Hewlett Packard
Enterprise

Release Notes

Compliance Insight Package for the
Payment Card Industry 4.0

ArcSight ESM and ArcSight Express

April 3, 2014

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. HPE 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 HPE 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

Contact Information

Phone	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://www.protect724.hpe.com

Contents

CIP for PCI 4.0

The Compliance Insight Package for the Payment Card Industry (CIP for PCI) provides a system of reports and real-time checks specifically designed to monitor systems that contain cardholder data, manage vulnerability and access control, monitor networks, and maintain security policies to help demonstrate to stakeholders and auditors that the controls over your company's credit card data systems expose little or no risk.

CIP for PCI 4.0 coupled with ESM can assist you in complying with the PCI requirements specified in Payment Card Industry Data Security Standard (PCI DSS) 3.0 and includes support for logs generated by payment applications subject to the Payment Application Data Security Standard (PA DSS) 3.0.

What's New in CIP for PCI 4.0

CIP for PCI 4.0 includes the following changes:

- Support for the PCI DSS 3.0 and PA DSS 3.0.
- An entirely redesigned compliance framework, which can be leveraged and extended to address other regulations and future versions of the PCI DSS. The new framework provides the following benefits and changes:
  - CIP for PCI maintains a *compliance score* for each asset in your PCI environment, so dashboards and reports can demonstrate the overall PCI compliance and individual asset compliance for your organization.
  - The PCI DSS sub-requirements (1.2.1, 1.2.3, and so on) addressed by CIP for PCI are mapped to out-of-the-box *compliance scenario rules* that help determine the compliance score for each asset. You can also create custom scenario rules to address organizational, regional, and national regulations and policies.
  - The CIP for PCI resources are no longer grouped by PCI DSS requirements in the Navigator panel of the ArcSight Console. Instead, they are grouped into general security *domains*, such as Access Control or Privacy Protection, that apply to multiple regulations. Also, the high-level solution group is now CIP instead of PCI.
  - There are fewer CIP for PCI use case resources. Instead of several use cases for each PCI DSS requirement, there is an overall compliance status use case and a use case for each security domain group. Unlike the previous use cases, which were PCI-specific, the domain-based use cases apply to multiple regulations.

- In the *Compliance Insight Package for the Payment Card Industry 4.0 Solution Guide* and several CIP for PCI resources, the PCI DSS sub-requirements are called *controls*. CIP for PCI tracks asset compliance for each control; this relationship is called a *control-asset pair*.

The new compliance framework results in fewer resources, more resources shared by different regulations, simplified configuration, and timely support of new regulation versions.

Requirements

CIP for PCI 4.0 is supported on the following products:

- ArcSight ESM 5.2 or later
- ArcSight Express 4.0 with CORR-Engine or later

Release Contents

The following files are included in this release.

File name	Description
`ESM_PCI_Solution_RelNotes_4.0.pdf`	Product description and open issues (this document).
`ESM_PCI_SolutionGuide_4.0.pdf`	Compliance Insight Package for the Payment Card Industry 4.0 Solution Guide—Product architecture, installation, configuration, and operation instructions with a description of product contents.
`ArcSight-ComplianceInsightPackage-PCI.4.0.1353.0.arb`	Installable package bundle for all operating systems. Contains all the resources for the Compliance Insight Package for the Payment Card Industry. **Note:** Internet Explorer sometimes converts the ARB file to a ZIP file during download. If this occurs, rename the ZIP file back to an ARB file before importing into ESM.

Installing CIP for PCI

For CIP for PCI installation and configuration instructions, see the *Compliance Insight Package for the Payment Card Industry 4.0 Solution Guide*.

You can install CIP for PCI alongside other solutions on the same ArcSight Manager; however, HPE recommends that you do not install CIP for PCI alongside earlier versions of CIP for PCI, such as CIP for PCI 3.0 or CIP for PCI 3.01.

