. Interrogate allows you to search endpoint computers for content by using keywords, file names, hash values and patterns such as social security and credit cards. Once identified you can interactively analyze results, create reports or collect files to specific locations.

Interrogate automatically tracks sensitive data such as PII and keeps a running 30 day history for you on the Risk Dashboard.

## Risk Dashboard

The risk dashboard displays both current and historic risks based on the overall amount of PII data discovered on each endpoint. Risk is automatically updated each day when the endpoint completes a reindex of information.

### Using the Risk Dashboard

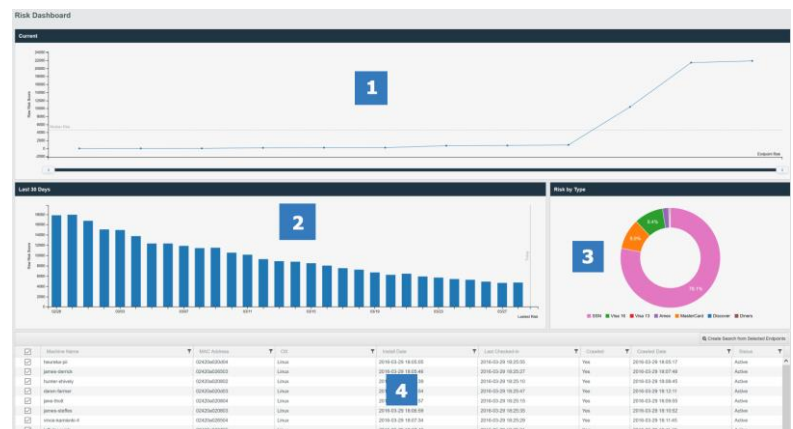
#### Current Risk

The **current risk** grid displays the most recent risk for each endpoint. The numbers at the far left (Y-Axis) show the **Raw Risk Score**. The raw risk score is a sum of all files that have associated PII information contained within.

If you hover your cursor over an endpoint node you will see the current risk score. You will also see a **slider** at the bottom of the current risk grid. Dragging the handles will allow you to change focus and interactively turn endpoints on/off in the lower endpoint view grid. This function gives you the ability to zoom directly to endpoints of interest whereby you can then create a detailed search for the endpoint.

#### Last 30 Days (Historical)

Interrogate keeps a running history of total risk across a 30 day time period. This at-a-glance chart displays historical risk and makes it easier for you to get a sense of where the organization is in terms of PII compliance.



## Risk by Type

Interrogate breaks down risk by card type and social security. As you hover over the areas of the donut chart, you will see the percentage of card types and social security numbers. The percentage display represents the **current** risk.

## Endpoint View

The bottom grid represents all of the endpoint services available to the system. You will note that there is a checkbox on the right side of each endpoint service. The endpoint view grid is **interactive** with the risk by type and current risk grid. In other words, as you select or deselect endpoints, the current and risk by type charts will interactively update themselves to display the information for the selected endpoints.

### Create Search from Selected Endpoints

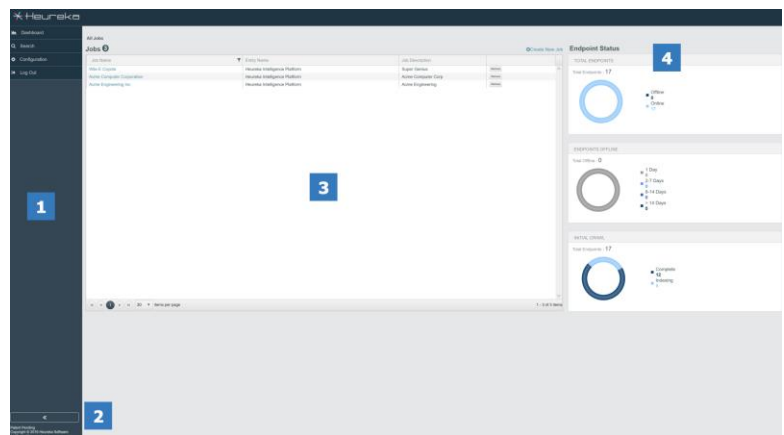
If you have selected specific endpoints and would like to run a search for file-level patterns, you may click on the **create search from selected endpoints** button in the upper right corner. You will be asked to select which job you would like the search to be placed in and then directed to the Search Criteria page. If you only want to see the patterns auto-detected by Interrogate, simply click the **search** and create a name.

