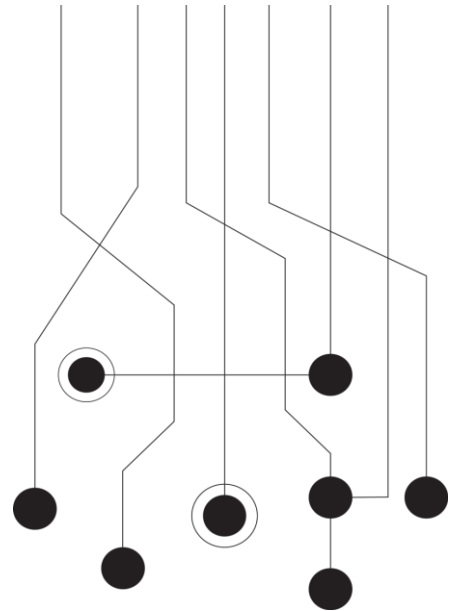




HEUREKA INTELLIGENCE PLATFORM



Heureka Interrogate® Software Update Version 2.6

Rev. May, 2016

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

Table of Contents

| | |
|------------------------------------|---|
| Version 2.6 | 3 |
| Getting Started..... | 3 |
| Configuration | 3 |
| Endpoint Info | 4 |
| User Management | 4 |
| My Information | 5 |
| Creating a new job | 5 |
| Interrogate Search | 5 |
| Running a search..... | 6 |
| Creating and running a search..... | 6 |

Version 2.6

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.

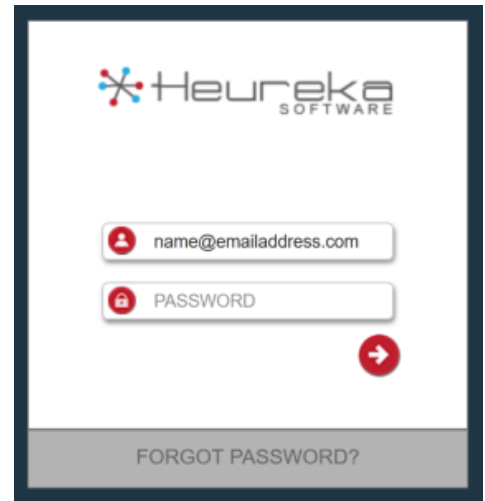
Interrogate automatically tracks sensitive data such as PII and keeps a running 30 day history for you on the Risk Dashboard.

Getting Started

Login

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

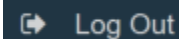
If you have **forgotten your password**, you may reset it by clicking on the "Forgot Password?" button at the bottom of your login screen. An email will be generated allowing you to reset your password.



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

Log Out

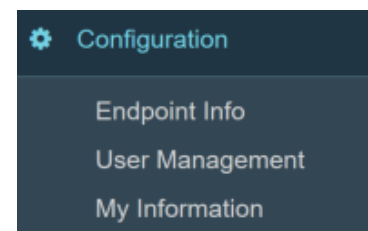
Once you are logged into the system, you may **log out** at any time by clicking on "Log Out" button on the left navigation pane.

A dark blue rectangular button with a white right-pointing arrow icon and the text "Log Out" in white.

Configuration

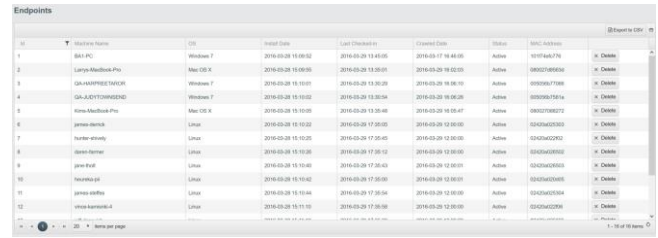
Interrogate has three configuration screens.

- **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.



| ID | Machine Name | OS | Install Date | Last Check-In | Crawl Date | Status | MAC Address |
|----|-------------------|-----------|---------------------|---------------------|---------------------|--------|-------------|
| 1 | Bill PC | Windows 7 | 2016-03-28 16:00:02 | 2016-03-28 13:44:00 | 2016-03-17 16:46:00 | Active | 9419766A776 |
| 2 | Laura@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 02:00:00 | Active | 0402306680 |
| 3 | GA-ADP01021540C6 | Windows 7 | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:30:00 | Active | 00096A78564 |
| 4 | GA-ADP01021540C6 | Windows 7 | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:30:00 | Active | 00096A78564 |
| 5 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 00007F88712 |
| 6 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 7 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 8 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 9 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 10 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 11 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |
| 12 | John@MacBook-Pro | Mac OS X | 2016-03-28 16:00:00 | 2016-03-28 13:00:00 | 2016-03-28 16:00:00 | Active | 0402306680 |

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.

