

# **ArcSight Interactive Discovery Release Notes**

---

Version 5.6

April 2012



## ArcSight Interactive Discovery Project Guide Version 5.6

Copyright © 2012 Hewlett-Packard Development Company, LP. All rights reserved.

Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

<http://www.arcsight.com/copyrightnotice>

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

This document is confidential.

### Revision History

Date	Product Version	Description
04/10/12	AID 5.6	Final Version for AID 5.6

### ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	<a href="http://www.support.openview.hp.com">http://www.support.openview.hp.com</a>
Protect 724 Community	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

# Contents

---

**ArcSight Interactive Discovery**

**Version 5.6** ..... 5

    Extracting the Zip Archive ..... 5

    System Requirements ..... 5

    What's New? ..... 6

    Installing ArcSight Interactive Discovery ..... 6

    Known Issue ..... 7

---

# ArcSight Interactive Discovery

## Version 5.6

---

These release notes describe how to extract the ArcSight Interactive Discovery zip file and where to find information relevant to getting started.

### Extracting the Zip Archive

Download the file ArcSightAID-5.6.zip from the HP Software Support Online site where you got these release notes (<http://support.openview.hp.com>).

If your ESM Manager has many events to correlate, ArcSight will also have many events to analyze. For best results, extract and install the ArcSight Interactive Discovery product on a different machine than the one running the ESM Manager.

The zip file contains three components:

- ArcSight Interactive Discovery product installer files and folders.
- The ArcSight Interactive Discovery Project Guide, in the OEM folder.
- The [AID\\_Content.zip](#) file, also in the OEM folder. This zip file contains:
  - ◆ An ESM package file with an ARB extension.
  - ◆ Full and Partial project files with an ADV extension.
  - ◆ Full and Partial CSV data files and INI files that go with them.

All of the zip file contents are extracted to a folder called [ArcSightAID-5.6](#).


### System Requirements

ArcSight Interactive Discovery can only be installed on Windows operating systems. The following minimum requirements are recommended for optimum performance:

System	Requirement
Operating System (Supported on the en-us Locale)	<ul style="list-style-type: none"><li>• Microsoft Windows XP SP1</li><li>• Microsoft Windows Vista 32 or 64</li><li>• Microsoft Windows 7 32 or 64</li><li>• Microsoft Windows Server 2003 SP1</li><li>• Windows Server 2008.</li></ul>
Browser	Internet Explorer 7 or 8

System	Requirement
Hardware	<ul style="list-style-type: none"> <li>Any current, business-focused PC or laptop. Excluding computers with low-end, entry level processors.</li> <li>2 GB of RAM or greater (See Note below). At least 2GB is required for larger volumes of data, about 750K rows.</li> <li>Graphics display processor with at least 256 MB of video RAM</li> <li>Either shared or dedicated video RAM (be sure to use the most recent drivers for the video processor)</li> <li>Video display resolution of 1024 x 768 or greater</li> <li>Video display color depth of 16 million colors</li> <li>CD-ROM drive</li> <li>Mouse or compatible pointing device</li> </ul>
ESM	ESM v5.0 SP2 Patch 1 or later

---



For a given data set, performance is dependent on:

- 1) Amount of RAM
- 2) Processor speed
- 3) Processor architecture/technology

The amount of RAM required depends on the number of rows and fields and the type of data.

For best results do not install ArcSight Interactive Discovery on the same machine as an ESM Manager.

## What's New?

- This version of the ArcSight Interactive Discovery project contains essentially the same event data fields, however the tabs in both the Full and Partial projects files have been improved with some different charts and graphs.

For a complete description of the tabs in the full and partial projects see the *ArcSight Interactive Discovery Projects User's Guide*.

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

## Installing ArcSight Interactive Discovery

Log in to the Interactive Discovery target system with Administrator privileges; the installer makes modifications to the registry.

- 1 Verify system requirements listed on the previous page.
- 2 Uninstall any previous version of ArcSight Interactive Discovery.
- 3 From the ArcSight support site (<http://www.support.openview.hp.com>) download the Interactive Discovery zip file ([ArcSightAID-5.6.zip](#)) using the log-in credentials supplied by ArcSight.
- 4 When you extract the AID files, the ZIP file creates and writes the files to an [ArcSightAID-5.6](#) subdirectory.
- 5 Run the Interactive Discovery executable [setup.exe](#) on the Interactive Discovery system. Follow the instructions in the installation wizard.
- 6 When the installation is complete, review the What's New section of the online help for important information regarding this release.

When the installation is complete, refer to the *ArcSight Interactive Discovery Projects User's Guide* for information on extracting the ArcSight ESM content package. This guide is in the file [ESM\\_AID\\_ProjectGuide\\_5.6.pdf](#).

## Known Issue

When reports in ArcSight ESM export data as a CSV file, commas and double quotes (") within the data are not always handled properly and can cause the data to show up incorrectly in ArcSight Interactive Discovery. Try to ensure that event data fields do not contain values that include commas.