## Auto-Group

Interrogate automatically creates an endpoint group for you when using the create search from selected endpoints function. Your group name will be called "Dashboard Search <Date/Time>".

## Jobs View

- 1 - Log Out and Configuration Area
- 2 - Maximize/Minimize sidebar
- 3 - Job Listing View and Description
- 4 - Endpoint Status Area



The **Job List** page shows a listing of all your Interrogate jobs, allows you to create new jobs (with proper credentials) and displays endpoint information.

See [Creating a Job](#) for information on how to create jobs

### Log Out and Configuration Area

This left navigation pane allows you to access the dashboard, search, configuration and log-out functions.

### Maximize/Minimize sidebar

Clicking the arrow will minimize the side navigation area to maximize your screen space.

## Job List

The job list shows you all accessible jobs currently available. Selecting the name of the job will direct you to the Search List. Selecting "Remove" will remove/hide the job from your view. In the current version of Interrogate the job is NOT deleted from the master database. It simply hides the Job from your view and thus makes it inaccessible. **NOTE:** Since jobs are not deleted from the database, it is not possible to duplicate job names. If you select a duplicate job name, you will see a pop-up message telling you that the job already exists in the database. Simply select a new name for your job or amend your job name with a "\_2" or the date.

## Endpoint Status

The job list shows you the status of your endpoints from a high level. **Total Endpoints** displays the current number of endpoints along with the online/offline status. **Endpoints Offline** displays the amount of time that endpoint agents have been offline.

## Offline Status

It is completely normal for agents to be offline. For example, if an employee is on vacation or traveling their desktop or laptop may be turned off or in sleep mode. Interrogate keeps track of this and will begin to show the amount of days an endpoint has been offline. As agents begin to cross the 8-14 day threshold you may want to check in on the computer in question to verify whether the endpoint should or should not be communicating with Interrogate.

## Initial Crawl

Upon installation, the initial crawl and index of the system will begin. During this process the endpoint will show as "indexing" and once finished change to "complete".

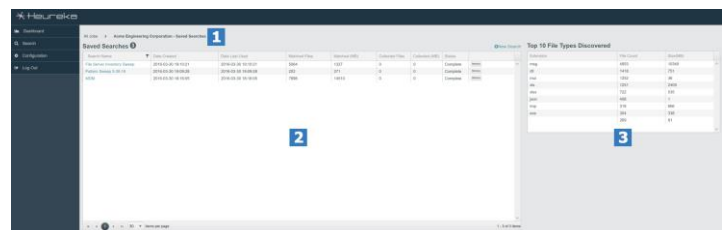
### *Initial Crawl*

*Before you execute a search, an endpoint must have completed the initial crawl or you will receive incomplete search results.*

## Saved Searches List

### Saved Search Overview

1. Breadcrumb navigation
2. Search name information area
3. Top 10 File Types Discovered (summary for all searches)



## Breadcrumb Navigation

The breadcrumb navigation bar allows you to quickly move backward to your search or job. Simply click the desired hyperlink to return to the required page.

## Search Name Information

Your saved searches are listed in the saved search grid. To view the search details simply click on the saved search name. Other information is available in the grid including the date created, matched file count and size in megabytes as well as a collected file count and size in megabytes. Click the "New Search" to create a search.

Clicking "Remove" from a search will remove the search from view. The current version of Interrogate does not delete the search from the database, rather hides the search from view. If you attempt to reuse the exact same name, you will be prompted by the system to create a different search.

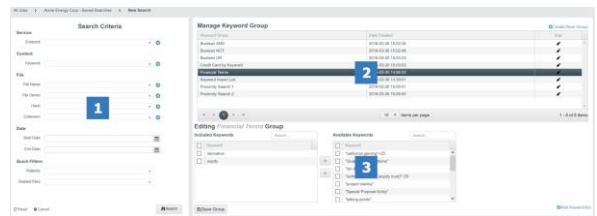
## Top 10 File Types Discovered

The top 10 grid gives you a quick summary display of all of your searches combined together.

