



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight Interactive Discovery**

Software Version: 6.4.2

Release Notes

August 11, 2015

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 2015 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

This software is based in part on the work of the Independent JPEG Group.

## Support

### Contact Information

|                              |                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Phone</b>                 | A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: <a href="https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list</a> |
| <b>Support Web Site</b>      | <a href="https://softwaresupport.hpe.com">https://softwaresupport.hpe.com</a>                                                                                                                                                                                         |
| <b>Protect 724 Community</b> | <a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>                                                                                                                                                                                           |

# Contents

- What's New ..... 4
  - In Version 6.4.2 ..... 4
  - In Previous Versions ..... 4
  
- System Requirements ..... 7
  
- Resolved Issues ..... 8
  
- Known Issues ..... 9
  
- Send Documentation Feedback .....10

# What's New

## In Version 6.4.2

Version 6.4.2 of the ArcSight Interactive Discovery project contains the following new features:

- **Logger 6.0 and 6.1:** AID includes support for ArcSight Logger versions 6.0 and 6.1. Logger Search and Export method to .csv by both the UI and API are limited to 1 million rows each.
- **AID\_Schema:** The AID\_Schema contains sample fields suitable for use with your projects.
- **Active Channels:** Active Channels that match the filters used in each focused report. Use Active Channels to preview events and event counts that would be processed in a report. It is suggested that you only run reports of less than 1 million rows.

For a complete description of the tabs in the projects, see the ArcSight Interactive Discovery Project Guide.

ArcSight Interactive Discovery product changes are described in the What's New topic of the online help. Select Help > Topics > What's New.

## In Previous Versions

Version 6.4.2 includes updates from previous versions, described here.

### Version 6.3

- **Look and Feel:** Building on the changes in 6.0, 6.3 includes continuation of the "thinner" look, removal of 3D shading on bars (can be turned back on if desired), new default color scales, removal of plot points on lines, etc.
- **Running Accumulation:** New 6.3 feature for line chart and summary sheet. Dynamic accumulation of a measure across time. Will recalculate based on selections and exclusions
- **Bar and Line Measures:** Ability to put measures on bars and lines for presentation and chart export. Can be turned on and off.
- **Currency Symbols:** Expanded, and set by the data vs. the local operating system. Interface similar to Excel.
- **Maps:** Access to a variety of regional, country, state, and metroarea maps and geocodes.
- **Null or missing values:** Now by default are represented by the string "-" rather than "<null>".
- **Data Sheet default color as black.**

- **Information Builders Data Connector:** Direct URL data connection to IBI WebFocus has been added.
- **Localization improvements:** English and Japanese translations available simultaneously at launch. Text exported from grid charts may be imported directly into Microsoft Excel in locales using UTF8 character sets. Titles in PDFs exported from ADVIZOR Analyst now correctly represent characters in multibyte languages.

### Version 5.9

- **Capacity Improvements:** A number of improvements have been made to our in-memory storage capability in order to accommodate larger amounts of data.
- **Other Updates:** Approximately 20 existing defects have been fixed.

### Version 5.8

Key features and enhancements in version 5.8 include:

- **Microsoft Excel and Access data loading (both 32 and 64 bit versions) on both 32 and 64 bit ADVIZOR products:** Previously we only loaded 32 bit versions of Excel and Access and only with our 32 bit products
- **Navigation Panes available on ADVIZOR Server:** Navigation panes, which provide project page level help context, description, and navigation have only been available on our client software prior to this release. With 5.8 ADVIZOR Server displays navigation panes in sliding browser panels. Content for Server navigation panes should be inserted as RTF.
- **The Project Explorer has been completed.** The older Data Workshop has been removed.
- **Scatterplot trendline equations added:** The parameters of the equation for the scatterplot linear trend line(s) are displayed in the Property Grid, as is the correlation coefficient (r2).
- **3D charts are anti-aliased:** for better quality
- **Flight Recorder enhancements:** The Flight Recorder now creates constraints for Maps, Goal Lines, Data Constellations, and searches in the Data/Summary Sheet
- **Other Updates:** This release includes a variety of other updates and performance improvements, including fixing some stability issues that cropped up in 5.7 priced service that is not part of our support and maintenance program.

