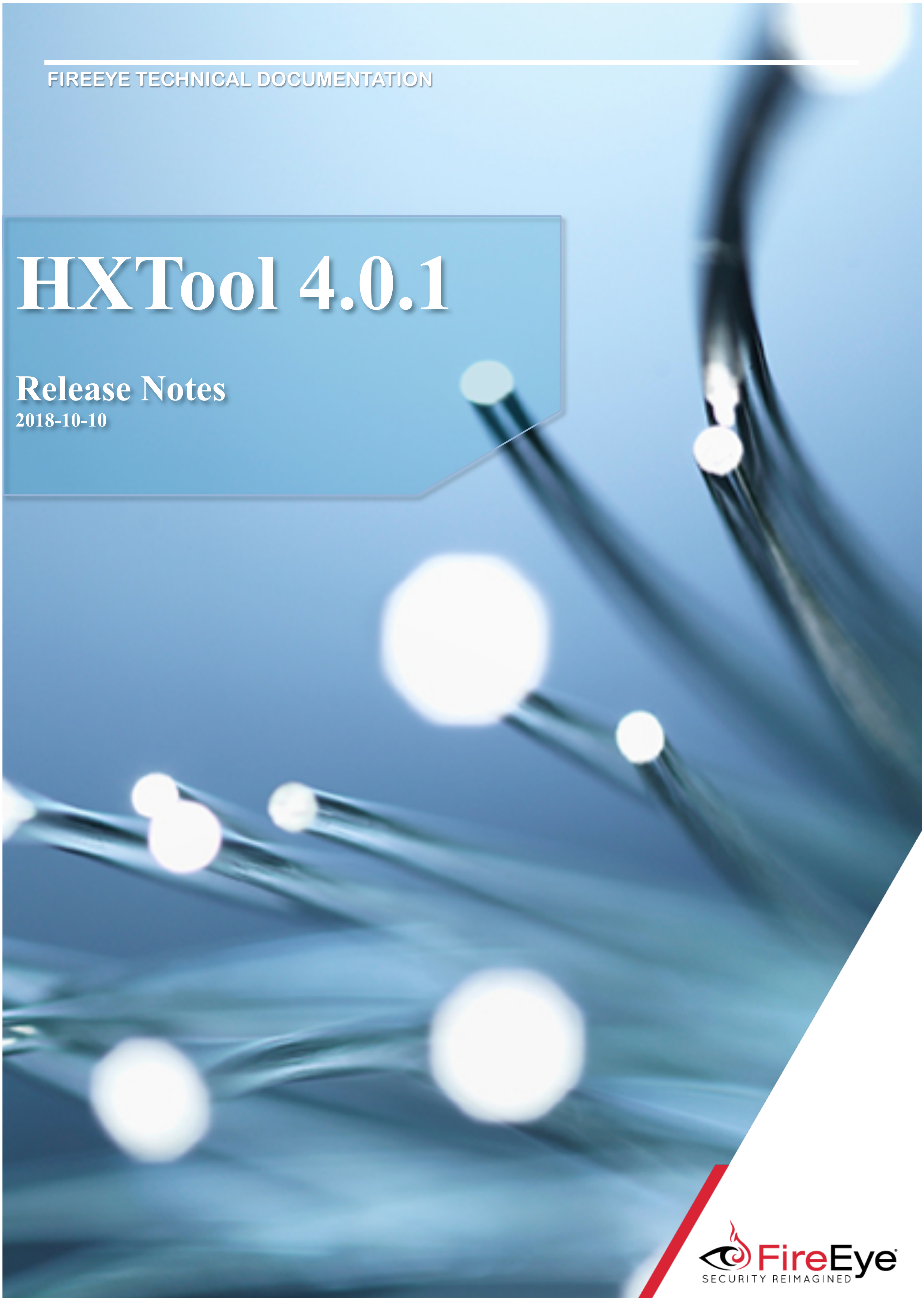

FIREEYE TECHNICAL DOCUMENTATION

HXTool 4.0.1

Release Notes

2018-10-10

HXTool 4.0.1 – Release notes

NEW FEATURES

- Acquisition scripts can now have timestamp macros. Example: --#{-30m}-- would be current timestamp minus 30mins and --#{now}-- would be the current timestamp
- If you are running HX 4.5.1 you can now give your Enterprise Searches a name

BUGFIXES

- Fixed an issue where the requests library would complain about unverified connection before background processing credentials was set
- Fixed a bug where Enterprise search would not work on HX 4.5.1 or newer
- Added a limit to the number of alerts shown on the alerts page to prevent long loading times where there are many alerts on the controller
- Added a limit to the max number of alerts shown in the alert investigation panel to prevent long loading times

KNOWN LIMITATIONS

- Some features greatly depend on the number of alerts/acquisitions or other type of data contained in your FireEye endpoint controller. We have limited means of testing with very large configurations so certain panels or tables might take a while to load. The reason behind this is that we need to poll certain data from the endpoint API which depends on resources, hardware specification where you run HXTool and network performance.
- Data stacking does currently not have any limitations of the number of rows that can be returned. Very large data stacking jobs can potentially return too much data causing long load times and high memory use in your web browser
- Scheduler is multi-threaded and the number of threads can be controlled in the configuration file. When using the feature bulk acquisition with task-processor profiles each thread can allocate up to 800Mb of memory usage. Make sure you have enough memory in your system to accommodate each thread.
- With the addition of task processors HXTool can now potentially use much more system resources than earlier versions due to the fact that we are ingesting and processing each acquisition result. If this feature is heavily used we recommend running HXTool on a dedicated server