## Search Criteria View

### Search Criteria Overview

- 1 - Search Criteria Area
- 2 - Manage Group Area
- 3 - Group Edit area showing available and included areas



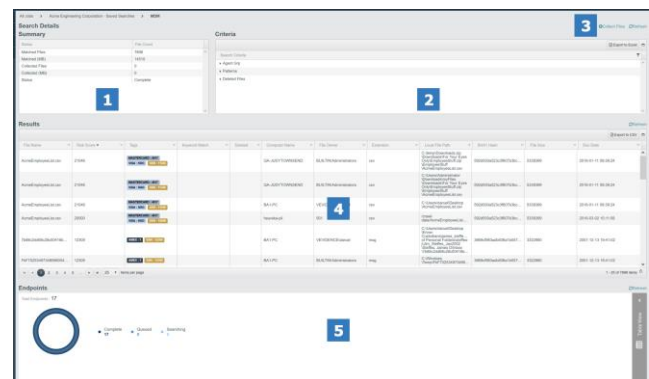
### Search Criteria Area

The search criteria area is the location by which you select options for your search. Search options have been broken down into the following categories:

1. Service - Area in which to select your endpoints for searching
2. Content - Area in which to select keywords
3. File - Area in which to select file name, owner, hash and extension groups
4. Date - Area in which to choose a start and end date for narrowing the scope of the search
5. Quick Filters - Filter to return only the selected types (patterns or deleted files)

## Search Details Summary Overview

- 1 - Search Status Area
- 2 - Search Criteria Area
- 3 - Collect File Area
- 4 - Search Results Grid
- 5 - Endpoint status (Chart View)



## Search Details Summary

The **search details summary** page displays the status, original search criteria, file results and requested endpoints. Please see [Search Detail Summary](#) for more information and proper use.

## Login

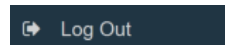
1. Log into Interrogate by entering email address password.
2. Click the red arrow or press <enter> on your keyboard.

If you have **forgotten your password**, you may reset it by clicking on the "Forgot Password?" button at the bottom of your login screen. An email will be generated allowing you to reset your password.



### Passwords

Passwords will be provided by your system administrator or service provider.



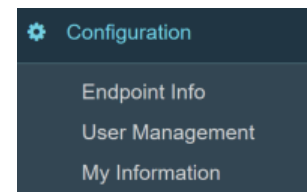
## Log Out

Once you are logged into the system, you may **log out** at any time by clicking on "Log Out" button on the left navigation pane.

## Configuration

Interrogate has three configuration screens.

- **Endpoint Info** window gives you an overall view of all your endpoints.
- **User Management** allows you to create, delete and manage users and user permissions within the system.
- **My Information** allows you to quickly update your user name, email address as well as resetting of passwords.



## Endpoint Info

The **Endpoint Info** screen shows you a complete listing of all the configured endpoint computers. This window gives a complete at-a-glance view of machine name, MAC Address, Operating System, Endpoint Service installation date, Last Check-In, Crawl status and Crawl Date as well as an overall status.

Endpoint Info is an excellent way to check in on the health of an endpoint. For example, you can easily see the last time your endpoint checked in Interrogate. This will show you if any endpoint has dropped offline or simply does not currently have a network connection.

Additionally, you can see how fresh your endpoint index is by checking out the last Crawled Date.

You may delete an endpoint from your system by using the "delete" button at the far end of the column.

ID	Machine Name	OS	Install Date	Last Checksum	Created Date	Status	MAC Address	
1	BA1-PC	Windows 7	2016-03-29 15:08:52	2016-03-29 11:45:03	2016-03-17 16:46:05	Active	1017746A776	X Delete
2	Lamp-MySQL-Plo	Mac OS X	2016-03-29 15:08:52	2016-03-29 13:30:51	2016-03-29 16:02:02	Active	26022489654	X Delete
3	DA-NMPRELECTOR	Windows 7	2016-03-29 15:10:01	2016-03-29 13:30:29	2016-03-29 16:06:10	Active	03036877966	X Delete
4	DA-JEDYTORINEND	Windows 7	2016-03-29 15:10:02	2016-03-29 13:30:54	2016-03-29 16:06:28	Active	03036878919	X Delete
5	Wm-MySQL-Plo	Mac OS X	2016-03-29 15:10:06	2016-03-29 13:30:48	2016-03-29 16:06:47	Active	03036878673	X Delete
6	perma-jenkins	Linux	2016-03-29 15:10:22	2016-03-29 17:35:05	2016-03-29 12:00:00	Active	02424020363	X Delete
7	hacker-ubuntu	Linux	2016-03-29 15:10:22	2016-03-29 17:35:45	2016-03-29 12:00:00	Active	02424020252	X Delete
8	perma-jenkins	Linux	2016-03-29 15:10:26	2016-03-29 17:35:12	2016-03-29 12:00:00	Active	02424020692	X Delete
9	perma-put	Linux	2016-03-29 15:10:40	2016-03-29 17:35:43	2016-03-29 12:00:01	Active	02424020039	X Delete
10	heureka-plo	Linux	2016-03-29 15:10:42	2016-03-29 17:35:30	2016-03-29 12:00:01	Active	02424020478	X Delete
11	perma-ubuntu	Linux	2016-03-29 15:10:44	2016-03-29 17:35:54	2016-03-29 12:00:00	Active	02424020304	X Delete
12	perma-ubuntu-4	Linux	2016-03-29 15:11:10	2016-03-29 17:35:58	2016-03-29 12:00:00	Active	02424020298	X Delete