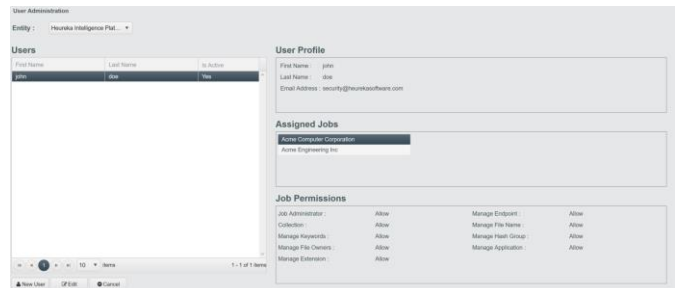
You may delete an endpoint from your system by using the "delete" button at the far end of the column.

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:



| First Name | Last Name | is Active |
|------------|-----------|-----------|
| John | Doe | Yes |

User Profile

First Name: john
Last Name: doe
Email Address: security@heurekasoftware.com

Assigned Jobs

Acme Computer Corporation

Job Permissions

| | | | |
|--------------------|-------|--------------------|-------|
| Job Administrator | Allow | Manage Endpoint | Allow |
| Collection | Allow | Manage File Name | Allow |
| Manage Keywords | Allow | Manage Hash Group | Allow |
| Manage File Owners | Allow | Manage Application | Allow |
| Manage Extension | Allow | | |

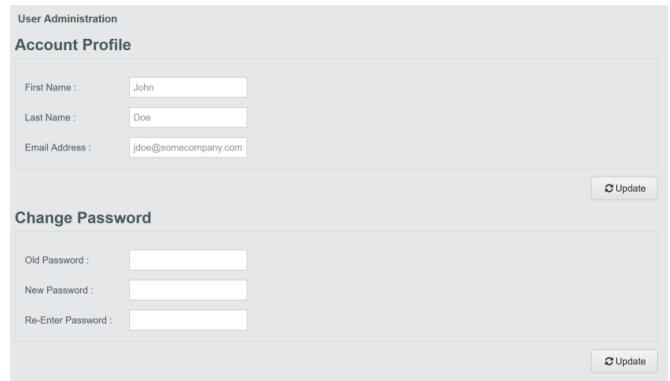
- Job Administrator - Administrator access to all permissions associate to a Job
- Collection - Ability to collect files identified by a search
- Manage Keywords - Ability to select and modify keyword groups
- Manage File Owners- Ability to select and modify file owner groups
- Mange Extension - Ability 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

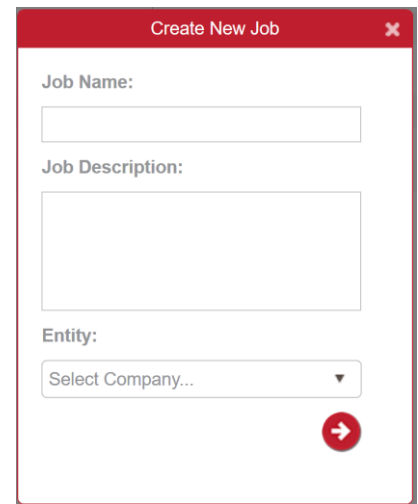
Creating a new job

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 with a red header and a close button (X). It contains three main sections: "Job Name:" with a text input field; "Job Description:" with a larger text area; and "Entity:" with a dropdown menu showing "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

Creating and 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

The image shows two parts of the user interface. The top part is the 'Search Criteria' form, which is organized into several sections: 'Service' (Endpoint), 'Content' (Keyword), 'File' (File Name, File Owner, Hash, Extension), 'Date' (Start Date, End Date), and 'Quick Filters' (Patterns, Deleted Files). Each field has a dropdown menu and a gear icon for configuration. At the bottom of the form are 'Reset' and 'Cancel' buttons, and a 'Search' button with a magnifying glass icon. The bottom part of the image shows a modal dialog box with a red header 'Criteria Name' and a close button. It contains a text input field with the placeholder 'Enter the criteria name :', a red arrow button, and a red close button.

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:

- 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 |

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.