Due to the extensive redesign of CIP for PCI 4.0, there is no migration path from earlier versions of CIP for PCI. If you are running an earlier version of PCI and you need to keep your current data, do not uninstall the earlier version; instead, install CIP for PCI 4.0 on a different system.

Performance Impact of CIP for PCI

ArcSight solution packages contain data monitors, trends, and rules that can place an additional load on the ArcSight Manager, which might impact the ArcSight Manager performance. If your ArcSight system is operating at an average event per second (EPS) rate that has maximized the CPU utilization, you might experience a reduced average EPS rate after installing the CIP for PCI package. If this performance impact occurs, you can disable unneeded data monitors, trends, and rules to reduce the load on the ArcSight Manager.

Open Issues in this Release

This release contains the following open issues.

Number	Description
SOL-3931	The `All Trends/ArcSight Solutions/CIP/Network Security/DMZ Zones` and `DMZ Assets` trends (used by the `All Rules/ArcSight Solutions/CIP/Network Security/Implement a DMZ` rule to determine if a DMZ segment is implemented within the network) have a very short Trend Interval. These trends might time out on high EPS systems and be disabled automatically by ESM. **Workaround**: Run the DMZ Zones and DMZ Assets trends manually on recent events with a longer Trend Interval (where the start time is close to the trend schedule time) whenever the information on DMZ segments is required.
SOL-3913	In ArcSight ESM 6.0c and later, and ArcSight Express 4.0 with CORR-engine, the following rules are CPU intensive and might affect system performance. • `/All Rules/Real-time Rules/CIP/Compliance Scenarios/Network Security/Network IDS Detected` • `/All Rules/Real-time Rules/CIP/Compliance Scenarios/Monitoring/Non-empty Origination of Event` • `/All Rules/Real-time Rules/CIP/Compliance Scenarios/Monitoring/Events from External-Facing Technologies` • `/All Rules/Real-time Rules/CIP/Compliance Scenarios/System Hardening/Multiple Functions Implemented on a Server` • `/All Rules/Real-time Rules/CIP/Compliance Scenarios/Network Security/Private IP Protected From Disclosure` **Workaround:** Set the ArcSight ESM Manager Java heap memory size to at least **16 GB**, and enable the CIP for PCI rules listed above for short periods of time (for example, one hour a day) to collect relevant data and update compliance status. For information about setting the Java heap memory size in ArcSight ESM, see the ArcSight Command Center User's Guide. For ArcSight Express, see the ArcSight Management Console User's Guide.
SOL-3836	On high EPS systems, certain query viewers might not return data and some reports take a long time to run. **Workaround**: Edit the query viewer and the report to change the interval to one hour by setting the Start Time and End Time parameters.

Number	Description
SOL-3832	The `Anti-Virus Updates by Product` and `Anti-Virus Updates by Outcome` query viewers on the `All Dashboards/ArcSight Solutions/CIP/Vulnerability Management/Anti-Virus Update Status` dashboard do not show events in which the Category Outcome is empty.
SOL-3822	The `All Dashboards/ArcSight Solutions/CIP/General/Negative Impact Compliance Scenarios in the Last 7 Days` and `Negative Impact Compliance Scenarios in the Last 7 Days` dashboard drilldowns do not display any data.
SOL-3810	When you uninstall the CIP for PCI 4.0 package on ESM 6.0c, an error message might display on the Console and the uninstall process might fail. On ESM 6.5, uninstallation proceeds but you might see exceptions in the `server.log` file. **Workaround**: Restart the ArcSight Manager, then uninstall the package.
SOL-3716	The `All Filters/ArcSight Solutions/CIP/General/After Hours` filter does not work as expected; therefore, the After Hours Physical Accesses report incorrectly shows physical access to a building during business hours as well as after business hours.
SOL-3594	For certain rules, the AssetName, AssetID, and AssetZone local variables are not resolved; therefore, the `All Active Lists/ArcSight Solutions/CIP/General/Compliance Score` active list displays $AssetName, $AssetID, and $AssetZone instead of the actual asset name, ID, and zone.