## Endpoint Deletion

Caution should be taken when deleting endpoints as it is difficult to re-enable!

## User Management

The **User Management** windows enables creation or modification of users and permissions.

Steps to Create a new user:

1. Select "Entity" from the drop-down list at the top of the page. (Most deployed systems will only display a single entity.)
2. Select "New User"
3. From the "New User" Window, select a job(s) that the new user will have access to.
4. Type in First Name, Last Name and valid Email Address
5. Select either "Auto Generate Password" for an auto generated password OR select "Enter The Password" and type a password into the password field.
6. **OPTION 1** - Select "Company Administrator" to give the user full access to all jobs/searches in the system.
7. **OPTION 2** - If you do not assign the new user company administrator privileges, you may individually select permissions from the permissions area. Assignments are listed below:

- Job Administrator - Administrator access to all permissions associate to a Job
- Collection - Ability to collect files identified by a search
- Manage Keywords - Ability to select and modify keyword groups
- Manage File Owners- Ability to select and modify file owner groups
- Mange Extension - Ability to select and modify extension groups
- Manage Endpoint - Ability to select and modify endpoint groups
- Manage File Name - Ability to select and modify file name groups
- Manage Hash Group - Ability to select and modify hash groups
- Manage Application - Ability to select and modify application groups

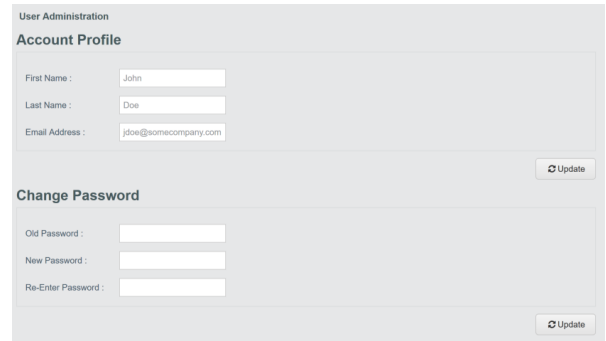
8. Select Save to save your new user or "Cancel" to cancel setup



## My Information

**My Information** allows you to view and change your name, email address and password.

Select and edit your desired field to change. Once finished, select the "Update" button to update your information.



The screenshot shows two sections of a user administration interface. The top section, titled "Account Profile", contains three input fields: "First Name" with the value "John", "Last Name" with the value "Doe", and "Email Address" with the value "jdoe@somecompany.com". An "Update" button is located to the right of these fields. The bottom section, titled "Change Password", contains three input fields: "Old Password", "New Password", and "Re-Enter Password". An "Update" button is located to the right of these fields.

Passwords must be at least 8 characters long and contain at least 3 numbers

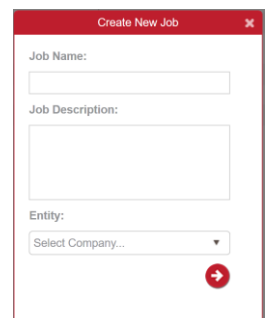
## Creating New Job

You may create a new job by selecting **Create New Job** displayed on the top right of your job list grid.

Once selected, you can enter a **job name**, a brief **job description** and then select the system **entity**. For most installations there will only be a single entity selection, however if Interrogate has been configured to accept multiple entities, you may see more than one choice available.

Click the arrow button or **Enter** on your keyboard.

A new job will automatically be created and you will see an empty search grid.



The screenshot shows a "Create New Job" dialog box. It has a red title bar with the text "Create New Job" and a close button. The dialog contains three input fields: "Job Name", "Job Description", and "Entity". The "Entity" field is a dropdown menu with the text "Select Company...". A red arrow button is located at the bottom right of the dialog.

