



PERFORCE

Perforce Helix Threat Detection

Release Notes

Release Notes

What's New

What's New for Version 3.0.0

Changes since version 2.2.0

- Support for endpoint (sensor) data, to provide analytic insight into anomalous behaviour on end-user workstations
 - **Note:** This is a separate installation than the Perforce offering
- Support for Red Hat Enterprise Linux 6
- Configurable handling of 'bot' accounts, to override the built-in bot-detection
- Improved user experience, including a more detailed view into user behaviour through the improvement of risk stories, including baseline information where applicable.
- Many performance improvements
- Full support for multiple character encodings
- Improvements to the installation experience and runtime management, including unified service startup, and an easily configurable OVA setup
- Flexible heuristics for project identification from filenames
- Improved API documentation

What's New for Version 2.2.3

Changes since version 2.2.2

- Support for Perforce CSV-formatted logs
- Improved aggregation for working hours & days
- Improved default analytics tuning
- Improved risk story scoring
- Added support for overriding bot classifier (not-bot)
- Enhanced configuration support for project heuristics
- Improved scalability, stability, diagnostics, and performance
- Fixed: Files were being set as projects by Connector in some cases
- Other bug fixes

Known Issues

Connector: Compressed Files Fail On Import

The Perforce branded connector is not designed to use any type of compressed files as a source. Logs must be in an uncompressed format for importing.

Connector: Disk Space Usage On Machine Running Connector

When the log files are being uploaded, there are activities run that will cause the amount of disk space that is needed on the machine being used by the connector to increase significantly. To prevent issues related to out of disk errors, please ensure that there is a significant amount of free disk on the partition running the operating system.

For example, if the connector is installed on the C:\ drive of a machine running Windows, there will need to be as much free disk as there are logs to upload on the C:\ drive to accommodate the operations run during the upload.

Connector: Time Required For Log Upload Completion

As with any network dependent activity, there are many factors that will affect the time needed to upload logs via the connector. As a guideline, a reasonable expectation for uploading and processing 1 months worth of logs would be anywhere from 2-4 days.

This could be affected by network latency, speed of upload and the speed of the machine processing and sending via the connector.

API (Swagger): 401 Unauthorized

Invalid bearer token in the "Authorization" header.

API (Swagger): 405 Method Not Allowed

The HTTP method is invalid, e.g. if you tried to add a user with POST you would get a 405 response because the HTTP verb should be PUT.