### Version 5.7

- **Improved Start-up Experience:** The Task View has been rewritten and updated, additional help has been added, and the quick start capability has been updated to make the start-up and new project build experience easier and more intuitive.
- **New Regression Algorithms in Analyst/X:** We have updated the predictive modeling algorithms in the Analyst/X product with a more robust version. There is no operational change. In addition, the modeling license key has been updated for an extended time period. If you are running prior versions including 5.6 (other than 5.6.2, which began shipping in August, 2010), you will need to upgrade to 5.7 before April 23, 2011 or else the modeling will cease functioning on that date.

- **Updates to the Map Chart:** The wizard for configuring the Map chart has been improved. You can now edit the configuration of an existing map chart (previously all configuration information had to be re-entered). The wizard has been re-organized. We also now include geocodes for US City and State, Canadian Cities, and Countries in the Map Chart.
- **Ratio Weights in the Summary Sheet:** Summary Sheets now support "ratio" as a weight. This enables "weighted averages" as a metric. Performance of large Summary Sheets on startup has also been dramatically improved
- **New Project Workshop (beta):** A beta version of a new "Project Workshop" is included. This will ultimately replace the Data Workshop as the user interface to define how data is managed in ADVIZOR Analyst. Since it is a new feature that requires more feedback, the existing Data Workshop is still available; it will be removed in a future release.
- **Flight Recorder:** The export - import capability has been temporarily disabled until we can complete its development. This is the top priority for our next release, in addition to bringing this capability to ADVIZOR Server.
- **Other Updates:** This release includes a variety of other updates and performance improvements.

# System Requirements

For supported AID installation platforms and minimum system specifications for installation and running the software, see the *Advizor Implementation Guide*, available in the AID download package.

For details on the supported versions of ESM or Logger, consult the HPE ArcSight ESM Product Support Matrix, or the HPE ArcSight Logger Support Matrix, available from the HPE support community, [Protect724](#).

## Resolved Issues

This version of AID resolves the following issues:

- Re-writing a string field with a changed expression could cause a field to be corrupted.
- Clearing the Datasheet SortBy property would not update the display.
- Clearing the Summary Sheet SortBy property would not clear the column sorting.
- A color link that cannot be created is no longer removed from the project.
- In some cases, Expression Builder: match() would crash when comparing string to result of || operator.
- In some circumstances, there could be a crash on reload.
- Advizor no longer fails with an exception on save with un-configured charts.
- Project crashes after selection in Data Sheet with particular state.
- The Analyst could hog CPU for 5-10 seconds on a chart resize with Project Workshop open.
- Flight recorder playback would not go to the same state for this sample.
- In some cases, a drill down on hierarchy on a bar chart with measure labels could mangle the display of labels.
- A filter would reflect undo but not redo.
- Summary Sheet will now keep unselected items in previous order after selection.
- Deleting tables in a project color model is now simpler and less confusing.
- In some cases, the expression builder would add in a \$-character.
- Warnings about links that can't be created now supports removing the links.
- Expression Builder date calculation now works for all rows, not just the first non-null row.
- Rollup with calculated key field no longer adds NULL first row.
- Expression including lower() will now correctly handle NULLs correctly: evaluation stops.
- Temporary files will no longer be left behind when writing .advm output file.



# Known Issues

This version of AID includes the following known issues.

- **AID-20, AID-42:** When reports in ArcSight ESM export data as a CSV file, commas, line feed characters and double quotes (") within the data are not always handled properly. This can cause the data to show up incorrectly in ArcSight Interactive Discovery. When possible, ensure that event data fields do not contain values that include commas or line feed characters.
- **AID-12:** The error message dialog includes an email link to send email to HPE ArcSight Support. This email link should not be used. Instead, to inform Support about an error, open a ticket in the Support Portal, and include this ticket number in any email sent to Support.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Release Notes (Interactive Discovery 6.4.2)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arc-doc@hpe.com](mailto:arc-doc@hpe.com).

We appreciate your feedback!