## Interrogate Search

Once a job has been created your next step is to **create a search**. This is accomplished by clicking on the **New Search** icon at the top right of the Saved Search grid.



You will be directed to the Search Criteria page where you can input specific criteria for your search

## Running a Search

1. Select/create/modify any or all of the groups required to complete your search. See [Search Criteria](#) for detailed information
2. If filtering on dates, select your **start/end dates**.
3. Select any **quick filter** to view patterns or deleted-only files
4. Select **Search** and input your save search criteria name and hit **<Enter>**

Once your search is saved, you will be returned to the **Saved Search** list view. Your newly created search will show up at the top of the list with a **Queued** status showing in the status column.

The **Reset** button will clear all of your groups

The **Cancel** button returns you to the main saved search view

**Search Criteria**

**Service**  
Endpoint:

**Content**  
Keyword:

**File**  
File Name:   
File Owner:   
Hash:   
Extension:

**Date**  
Start Date:   
End Date:

**Quick Filters**  
Patterns:   
Deleted Files:

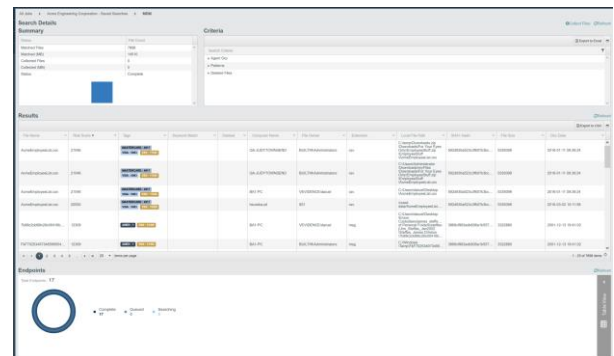
**Criteria Name**

Enter the criteria name :

## Search Details Summary

The **Search Detail Summary** page gives you complete details on a selected search. You will see the status of your search including the matched files and collected files along with the search criteria, file-level results along with details of each endpoint requested.

Details of each grid area are listed below.



## Status

Once a search is executed, you will be able to view the status of a search in the upper left corner of the search details summary. Using the **refresh** button located throughout the interface will refresh the results of the page as files are brought back to the **results** grid. The status grid contains the following elements:

Status	File Count
Matched Files	7898
Matched (MB)	14510
Collected Files	0
Collected (MB)	0
Status	Complete

- Matched Files - Displays total file count of executed search
- Matched (MB) - Displays total megabyte size of executed search
- Collected Files - Displays total collected file count of executed search\*
- Collected (MB) - Displays total collected megabyte size of executed search
- Status - Consists of three states: **Queued**, **Searching**, **Complete**
- Queued indicates that endpoints are currently waiting to pickup a command to search
- Searching indicates that endpoints are actively searching and returning results

- Complete indicates that all endpoints have completed their searches

## Criteria

The criteria by which a search was executed is displayed in the criteria area. Click on the arrows to expand the fields for a more complete view. If you would like to export your results to a spreadsheet, simply click the **Export to Excel** in the upper right corner of the grid.



If you would like to maximize your grid to the entire screen, simply click on the **expansion/contraction button** to the right of the export button. Your grid will now maximize to the entire screen. To return to the original size and position click on the button again.

## Results

The results grid displays file-level information from your search. It includes the following fields:

- File Name - File name as shown on the endpoint including the file extension
- Risk Score - The sum of all credit cards and social security numbers identified in a specific file
- Keyword Match - If using keywords Interrogate will display a snippet of text along with the first word highlighted in yellow
- Deleted - If a file has been deleted from the endpoint, a deleted flag will be displayed
- Computer Name - The name of the endpoint computer
- File Owner - File owner is automatically identified by the Interrogate endpoint service when indexing files
- Extension - A file's extension (a file is NOT required to have an extension)
- Local File Path - The path to the local file on the endpoint
- SHA1 Hash - A file's hash value. Hash values are automatically calculated by the endpoint service during indexing
- File Size - The file's size in megabytes
- Doc Date - Document dates displayed are as follows:

Document Type	Display Date
Email	Date Sent or Date Last Modified
File (Loose File) 1st Method	Date Last Modified
File (Loose File) 2nd Method	Date Created
File (Loose File) 3rd Method	Field Left Empty

## Collect

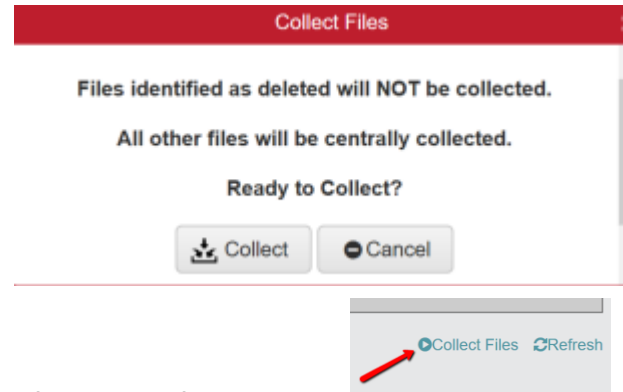
Interrogate allows you to collect files identified in a search. To gain access to your downloaded files via FTP, we recommend a tool such as [Filezilla](#).

### Collect Files

The **Collect Files** button can be found on your Search Details Summary page in the upper right corner.

Collected files will be **copied** to a file or preservation share set up by your system administrator.

1. Once a search is complete, click "Collect Files" on the Search Details Window
2. Select "Collect" in the file pop-up message.



The "Status" of your search will return to "Queued" as the collection request is sent to the endpoints. When the collection process begins, the status will change to "Collecting". Once complete, you should see a status of "Complete". Use the "Refresh" button to refresh the status of your collection.

### Collected File Information

Files will keep their original file path and will appear in the collected folder in the following manner:

*Interrogate Job Name > Interrogate Search Name > Interrogate Machine Name\_Endpoint ID > Endpoint File path*

*Example:*

Using Interrogate, I create a Job called Acme Energy with a search called HR Department. The HR Department consists of three employees (Judy Townsend, Pat Lewis, Patricia Turner). When I execute my search (Employee Record Search) I find documents on all three employee's laptops that I want to collect. When I click on the "Collect Files" button my collection will look like the following:

Acme Energy > Employee Record Search > Judy Townsend\_126 > C > ...

### Collected Files

This version does **NOT** collect files in containers such as ZIP, PST or OST. If you need to collect these files, create a search for the specific file name search in Interrogate and collect separately.

### Search Details Summary Collected File Count

Because this version of Interrogate does NOT collect files in containers, it is possible that the Matched Files count will be different from the Collected Files count. You can use Interrogate's Local File Path filter on the Search Details page to see how many files reside in containers such as ZIP, PST, OST.

## Deleted Files

Files identified as deleted will not be collected as they no longer exist on the endpoint.

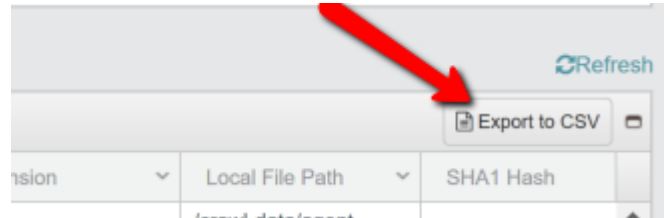
You will be provided an **FTP link** which will act as your collection location. Please see your network administrator or contact Heureka support for more information.

Status	File Count
Matched Files	33
Matched (MB)	13
Collected Files	29
Collected (MB)	12
Status	Complete

## Reports

Many of the grids within Interrogate can be exported. The search results grid is exported as a flat-file CSV. All other grids will be exported to Excel.

To export your report, simply click on the "Export to" button in the upper right corner of your grid.



## Grid Report

Large search result grids will take time to export to CSV. When the system is creating a grid you may notice the "Export to" button change to a spinning icon.

To export grids showing in "Chart View", simply click on the "Table View" to slide your grid details into table mode. Once in table mode you will see the "Export to Excel" option in the upper right corner of the grid.

## Legal Notice

This documentation (“**Documentation**”) and the software to which it relates (“**Software**”) belongs to Heureka and/or Heureka’s third party software vendors. Heureka grants written license agreements which contain restrictions. All parties accessing the Documentation or Software must: respect proprietary rights of Heureka and third parties; comply with your organization’s license agreement, including but not limited to license restrictions on use, copying, modifications, reverse engineering, and derivative products; and refrain from any misuse or misappropriation of this Documentation or Software in whole or in part. The Software and Documentation is protected by the Copyright Act of 1976, as amended, and the Software code is protected by the State of Ohio Trade Secrets Act. Violations can involve substantial civil liabilities, exemplary damages, and criminal penalties, including fines and possible imprisonment.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. HEUREKA, LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

©2016. Heureka Software, LLC. All rights reserved.